Private Settlement in Blockchain Systems

Alfred Lehar[*]
Haskayne School of Business
University of Calgary

Motahhareh Moravvej-Hamedani [†]
Haskayne School of Business
University of Calgary

May 2022

[*] Haskayne School of Business, University of Calgary, 2500 University Drive NW, Calgary, Alberta, Canada T2N 1N4. e-mail: alehar@ucalgary.ca

[†] Haskayne School of Business, University of Calgary, 2500 University Drive NW, Calgary, Alberta, Canada T2N 1N4. e-mail: motahhareh.moravvejh@ucalgary.ca

Private Settlement in Blockchain Systems

Abstract

We provide evidence that the settlement market in blockchain systems deviates from a perfectly competitive market. Examining the bitcoin blockchain, we document that 5.88% of transactions, which we label as private, bypass the competitive process and seem to be channelled directly to miners. Users of private transactions post more transactions on the blockchain and space their transactions more evenly. Despite being more active than the average user, they tend to get their transactions confirmed by only one miner, which is statistically a very unlikely outcome in competitive markets. Our findings are consistent with frequent users engaging in long-term agreements with specific miners. In return for channeling all their transactions to one miner, they pay on average lower fees and face a lower variation in fees. Our paper provides novel evidence of how settlement contracts are structured and how potential gains and incentives can be shared amongst the system participants.

Keywords: Blockchain Technology, Bitcoin, Settlement, Fintech, Distributed Ledger, Cryptocurrency, Private Settlement, Contract

1 Introduction

The Economist magazine recently reported, the Ethereum blockchain alone settled transactions worth 2.5 trillion dollars in the second quarter of 2021, roughly the same amount as the Visa network.[1] The premise that decentralized blockchain systems improve efficiency relies on the assumption of a competitive market for settlement of transactions. Nevertheless, very little is known about the settlement agreements that endogenously emerge in an unregulated market with free entry. Blockchain systems were conceived to provide competitive settlement, where users compete by attaching fees to their transactions and competitive miners freely pick transactions to include in blocks and settle them. This market is widely believed to be transactional in nature.

In this paper we provide evidence that is consistent with some users and miners bypassing the competitive settlement market and forging private, exclusive, long term settlement agreements with miners. We study Bitcoin, which is the oldest and most valuable cryptocurrency. At the time of writing this paper, Bitcoin's market cap is larger than all other crypto currencies combined.[2]

Under Bitcoin's original design users post transactions to a public mempool from which miners can pick transactions to include into blocks. We document that almost six percent of settled transactions have never appeared in the mempool and thus not followed the standard settlement process. We argue that miners receive them from private channels outside of the Bitcoin system. One potential reason for the existence of these channels is risk sharing. Miners are exposed to variation in average fees and transaction demand while facing fixed costs of operations.[3] Users who have a high demand for regular transactions face similar risks which creates a risk sharing opportunity using long term contracts at fixed prices.

[1] https://www.economist.com/leaders/2021/09/18/the-beguiling-promise-of-decentralised-finance

[2] https://www.visualcapitalist.com/Bitcoin-market-cap-compared-to-crypto/

[3] This risk is orthogonal to the uncertainty on how many blocks a miner can find in a given time.

Using a sample of over hundred million transactions, we find that private transactions pay lower average fees and exhibit lower fee variation. Using a standard algorithm, we attribute the individual transactions in our sample to 59 million users. Users of private transactions are more likely to insert data into the blockchain as it is done by various layer two protocols that have regular transaction demand. We document that users of private transactions post regular and evenly spaced transactions on the Bitcoin blockchain. Users of private transactions in our sample post on average 84,045.36 transactions compared to 42.92 for regular users. Despite being more active, private users use only 1.002 distinct miners to process their transactions, while normal users' transactions are, on average, mined by 9.73 distinct miners.

Anecdotal evidence is consistent with the existence of private transaction channels. For example Bitcoin SV developed an API which is freely available on Github that allows users to directly interact with miners. On their website they advertise that their product allows for "Direct transaction submission: This allows users to bypass the outer layers of the Bitcoin peer-to-peer network and submit transactions directly to miners."[4] Their product also allows for "User based fee policies to enable different fee structures for different use cases." Other forum posts also discuss how to pass transactions to specific mining pools by forwarding them directly to a node that is run by the pool. The pool can then decide whether or not to share these transactions with other nodes.[5]

Dark pools and electronic communication networks (ECNs) offer a mechanism to bypass the public trading venues in traditional financial markets. Like private transactions in bitcoin, dark pool transactions reduce trading cost (Hu, Jones, and Zhang 2021). In the United States, this type of transactions executed approximately 13.66% of the equity volume in November 2021.[6] However, the primary reason to utilize dark pools is different from our setting. Dark pools lessen the negative price impact of large orders. In Bitcoin there is no price impact of

[4] https://bitcoinassociation.net/bitcoin-sv-miner-id-and-merchant-api-beta-release/

[5] https://bitcoin.stackexchange.com/questions/5337/how-do-i-send-a-transaction-directly-to-a-miner-or-pool-for-processing

[6] https://www.rblt.com/market-reports/let-there-be-light-us-edition-31

transactions nor is there price discovery as the blockchain is used for settlement of previously contracted transfers of Bitcoin. Brogaard, Carrion, Moyaert, Riordan, Shkilko, and Sokolov (2018) demonstrate the impact of dark pool transactions on price discovery that leads to inefficient information acquisition and lack of transparency. Bodie and Kane (2020) studies the mechanism of ECNs and highlight several attractions for both buyer and seller in ECNs trading. Without using a broker-dealer system, both sides can eliminate bid-ask spread limits and communicate privately through the direct link, with typically lower cost. ECNs are attractive for higher trade speed and the anonymity in this infrastructure.

While previous research documented deviations from competitive behaviour in transaction settlement on blockchain markets, this paper is to the best of our knowledge the first one to document that some users bypass the competitive settlement market. We find evidence consistent with price discrimination where some users who settle many transactions and frequently use the system seem to get a different price than infrequent users. This finding casts some doubt on whether all users of decentralized systems can equally benefit from any costs savings that this new technology will bring.

Our paper is part of nascent literature on settlement in unregulated markets. In the original Bitcoin paper (Nakamoto 2008) assume as first step to run the network that *new transactions are broadcast to all nodes*. Competitive mining is the standard assumption in many works on the bitcoin network, e.g. Antonopoulos (2014).

Easley, O'Hara, and Basu (2019) model the emergence of fees in blockchain systems. Lehar and Parlour (2022b) examine the potential for miners to implicitly collude by strategically managing the effective capacity of the blockchain. They argue that miners price disciminինate among users to increase fee revenue. Huberman, Leshno, and Moallemi (2017) argue that keen users post higher fees to get their transaction included in the next block when there is uncertainty on the blocks arrival time. Both papers assume that all transactions pass through the mempool and assume a one-off transnational relationship between miners and users. Our paper explores a novel mechanism where transactions bypass the mempool all together and users and miners can sign long term contracts.

Our paper is related to a stream of literature that is concerned about regulation in settlement systems. Currently, settlement is highly regulated and often performed by the government near entities that offer their services at a flat price for every participant. Blockchain systems open a market for private settlement where users offer fees to miners to confirm their transactions (Auer 2019). Schmiedel, Malkamäki, and Tarkka (2006) model the traditional settlement markets considering tight regulation in financial markets. Russo, Hart, Malaguti, and Papathanassiou (2004) examine conflicts of interest typically arising in the securities settlement infrastructure and propose improvements in regulation. We augment this literature by examining a somewhat competitive, and completely unregulated settlement market.

