EXCLUSIVE MINING OF BLOCKCHAIN TRANSACTIONS

Elias Strehle[1], Lennart Ante[1, 2]
[1] Blockchain Research Lab, Max-Brauer-Allee 46, D-22765 Hamburg
[2] Universität Hamburg, Von-Melle-Park 5, D-20146 Hamburg

After creating a new blockchain transaction, the next step usually is to make miners aware of it by having it propagated through the blockchain's peer-to-peer network. We study an unintended alternative to peer-to-peer propagation: Exclusive mining. Exclusive mining is a type of collusion between a transaction initiator and a single miner (or mining pool). The initiator sends transactions through a private channel directly to the miner instead of propagating them through the peer-to-peer network. Other blockchain users only become aware of these transactions once they have been included in a block by the miner. We identify three possible motivations for engaging in exclusive mining: (i) reducing transaction cost volatility ("confirmation as a service"), (ii) hiding unconfirmed transactions from the network to prevent frontrunning and (iii) camouflaging wealth transfers as transaction costs to evade taxes or launder money. We further outline why exclusive mining is difficult to prevent and introduce metrics which can be used to identify mining pools engaging in exclusive mining activity.

1. Introduction: What is exclusive mining?

Every blockchain user can create new transactions. These transactions are regarded as unconfirmed until they have been mined, i.e. included in a new block. In principle, every user can mine new blocks and thus confirm his own transactions. In practice, however, mining on popular blockchains like Bitcoin and Ethereum has become so resource-intensive that it is only performed by a handful of miner collectives, known as mining pools.[1] The vast majority of blockchain users must therefore rely on miners to have their transactions confirmed.

How do miners become aware of new transactions? In the absence of a central coordinator, blockchains rely on their peer-to-peer network to transmit new transactions. In a peer-to-peer network, every network node maintains connections with a number of peer nodes. Whenever a node receives or creates new information (e.g. a new transaction), it forwards the information to its peers, which forward it to their own peers, and so on. In this way, information is propagated through the network quickly and reliably.

To make transactions attractive to miners, they typically include a fee. The miner who confirms the transaction can redeem the fee. This approach – propagating a transaction through the peer-to-peer network and offering a fee to whoever confirms it – enables users to have their transactions confirmed without interacting with a miner directly, even without knowing who the miners are. In principle, every blockchain user has a shot at confirming the transaction and collecting the transaction fee. This maximizes the probability that the transaction is confirmed quickly. It also limits the power of every individual miner to censor transactions or demand excessive fees.

Every blockchain node is a black box to its peers, characterized only by the information it chooses to share. As a result, most blockchains cannot enforce full compliance with their protocol. The Bitcoin protocol, for example, prescribes that all blockchain nodes should forward all new transactions to their peers.[2] But the absence of a central coordinator and the inherent unreliability of a peer-to-peer network on the internet makes misbehaviour difficult to detect. Slow connections and failing nodes occur on a regular basis, meaning that some nodes might become aware of a transaction very late or not at all. It is therefore not possible for other nodes to determine whether a suspicious node deliberately withheld a transaction or simply did not receive it.

This non-enforceability of protocol opens the door to an alternative way of having transactions confirmed, which we refer to as *exclusive mining*.

In exclusive mining, a transaction initiator and a miner set up a private communication channel outside the blockchain network. Through this channel, the initiator sends transactions directly to the colluding miner. Neither the initiator nor the miner propagates the transactions through the peer-to-peer network; no other network members can become aware of the unconfirmed transactions. The miner then confirms the transactions by including them in new blocks, collecting the associated transaction fees in the process. All other members of the network only become aware of the exclusively mined transactions as part of the blocks in which the miner has confirmed them. Table 1 contains a systematic comparison of the two approaches. Figure 1 compares the information flows of regular mining and exclusive mining.

To our knowledge, exclusive mining has not been discussed in the academic literature until now. A close relative, however, is studied in Babaioff et al. [1]. The authors observe that blockchain nodes have no incentive to forward new transactions to their peers. In fact, miners have an incentive to do the opposite and keep transactions secret in the hope of

[1] We use the term miner to refer to both individual miners and mining pools.

[2] For details, see Chapter 7 of Antonopoulos [25].

Table 1. Comparison of regular mining and exclusive mining.

	Regular mining	Exclusive mining
Cost for initiator	Transaction fee	Off-chain payment + Transaction fee (can be lower or higher than in regular mining)
Gain for colluding miner	If colluding miner confirms transaction first: Transaction fee Otherwise: Zero	Off-chain payment + Transaction fee (guaranteed)
Visibility of unconfirmed transaction	Network aware of unconfirmed transaction	Network unaware of unconfirmed transaction
Time until confirmation	Depends on size of transaction fee	Depends on hashrate of coll. miner

