Merged Mining: Curse or Cure?

Aljosha Judmayer(✉), Alexei Zamyatin(✉), Nicholas Stifter(✉),
Artemios G. Voyiatzis, and Edgar Weippl

SBA Research, Vienna, Austria
{ajudmayer,azamyatin,nstifter,avoyiatzis,eweippl}@sba-research.org

Abstract. *Merged mining* refers to the concept of mining more than one cryptocurrency without necessitating additional proof-of-work effort. Although merged mining has been adopted by a number of cryptocurrencies already, to this date little is known about the effects and implications. We shed light on this topic area by performing a comprehensive analysis of merged mining in practice. As part of this analysis, we present a block attribution scheme for mining pools to assist in the evaluation of mining centralization. Our findings disclose that mining pools in merge-mined cryptocurrencies have operated at the edge of, and even beyond, the security guarantees offered by the underlying Nakamoto consensus for extended periods. We discuss the implications and security considerations for these cryptocurrencies and the mining ecosystem as a whole, and link our findings to the intended effects of merged mining.

1 Introduction

The topic of merged mining has received little attention from the scientific community, despite having been actively employed by a number of cryptocurrencies for several years. New and emerging cryptocurrencies such as *Rootstock* continue to consider and expand on the concept of merged mining in their designs to this day [19]. *Merged mining* refers to the process of searching for proof-of-work (PoW) solutions for multiple cryptocurrencies concurrently without requiring additional computational resources. The rationale behind merged mining lies in leveraging on the computational power of different cryptocurrencies by bundling their resources instead of having them stand in direct competition, and also to serve as a bootstrapping mechanism for small and fledgling networks [27,33].

In the past, concerns have been voiced that merged mining could lead to additional security risks and challenges [27]. In particular, the realistic threat of network centralization has rendered merged mining a controversial topic. Ali et al. [1] observed a critical level of mining centralization in the merge-mined cryptocurrency *Namecoin*, concluding that merged mining is failing in practice. These alarming findings were not the result of direct investigations into merged mining itself, but rather emerged as part of a report on the experiences with the real-world deployment of a decentralized PKI service on top of the Namecoin blockchain. Hence, an in-depth analysis of merge-mined cryptocurrencies based on real-world data is necessary to determine if such observed failures in practical applications are systemic to the underlying concept of merged mining.

J. Garcia-Alfaro et al. (Eds.): DPM/CBT 2017, LNCS 10436, pp. 316–333, 2017.
DOI: 10.1007/978-3-319-67816-0_18

In this paper we conduct the first extensive study on the impacts of merged mining on individual cryptocurrencies. We discuss security implications and considerations regarding merged mining, while relating previous arguments from [27] to the results of our study. We seek to provide empirical evidence either confirming or falsifying these arguments and extend the discussion by providing ideas and examples for future experiments, which can lead to a better understanding and classification of merged mining.

To cover a broad spectrum of merge-mined cryptocurrencies we analyzed two established players and pioneers of the field, namely Namecoin and Dogecoin, as well as two relatively young merge-mined cryptocurrencies supporting merged mining with more than one PoW algorithm, namely Huntercoin [14] and Myriadcoin [23]. Thereby, we present the following contributions:

- We analyze the effects and implications of merged mining in four cryptocurrencies over time and comment on its adoption, the related difficulty increase, as well as other characteristic patterns.
- We introduce a deterministic mapping scheme that attributes blocks to specific miners and mining pools.
- We provide empirical evidence for centralization risks in cryptocurrencies involved in merged mining. Furthermore, we are successful in attributing merged mining activity to an apparently small set of mining pools.
- Concluding, we discuss the related security implications for cryptocurrencies implementing merged mining.

The remainder of this paper is structured as follows. Section 2 provides the necessary background information on fundamental concepts regarding proof-of-work based cryptocurrencies and merged mining. Section 3 describes the cryptocurrencies considered in our study as well as the experimental methodology. Section 4 presents the results of our empirical analysis. In Sect. 5, we discuss the security implications in relation to established claims and theoretical arguments regarding merged mining. Furthermore, we propose new research questions and conclude the paper in Sect. 6, pointing out interesting directions for future work.