We study the bitcoin blockchain because by its nature we can abstract from many more complicated settlement issues that are present on other blockchain systems. In bitcoin the ordering of transactions within a block is irrelevant. This is not the case in Ethereum where users interact with smart contracts based on the order that the transactions are recorded in the block which creates opportunities for front-running. Daian, Goldfeder, Kell, Li, Zhao, Bentov, Breidenbach, and Juels (2019) document several ways in which users can try to benefit from strategically placing their transaction ahead of the ones from other users. Park (2021) discusses front-running for automated market makers in such systems. Daian, Goldfeder, Kell, Li, Zhao, Bentov, Breidenbach, and Juels (2020) demonstrate how miners in Ethereum can strategically alter the ordering of transactions or execute other user's transactions in their own name for financial gain, they pocket the so called, Miner Extractable Value (MEV). Lehar and Parlour (2022a) document that 80% of blocks on Ethereum are not sorted by fees and that miners collect over a million USD per day from prioritizing some transactions. These opportunities for miners to extract rents are absent in bitcoin as bitcoin offers no smart contract ability and the ordering of transactions within a block is irrelevant.

2 The Bitcoin System and private transactions

Transactions transfer Bitcoin between wallets. A transaction involves at least one sender and one receiver.[7] The former digitally signs a transaction to verify that she is the rightful owner of the Bitcoin and propagates her request through the decentralized peer-to-peer network of Bitcoin nodes. These pending transactions constitute what is called the mempool (or Memory pool). Theoretically, each node could see a different set of pending transactions, but recent innovations such as the fibre network allow rapid transmission of pending transactions so that latency is not a practical problem any more. Empirical results from computer science, for example Dae-Yong, Meryam, and Hongtaek (2020) show that mempools are practically identical.

Miners pick pending transactions from the mempool to be included in a block. Users can attach fees to their pending transactions that the miners can keep when they include the transaction in a block. The Bitcoin protocol has been designed with the idea that all pending transactions go through the mempool and are ordered based on the ageing algorithm discussed in Antonopoulos (2014) in which old and high-fee inputs have higher priority over newer transactions that offer smaller fees. One miners have selected a set of transactions they solve a computationally complex puzzle to create a valid block which can be added to the chain.

In practice, however, miners have complete discretion on which transactions to include in a block. Specifically they can include transactions that did not go through the mempool. Users can contract privately with individual miners and forward transactions directly to miners (outside of the peer-to-peer network), and miners can then include these transactions in a block that they will mine. We label such transactions that bypass the mempool as *private* transactions. Private transactions are not visible to other miners, and thus their fees accrue exclusively to the miner who confirms that transaction.

[7] Each Bitcoin transaction can have many inputs and many outputs. The inputs are amounts of Bitcoin that are individually locked up by a locking script. The sender can unlock all these inputs and transfer funds to output addresses, which do not necessarily belong to the same owner. The process is similar to making a $23 payment with a $20 and a $5 bill (2 inputs) and giving $23 to the merchant and keeping $2 in change (2 outputs).

We argue that miners and users who have a high transaction demand have an incentive to contract for a fixed fee out of a risk sharing motive. Miners who face medium term fixed costs for electricity and infrastructure are concerned about variation in future fee revenue. Users with predictable transaction needs are similarly worried about changes in fees. This risk sharing motive is orthogonal to the risk regarding the number of blocks mined in a given interval of time that has been analyzed in the literature.[8]

To illustrate our point assume that mining fee revenue varies over time and can either be high or low with equal probability. Variation in fees may be induced by changes in demand for transactions by users, variation in the utility that users place on getting their transactions included in the blockchain, or by the random arrival time of blocks. A miner could solve the puzzle immediately after a previous block was found in which case there might be fewer transactions waiting the mempool and hence the miner's fee revenue might be lower. Specifically assume that a miner can either obtain fees worth f or 0 upon finding a block.

Miners are risk neutral and mine a fixed number ν blocks in a given period. To introduce a motive for risk sharing assume that miners are in financial distress and face a loss l whenever they only mine blocks where the fee revenue is low within a period. The probability of financial distress is then

$$p = \frac{1}{2^{\nu}} \tag{1}$$

The expected profit of a miner of size ν who takes transactions with an expected value of $f/2$ from the mempool and is exposed to fee risk is therefore

$$\pi^m = \nu\frac{f}{2} - pl = \nu\frac{f}{2} - 2^{-\nu}l \tag{2}$$

In contrast a miner who would sign an agreement with a user to mine a certain number of

[8] Xue, Xu, Wu, Lu, and Xu (2021), and Cong, He, and Li (2021) discuss and analyze the incentives for rational miners to share risk and form pools. A pool will reduce the uncertainty around the number of blocks that are mined. Participants share the cost of finding a new block as well as the revenue proportional to their contribution.

transactions for a fixed fee revenue c can avoid financial distress and would obtain

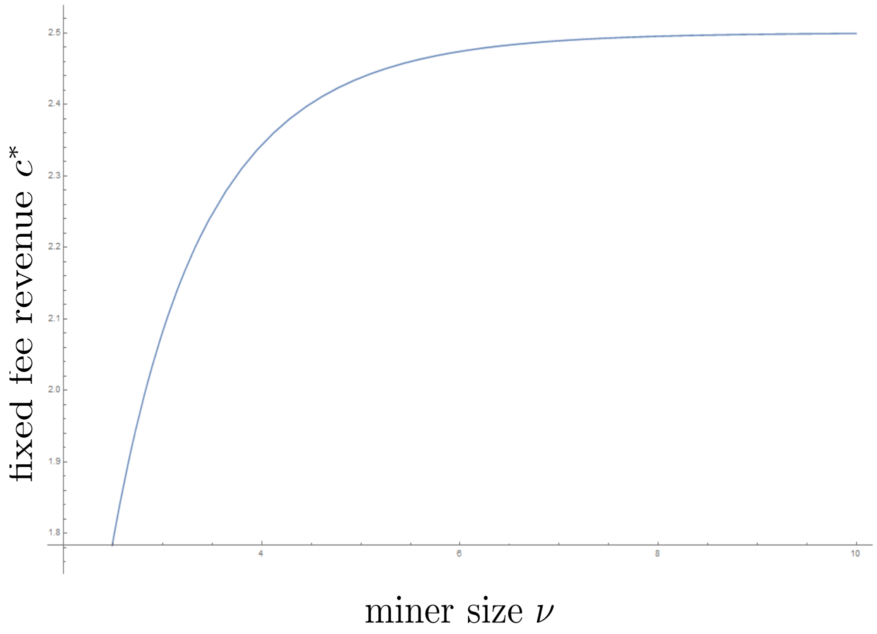
$$\pi^c = \nu c \tag{3}$$

Solving for the fixed fee revenue c^* that makes the miner indifferent we obtain

$$c^* = \frac{2^{-\nu-1}(2^\nu f \nu - 2l)}{\nu} \tag{4}$$

which is increasing in ν. Figure 1 illustrates the fee revenue as a function of miner size ν for an example.

Figure 1. Fixed fee revenue c^* at which a miner would be indifferent between fixed and variable revenues as a function of miner size ν. The parameters are $f = 5, l = 10$.



From this simple toy model we can derive several empirical predictions. Miners will offer lower fees in exchange for a fixed or less volatile guaranteed fee flow. We therefore expect private transactions to have lower and less variable fees. As illustrated above smaller miners face more uncertainty over fee revenue and are thus willing to offer a lower fee for private transactions. We therefore expect that smaller miners are more engaged in processing private transactions.

It only makes sense for a miner to enter a risk sharing agreement with a user who has a steady demand for transactions. A user posting a one off transaction cannot provide a steady flow of fees for the miner to make a long term contract useful. We therefore expect that users who engage in private transactions to post more transactions than an average user and post the transactions more regularly than other users. One such user type with a high transaction demand are meta-layers or side-chains that synchronize to the bitcoin blockchain.[9] These system use data insertion transactions which are identified by their use of the data insertion operation code OP_RETURN in the bitcoin lock script. We therefore predict that users that utilize data insertion transactions are more likely to post private transactions. When miners and users enter such an agreement to mine private transactions we also expect users of private transactions to have all their private transactions mined by one miner.