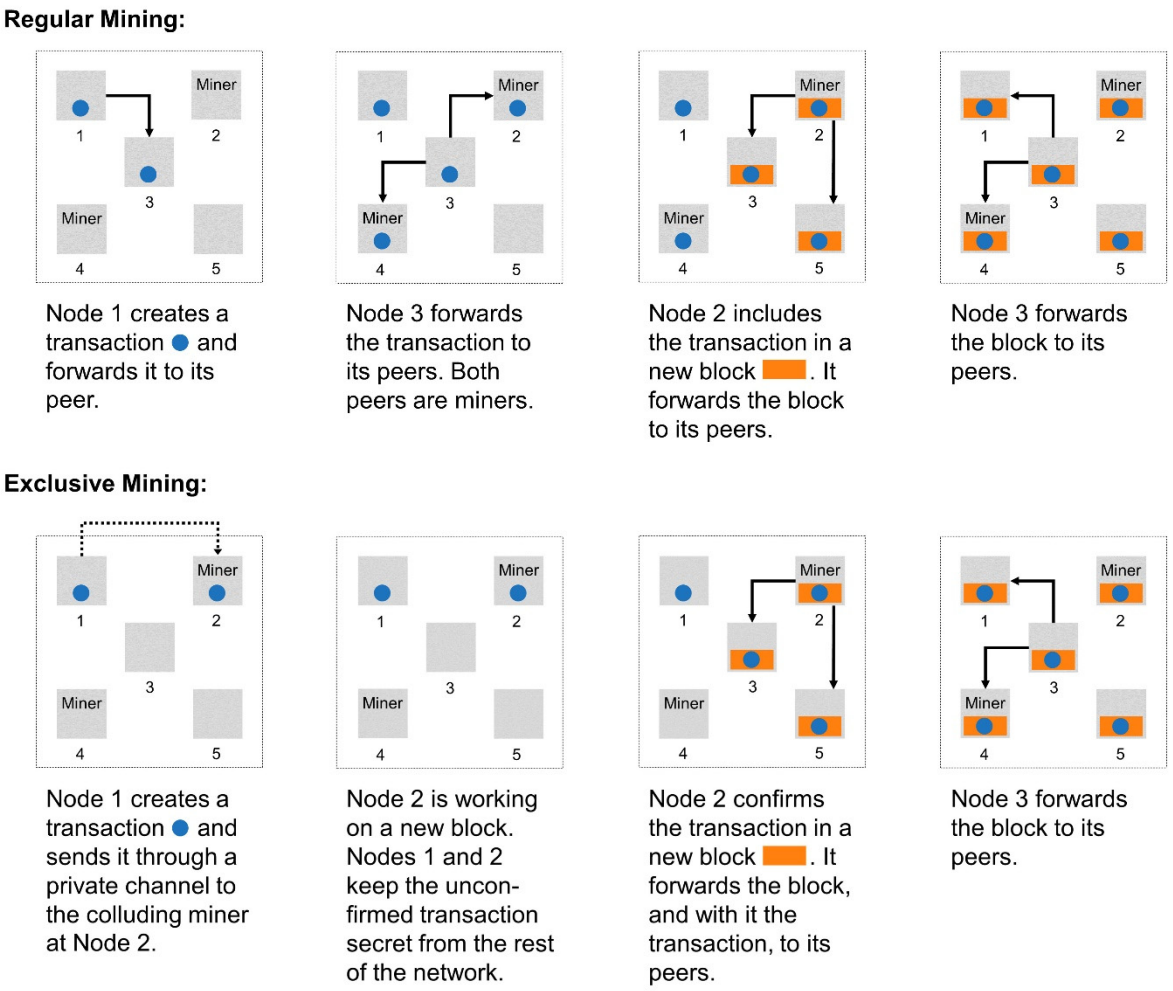

Figure 1: Information flow in regular mining and exclusive mining.

being the only one who can earn the associated transaction fees. While this observation has resonated in academia (see e.g. a proposed solution in Ersoy et al. [2]), it appears to be irrelevant in practice. Propagation through a peer-to-peer network is highly robust to misbehaving nodes, unless there are very many of them or they eclipse a part of the network. As long as the majority of blockchain nodes forwards transactions as prescribed, it hardly makes a difference whether a miner forwards transactions or not. Exclusive mining, on the other hand, is guaranteed to succeed. The transaction initiator and the miner share new transactions only through the private channel, therefore ensuring that no-one except the colluding miner can confirm them.

Another mechanism which at first glance shares similarities with exclusive mining is selfish mining, which was first described in Eyal and Sirer [3]. In selfish mining, a miner does not immediately share successfully mined blocks with the network but secretly generates a competing chain. Once the competing chain is long enough, it is revealed to the network and has a chance of becoming the new main chain, effectively putting the mining effort of competing miners to waste. Thus, both exclusive mining and selfish mining rely on a miner holding

back information. The difference is that in the case of exclusive mining, a transaction is held back, not a block. Exclusive mining does not aim to fork the blockchain. The intention and the results are therefore very different. Unlike selfish mining, exclusive mining is not an attack on the network; it is merely an unintended way of confirming new transactions.

In Chapter 2, we explain why transaction initiators and miners would employ exclusive mining. We describe how miners can use it to offer "confirmation as a service" or offer users protection from frontrunning, but also how criminal entities might utilize it in money laundering and tax evasion schemes. In this way, we illustrate that exclusive mining does have useful and potentially desirable applications, but also characteristics that can make it highly problematic. In Chapter 3, we describe how other members of the network can detect exclusive mining activity. Our results contribute to the literature on the mining of blockchain transactions and on the incentives and the behaviour of blockchain users [4–7].

