Colin Murphy*

The Cryptocurrency Filabuster: an Analysis of Blindly Signed Contracts as a Feather Forking Countermeasure

Abstract: The cryptocurrency market has expanded rapidly over the past few years with platforms (e.g. Bitcoin) becoming household names; furthermore, the mainstream has realized its potential and professional investors are entering the market. The decentralized structure of cryptocurrency is one of the most appealing components to many users - a component of which is a result of the blockchain-based structure. However, many vulnerabilities exist within this design that allow for malicious actors to perform attacks which threaten the stability of the entire network. One such attack that can be performed by miner nodes is known as Feather Forking.

This study investigates the architecture of the popular cryptocurrency platform, Bitcoin, and the underlying protocols that allow for Feather Forking attacks to occur - namely, Proof-of-Work (POW), Peer-to-Peer communication (P2P), and miner strategy. We also propose that the Blindly Signed Contracts anonymity protocol can be used as a countermeasure for such attacks while also providing greater privacy.

Keywords: cryptocurrency, bitcoin, privacy, security, feather fork, blockchain, proof-of-work, blindly signed contracts, anonymity

1 Introduction

Bitcoin has gained a reputation as an anonymous, decentralized, and cryptographically secure payment system for use in the familiar capitalistic context. Bitcoin's decentralization is achieved by its distributed, publicly verified ledger of transactions, known as blockchain. Potential transactions of bitcoins are combined into a single block to be "mined" by network nodes (known as miners) who then verify the block and add it to the blockchain. Each transaction within the node is charged a fee in order to have the transaction verified which in turn serves as the reward for the miner nodes. The mining operation is computationally intensive and miners compete to verify the transaction first, thus the more computational power (α) the higher the chance that the miner will be first. Success of this construct requires that a majority (>51%) of miners are acting honestly and mine to maximize revenue. With a significant amount of mining power, colluding miners can influencing the manner in which blocks are mined and if they are to be added to the blockchain. Although a mining power >51% would be required for an attacker to upend the decentralization of the network, an attacker with a smaller amount of mining power can still hold significant influence over a network to serve their own needs by using deceptive mining strategies.

It has been noted by some that Bitcoin's theoretical bases of it's protocol is not well understood, thus it's users are at risk[1] of attack. One type targeted attack in particular, known as feather forking [9], can result in a user's bitcoins being frozen indefinitely. This result is achieved by abusing the cooperative structure of the system to force other miners to invalidate the transition of a particular user by essentially working against the other miners. Furthermore, the individual user may be directly blackmailed by threatening to continually invalidate their transactions until a ransom is paid. However, in practice the actual probability of a feather attack itself being carried out successfully is marginal (i.e. the block containing the target's transaction is actually excluded from the main chain). This is due to the most successful countermeasure being a higher transaction fee payed by the user, ensuring the block is valuable enough for other miners to focus on it. The objective of a real-world feather fork attack is to increase the transaction fees the victim must pay, rather than actually creating a fork of the chain to drop the block entirely. Therefore, a thorough analysis of this attack and how it propagates through the network is needed.

The contribution of this work is investigation of an attack's potential to carryout a feather fork attack (causing a targeted inflation of transaction price) given their mining power, ability to identify (deanonymize)

***Corresponding Author: Colin Murphy:** Drexel University, E-mail: cjm486@drexel.edu

a target transaction, and overall mining strategy. Furthermore, we consider the application of the coin mixing/tumbling protocol, Blindly Signed Contracts protocol [5], proposed for bitcoin and its potential impact on an attacker's feather fork capabilities.

The paper structure is as follows. In Section 2, we discuss related work of Bitcoin privacy and security, feather fork specific research, and provide a background on Bitcoin's organization and functions. In Section 3, we provide current Bitcoin market data to contextualize our analysis. In Section 4, we outline the methods used to construct our model and the Bitcoin ecosystem assumption required. Further in Section 4, we present our analysis of the theoretical feather forking capabilities of a miner and discuss the impact of the Blindly Signed Contracts protocol. Section 5 concludes the paper and offers prospects for future work.