3 Data

In order to trace transactions from their origination to their confirmation, we combine mempool and blockchain data. For the former, we set up Bitcoin nodes on two separate instances in the Compute Canada cloud and take snapshots from the mempool every minute. These snapshots include all transactions that wait to be confirmed at that given time. Their unique hash value

[9] Such systems keep information in a separate ledger, often an independent blockchain, and post a hash of their state in regular intervals to the bitcoin blockchain. Users of the sidechain or meta-layer can therefore verify the state of the system by verifying the state with the posted state on the bitcoin blockchain. These system take advantage of bitcoin's security and assure consensus at least at the points in time when the state is posted. One example of such a meta layer is the Omni-layer which allows the creation of tokens and was for a long time the main home of the USD stablecoin Tether.

identifies transactions. We collect blockchain data on transactions that are mined into blocks directly from a modified Bitcoin node. For each transaction, we know when and in which block it was mined. We identify miners based on a unique text most mining pools put in the input script portion of the coinbase transaction, the first transaction of each block that grants the miner newly minted Bitcoin as a reward for finding a block. We describe our data-set in three parts: transactions, miners, and users.

3.1 Transactions

Our sample consists of 97,796,453 Bitcoin confirmed transactions for 2021. We collect senders, receivers, the amounts sent, and the fee paid to the miner for each transaction as reported in Table 10 in the appendix. We classify a transaction as normal if it is observed in the mempool before being mined into a block. For those transactions, we record the timestamp when the transaction entered the mempool, and when it was mined. Transactions that never enter the mempool but still get recorded on the blockchain are identified as private transactions. We collect mempool data starting in January 2021 to get a consistent state of all pending transactions till January 2022. We tag transactions based on their state as either *pending* or *confirmed*, where pending transactions are still waiting in the mempool to be added to a block by a miner. We observe 93,374,343 pending transactions in our sample period, most of which are then confirmed in that year. When a miner confirms a transaction, it will be added to a block and will be removed from the mempool. Table 1 reports the summary of statistics for transactions in our sample.

We define the waiting time as the difference between the block number in which the transaction was included and the highest block number when the transaction first entered the mempool. We do not measure the delay based on timestamps so that random fluctuations in times between blocks do not drive our delay measure. On average transactions wait for 6.66 blocks in the mempool. Some transactions get confirmed immediately, the longest time a transaction waited in the mempool was for 23 blocks. In our sample the mempool is never empty and therefore we observe positive delays. Our findings are consistent with Pappalardo, Di Matteo, Caldarelli, and Aste (2018) who document an average delay of 6 blocks.

Items	**Confirmed Transactions**
Number of Days	365
Starting Date	1/1/2021
Ending Date	31/12/2021
Transactions	97,637,471
Mixers' Transactions	107,639
Miners' Transactions	152,556
Private Transactions	5,738,085
Number of Blocks	52,686
Starting Block	663913
Ending Block	716598
Maximum Fee (Sats)	1.83e+08
Average Fee (Sats)	21,940.77
Fee Variation (Sats)	2.18e+10

Table 1. Transactions Summary of Statistics This table reports the summary of statistics for 2021 sample. The *Confirmed Transactions* are those who already recorded in chain by miners. The *Pending Transactions* shows the statistics related to the waiting transactions in the Mempool. Fees are in Satoshi.

3.2 Miners

For each block, we record the mining pool, block hash, block height, block weight and the block creation time. We report summary of statistics on mined blocks in Table 1. We identify 28 miners for 91.16% of the blocks in our sample based on their signature in the input section of the coinbase transaction.[10] We label miners in the highest 25th percentile of their number

[10] In some cases, these signatures do not allow us to attribute the block to a certain miner. We report the very small or undetectable mining pools in our one-month sample as 'Other'.

of blocks mined as big and the remaining miners as small. Table 2 shows the market share classification of the mining pools in our sample.

Mining Pools	**Block Mined**	**Market Share**	**Category**
F2Pool	6695	15.65	Big
AntPool	6504	15.20	Big
poolin	5342	12.49	Big
ViaBTC	4799	11.22	Big
binance	4644	10.86	Big
BTC.com	3965	9.27	Small
foundry_usa	2428	5.67	Small
Huobi	2010	4.70	Small
SlushPool	1786	4.17	Small
1THash	1110	2.59	Small
WAYI.CN	689	1.61	Small
SBICrypto	530	1.23	Small
(15 others)	405	5.28	Small

Table 2. Mining Pools' Market Share in 2021 The market share per mining pools is calculated based on the number of blocks they mined in 2021 to the total blocks mined in the same period. This measure is a size proxy. The big miners are in the first 25th percentile in descending order.

Mining is a concentrated industry. The five big miners have 83.55% of the market. F2Pool, Antpool, Poolin, ViaBTC and binance are the top five mining pools in our sample. We rank mining pools based on their mined blocks divided by the total block mined in a year.

3.3 Users

To study the user behaviour, we use a standard algorithm from the computer science literature that we explain in detail in Section 3.4 to assign bitcoin addresses to users. We observe 161,482,396 unique input wallet addresses. Table 3 shows summary statistics for input and output addresses in our sample. We observe 300,147,341 usages of wallet addresses as input in transactions and map them to 59,086,692 distinct users.

Some transactions on the bitcoin blockchain are initiated by miners, for example when they pay mining rewards to their pool members. These transactions can be different, for example it is likely that miners will mine their own transactions as they do not want to pay fees to other miners. We define a user as miner if they collect fees or block rewards to one of their wallet addresses. We exclude miner transactions from our empirical analysis.

Users that use at least one private transaction are classified as private users and all remaining users are labeled as normal. Our classification algorithm detects 3,408,352 private users and 55,678,340 normal users. In our sample, we classify 6.12% of the users as private.

In Figure 2 we show the fraction of private transactions per miner. Private transactions are not equally distributed, which is consistent with strategic behaviour by some miners and makes it unlikely that transactions are misclassified as private. Two pools, KanoPool and ckpool, stand out with a fraction of 10.56% and 4.12% private transactions, respectively. These pools are also the two smallest pools in our sample. Table 4 presents summary statics per user group. We see that private transactions pay on average lower fees and have lower fee variation than normal transactions. The average private user is more active with 84,045.36 transactions compared to only 42.92 transactions for normal users. Yet, their transactions get on average mined by only 1.002 miners. If miners and users are competitive we should see that transactions are randomly allocated to multiple miners based on their mining capacity. The probability that a user gets randomly allocated to the same miner for n transactions is p^n where p is market share of a miner. Even for the largest pool with a market share of 15.28% the probability that a user gets allocated to the same miner for 5 transactions is 0.0083%. We also see that users of private transactions insert more data into the blockchain consistent with the idea that they are frequent users such as second layer protocols.

Items	**Values**
Number of Observations	300,147,341
Distinct Input Wallet Addresses	161,482,396
Average Input Value (BTC)	392,505,564.62

Table 3. Input Wallet Addresses Summary of Statistics The summary of statistics for input wallet addresses in 2021 is reported. The number of observations shows the one-to-one relationship between transaction hash and input wallet addresses.

For each user we define the transaction window as the time difference between the first and the last transaction of that user in our sample. We also record the transaction frequency for each user. Table 4 reports the summary of statistics for all users detected by the classification algorithm. Mining pools are utilizing the settlement channels more than the other types. To address any selection bias, we remove miners from the sample. With and average of 84,045.36 transactions private users are more active compared to normal users with 42.94 transactions. To measure fees, we use the fee per weight unit. For miners, the opportunity cost of a transaction is determined by its physical size in bytes, as block size is limited. With the introduction of SegWit (segregated witness), parts of the scripts can be outsourced to the witness section, which does not count towards the physical block limit. The SegWit update thus introduced weight units for measurement of transaction size as weight considers how effectively a transaction utilizes the witness section. Private users also post larger transactions with 45.07% more weight units on average.