2. Applications of exclusive mining

In the following, we discuss three potential applications of exclusive mining. First, transaction processing agreements between miners and entities regularly generating transactions, such as crypto-currency exchanges ("confirmation as a service"). Second, bypassing the mempool of unconfirmed transactions to hide activity from frontrunning bots. Third, money laundering or tax evasion by means of transaction fees in exclusively mined transactions.

2.1 Confirmation as a service

On popular blockchains like Bitcoin or Ethereum, transaction fees have been highly volatile, creating significant cost uncertainty especially for "power users" like cryptocurrency exchanges or services which regularly write information to a blockchain, e.g. supply chain tracking services. Significant unexpected changes in transaction fees on the blockchain could endanger the profitability or even the viability of these users. This danger is far from hypothetical, as e.g. the "CryptoKitties incident" shows, in which the popularity of a game on the Ethereum blockchain led to a significant increase in transaction fees [8]. Against this background, an exclusive mining agreement can provide a safety mechanism to ensure that critical processes are shielded from extreme situations.

When exclusive mining is employed as a safety mechanism against volatile transaction fees, we refer to it as "confirmation as a service." The colluding miner promises to confirm all transactions of the transaction initiator as quickly as possible. For this, he receives an off-chain fee. The initiator can be sure that his transactions are confirmed within a certain time (depending on the agreement and the miner's hashrate). In effect, exclusive mining works as a hedge for both the initiator and the miner: The initiator has his transactions confirmed at a pre-agreed cost; the miner secures a predictable source of income. Thus, both parties reduce their exposure to the volatility of blockchain transaction fees.

Until now, fee volatility has been less impactful for miners than for transaction initiators, as the majority of miner income has come from fixed block rewards. But most blockchains are reducing block rewards over time (Bitcoin's block reward, for example, is halved every four years), such that miners will increasingly need to secure a reliable stream of well-paying transactions to remain profitable. Indeed, researchers have argued that declining block rewards might drive blockchain miners towards protocol violations in search of profit [9].

In principle, different arrangements of confirmation as a service are conceivable, depending on the agreement reached by the parties. In the case of fully exclusive mining, the transaction initiator sends transactions exclusively to the colluding miner; neither the exchange nor the miner propagates them through the blockchain's peer-to-peer network before they are confirmed. It is also conceivable that an initiator enters an exclusive mining agreement with a miner but also propagates transactions to the rest of the network. This increases the chances of having the transactions confirmed quickly. The agreement with the miner acts as a safeguard – if the transaction is not confirmed by non-colluding miners, the colluding miner will do so eventually.

2.2 Anti-frontrunning strategies

While an unconfirmed transaction is propagated through the network, more and more blockchain nodes become aware of it. The fact that other users learn about a transaction before it is confirmed and thus executed can have undesirable or even catastrophic consequences for the transaction initiator. Users who closely monitor their mempool of unconfirmed transactions can exploit the information leaked by these transactions and attempt to profit from frontrunning.

Frontrunning involves replicating or countering an unconfirmed transaction with another transaction and ensuring that the latter is executed first, usually by offering a higher transaction fee to miners. While frontrunning of large transfers on Bitcoin and other single-purpose blockchains is possible under certain circumstances, the issue is particularly problematic for multi-purpose ("Turing-complete") blockchains. In a ground-breaking study, Daian et al. [10] observed a large number of highly profitable arbitrage bots on the Ethereum blockchain. These bots engaged in frontrunning by jumping the queue in decentralized exchanges (DEXes) or exploiting erroneous transfers (e.g. transfers with typos or misplaced decimal points). Robinson and Konstantopoulos [11] provide an especially vivid example in which an attempt to "rescue" misplaced funds is spotted and pre-empted by a predatory bot.

Through exclusive mining, a transaction initiator can hide transactions from the network until they are

confirmed and thus effectively prevent frontrunning – unless it is conducted by the colluding miner. Miners could therefore offer exclusive mining to transaction initiators who want to avoid frontrunning. Miners could do this for profit or to gain reputation within the blockchain community by acting as "white-hat hackers."

Is exclusive mining also attractive to the frontrunners themselves? Possibly, because collusion with a miner (or being a miner oneself) gives power over the selection and ordering of transactions in a block. On proof-of-work blockchains, however, it is uncertain which miner will mine the next block. This might make exclusive mining too unpredictable for frontrunners.

Frontrunning attacks on blockchains do not only relate to decentralized exchanges but also to double-spending attacks, decentralized applications (dApps), initial coin offerings (ICOs), decentralized auctions, blockchain name services and other on-chain activity [12,13]. While modifications of blockchain protocols with regard to confidentiality or transaction ordering may prevent frontrunning in the future, exclusive mining is a safety mechanism that is applicable right now.