2 Related Work

The underlying architecture of cryptocurrencies (including Bitcoin) and their potential pitfalls are well described by Conti, Mauro, et al. [2]. Conti outlines the different categories of malicious attacks, their targets (e.g. users, miners, sellers or the network), and potential countermeasures. The paper also provides real-world instances of attacks that disrupted the decentralization of the system.

Many of the countermeasures available to for blockchain abuse are outlined in [11], while also proposing the taxonomy of defense strategies: monitoring, alert forwarding, alert broadcasting, inform, detection, and conceptual research design. However, many of the defense strategies suggested as changes to the blockchain or Proof of Work design [14] and do not address the mining choices made by individual mining nodes. In [12] the mining protocols of individual miners is analyzed, such as rationale mining, and the theoretically negative impact on Bitcoin's decentralization is discussed. On the other hand, the potentially positive impacts of a rationale miner have been proposed by [6], stating that electricity consumption of mining can be reduced by this protocol (in turn, reducing CO2 emissions).

The feather-fork attack in conjunction with bribing mechanisms (i.e. bribing mining peers) as a form of censorship was evaluated in [13] and presented as a Markov Game structure of independent states. It is also worth noting that the method of feather forking in a blockchain has been proposed as a beneficial tool to incentivize renewable energy in smart grids [8].

2.1 Bitcoin Organization Background

The Bitcoin e-payment system was originally introduced by Nakamoto in 2008 [10]. The system is maintained by a set of nodes (aka mines) that communicate with each other to ensure consensus (probabilistic distributed consensus protocol). This allows for inconsistencies of the system's state (due to any number of reasons) to be reconciled by using the state that a majority agrees upon. These miner nodes are intended to "honestly" process, verify, and record electronics transactions within the system, of which are the transfer of *bitcoins*. This is done bundling several transaction together into a *block* and announced to fellow miners upon verification to claim their reward. If a majority of other miners agree with the validity of the new block it is added to the public, immutable ledger called the *blockchain*, of which all miners maintain a copy of.

The verification of blocks is a computationally intensive proof-of-work process where miners must find a solution to a complex cryptographic math puzzle. Thus, the greater computational resources that a miner has the greater their chance is of verifying a block before their peers.

As many miners are competing to verify blocks and then report them to the rest of the network, it is likely (and even common) that two or more miners will present a block verification at nearly the same time, of which results the blockchain to *fork* into two different, yet valid, states. Although this presents an inconsistency in the blockchain consensus, the miners are free to mine on top of any of the forks they deem valid in their local view. This inconsistency is later reconciled when another block is successfully added to one of the forks and verified by a majority of miners, making it the longest valid chain and the most rationale choice for other miners to build on while the other fork's block is discarded. This method of reconciliation will then have two major consequences for the miners working on the fork with the discarded block, a) the miner that originally reported the discarded block will not receive any reward because the block has been invalidated and b) all other miners will have decreased their overall revenue as they have wasted a significant amount of mining power that could have been used on the other fork. This feature of the blockchain can be exploited by malicious miners to unfairly gain profits or undermine the normal functions

of Bitcoin. The abuse of blockchain forking by a miner is the focus of of our work presented here.

3 Bitcoin Market Data

Due to the decentralized of nature of Bitcoin and the subtlety of feather fork attacks (and lack of regulation), there are no standardized method for reporting attack instances; therefore, this study will focus on the theoretical instances of a feather fork attack in the context of the Bitcoin system with the application of the proposed Blindly Signed Contracts (BSC) anonymity protocol [5]. The current mining power distribution is given to provide context of a miner's potential to act maliciously.