2 Background

A key aspect of Bitcoin constitutes its novel distributed consensus mechanism, generally termed *Nakamoto consensus*. It leverages on proof-of-work (PoW) puzzles and the *blockchain* data structure to achieve eventual agreement on the set and ordering of transactions by an anonymous and changing set of participants. Nakamoto consensus thereby facilitates decentralized or so-called *permissionless* cryptocurrencies. The process by which consensus participants in proof-of-work cryptocurrencies search for valid PoW puzzle solutions is referred to as *mining* and the speed at which such *miners* find solution candidates for the PoW is called *hash rate*.

While efforts towards replacing the resource-intensive mining process have so far yielded various promising approaches such as [5,18,22], their viability

in practice is yet to be tested at a larger scale. Furthermore, due to the high degree of adoption of proof-of-work in various cryptocurrencies and the difficulties related to changing this consensus critical component, it can be assumed that PoW will remain an integral part of the overall cryptocurrency landscape in the foreseeable future.

2.1 Attacks on the PoW Security Model

The security properties of PoW cryptocurrencies are derived from the assumption that the majority of the overall mining power belongs to honest miners. Early work in Bitcoin security modeling concluded that the mining power of all the honest miners has to be strictly greater than 50% to sustain the security of the blockchain [24,31]. Should adversaries accumulate the majority of mining power, they can control the insertion of new transactions, the transaction fee market, and the supply of newly-mined coins, as well as potentially revert already recorded transactions.

Attack strategies which can be successful even without controlling the majority of mining power, most notably *selfish mining* [10,32] and *eclipse* attacks [12,13,28] have been the topic of recent work. The success probability of such adversarial strategies depends on the mining power share (α), as well as the network connectivity (γ) of the adversary [10,28]. While a poorly connected attacker ($\gamma \approx 0.1$) is shown to require $\alpha > 0.33$ to successfully perform selfish mining attacks, an adversary connected to half of the nodes in the network ($\gamma \approx 0.5$) only requires $\alpha > 0.25$. Hence, in a conservative analysis, successful attacks on PoW cryptocurrencies are more likely when dishonest entities control more than 25% of the total mining power.

2.2 Merged Mining

Merged mining refers to the process of reusing (partial) PoW solutions from a *parent* cryptocurrency as valid proofs-of-work for one or more *child* cryptocurrencies. It was introduced as a solution to the fragmentation of mining power among competing cryptocurrencies and as a bootstrapping mechanism for small networks. Merged mining was first implemented in Namecoin in 2011, with Bitcoin acting as the parent cryptocurrency. One of the earliest descriptions of the mechanism as it is used today was presented by Satoshi Nakamoto in [33]. Apart from the source code of the respective cryptocurrencies implementing merged mining, a detailed technical explanation is presented in the Bitcoin Wiki [25].

The general idea of reusing proof-of-work such that the computational effort invested may also serve to verify a separate computation was first introduced by Jakobsson and Juels under the term *bread pudding protocols* in 1999 [15]. Previous research related to merged mining is mostly limited to the application layer of the underlying cryptocurrencies. A short description of merged mining is provided by Kalodner et al. in an empirical study of name squatting in Namecoin [16]. Ali et al. highlights that Namecoin suffers from centralization issues linked to merged mining, but provides no detailed study on the extent

of the problem, nor on merged mining in general [1]. Other descriptions of and references to merged mining can be found in [2,11,27], whereas [4,19] seek to employ merged mining as a component of various blockchain-based applications.

For a cryptocurrency to allow merged mining the parent blockchain must fulfill just one requirement: it must be possible to include arbitrary[1] data within the input over which the proof-of-work in the parent is established. The main protocol logic of merged mining resides in (i) the specification and preparation of the data linked to (or included in) the block header of the parent, e.g., a hash of the child block header, and (ii) the implementation of the verification logic in the client of the child blockchain.