2.3 Money laundering and tax evasion

On June 10, 2020, an Ethereum transaction sent 0.55 Ether (ETH), worth around $136 at the time, for a record-breaking transaction fee of 10,669 ETH, worth around $2.6 million.[3] One day later, 350 ETH were sent from the same address, again for a transaction fee of 10,669 ETH.[4] The intention behind these transactions remained unclear. The extreme fees might have resulted from a typo or a software bug. This had happened before. In that case, the mining pool which confirmed the transaction, SparkPool, agreed to reimburse half of the fee [14].

However, the high fees may also have been deliberate, which could have various reasons. One reason could be that access to the address had been compromised but transfers could only be made to certain whitelisted addresses. In this scenario, the high transaction fees would be a kind of blackmail. The hijacker demands ransom money and lends weight to his demand by "burning" funds through transaction fees [15].

Another reason might be that these and similar transactions were part of a money laundering or tax evasion scheme. Exclusive mining allows miners to retain transactions and integrate them exclusively into their own blocks. In this way, a miner can ensure that a transaction with very high transaction costs will never be confirmed by other miners. Since transaction costs represent regular income for miners, significantly increased transaction costs could be used to launder money by colluding with a miner.

Money laundering in the context of cryptocurrency markets has been assessed by a variety of studies. Yet, none of the studies we identified explicitly describe or analyse the mechanism of money laundering via exclusive mining [16–18].

Figure 2 shows a schematic overview of the money laundering process, where an initiator is transferring funds to a colluding miner via exclusive mining. We show two different entities – a transaction initiator and

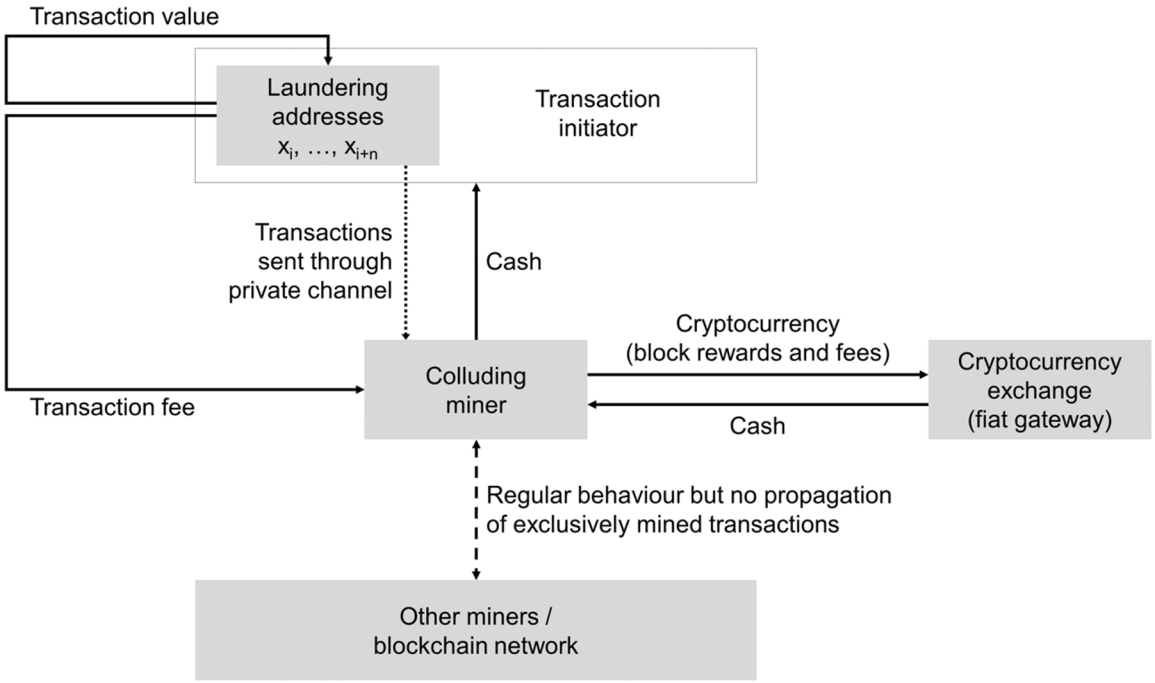

Figure 2: Schematic model of money laundering through transaction fees in exclusive mining.

[3] https://etherscan.io/tx/0xca8f8c315c8b6c48cee0675677b786d1babe726773829a588efa500b71cbdb65.

[4] https://etherscan.io/tx/0xc215b9356db58ce05412439f49a842f8a3abe6c1792ff8f2c3ee425c3501023c.

a miner that come to terms about laundering funds. Both entities could however be controlled by the same actor.

During the process of laundering money through exclusive mining, the initiator always retains control of all transferred funds since all sender and receiver addresses are under his control. Transaction costs are deducted from the initiator's blockchain asset balance and redeemed by the colluding miner. Thus, this mechanism works for all blockchains where transaction fees are directly transferred to the miner of the transaction. Depending on the size of the respective fee per transaction and the quantity of funds to be laundered, all of the initiator's funds can be transmitted to the miner via transaction fees. The latter in turn can declare these fees – together with the "clean" fees earned as a miner – as regular income and exchange them to fiat currency on cryptocurrency exchanges. In the case of tax evasion, the initiator deducts the transaction fees as costs whereas the miner declares them as income. In the case of money laundering, the miner transfers the laundered funds back to the initiator as fiat currency.