3.1 Mining Power Distribution

The work of block verification is described as being performed by individual *miners*; however, the current scale of Bitcoin makes it nearly impossible (i.e. very low probability of winning the block) for an independent miner to be profitable. To overcome this issue, miners collectively mine in "mining pools" and share the rewards upon successfully mining a block. In Figure 1 the current (as of March, 2021) distribution of mining power (hashrate) is shown, where the largest pool, F2Pool, controls only 17.54% of the total market hashrate – this is well below the classic 51% required to decentralize the system and even beyond the 33% or 28% required for selfish mining [3] or rationale mining [12], respectively.

It is also worth noting that there are many pools with sub-10% hash power, of which will be more likely to mine upon whatever chain allows for maximum profitability and minimal risk. Furthermore, these lesser pools account for for 34% of the overall system.

4 Methodology

Here we perform the analysis by adapting a simple, static state model of the Bitcoin system to describe the addition of blocks to the blockchain. This allows us to evaluate events (e.g. block commitment or forking) probabilities, given the fixed distribution of hash power and strategies among the other miners. We also perform a statistical evaluation of the feather fork attack within the context of a proposed anonymity protocol. Specifically, we describe the classic example of the feather fork

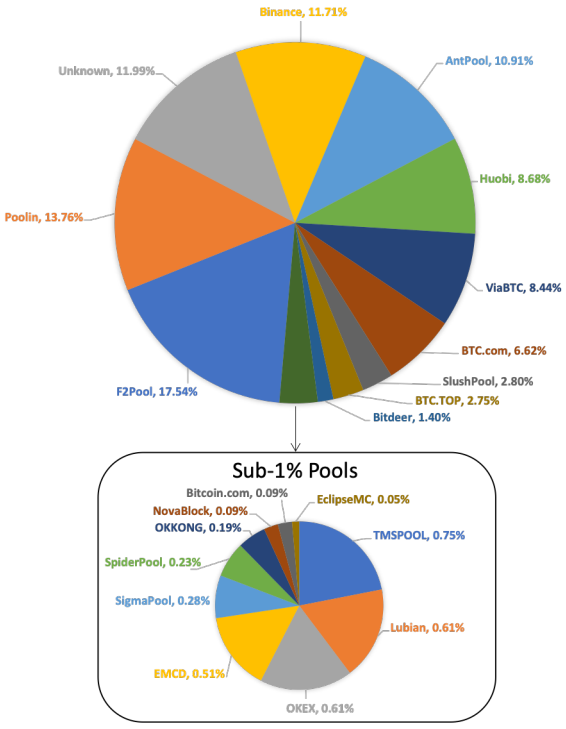

Fig. 1. Current Bitcoin market hashrate distribution (March 2021, data from blockchair.com)

attack given a state and compare this same instance with the implementation of the BSC protocol – to narrow our analysis, we will outline several assumptions about the system we model.

4.1 Blockchain and Miner Assumptions

4.1.1 Rewards

Although the actual reward that a miner receives for verifying a block to be added to the blockchain depends on several real time factors (e.g. current publish time and previous blocks), the reward in this analysis will be assumed as a constant, $r \in \mathbb{R}_{>0}$. Thus this also assumes that the nominal transaction fees paid by users is constant and any transaction offering a greater fee will increase the reward that the miner will receive - a greater incentive for miners to include the transaction in a block. This increased reward is assumed to not be great enough to incentivize forking from the longest chain on its own [7].

4.1.2 Mining Strategy

We also make assumptions about the miner's rationality for choosing strategy, of which is reliant upon the fact that all miners share some common knowledge of the blockchain, previous states, and transactions. This can be assumed as a suitable extension of the blockchain consensus protocol. And by this common knowledge, the miners will act rationally, meaning that they will adopt a mining strategy that maximizes their potential gains.

On the other hand, this rationality may not apply to the attacker as we assume the attacker is malicious and may have hidden utilities that will allow them to accept negative impacts on revenue/gain. Furthermore, the victim (in this case, a bitcoin user) only acts honestly by trying to complete a transaction even with exceedingly greater fees.