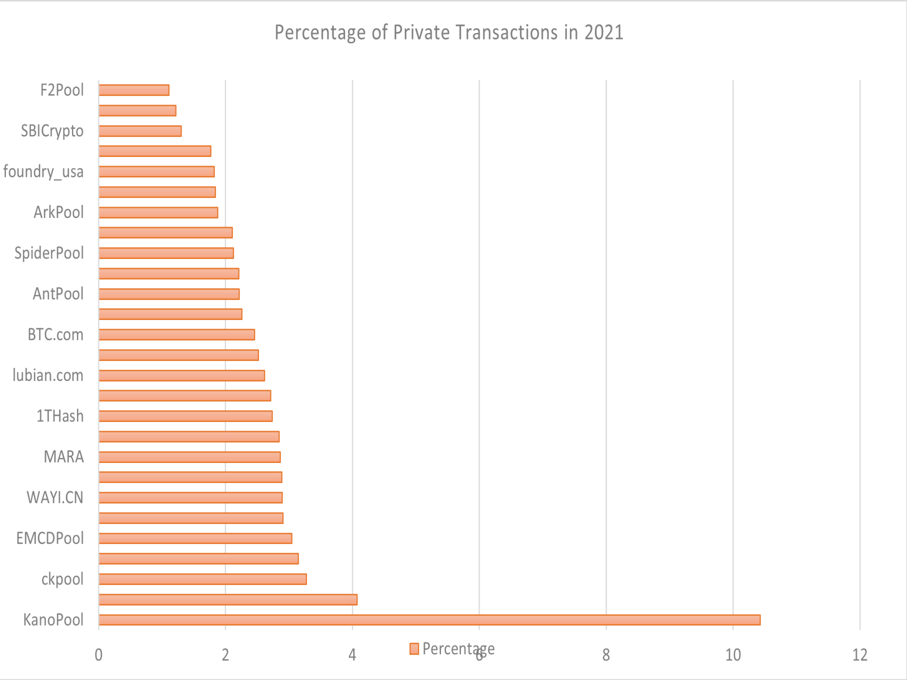
Items	Average Fee	Fee Variation	Average Transaction Count	Average Miner Count
Normal	12.82	11.82	42.94	9.73
Private	10.42	11.62	84,045.36	1.002
All Users	12.77	11.83	54,440.01	7.01

Table 4. Summary of Statistics for Group Types The summary of statistics for each criteria is calculated on average for each user group. Fee per weight is the measure of comparing fees. The Fee Var is the average variation of Fee per Weight in each user group type. Miner Count is the average number of distinct miners that confirmed the transactions for each type of users. To deal with sample selection bias, we exclude miner's and mixers' Transactions. The private users paying 18.72% lower fee on average.

3.4 User Classification

By design, it is hard to trace individual users' activities through the Bitcoin blockchain. A transaction's inputs and outputs are associated with addresses, but modern wallets frequently generate new addresses for security reasons. It is impossible to group observed addresses by wallets based on the address characteristics. We ascribe transactions to users based on this Union-Find

Figure 2. Percentage of Private Transactions per Mining Pools The number of transactions received through private channels are lower comparing to the normal ones in 2021. The orange bars show the percentage of private confirmed transactions per miner.



algorithm, a widely used approach to classify the transaction-level data into user-level data. It first introduced by Cormen, Leiserson, Rivest, and Stein (2001) and then widely applied in academic works such as Ron and Shamir (2013), Meiklejohn, Pomarole, Jordan, Levchenko, McCoy, Voelker, and Savage (2013), (Khalilov and Levi 2018), (Greaves and Au 2015) and Foley, Karlsen, and Putniņš (2019). The idea that all inputs, and thus all input addresses, in a transaction must belong to the same user. Because the transaction with all the inputs needs to be digitally signed. We attribute all other transactions that use input addresses to the same user starting from one transaction and continue iteratively. It creates minimal disjoint sets by investigating the relationship between input addresses and transactions' hash. We develop the logic based on transitivity. The two transactions with at least one sender address in common belong to one user and should be merged. These newly identified transactions have input addresses, and we add all other transactions that use the same input addresses as belonging to the same user.[11] We repeat the process until we find no new transactions that we can attribute to this user.

This program clusters 300,147,341 records of observations to a set of 59,086,692 users. We mark a user as private if at least one transaction of that user is private. All other users are labelled as normal. Our user classification works well given the short sample period. Using a sample of 605 million transactions, Foley, Karlsen, and Putniņš (2019) identify 106 million users. Using our sample of 300 million transactions we identify 59 million users. Private users utilize the blockchain more frequently. The average private user posts 84,045.36 transactions, while a normal user only posts 42.94 on average. Private users tend to stay with the same miner. Transactions from a private user are mined on average by 1.002 distinct miners, compared to 9.73 miners for normal users. This difference is especially noteworthy because private users post more transactions than normal users. If the allocations of users to miners was random we would therefore expect that private users' transactions get mined by more miners. We measure fees as fee per weight unit. Transaction weight is an opportunity cost for the miners and the bitcoin protocol limits the physical size of a block (measured in weight units). Average fees are 10.42 and 12.82 for private and normal users, respectively. Therefore, private users pay lower fees compared to normal ones by 18.72%.

We extend the base classification program to identify and exclude transactions initiated by miners through two steps.[12] First, we collect miners' addresses by investigating the coinbase transaction in each block.[13] The coinbase transaction transfers an amount that contains reward and the total fee of confirmed transactions of a corresponding block to the miner's wallet. In this transaction, the sender is blank, and the receiver is the miner. Second, by analyzing the receiver addresses, we capture the miners' Bitcoin addresses through time. Mining pools use these addresses for daily settlement processes with individual miners that are part of the pool or

[11] In appendix section, an example is provided to describe the mechanism in detail.

[12] To the best of our knowledge, this approach is unique for assessing miners' activity in the Bitcoin network.

[13] The first confirmed transaction in each block, called coinbase.

other means. We exclude miners' transactions from our sample before classification.

This algorithm and other user group classification algorithms may not be perfectly accurate in clustering in this context from two perspectives. First, Mixers can potentially combine the input addresses of several different users and create several transactions to keep the users untraceable.[14] The goal of mixers is to reduce the tractability of transactions. To be more accurate, we detect and exclude mixed transactions from our sample. Our approach is described in Appendix C. Second, If an actual user never utilizes its various addresses together, it may result in two disjoint sets that conceptually belong to one user. Because in this case, the algorithm can not find any mutual sending address. We believe that for our purposes, this algorithm is adequate. The case we have more than one cluster which is related to one actual user in the real world should not bias our results because we are looking for specific behaviour of a user type.[15]

4 Empirical Findings

4.1 Average Fee

We expect users who contract long-term with one miner to expect lower fees for two reasons: first, a risk-averse miner replaces a risky cash flow with a safe cash flow and is willing to charge a lower fee. Second, the user can face longer confirmation delays because she has to wait for the next block found by a particular miner rather than waiting in the mempool for potential confirmation by any miner; therefore her willingness to pay a fee is reduced. We, therefore, consider the fee paid per weight unit, or average fee, as our measure of transaction fee. The summary of statistics for this variable is reported in Table 4. To make the result more robust

[14] Mixers are proxies that increase the anonymity of the senders by mixing different input addresses in a transaction. The inputs may be logically not related to each other.

[15] In other words, it means the first issue does not change the category type. It may change the number of user groups of each type.

toward outliers, for the econometric analysis we winsorize the average fee and the total input value of the transaction at the 99 percent quantile.

We regress fee per weight on a dummy for private transactions and miner and transactions specific controls. Table 5 presents our results. our sample size is reduced to 97,637,471 removing miners' and mixers' transactions. Private transactions are labeled with a dummy.[16] We control for the sum of input values in BTC, which measures the monetary value of the transactions, transaction weight, the size of the block and the number of transactions. To control for heterogeneity in fee variation we cluster the standard errors per user. In Columns (3) we control for miner fixed effects. The relationship between the private dummy and the total fee per weight is negative and significant. Consistent with our hypothesis we find that private transactions are cheaper compared to normal ones. We can observe that private transactions are more stable over time and show lower variation in line with the idea that they are governed by a long term agreement. Our findings are consistent with our hypothesis that private transactions are on average cheaper than normal. Therefore, miners consider a sizable discount for having a long-term relationship with private users.

4.2 Variation of Average Fee

To study the impact of long term contracts on fee variation we need to study fees on a per-user basis. We therefore compute variation of fees for each user that we identify in our sample. In order to make the results more robust, we only include users with at least ten transactions. We first repeat the analysis of Section 4.1 on a per-user basis to study the variation. We present our findings in Table 5 in columns (3) and (4). We observe that users who utilize private transactions pay significantly lower fees than normal users by almost 20 percent.