On Bitcoin, some mining pools distribute earned transaction fees to their members while others do not [19]. Arguably, the risk of systematic money laundering is much lower in pools which distribute fees. Indeed, it might be easier for the initiator to run its own mining pool. This would eliminate the complexity of transferring fiat money and reduce the costs and risks of colluding with a third-party miner.

If money laundering processes are to be hidden from the rest of the network, the colluding miner must take care not to be seen as untrustworthy by the blockchain network. If it became obvious that the miner engaged in illegal activity, cryptocurrency exchanges could block his access to fiat currency. We describe two obfuscation mechanisms which the initiator and the miner could use to conceal their activity: initiate a small number of high-fee transfers and send cheap quality signals, or initiate a large number of average-fee transfers.

In the first scenario, a small number of transactions with very high transaction costs is initiated. To hide his involvement, the colluding miner can then announce that he would like to reverse the transactions or reimburse some of the fees. From the perspective of signalling theory [20], this acts as a positive quality signal to the market – even though it is a morally hazardous or cheap (to fake) signal [21]. The transaction initiator, of course, does not step forward. The colluding miner then declares the fees as regular mining income and completes the laundering process. This scenario is likely to attract attention from the community, miners, researchers and law enforcement, thus it cannot be repeated indefinitely.

In the second scenario, many transactions with average or slightly higher fees are created. This makes it easier to hide the exclusive mining activity, making the approach potentially viable over a long time. However, various metrics must be considered to ensure that such a system does not attract attention. Since blockchains are transparent, every network participant can see the total and the average transaction fee per mined block. Therefore, the transaction initiator and the miner must make an effort to obfuscate their activity in the best way possible. In the next chapter we describe how such obfuscation techniques can be countered to nonetheless uncover exclusive mining activity.

3. Detection of exclusive mining

Exclusive mining is not easy to detect. Private channels between nodes are easily kept secret, and there is no public record of when or how a node became aware of transactions. Thus, it is rarely possible to obtain definite proof of exclusive mining activity from public information alone.

In the absence of proof, one must resort to evidence. Exclusive mining activity creates characteristic patterns which can be observed by other blockchain nodes. In view of the role exclusive mining may play in tax evasion or money laundering schemes, it is important to be aware of these patterns and develop methods to detect them. In this section, we describe how any blockchain node can utilize the information it receives from peers to monitor the network for exclusive mining activity.

We introduce some clarifying notation. Let T denote the set of all transactions on the blockchain which were confirmed during a given time period. Any individual transaction will be denoted by $\tau \in T$. In principle, the aim of our analysis is to determine the set of all transactions which were exclusively mined:

$$T_{exclusive} := \{\tau \mid \tau \; was \; exclusively \; mined\}.$$

As argued above, $T_{exclusive}$ cannot be determined from publicly available information alone. Finding every exclusively mined transaction would require the cooperation of all miners or complete knowledge of the inner workings of all mining nodes. Neither seems realistic. Nonetheless, every blockchain node is able to determine a set of "suspicious" transactions; this set can then be perused for evidence of exclusive mining.

Let n denote "our" blockchain node. As part of the peer-to-peer network, n is made aware of new (unconfirmed) transactions and new blocks by its peers. We assume that the node is capable of timestamping incoming information, i.e. that it has a local clock and knows when it first became aware of any given transaction or block. Notice however that this clock need not be synchronized with the clocks of other nodes.

For a transaction τ, let $t_{received}(\tau)$ denote the time when n first became aware of the transaction, and let $t_{confirmed}(\tau)$ denote the time when n first became

aware of the block containing the transaction.[5] Since becoming aware of a block also means becoming aware of the transactions it contains, it always holds that $t_{received}(\tau) \leq t_{confirmed}(\tau)$.

The defining characteristic of exclusively mined transactions is that uninvolved nodes only become aware of them once they have been confirmed: If τ has been exclusively mined, then[6]

$$t_{received}(\tau) = t_{confirmed}(\tau). \qquad (*)$$

We refer to transactions which satisfy condition (*) as late transactions. Define the set of all late transactions:

$$T_{late} := \{\tau |\ t_{received}(\tau) \ = \ t_{confirmed}(\tau)\}.$$

Every exclusively mined transaction is a late transaction. The converse statement does not hold. Indeed, even in the absence of exclusive mining, it is not unusual that a node only becomes aware of a transaction through the block which confirms it. Figure 1 illustrates this: Even in the case of regular mining, the bottom right node remains unaware of the transaction until it becomes aware of the block in which it is confirmed. In other words, condition (*) is necessary, but not sufficient, for exclusively mined transactions; or equivalently:

$$T_{exclusive} \subseteq T_{late}.$$

Be aware that $T_{exclusive}$ is "objective" while T_{late} is "subjective." A transaction τ was either mined exclusively or not; given full information, different nodes would not disagree over this fact. The timestamps $t_{received}(\tau)$ and $t_{exclusive}(\tau)$, on the other hand, are different for every node in the network.[7] Indeed, one could denote T_{late} as T_{late}^{n} to clarify that the set pertains to node n only. We omit the n only to avoid visual clutter.