The public ledger (blockchain) is maintained by a set of n miners $M = \{M_1, ..., M_n\}$. And each miner controls fraction of the computing power, such that $\sum_{i=1}^{n} p_i = 1$. Each miner knows the computational power of each other miner, thus they have knowledge of a each miner's probability to solve a block first.

An attackers probability of successfully carrying out a feather fork attack is thus directly linked with their share of network hash power, α, where $\alpha \in [0,0.5]$. Which can be used as the indicator of an individual miner's ability to cause a disruption the blockchain system – it should be noted that in practice, the hash power that would be required to cause decentralization would be shared by a mining pool.

4.2 Blindly Signed Contracts Protocol

The Blindly Signed Contracts (BSC) protocol proposed by Heilman et al [5] was presented as an on-blockchain solution to improve Bitcoin anonymity. The BSC design relies on an untrusted third party to fairly issue vouchers and bitcoins between the payer and payee.

The BSC protocol achieves anonymity for parties of a transaction (unlinkability of payer and payee), but the bitcoin user's involvement in the transaction is publicly know, thus a malicious miner can still perform a feather fork attack. However, we will describe how this protocol can be an effective deterrent for feather fork attacks as well as its intended use.

The BSC payment occurs in an epoch of 3 consecutive blocks, with each block carrying out fair-exchange transaction contracts (smart contracts):

1. A voucher, V is offered by B to the untrusted intermediary, I, in exchange for a bitcoin - confirmed on the blockchain.
2. A bitcoin is offered by A to the untrusted intermediary, I, in exchange for a voucher - confirmed on the blockchain.
3. Both A and B create a transaction with I to fulfill the offers made, ensuring that I cannot act maliciously

The BSC relies upon the timelocking of transactions that allows for the bitcoin to be paid if and only if contracts are fulfilled within the allotted time, otherwise they are reclaimed by the originator. Details of the implantation of the protocol and anonymity features are outside the scope of this paper, thus we refer the reader to [5].

There are also numerous other privacy and anonymity techniques that exist for cryptocurrency, each with varying levels of utility. A technique similar to BSC, called Tumblebit [4], was also proposed by Heilman et al., of which is described as an improvement on BSC to provide greater anonymity and faster transaction time (within 2 blocks). However, we argue that that the longer 3 block design of BSC is an advantage that allows it to perform as a countermeasure to the feather fork attack – this is discussed later in Sec. 4.3.

4.3 Analysis Methodology

4.3.1 Classic Feather Attack Instance

Given the assumptions we've outlined in the previous sections, we can now analyze the feather forking attack itself. The feather fork is performed to target a particular Bitcoin user by refusing to mine any block that contains a transaction from their address – potential (temporarily) blacklisting them or forcing them to pay a higher transaction fee to incentives miners to ignore the feather fork. The attack is initiated by the miner announcing to fellow miners that they will attempt to fork the block containing the target transaction, but will give up the fork after k blocks in the main chain have been confirmed by the network.

In a classic two block feather fork attack ($k = 2$), a miner with α hash power has only an α^2 chance of winning the next two consecutive blocks before the others miners extend the main chain (assuming that no other miners assist in mining the fork). In Figure 2, we show this diminishing success rate for an attacker to mine

the next block, 2-consecutive blocks, and 3-consecutive blocks given the attackers available hash power – with 50% hash power being the point at which the system becomes decentralized.

Although the attacker's chance of success is low relative to the cumulative power of the other miners, it results in all miners effective hash rate to be reduced by α^2 if they choose to include the target transaction. In this model, our miners are acting rationally in order to maximize profit, thus the target transaction would be required to pay greater transaction fee to compensate for the miners loss – an increase of $\alpha^2 U_0$ where U_0 is the average block reward. As of the the last reward halving (May 11 2020), the current block reward is 6.25 BTC or ≈$372,000 USD.