Furthermore we include an interaction of transaction count, the number of transactions that

[16] The number of private transactions in our regression analysis is 5,738,085 from 97,637,471 observations. Therefore, the private type is 5.88 percent of the total sample as expected.

Table 5. Regression Results for Fee per Weight Private transactions having lower average Fee per Weight. Moreover, they have lower variation of Fee per Weight.

	(1)	(2)	(3)	(4)
	Fee per Weight	Fee per Weight	Std Fee per Weight	Std Fee per Weight
Private Dummy	-2.604***	-2.584***	-0.0360***	-0.0330***
	(-40.19)	(-38.27)	(-4.48)	(-4.14)
Sum of Input Values		7.91e-12***		-1.10e-13***
		(10.89)		(-4.42)
Block Size		0.000000607***		0.000000170***
		(11.04)		(24.48)
Transaction Count		0.0000126		-4.06e-09
		(1.35)		(-1.21)
Transaction Weight		-0.0000284***		-0.00000179***
		(-7.07)		(-7.67)
Constant	12.93***	11.93***	0.00214***	-0.219***
	(80.89)	(88.63)	(4.41)	(-23.51)
Observations	97,637,471	97,637,471	59,086,692	59,086,692
R^2	0.001	0.005	0.000	0.003

t statistics in parentheses

* $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$

a user posts, and the private dummy which we find to be negative and significant. Thus fees are lower for private users that post more transactions. This trend is opposite for normal users as the coefficient of transaction count is positive and significant. We expect private users who contract with a miner to have lower variation in fees when miners and users have long term agreements. Our findings in Table 6 are consistent with this idea. We find that fees for private users are more stable and that this effect increases in the number of transactions a user posts to the blockchain.

4.3 Likelihood to Stay with Same Miner

Communicating with the same miner through time is the core of our hypothesis. If private users have an underlying contract with a settlement agent, we expect all of their transactions to

Table 6. Regression Results for the Transaction Count Increasing the number of transactions have decreasing effect on variation of Fee per Weight. We study this fact by interaction term private*transaction count which has the negative effect.

	(1) Std Fee per Weight
Private Dummy	-0.0245***
	(-3.65)
Transaction Count	7.21e-09*
	(1.96)
Transaction Count*Private Dummy	-0.000000200***
	(-3.33)
Sum of Input Values	-1.10e-13***
	(-4.42)
Block Size	0.000000170***
	(24.42)
Transaction Weight	-0.00000179***
	(-7.66)
Constant	-0.219***
	(-23.73)
Observations	59,086,692
R^2	0.003

t statistics in parentheses

* $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$

be mined by the same miner. In fact since private transactions never enter the mempool other miners cannot include these transactions in their blocks. We count for each user the number of distinct miners that process the users transactions. Our findings highlight the fact that the private users stay with the same miner through time as reported in Table 7. The coefficient of a private dummy is negative and significant, which lowers the value of the miner count. This behaviour is consistent with our hypothesis that private users forge long term exclusive contracts with mining pools.

Table 7. Regression Results for Likelihood to Stay with the Same Miner The independent variable is number of miners per user and is named Miner Count. We study the effect of private transactions on number of miners per users. The private transactions have decreasing role in number of miners.

	(1)	(2)
	Private Dummy	Private Dummy
Number of distinct Miners	-0.00352***	-0.00443***
	(-7.50)	(-10.04)
Sum of Input Values		8.79e-14***
		(7.35)
Block Size		-9.65e-08***
		(-25.16)
Transaction Count		0.000000184**
		(2.18)
Transaction Weight		0.000000609***
		(3.34)
Constant	-1.541***	-1.412***
	(-710.74)	(-278.25)
Observations	97,637,471	97,637,471
R^2		

t statistics in parentheses

* $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$

4.4 Regularity of Transactions

Aligned to our hypothesis, we believe private users utilize their specific channel with miners more frequently than normal ones. In addition, we anticipate private types to have evenly spaced out transactions over time. We consider two measures to study the regularity of transactions to find out how transactions are spaced out over time. We calculate the standard deviation of the time interval between two consecutive transactions for each user.[17] Then, we regress the standard deviation of block height difference on a dummy for private users and control variables. From the results in Table 8 we observe that private transactions have significantly

[17] Block height difference for consecutive transactions ordered by time, shows the time interval between transactions for each user. We study the standard deviation to see how these intervals are spaced out through time.

lower variation in times between transactions. Private transactions are more regular and evenly spaced over time.

Table 8. Regression Results for Regularity of Transactions The private transactions have decreasing effect on standard deviation of height difference. The regression on column 2 is controlled with transactions size and input values and number of confirmed transactions.

	(1) Std of Block Height Difference	(2) Std of Block Height Difference
Private Dummy	-1682.2***	-1276.9***
	(-259.22)	(-191.97)
Sum of Input Values		-6.20e-11***
		(-11.65)
Block Size		0.0000808***
		(20.52)
Transaction Weight		-0.000518***
		(-8.37)
Transaction Count		-0.000333***
		(-3.42)
Constant	1779.0***	1296.6***
	(696.49)	(199.61)
Observations	36,421,771	28,828,629
R^2	0.186	0.219

t statistics in parentheses

* $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$

4.5 Miner Size

Not all miners are equally involved in the settlement of private transactions. We conjecture that smaller miners have a greater desire for a dedicated source of income from settlement of private transactions. Using the sample of all transactions we use a logit model to regress the dummy that a transaction is private on a dummy for big miners and other control variables. As reported in Table 9 big miners are significantly less likely to mine private transactions than small miners.

Table 9. Regression Results for Miner Size The larger the market share, the lower the chance of mining a private transactions. This finding is compatible to our model. Market share is the percentage of mined block for each miner and has negative coefficient. The positive coefficient of the market share to the power of two shows the positive curvature.

	(1)	(2)
	Private Dummy	Private Dummy
Market Share	-0.0983***	-0.0998***
	(-217.63)	(-221.23)
Market Share^2	0.00778***	0.00789***
	(247.14)	(250.69)
Transaction Count		6.32e-08*
		(1.65)
Sum of Input Values		-2.16e-14*
		(-1.72)
Block Size		-0.000000250***
		(-92.56)
Transaction Weight		0.000000446**
		(2.45)
Constant	-1.768***	-1.440***
	(-896.01)	(-341.90)
Observations	97,637,471	97,637,471
R^2		

t statistics in parentheses

* $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$

5 Conclusion

Our paper is part of growing literature on settlement in unregulated markets. In such systems, users can offer a fee to the settlement agent. We study private settlement in Bitcoin blockchain and provide evidence that is consistent with private long term contracts between frequent users and miners. We analyze the miners' behaviour because they are the decentralized validation authorities with great liberty in the Bitcoin settlement ecosystem. In this study, we highlight that First: private settlement exists, and Second: Private users and their designated miner have incentives to utilize private channels. Our findings contribute to the research on the market competitiveness of cryptocurrencies. In addition, it served to understand better the link between Bitcoin miners' activity and the free settlement market. We believe that this study can pave the way for analyzing contractual structures in a private settlement market.

References

Andola, Nitish, Vijay Kumar Yadav, S Venkatesan, Shekhar Verma, et al., 2021, Anonymity on blockchain based e-cash protocols—A survey, *Computer Science Review* 40, 100394.

Androulaki, Elli, Ghassan O Karame, Marc Roeschlin, Tobias Scherer, and Srdjan Capkun, 2013, Evaluating user privacy in bitcoin, in *International conference on financial cryptography and data security* pp. 34–51. Springer.

Antonopoulos, Andreas M, 2014, *Mastering Bitcoin: unlocking digital cryptocurrencies*. (" O'Reilly Media, Inc.").

Athey, Susan, Ivo Parashkevov, Vishnu Sarukkai, and Jing Xia, 2016, Bitcoin pricing, adoption, and usage: Theory and evidence, .

Auer, Raphael, 2019, Embedded supervision: how to build regulation into blockchain finance, .

Balthasar, Thibault de, and Julio Hernandez-Castro, 2017, An analysis of bitcoin laundry services, in *Nordic Conference on Secure IT Systems* pp. 297–312. Springer.