2.3 Mining Pools

To generate a constant stream of revenue, miners may team up and form so called *mining pools*, where they bundle their resources and share the rewards based on their contribution and according to the rules of the pool. A mining pool can be described as a "*pool manager and a cohort of miners*" [9]. To compensate the administrative effort, the mining pool keeps a small proportion of the total revenue as a fee[2]. Different reward distribution policies and related game-theoretic aspects are studied in [20,30,34]. Optimal strategies for mining pools in the context of adversarial behavior are discussed in [9,28,32]. Pool managers can have the ability to maliciously mislead their miners into participating in attacks, as happened in the case of Eligius (See Footnote 9). Although doing so might result in miners switching to another pool once they learn about the attack. The delay of these consequences however might be enough for the pool to complete the attack.

3 Methodology

In this paper we consider the following subset of cryptocurrencies exemplary for merged mining. Bitcoin, the first and currently largest cryptocurrency based on a SHA256 PoW, serves as a starting point of our analysis and acts as one of the two parent blockchains for merged mining we consider. Litecoin [21] is a fork of Bitcoin, which replaces SHA256 with the memory-hard *Scrypt* cryptographic hash function in its PoW algorithm. Litecoin's primary aim was to counter the domination of *ASICs*, i.e., hardware devices specifically-built for high-performance SHA256 hashing operations, in Bitcoin. At the time of writing it is the largest Scrypt PoW cryptocurrency.

Namecoin [26], which intends to provide a decentralized and censorship resistant alternative to the Domain Name System (DNS), was the first alternative cryptocurrency and the first blockchain to introduce merged mining, in this case with Bitcoin. While its design is heavily based on Bitcoin, Namecoin extends

[1] In practice, being able to include the output of a cryptographically secure hash function can be considered sufficient space.

[2] Usually between 1 and 5%.

the underlying protocol by introducing new *transaction types*, which enable the storage and management of additional information in the blockchain (e.g., DNS entries). Dogecoin [8] initially started as a non-serious project based on an internet meme but was able to attract and maintain a vivid community. It is roughly based on the Litecoin codebase and was the first cryptocurrency to introduce Scrypt-based merged mining with Litecoin.

A new generation of so called *multi-PoW* cryptocurrencies was marked by the introduction of Huntercoin [14] which supports SHA256 and Scrypt. Another notable pioneer in this field is Myriadcoin [23], maintaining five different PoW algorithms in parallel. The concept of multi-PoW aims to provide resistance to mining centralization by including different types of proof-of-work in a single cryptocurrency. Huntercoin and Myriadcoin furthermore are the first *multi-merge-mined* cryptocurrencies, as they allow merged mining with multiple parent chains, namely Bitcoin and Litecoin.

3.1 Data Set Collection

For our analysis we rely on the open and publicly-accessible ledgers (i.e., blockchains) of the examined cryptocurrencies, as they represent the most reliable source of information with regards to historical data[3]. The results presented in the rest of this paper are based on data collected from Bitcoin, Litecoin, Namecoin, Dogecoin, Huntercoin and Myriadcoin up to a cut-off date set to June 18, 2017 23:59:59 (UTC), i.e., Block 471,892 in Bitcoin, 347,175 in Namecoin, 1,224,533 in Litecoin, 1,763,524 in Dogecoin, 1,788,998 in Huntercoin and 2,089,974 in Myriadcoin.

3.2 Block Attribution Scheme

A key element for the investigation of mining power centralization issues is a correct attribution of blocks to the original miners. Hence, we devise an attribution scheme using publicly-available information contained in the *coinbase transactions* of both the parent and child blockchains as indicators. Thereby we rely on the following fields:

Reward payout addresses. The *coinbase transaction* represents the first transaction in a block and creates new currency units as reward for its miner. Assuming miners act rationally and profit-oriented, they are expected to specify one of their own addresses as output of this transaction. Hence, the reward payout addresses of blocks can be used as strong indicator in the attribution scheme.

Coinbase signatures (markers). Miners and especially mining pools often utilize the `coinbase` field of the coinbase transaction to publicly claim the creation of the respective block, by inserting their so-called *block-* or *coinbase signature*. As the latter represents a human-readable string indicating the pool name or

[3] While some public APIs are available for Bitcoin (e.g., http://blockchain.info/), online sources the other cryptocurrencies are scarce and not well-maintained.

an abbreviation thereof, rather than a cryptographically-strong signature, we hereafter refer to this piece of information as *marker*.