The advantage of T_{late} over $T_{exclusive}$ is that it can be determined using only the information available to node n. Thus, T_{late} can be considered a noisy but observable approximation of the desired but unobservable set $T_{exclusive}$. Because T_{late} also contains transactions which were late by chance and not because of exclusive mining, one must resort to statistical methods to detect unusual patterns within the set.

Let M be the set of miners. For $m \in M$, define the set of transactions contained in blocks which were mined by miner m:

$$T^m := \{\tau \mid \tau \ was \ confirmed \ by \ m\}.$$

Furthermore, define the set of late transactions mined by m:

$$T_{late}^m := \{\tau \mid \tau \ was \ confirmed \ by \ m \ and \ t_{received}(\tau) \ = \ t_{confirmed}(\tau)\}.$$

Notice that $T_{late}^m = T^m \cap T_{late}$.

If m engages in exclusive mining, he will have a larger share of late transactions than the average miner. Therefore, a first metric which correlates with exclusive mining activity is the share of late transactions for a given miner:

$$\alpha^m := \frac{|T_{late}^m|}{|T^m|} = \frac{|T^m \cap T_{late}|}{|T^m|}.$$

A second metric derives from the fees associated with late transactions. When exclusive mining is employed as part of tax evasion or money laundering schemes, the intention is to transfer a significant amount of value to the miner through transaction fees. As described in Chapter 2, this may be accomplished through a small number of high-fee transactions or a high number of average-fee transactions. Regardless of the number of transactions, however, the exclusive mining activity will show up as a large amount of transaction fees earned through late transactions. For a transaction τ, let $f(\tau)$ denote its fee. Define the total fees earned by miner m through late transactions:

$$\beta^m := \sum_{\tau \in T_{late}^m} f(\tau).$$

The variable β^m is the sum of fees earned by m through exclusive mining plus the fees earned by m through other late transactions. It is therefore an upper bound on the amount transferred to m as part of tax evasion or money laundering schemes. However, one must keep in mind that a high value of β^m does not in any way prove that m engages in money laundering or tax evasion. It may, however, hint towards unusual activity.

Two additional metrics can be used to study the fee structure of late transactions. One is the share of fees earned by miner m through late transactions:

$$\gamma^m := \frac{\sum_{\tau \in T_{late}^m} f(\tau)}{\sum_{\tau \in T^m} f(\tau)} = \frac{\beta^m}{\sum_{\tau \in T^m} f(\tau)}.$$

While γ^m does not provide an upper bound on suspicious fees earned by miner m, it has the advantage of being independent of the miner's total hashrate. In particular, under the assumption that there is no exclusive mining, the expected value $E[\gamma^m]$ is the same for small and large miners.

Another metric is the average fee of late transactions relative to the average fee of non-late transactions:

$$\delta^m := \frac{\sum_{\tau \in T_{late}^m} f(\tau)/|T_{late}^m|}{\sum_{\tau \in T^m} f(\tau)/|T^m|}.$$

The metric δ^m can provide valuable insight but should be interpreted with care. Miners engaging in

[5] For simplicity, we ignore blockchain forks and thus the possibility that a transaction is confirmed in more than one block. When analyzing historical blockchain data, this is easily accomplished by considering only the main chain.

[6] A miner may try to obfuscate exclusive mining activity by propagating the transaction after finding, but before propagating the new block. In this case, the equality would not hold. However, by doing so he risks that another miner finds a new block first, causing him to lose all gains associated with his block.

[7] Bitcoin's blocks contain a timestamp. One might therefore argue that there is an objective time when transactions were confirmed. The block timestamp, however, is set by the miner of the block. In the presence of clock drift, it cannot be compared to another node's timestamps. Thus, a comparison between the time when a transaction was received and the time it was confirmed is only sensible when both times have been determined by the same node.

confirmation as a service are likely to earn lower fees for their exclusively mined transactions (because they receive an additional off-chain fee), which would result in δ^m being significantly smaller than 1. Miners engaging in money laundering or tax evasion through exclusive mining are likely to earn higher fees for their exclusively mined transactions (because these transactions need to transfer significant value to the miner), which would result in δ^m being significantly larger than 1. For exclusive mining employed in anti-frontrunning strategies, the effect on δ^m is unclear: The miner may demand higher fees as remuneration, or lower fees plus an off-chain fee. In any case, it is easy to "whitewash" δ^m by offsetting high-fee transactions with a number of low-fee transactions or vice versa. The metrics α^m, β^m and γ^m appear less susceptible to such attempts of hiding exclusive mining activity.

Additional insight may be gained from studying the transactions in T_{late} in more detail. Transactions which are part of tax evasion or money laundering schemes are self-transfers, i.e. the transaction initiator controls all input and output addresses. While self-transfers can be obfuscated by using a large number of addresses and emulating realistic transaction behaviour, sophisticated pattern recognition may be able to detect such self-transfers and thus uncover entities which potentially engage in exclusive mining.