Bodie, Zvi, and Alex Kane, 2020, Investments, .

Brogaard, Jonathan, Allen Carrion, Thibaut Moyaert, Ryan Riordan, Andriy Shkilko, and Konstantin Sokolov, 2018, High frequency trading and extreme price movements, *Journal of Financial Economics* 128, 253–265.

Cong, Lin William, Zhiguo He, and Jiasun Li, 2021, Decentralized mining in centralized pools, *The Review of Financial Studies* 34, 1191–1235.

Cormen, Thomas H, Charles E Leiserson, Ronald L Rivest, and Clifford Stein, 2001, Introduction to algorithms second edition, *The Knuth-Morris-Pratt Algorithm*.

Dae-Yong, Kim, Essaid Meryam, and Ju Hongtaek, 2020, Examining Bitcoin mempools Resemblance Using Jaccard Similarity Index, in *2020 21st Asia-Pacific Network Operations and Management Symposium (APNOMS)* pp. 287–290. IEEE.

Daian, Philip, Steven Goldfeder, Tyler Kell, Yunqi Li, Xueyuan Zhao, Iddo Bentov, Lorenz Breidenbach, and Ari Juels, 2019, Flash boys 2.0: Frontrunning, transaction reordering, and consensus instability in decentralized exchanges, *arXiv preprint arXiv:1904.05234*.

Daian, Philip, Steven Goldfeder, Tyler Kell, Yunqi Li, Xueyuan Zhao, Iddo Bentov, Lorenz Breidenbach, and Ari Juels, 2020, Flash boys 2.0: Frontrunning in decentralized exchanges, miner extractable value, and consensus instability, in *2020 IEEE Symposium on Security and Privacy (SP)* pp. 910–927. IEEE.

Easley, David, Maureen O'Hara, and Soumya Basu, 2019, From mining to markets: The evolution of bitcoin transaction fees, *Journal of Financial Economics*.

Foley, Sean, Jonathan R Karlsen, and Tālis J Putniņš, 2019, Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies?, *The Review of Financial Studies* 32, 1798–1853.

Greaves, Alex, and Benjamin Au, 2015, Using the bitcoin transaction graph to predict the price of bitcoin, *No data*.

Hu, Danqi, Charles M Jones, and Xiaoyan Zhang, 2021, When Do Informed Short Sellers Trade? Evidence from Intraday Data and Implications for Informed Trading Models, *Evidence from Intraday Data and Implications for Informed Trading Models (February 16, 2021)*.

Huberman, Gur, Jacob Leshno, and Ciamac C Moallemi, 2017, Monopoly without a monopolist: An economic analysis of the bitcoin payment system, .

Khalilov, Merve Can Kus, and Albert Levi, 2018, A survey on anonymity and privacy in bitcoin-like digital cash systems, *IEEE Communications Surveys & Tutorials* 20, 2543–2585.

Lehar, Alfred, and Christine A Parlour, 2022a, Battle of the Bots: Miner Extractable Value and Efficient Settlement, *Working paper*.

Lehar, Alfred, and Christine A Parlour, 2022b, Miner Collusion and the BitCoin Protocol, *Available at SSRN*.

Leskovec, Jure, Kevin J Lang, and Michael Mahoney, 2010, Empirical comparison of algorithms for network community detection, in *Proceedings of the 19th international conference on World wide web* pp. 631–640.

Meiklejohn, Sarah, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M Voelker, and Stefan Savage, 2013, A fistful of bitcoins: characterizing payments among men with no names, in *Proceedings of the 2013 conference on Internet measurement conference* pp. 127–140.

Nakamoto, Satoshi, 2008, Bitcoin: A peer-to-peer electronic cash system, .

Pakki, Jaswant, Yan Shoshitaishvili, Ruoyu Wang, Tiffany Bao, and Adam Doupé, 2021, Everything you ever wanted to know about bitcoin mixers (but were afraid to ask), in *International Conference on Financial Cryptography and Data Security* pp. 117–146. Springer.

Pappalardo, Giuseppe, Tiziana Di Matteo, Guido Caldarelli, and Tomaso Aste, 2018, Blockchain inefficiency in the Bitcoin peers network, *EPJ Data Science* 7, 1–13.

Park, Andreas, 2021, The Fatal Flaws of Constant Product Automated Market Making, working paper.

Ron, Dorit, and Adi Shamir, 2013, Quantitative analysis of the full bitcoin transaction graph, in *International Conference on Financial Cryptography and Data Security* pp. 6–24. Springer.

Russo, Daniela, Terry L Hart, Maria Chiara Malaguti, and Chryssa Papathanassiou, 2004, Governance of securities clearing and settlement systems, *ECB occasional paper*.

Schmiedel, Heiko, Markku Malkamäki, and Juha Tarkka, 2006, Economies of scale and technological development in securities depository and settlement systems, *Journal of Banking & Finance* 30, 1783–1806.

Wu, Lei, Yufeng Hu, Yajin Zhou, Haoyu Wang, Xiapu Luo, Zhi Wang, Fan Zhang, and Kui Ren, 2021, Towards understanding and demystifying bitcoin mixing services, in *Proceedings of the Web Conference 2021* pp. 33–44.

Xi, He, He Ketai, Lin Shenwen, Yang Jinglin, and Mao Hongliang, 2021, Bitcoin Address Clustering Method Based on Multiple Heuristic Conditions, *arXiv preprint arXiv:2104.09979*.

Xue, Gang, Jia Xu, Hanwen Wu, Weifeng Lu, and Lijie Xu, 2021, Incentive mechanism for rational miners in bitcoin mining pool, *Information Systems Frontiers* 23, 317–327.

Yanovich, Yuriy, Pavel Mischenko, and Aleksei Ostrovskiy, 2016, Shared send untangling in bitcoin, *bitfury. com* 2016, 1–25.

A Variable definitions

#	Items	Description
1	Block Height	For a particular Block, a block height is defined as the number of blocks preceding it in the blockchain. If we consider the Block height for a transaction, it reference the location of a completed transaction in the blockchain.
2	Block Size	The original Block size limit in Bitcoin blockchain is one megabyte. This factor constrain the on-chain transaction processing capacity jointly with the average block creation time of ten minutes.
3	Data Insertion	This is a method to utilize underlying blockchain mechanism to store data in the chain by overwriting output script. There are various methods for that which differ from cost and efficiency based on the size of the data one wants to add. A data insertion transaction is similar to the ordinary transaction and need to be confirmed by miners. Miners are receiving fee by providing the confirmation service as expected.
4	Block Reward	miner can get Block Reward after solving a hash puzzle. The amount is set by the Bitcoin protocol and is fixed for all miners. The current Block Reward amount is 6.25 BTC which is set in May 2020 after the Halving event.
5	Transaction Fee	Transaction fee that is charged to users when performing crypto transactions. The fee is collected by miners in order to process the transaction on the network.
6	Transaction Size	Each Bitcoin transaction consists of various fields such as input address, output address, amount, hash, timestamps and etc. The total size of these fields in byte is called a transaction size.
7	Transaction Weight	This is another measure for assessing the size of the transaction. Each byte unit is approximately four units of weights. In this measure, fields have different weights according to their importance.