Collecting and Linking Markers and Addresses. At the time of writing there exists no global registry for markers or reward payout addresses of miners or mining pools[4]. Therefore, this information must be collected by analysis of publicly-available records including but not limited to websites of mining pools and discussion forums, as well as direct contacts with pool operators. As an outcome of this process, we are able to compile a list of block attribution indicators for 95 miners and mining pools, which operated in the observed cryptocurrencies.

Merge-mined blocks can contain up to four attribution indicators: the coinbase marker and reward payout addresses of the child chain, as well as the coinbase marker and reward payout addresses of the parent chain, which are stored in the so called *AuxPoW* header[5]. This allows to establish connections between reward payout addresses across multiple cryptocurrencies and to detect if miners switch between multiple addresses. Hence, reward payout addresses appearing in parent and child coinbase transactions of all blocks are checked for intersections. More specific: an address of the parent chain appearing in the coinbase of the AuxPow header allows to link it to the child chain address used in the coinbase transaction of the block. The child chain address in turn can appear in blocks together with other parent chain addresses, creating more links, and so on.

Attributing Blocks to Miners. A block is considered attributed to a miner if one of his markers or reward payout addresses appears in the respective fields of the coinbase transaction. However, a miner is technically allowed to use this first transaction to immediately split the block rewards to multiple outputs, this way also potentially obfuscating his identity. It is not easily possible to determine the miner of a block, unless a known coinbase marker is used or all addresses appearing in the outputs of the coinbase transaction are associated with the same miner or mining pool. If this is the case, the block is marked as *non-attributable*. A visualization of the scheme for merge-mined blockchains is provided in Fig. 1. Payout addresses appearing often in mined blocks but which cannot be linked to an identified miner or mining pool are denoted as *other unknown miners*.

However, for a permissionless proof-of-work cryptocurrency, where participants are not obliged to disclose their activity, it is not feasible for a third party to fully reconstruct a miner's history of action retroactively. Furthermore, miners may actively try to hide their identity by avoiding the reuse of payout addresses, not using any markers or using markers associated with other identities. Hence,

[4] To the best of our knowledge, the most detailed list of Bitcoin mining pools can be found here: github.com/blockchain/Blockchain-Known-Pools/blob/master/pools.json.

[5] Additional header in merge-mined blocks, used to verify the PoW performed in the parent chain.

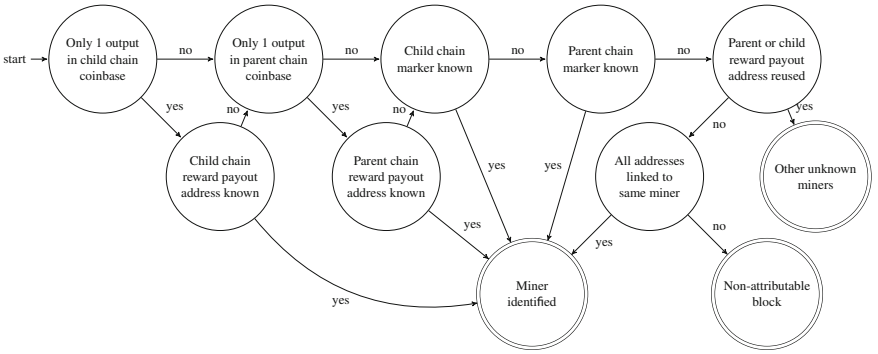

Fig. 1. Block attribution scheme for merge-mined blockchains. The process for parent chains like Bitcoin and Litecoin is analogous.

it is not possible to identify all miners and mining pools with 100% accuracy by relying only on the information present in the public ledger.

4 Merged Mining in Practice

In this section we present the results of our analysis of merged mining and provide evidence for mining power centralization issues in the implementing cryptocurrencies.