The metrics α^m, β^m and γ^m are positively correlated with exclusive mining activity. Large values suggest irregular mining behaviour and can thus be interpreted as possible evidence of exclusive mining of miner m. But how large is large, exactly? To obtain quantitative results, it is helpful to view the metrics as random variables. Under the null hypothesis that miner m does not engage in exclusive mining, and under appropriate assumptions on the propagation of information through the peer-to-peer network, it should be possible to derive the stochastic distributions of these random variables in dependence of m's share of total hashing power and the arrival rate of new transactions and blocks. Once the distributions are known, one can conduct statistical hypothesis testing for exclusive mining. We leave this to future research.

4. Conclusion

We have provided an overview of the concept of exclusive mining. Transactions are sent via a private channel to a colluding miner who confirms them in new blocks. The unconfirmed transactions are not propagated through the blockchain's peer-to-peer network, neither by the initiator nor the miner. Exclusive mining can be employed for various reasons, ranging from innocuous hedging of transaction fee volatility to money laundering and tax evasion.

Considering that it is difficult to identify exclusive mining and therefore the motivation behind it, we have outlined ways for node operators to identify evidence of exclusive mining and suggested a direction for future research into statistical testing for exclusive mining.

How realistic is it that money is being laundered through exclusive mining? As mentioned above, transactions with extremely high fees have attracted considerable attention from the media and the blockchain community. Some mining pools have offered to reimburse excessive or accidental fees [22,23]. This speaks in favour of self-regulation of the market, although one should not automatically assume that these reimbursements actually occur.

Of course, honest miners have an interest in the long-term success of their blockchain ecosystem. This may contribute to a miner's decision to reimburse fees. But miners are not necessarily honest. Arguably, comprehensive regulation of blockchain mining is the only measure that could fully prevent money laundering and tax evasion through exclusive mining. Considering that cryptocurrencies are decentralized networks whose miners are located all over the world; however, such regulation seems out of reach. It should also be borne in mind that over-regulation hampers innovation. Any regulation of mining should be designed with appropriate caution.

What if one abolished transaction fees altogether? In its current form, Bitcoin will eventually evolve into a fee market without any other rewards for miners. By contrast, parts of the Ethereum community argue that the current first-auction fee market is inefficient. The Ethereum Improvement Proposal (EIP) 1559 proposes the introduction of a base fee which adjusts based on network demand. When the transaction is confirmed, the base fee is burned, i.e. destroyed. The proponents of EIP 1559 argue that this would increase price efficiency and avoid unnecessarily high transaction fees [24]. While the proposal still allows for small tips for miners, the above-described ability to launder money via large transaction fees would become much more difficult. It is unrealistic, however, that all existing blockchains will adapt their fee mechanism. The associated risk of illegal activity based on exclusive mining must be assessed for each blockchain infrastructure individually.

It should be noted that exclusive mining is possible on a large number of blockchains. For instance, it should be possible to engage in exclusive mining on a proof-of-work blockchain as well as on a proof-of-stake blockchain. The incentive structure, however, might look entirely different. On proof-of-stake blockchains, the miner of the next block is typically known in advance, which could make confirmation as a service as well as anti-frontrunning strategies much more attractive [10]. We hope that future research builds on our study to determine to what extent different blockchains display evidence of exclusive mining activity and if associated risks differ based on underlying technologies and mechanisms.

It can also be useful to examine market characteristics such as trading volume or liquidity. Money laundering only works if the funds can reliably be redeemed for fiat currency. While Bitcoin and Ethereum are currently most suitable in this regard,

they are also the two blockchain where it is most difficult to mine blocks at regular intervals. In addition, both Bitcoin and Ethereum are observed closely by blockchain enthusiasts, researchers and the media. Criminals may see smaller blockchain networks as more suitable vehicles for money laundering or tax evasion via exclusive mining.

In summary, exclusive mining can be both a blessing and a curse for blockchains. It is in the best interest of blockchain communities and concerned authorities to develop appropriate monitoring tools which can detect exclusive mining activity, at least when it is employed towards criminal ends. We hope that our work serves as the foundation for further research and a heightened awareness of exclusive mining, its potential and its perils.

References

[1] M. Babaioff, S. Valley, S. Dobzinski, S. Oren, On Bitcoin and Red Balloons, in: Proc. 13th ACM Conf. Electron. Commer. - EC '12, 2012: pp. 56–73. https://doi.org/10.1145/2229012.2229022.

[2] O. Ersoy, Z. Ren, Z. Erkin, R.L. Lagendijk, Transaction Propagation on Permissionless Blockchains: Incentive and Routing Mechanisms, in: 2018 Crypto Val. Conf. Blockchain Technol., 2018. https://doi.org/10.1109/CVCBT.2018.00008.

[3] I. Eyal, E.G. Sirer, Majority Is Not Enough: Bitcoin mining is vulnerable, in: Eighteenth Int. Conf. Financ. Cryptogr. Data Secur., 2014.

[4] E. Strehle, F. Steinmetz, Dominating OP Returns: The Impact of Omni and Veriblock on Bitcoin, 2020.