Table 10. Transaction Variables Definition The description of the independent variables

#	Items	Description
1	Fee per Transaction	This measure the average Fee, each miner received by dividing Total Transaction Fee by Total number of Confirmed Transactions. This measure can be used for specific type of users or transactions such as normal and private.
2	Loyalty	This measure shows how users were in touch with the specific miners in their Transaction Window. We assume that the Loyalty in a long term contract should be high. So, the users do not change their designated miners frequently and stay with the same miner in a long run.
3	Market Share	The winner miner of each block is clear in the blockchain. The ownership potion of each miner from mined block is called miner's Market Share. This factor can be used as an indicator of size and complexity power of the miner.
4	Miner Revenue	This field is calculated based on the miners received amount from Total Transaction Fee plus the Block Rewards. The first one is related to the transactions that they confirmed and the second one is related to the blocks that they mined.
5	Miner Reward	This is the total Reward amount that a miner received by mining blocks in a specific period of time.
6	Miner Size	Ordering miners' Market Share in a descending preference, the first 25th percentile miners having the Large scale and the rest of them are in Small scale category.
7	Miner Traffic	This measure refers to the transactions that has been created by miners. This transactions contain miners wallet address as input or output field.
8	Normal Transaction	Transactions that are submitted and confirmed through the normal Bitcoin protocol is called normal in this research. These transactions are first waiting in the mempool and then will be confirmed by a miner based on Aging algorithm.
9	Private Transaction	Transactions that are submitted and confirmed through alternative channels of the Bitcoin protocol is called private in this research. These transactions never showed up in the mempool but got confirmation. Our Hypothesis emphasize that these transactions by passed normal channels and are send directly to the miners.
10	Regularity of Transaction	This measure can assess how transactions are deterministic or ad-hoc in a specific period of time. There are three ways to assess regularity: average rate, time interval, distribution comparison
11	Total Fee per Weight	This measure is the Sum of the calculated Fee per Weight for each Transaction.
12	Total Transaction Fee	It is the total value of all transaction fees paid to miners, not including the coinbase value of block rewards.
13	Transaction Fee per Weight	This measure has been calculated by dividing Transaction Fee by Transaction Weight to calculate the paid Fee based on one weight unit.
14	Transaction Window	This measure counts the time interval/number of created blocks between the first and the last transactions of each user group ordered in time. We utilized block height as a proxy for time measure for simplifying the calculations. This measure can be utilized in various granularity such as per miner or in General.
15	User Group	A User Group is a classified bunch of input addresses that have been utilized mutually in some transactions through time. We classified users based on our written computer program.
16	Variation of Fee per Weight	This is the Variance of the already calculate Fee per Weight measure for all transactions. The higher variation shows the Fee per Weight is not bound to the specific amount.

Table 11. Descriptive Measures Definition The description of the dependent variables

B User Classification

The union-find algorithm is the base mechanism for the user classification. It first introduced by Cormen, Leiserson, Rivest, and Stein (2001) and then widely applied in academic works such as Ron and Shamir (2013), Meiklejohn, Pomarole, Jordan, Levchenko, McCoy, Voelker, and Savage (2013), (Khalilov and Levi 2018), (Greaves and Au 2015) and Foley, Karlsen, and Putniņš (2019).

Our approach in detecting the users in bitcoin is aligned with other researchers perspective. Xi, Ketai, Shenwen, Jinglin, and Hongliang (2021) named it as common-input heuristic. In addition, extracting bitcoin miners' address based on the coinbase transactions has been utilized widely.

First, we assume that all transactions are unrelated. Therefore, we create a user identification per distinct input address and transaction hash in the primary iteration. In the second run, since a user can utilize more than one address to make a transaction, we group all the sender's input addresses in a given transaction. The merging process starts from the third iteration. This iterative process will continue till no mutual sender addresses are found.

B.1 Example 1:

The following example describes the process in a simple two step model. Consider we have the input file containing four records. According to the given sample, since add2 is mutual between transactions 1 and 2, the addresses will union, and we have just one user groups here. Therefore, the expected result should be as follows:

Expected Result: userid1, add1, add2, add3

Input File:

- T1, add1

- T1, add2

- T2, add3

- T2, add2

- T3, add4

- T4, add5

- T4, add6

Step1: Detecting add2 is mutual between two sets and then merge

- T1: add1, add2

- T2: add2, add3

- T3: add4

- T4: add5, add6

Step2: The algorithm output is matched with the expected result. The program can detect T1 and T2 is related to User1, since she used three three different addresses during the study period.

- User1 - T1,T2: add1, add2, add3

- User2 - T3: add4

- User3 - T4: add5, add6

B.2 Example 2:

To provide a more complex example and highlight the recursive nature of classification and user detection, here we have a set of transactions and addresses which have input address in common. After merging and detecting the mutual input addresses and their related groups, there may be a mutual address between newly merged ones. This type of mutual address, which we call it common after merge addresses, are detected in our implemenation.

Step1: Creating a set to find the relationship between transactions and addresses.

- T1: add1, add5

- T2: add2, add3

- T3: add3, add1

- T4: add2

- T5: add4

- T6: add1

Step2: Creating a reverse set to find the relationship between addresses and transactions.

- add1: T1, T3, T5

- add2: T2, T4

- add3: T2, T3

- add4: T5

Step3: Creating a mapping dictionary for transactions with common input.

- add1,add3,add5: T1, T3, T6

- add2, add3: T2, T3, T4

- add4: T5

Step4: Creating a mapping dictionary for already located addresses in mapping dictionary and keep it updated dynamically.

- add1: loc1

- add2: loc2

- add3: loc1 and loc2 (Therefore it needs to be merged)

- add4: loc3

Step5: Creating a result set using updated mapping dictionary.

As depicted, add3 is a common key in mapping dictionary. Therefore, the loc1 and loc2 will be merged and inserted in the final set which is the result. So, we have two disjoint groups in this example.

- add1, add2, add3, add5: T1, T2, T3, T4, T6

- add4: T5

C Mixed Transaction Detection

Bitcoin mixing services provide their users with improved anonymity by leveraging inherent characteristics of both Bitcoin and blockchain technology (Pakki, Shoshitaishvili, Wang, Bao, and Doupé 2021). In fact, these bitcoin blenders help users gain anonymity by breaking the connection between a certain bitcoin address and the identity of its true owner.

In general, mixing services have three phases including: taking inputs, performing mixing and sending outputs. One of the challenges in detecting mixing services is identifying the **Peeling chains**. Balthasar and Hernandez-Castro (2017) describes peeling chain as a laundry service in bitcoin blockchain. In fact, peeling chain is a technique to launder a large amount of cryptocurrency through a lengthy series of minor transactions.

There are two general strands for detecting Bitcoin Mixers in literature work. One strand is analyzing the anonymity based on Bitcoin addresses. The other strand try to identify the relations between bitcoin address and users by clustering (classification) such as (Khalilov and Levi 2018) and (Andola, Yadav, Venkatesan, Verma, et al. 2021) and (Yanovich, Mischenko, and Ostrovskiy 2016). Then the analyzer can detect an out of norm (irregular) behaviour in transactions by a specific user. Therefore, detecting mixed transactions improve the user classification algorithms.

In the following we describe general strands in literature work including our approach.

C.1 Transaction characteristics

The mixing services are different from fee and security point of view. (Balthasar and Hernandez-Castro 2017) study and rank various mixing services based on their design, tractability and their weakness in attacks. The fee range can be fixed rate which is almost 2% to 3% or it may vary based on BTC value such as 0.01 BTC. The other important factor is the user impatiences.

The mixing services may happen automatically (almost one minute), random time delay of few hours or more secure ones which is claimed to be hand-involved and take almost 24 hours. As mentioned in Pakki, Shoshitaishvili, Wang, Bao, and Doupé (2021) delays are maximized in mixed transactions comparing to the normal ones. Mixer services may have service limitation that one can utilize them to detect and exclude them from the sample. For example, they almost have an upper limit (1,000 BTC) and lower limit (0.01 BTC) for the amount. (Balthasar and Hernandez-Castro 2017).

Mixers are using addresses that their percentage or credit and debit transactions are similar. These addresses do not hold any amount and act like a distributor node in mixer's design. Therefore, they act like intermediary and temporal wallet addresses. The design of some mixers such as Helix is to generate multiple new wallets and recovers their money using few transactions. Therefore, there are always addresses that created and have not been used later. Coinjoin mixer asks users to set the input addresses, delay and fee and suggest to add randomness in tunning the values.[18]

Mixed transactions usually have multi-input and multi-output characteristics. Athey, Parashkevov, Sarukkai, and Xia (2016) showed that transactions having more than 4-inputs and 4-outputs at the same time, this transaction is suspicious to be created by mixers.