4.1 Degree of Adoption

Merged mining was introduced at block 19,200 in Namecoin (Oct. 2011), 11,163 in Huntercoin (Feb. 2014), 317,337 in Dogecoin (Jul. 2014) and 1,402,791 in Myriadcoin (Sept. 2015). The developers of Namecoin, Dogecoin and Huntercoin also disabled normal mining in the official clients at introduction. Hence, from that point forward over 99% of the blocks have been created through the process of merged mining in these cryptocurrencies. Table 1 shows the total distribution of normal and merge-mined blocks.

Table 1. Merge-mined blocks in examined cryptocurrencies.

Blockchain	Normal	Merge-mined	% of Total
Huntercoin	15,083	1,773,916	99.2
Namecoin	19,330	327,846	94.4
Dogecoin	373,927	1,389,553	78.8
Myriadcoin	1,789,994	299,981	14.4

4.2 Effects on PoW Difficulty

The main objective of merged mining is to attract more miners and hence increase the difficulty of the child blockchain [27]. By extracting the information on the PoW difficulty encoded in each block header, we are able to confirm merged mining indeed has a positive effect in this respect.

Figure 2 visualizes the development of the SHA256 PoW difficulty in Bitcoin compared to Namecoin, Huntercoin and Myriadcoin on a logarithmic scale. The PoW difficulty of the merge-mined chains rapidly increased after the introduction of merged mining. Furthermore, the behavior of Bitcoin's difficulty is, to some extent, mirrored to the merge-mined cryptocurrencies. For example, between January 2012 and April 2013 the difficulty remained stable in both Bitcoin and Namecoin, until an upward trend occurred in May 2013. The latter coincides with the wide deployment of specialized hardware dedicated to mining (ASICs) [35]. The visualization for Litecoin and Scrypt merge-mined cryptocurrencies is provided in Fig. 3. An interesting observation is that the PoW difficulty of the multi-merge-mined cryptocurrency Myriadcoin exceeded that of Litecoin, one of its parent blockchains, by 31,85%.

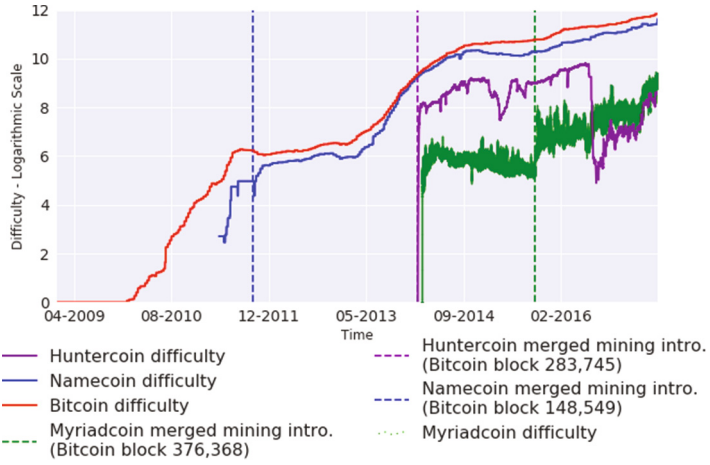

Fig. 2. Difficulty development in Bitcoin compared to SHA256 merge-mined cryptocurrencies over time on a logarithmic scale (since the launch of Bitcoin).

4.3 Impacts on Mining Power Distribution

In order to investigate the connection of merged mining and mining power centralization, we apply the attribution scheme described in Sect. 3.2 to the evaluated cryptocurrencies. A block is considered successfully mapped, if we can attribute it to either a known mining pool, or a reused reward payout address. Based on this scheme we are able to map the following percentage of blocks within the respective cryptocurrency: 59.1% for Bitcoin, 88.5% for Namecoin,