[5] A. Gervais, H. Ritzdorf, G.O. Karame, S. Čapkun, Tampering with the delivery of blocks and transactions in Bitcoin, in: Proc. ACM Conf. Comput. Commun. Secur., 2015: pp. 692–705. https://doi.org/10.1145/2810103.2813655.

[6] J.A. Kroll, I.C. Davey, E.W. Felten, The Economics of Bitcoin Mining or, Bitcoin in the Presence of Adversaries, in: Proc. WEIS, 2013: pp. 1–21.

[7] O. Schrijvers, J. Bonneau, D. Boneh, T. Roughgarden, Incentive Compatibility of Bitcoin Mining Pool Reward Functions, in: Int. Conf. Financ. Cryptogr. Data Secur., Springer Berlin Heidelberg, 2016: pp. 477–498.

[8] BBC, CryptoKitties craze slows down transactions on Ethereum, (2017). https://www.bbc.com/news/technology-42237162 (accessed August 12, 2020).

[9] M. Carlsten, H. Kalodner, S.M. Weinberg, On the instability of bitcoin without the block reward, in: Proc. 2016 ACM SIGSAC Conf. Comput. Commun. Secur., 2016: pp. 154–167. https://doi.org/10.1145/2976749.2978408.

[10] P. Daian, S. Goldfeder, T. Kell, Y. Li, X. Zhao, I. Bentov, L. Breidenbach, A. Juels, Flash Boys 2.0: Frontrunning in Decentralized Exchanges, Miner Extractable Value, and Consensus Instability, in: 2020 IEEE Symp. Secur. Priv., 2020: pp. 910–927. https://doi.org/10.1109/SP40000.2020.00040.

[11] D. Robinson, G. Konstantopulos, Ethereum is a Dark Forest, (2020). https://medium.com/@danrobinson/ethereum-is-a-dark-forest-ecc5f0505dff (accessed August 20, 2020).

[12] S. Eskandari, S. Moosavi, J.C. B, SoK: Transparent Dishonesty: Front-Running Attacks on Blockchain, in: Int. Conf. Financ. Cryptogr. Data Secur., Springer International Publishing, 2019: pp. 170–189. https://doi.org/10.1007/978-3-030-43725-1.

[13] G.O. Karame, E. Androulaki, Double-Spending Fast Payments in Bitcoin Categories and Subject Descriptors, in: Proc. 2012 ACM Conf. Comput. Commun. Secur., 2012: pp. 906–917. https://doi.org/10.1145/2382196.2382292.

[14] Coindesk, Ethereum mining pool Sparkpool has located and verified the accidental sender of an unusually high miners' fee and agreed to split the amount., (2019). https://www.coindesk.com/sparkpool-splits-2100-ether-mining-fee-with-accidental-sender (accessed June 13, 2020).

[15] Decrypt, Hackers blackmail exchange with $5 million of Ethereum fees - report, (2020). https://decrypt.co/32145/hackers-blackmail-exchange-with-5-million-of-ethereum-fees-report (accessed June 13, 2020).

[16] L. Ante, Cryptocurrency, Blockchain and Crime, in: K. McCarthy (Ed.), Money Laund. Mark. Regul. Crim. Econ., Agenda Publishing, 2018: pp. 171–198. https://doi.org/10.2307/j.ctv5cg8z1.10.

[17] M. Möser, R. Böhme, D. Breuker, An Inquiry into Money Laundering Tools, in: 2013 APWG ECrime Res. Summit, 2013: pp. 1–14. https://doi.org/10.1109/eCRS.2013.6805780.

[18] R. van Wegberg, J.J. Oerlemans, O. van Deventer, Bitcoin money laundering: mixed results?: An explorative study on money laundering of cybercrime proceeds using bitcoin, J. Financ. Crime. 25 (2018) 419–435. https://doi.org/10.1108/JFC-11-2016-0067.

[19] Bitcoin Wiki, Comparison of mining pools, (2020). https://en.bitcoin.it/wiki/Comparison_of_mining_pools (accessed June 15, 2020).

[20] M. Spence, Job Market Signaling, Q. J. Econ. 87 (1973) 355–374. https://doi.org/10.1055/s-2004-820924.

[21] L. Ante, I. Fiedler, Cheap Signals in Security Token Offerings (STOs), (2019). https://doi.org/10.2139/ssrn.3356303.

[22] Bitcoin.com, Mining Pool BTC.com Finds Accidental 80 BTC Fee – Offers a Refund, (2017). https://news.bitcoin.com/mining-pool-btc-com-80-btc-fee-refund (accessed June 15, 2020).

[23] Bitcoin.com, Bitcoin Miner Repays Customer Who Accidentally Paid 2.5 Bitcoins Transaction Fee, (2017). https://news.bitcoin.com/bitcoin-

miner-repays-customer-who-accidentally-paid-2-5-bitcoins-transaction-fee/ (accessed June 15, 2020).
[24] V. Buterin, E. Conner, R. Dudley, M. Slipper, I. Norder, Ethereum Improvement Proposal 1559 (EIP-1559), (2020). https://github.com/ethereum/EIPs/blob/master/EIPS/eip-1559.md (accessed June 16, 2020).
[25] A.M. Antonopoulos, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, 2014.