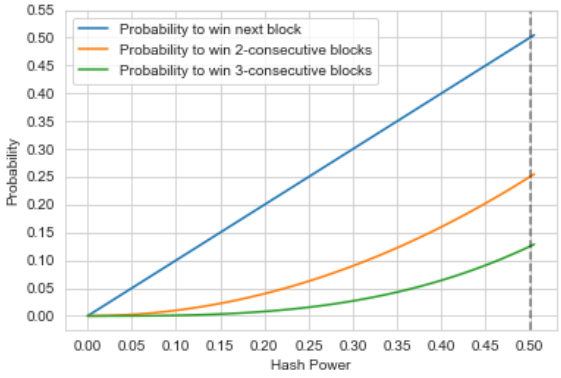

Fig. 2. Feather Fork Probability

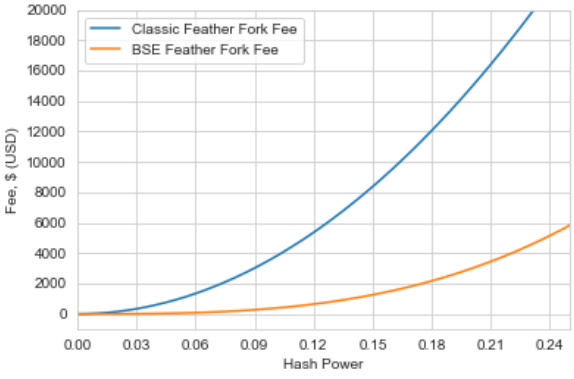

Fig. 3. Feather Fork Fees

4.3.2 BSC Epoch Feather Attack Instance

Extending the classic feather fork to the BSC protocol, we analyze the its impact on attacker's influence.

The initiation of the BSC epoch is announce publicly so that all miners are aware. The transactions in this epoch are now linked as a three block continuum, essentially altering the strategy that a feather fork attacker must take (i.e. threaten to take) in order to impact others miners revenue and the impose a potential fee. In this instance, the malicious miner will not be able to commit their fork after winning two consecutive blocks, but rather they will need to win three consecutive blocks. The attacker's influence is significantly reduced as it is even more unlikely that they are to win three consecutive blocks (that chance being α^3 in this case). As a result, any increased fee to incentivize the honest miners and offset potential loss by including the transaction is lowered – the fee now becomes $\alpha^3 U_0$. In Figure 3 the exponential difference in fees (in USD) for the normal feather fork and the BSC feather fork instance can be seen as the attacker is unable to impose extreme fees without a significant share of hash power (e.g. power equal to that of the 5 largest mining pools). To further illustrate this reduction of potential fees, we can consider the worst-case instance where the malicious miner is that with the greatest power – in this case, F2Pool with 17.54% hash power, where the cost imposed by the attack is reduced from $\approx$ \$11,500 to $\approx$ \$2,000.

4.4 Discussion

The BSC protocol offers both anonymity and protection against feather fork attacks within the Bitcoin network. It should be noted that these increased privacy/security attributes require trade-offs for convenience. The first and most easily quantifiable trade-off is the time required to complete the transaction – an epoch requires three consecutive blocks (≈30 minutes) as opposed to the nominal transaction time of a single block (≈10 minutes). Secondly, the feather fork attack cannot be entirely prevented, but rather minimized and some increased fee is still imposed upon the user.

We argue that the pros greatly outweigh the cons as users desiring greater anonymity may be willing to pay the additional fee. Furthermore, a user may prevent a future attack my anonymizing their bitcoins through a successful BSC transaction, thus making it a one-time fee.

.