In Whirlpool mixing services, most of the transactions have five inputs and five outputs. In addition, they have equal splited amounts (0.001, 0.01, 0.05 and 0.5). This type of mixed transactions are implementation of the coninjoin. [19] For Wasabi implementation, there is an API that can be used to check coinjoin transactions that are not confirmed yet and in mempool.[20]

[18] https://coinjoin.io/en

[19] A sample transaction of this type is tx: 5553386e94b07112fb7b6789cae2f89f380ca20a28935812c51f0f3387bd5243

[20] https://wasabiwallet.io/api/v4/btc/ChaumianCoinJoin/unconfirmed-coinjoins. This is an example of mixed waiting transaction. tx: 16a7c04139883d33997ed475918afcc4f54355478cb1737076cbb8b97c208316

Another implementation is Joinmarket. There is a github project , called snicker-finder.py, that can be used to find Joinmarket coinjoin transactions in blocks.[21]

C.2 Representative mixing services

The majority of public mixers are black-box services, which do not have their code available to the public. To tackle this challenge, Pakki, Shoshitaishvili, Wang, Bao, and Doupé (2021) and Wu, Hu, Zhou, Wang, Luo, Wang, Zhang, and Ren (2021) interact with Five and Four real public mixers respectively, to identify actual behaviours and indicative of their implementation and their resistance.

In this approach, the representative mixing services is detected based on ”Bitcoin Talk” and public media.[22] In ”Bitcoin Talk” forum, mixers advertise their services and there are multiple venues that people talk about mixing services from technical and application point of views. This forum can provide users with the ability to distinguish trusted mixers as mentioned in (Pakki, Shoshitaishvili, Wang, Bao, and Doupé 2021).

Based on interaction with the real mixing services, a sample of input-output transactions will be created based on return address to analyze. Interacting with Mixers have two general types based on cost and the technology.[23] Creating this sample is limited by budget constraint as some services may charge the sender. There are public APIs that one can re-engineer and reconstruct the user’s mixing record.[24] In other words, this approach is based on the returned information from Mixers’ services and analysing that based on user types and address prefixes.

[21] https://github.com/JoinMarket-Org/joinmarket-clientserver/blob/master/scripts/snicker/snicker-finder.py and tx: 422e0aec25e667eebb1c453b446b65726440623c69b2ab381681ede2afd7c514 in an example of this type.

[22] https://bitcointalk.org/

[23] Chipmixer and Bitmix.biz see (Wu, Hu, Zhou, Wang, Luo, Wang, Zhang, and Ren 2021)

[24] Wasabi Wallet and Shape shift see (Wu, Hu, Zhou, Wang, Luo, Wang, Zhang, and Ren 2021)

C.3 Change address

Other heuristics such as **Change address heuristic** can be added to the main mixer detection program as described in (Xi, Ketai, Shenwen, Jinglin, and Hongliang 2021). In the bitcoin system, every time a transaction occurs, a node will record the the transaction on the ledger. After removing the transfer amount and transaction fees, the remaining bitcoin will be stored in the change address. Since the bitcoin in the change address belongs to the entity where the input address in the transaction is located, there is an association between the current change address and the input address. So one can detect the same entity which control both addresses. Moreover, the change addresses may be used as an input address that can improve the identification method. Androulaki, Karame, Roeschlin, Scherer, and Capkun (2013) utilized this approach to detect users' privacy in bitcoin.

C.4 Address's types

In (Wu, Hu, Zhou, Wang, Luo, Wang, Zhang, and Ren 2021) the writer utilizes the three types of addresses in bitcoin to detect user types. The first type are addresses created directly from private keys which are called Pay-to-Public-Key-Hash(P2PKH). These addresses begin with the number prefix **1**. The second type are Pay-tp-Script-Hash(P2SPH) which are addresses starting with prefix **3**. The third type of addresses are related to UTXOs which are introduced after 2017 and based on SegWit idea. this addresses begin with prefix **bc1q**.

C.5 Community detection

The **Louvain algorithm** evaluate modularity to quantify the quality of a community network division as described in (Leskovec, Lang, and Mahoney 2010) and (Xi, Ketai, Shenwen, Jinglin, and Hongliang 2021). The measure Q has the range of [-1,1]. For the Q greater than 0.3, the community is observable. In this context, we can define and measure the gain of modularity by adding a new node to a group. The change in value of Q may reduce the modularity. Figure **??** describes a simple example of this approach.

C.6 Our Approach

Our approach is to detect various mixing implementation of coinjoin protocol which is widely-used peer-to-peer mixer type.[25] We detect two main types of mixed transactions:

1- Transactions having five equal outputs and exactly five equal inputs

2- Transactions having more than ten equal outputs and the number of inputs is greater than the number of outputs

In our 2021 bitcoin transaction sample, having 112,553,498 records, our program detects 110,956 transactions of type 1 and 1,864 for type 2 mixed transactions. The union of two sets, and making this set unique by transaction hash, result in 107,639 mixed transactions. Excluding the mixers' and miners' transactions provide 97,637,471 records of data which we call it pure sample. The pure sample then will be merged with 116,482,396 unique input wallet addresses. The result set which is now 300,147,341 records is the input for our classification program. This procedure is depicted in Figure 3.

[25] There is a github project, called dumplings, that scans various coinjoin transactions for different implementations. https://github.com/nopara73/Dumplings/blob/master/Dumplings/Scanning/Scanner.cs

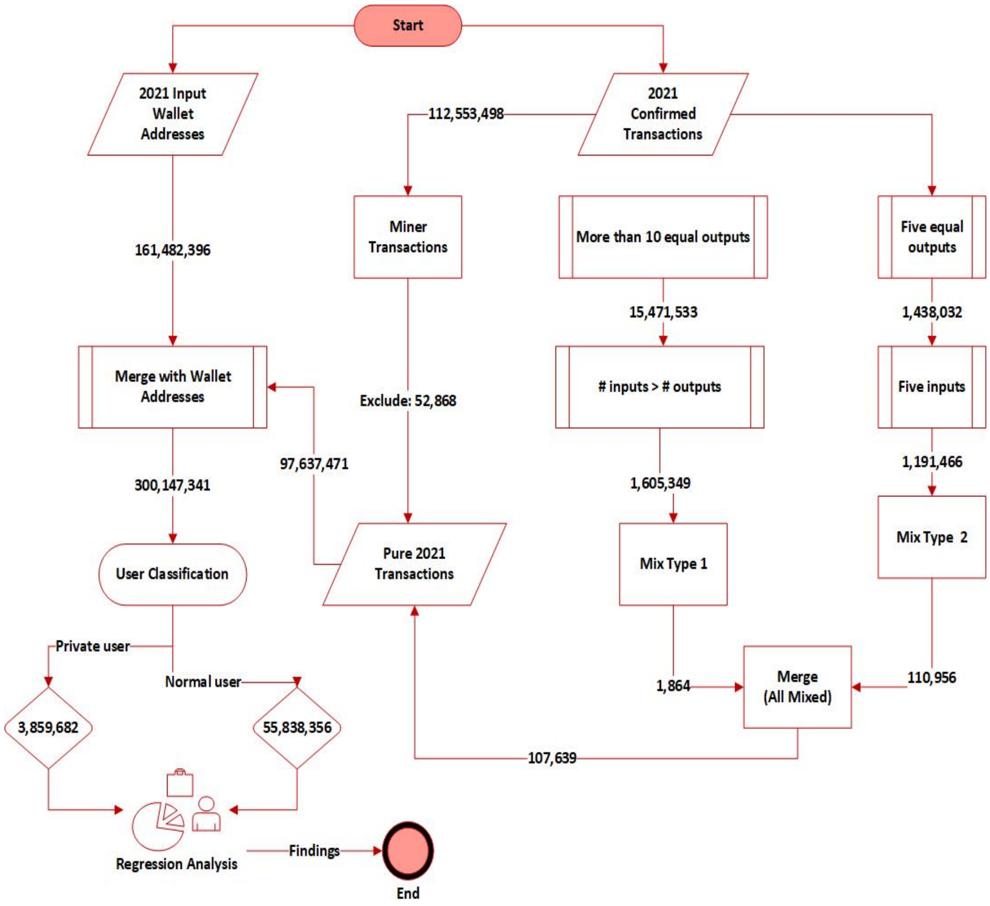


Figure 3. User Classification Action Plan The procedure to detect mixers' and miners' transactions to purify the sample for user classification is depicted in this flowchart.