5 Conclusion

The propagation of cryptocurrency comes with the promise of "democratization of currency" through its decentralization, allowing individuals to conduct transactions with a high level of privacy regardless of the governmental controls of their physical region. However, the current framework of many blockchain systems can result in a more centralized system where those with sufficient mining capacity can dominate (or significant influence) the blockchain and abuse it for extortion or selfish gain. Without a thorough assessment of these threats that face cryptocurrency, it will only continue to be plague by malicious actors and unable to compete with conventional currencies.

This study has shown that advanced anonymity protocols, such as Blindly Signed Contracts, can be implemented into the Bitcoin infrastructure to not only achieve greater privacy for payers/payees, but also act as an even greater deterrent against targeted malicious miner attacks like feather forking. Furthermore, this contributes to the overall decentralization and robustness of Bitcoin as a viable alternative to traditional modes of commerce.

Future areas of study exists to expand upon this work by considering the Bitcoin architecture and BSC's deterrence of similar attacks. Also, this model can be reevaluated to consider the feather fork attack as a type of bribery attack where a miner may greatly increase their chance of success by offering an incentive directly to other miners.

References

[1] Joseph Bonneau, Andrew Miller, Jeremy Clark, Arvind Narayanan, Joshua A Kroll, and Edward W Felten. 2015. Sok: Research perspectives and challenges for bitcoin and cryptocurrencies. In *2015 IEEE symposium on security and privacy*. IEEE, 104–121.

[2] Mauro Conti, E Sandeep Kumar, Chhagan Lal, and Sushmita Ruj. 2018. A survey on security and privacy issues of bitcoin. *IEEE Communications Surveys & Tutorials* 20, 4 (2018), 3416–3452.

[3] Ittay Eyal and Emin Gün Sirer. 2014. Majority is not enough: Bitcoin mining is vulnerable. In *International conference on financial cryptography and data security*. Springer, 436–454.

[4] Ethan Heilman, Leen Alshenibr, Foteini Baldimtsi, Alessandra Scafuro, and Sharon Goldberg. 2017. Tumblebit: An untrusted bitcoin-compatible anonymous payment hub. In *Network and Distributed System Security Symposium*.

[5] Ethan Heilman, Foteini Baldimtsi, and Sharon Goldberg. 2016. Blindly signed contracts: Anonymous on-blockchain and off-blockchain bitcoin transactions. In *International conference on financial cryptography and data security*. Springer, 43–60.

[6] Nicolas Houy. 2019. Rational mining limits Bitcoin emissions. *Nature Climate Change* 9, 9 (2019), 655–655.

[7] Kevin Liao and Jonathan Katz. 2017. Incentivizing blockchain forks via whale transactions. In *International Conference on Financial Cryptography and Data Security*. Springer, 264–279.

[8] Antonio Magnani, Luca Calderoni, and Paolo Palmieri. 2018. Feather forking as a positive force: incentivising green energy production in a blockchain-based smart grid. In *Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems*. 99–104.

[9] Andrew Miller. 2013. *Feather-forks: enforcing a blacklist with sub-50% hash power*. https://bitcointalk.org/index.php?topic=312668.0,2013

[10] Satoshi Nakamoto. 2008. *Bitcoin: A Peer-to-Peer Electronic Cash System*. https://bitcoin.org/bitcoin.pdf

[11] Kervins Nicolas, Yi Wang, George C Giakos, Bingyang Wei, and Hongda Shen. 2020. Blockchain System Defensive Overview for Double-Spend and Selfish Mining Attacks: A Systematic Approach. *IEEE Access* (2020).

[12] Soumen Pachal and Sushmita Ruj. 2019. Rational Mining Of Bitcoin. In *2019 11th International Conference on Communication Systems & Networks (COMSNETS)*. IEEE, 1–8.

[13] Fredrik Winzer, Benjamin Herd, and Sebastian Faust. 2019. Temporary censorship attacks in the presence of rational miners. In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 357–366.

[14] Ren Zhang and Bart Preneel. 2019. Lay down the common metrics: Evaluating proof-of-work consensus protocols' security. In *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE, 175–192.