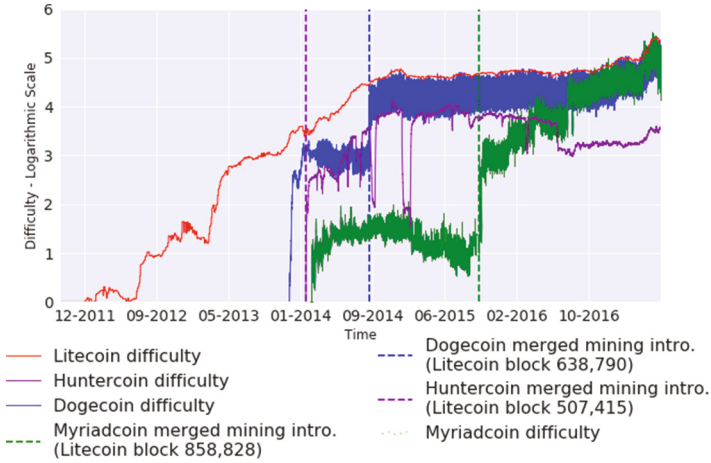

Fig. 3. Difficulty development in Litecoin compared to Scrypt merge-mined cryptocurrencies over time on a logarithmic scale (since the launch of Litecoin).

73.2% for Litecoin, 99.5% for Dogecoin, 82.7% for Huntercoin and 87.2% for Myriadcoin.

The low attribution success rate for Bitcoin may be explained by taking into consideration its early mining landscape, where blocks were primarily mined by individuals. It is generally considered best practice not to reuse reward payout addresses and the official client at the time would exhibit this behavior. The use of markers only became popular once miners started to join forces by forming mining pools in late 2011.

Similar observations can be made for the other cryptocurrecies we analyzed, albeit at a smaller scale.

The attribution results, summarized in Tables 2, 3, 4, 5, 6 and 7, suggest that a small set of mining pools are able to control significant portions of the overall mining power across multiple cryptocurrencies. While in some cases this is explained by their long-term commitment to mining on the respective chain, pools like *GHash.IO*, *BW Pool* and *F2Pool* appear to have enough capacity to concurrently conduct competitive mining operations in both Bitcoin and Litecoin (i.e., on different PoWs). In fact, F2Pool, which represents one of the largest mining pools across both SHA256 and Scrypt PoW cryptocurrencies, was able to accumulate block shares exceeding the security guarantees of the Nakamoto consensus protocol (cf. Fig. 4).

However, not all miners and mining pools currently participate in merged mining. A possible explanation is the economies of scale attributed to merged mining [27]. Since no additional computational effort is required for the PoW, the costs of merged mining, namely bandwidth, storage and validation of blocks/transactions, are the same for all miners, regardless of their mining power. In particular smaller mining operations may face the situation that their

Table 2. Bitcoin block attribution

Pool	Blocks	(%)
Smaller pools (share <1.5%)	74,753	15.8
F2Pool	35,955	7.62
BTC Guild	32,932	6.98
AntPool	26,884	5.70
GHash.IO	23,063	4.89
SlushPool	19,650	4.16
BitFury	16,070	3.41
BTCC	15,228	3.23
Other unknown miners	11,706	2.48
Eligius	11,424	2.42
BW Pool	11,075	2.35
Attributed (total)	278,740	59.1
Non-attributable blocks	193,151	40.9

Table 3. Namecoin block attribution

Pool	Blocks	(%)
F2Pool	88,795	25.6
BTC Guild	54,623	15.7
GHash.IO	34,239	9.86
SlushPool	26,726	7.70
Smaller pools (share <1.5%)	24,832	7.15
Eligius	21,144	6.09
BitMinter	18,788	5.41
EclipseMC	12,954	3.73
BTCC	11,298	3.25
ViaBTC	7,734	2.23
N3aNrkyTKY...	6,027	1.74
Attributed (total)	307,160	88.5
Non-attributable blocks	39,927	11.5

Table 4. Litecoin block attribution

Pool	Blocks	(%)
Smaller pools (share <1.5%)	284,339	23.2
F2Pool	240,691	19.7
LTm3aN5CbZ...	62,623	5.11
Clevermining	56,340	4.60
Other unknown miners	51,671	4.22
BW Pool	47,229	3.86
litecoinpool.org.	35,806	2.92
LTC1BTC/LTC.BTC.TOP	28,627	2.34
LTZaRkmkTJ...	23,342	1.91
GHash.IO	22,435	1.83
LiteGuardian	22,148	1.81
Give Me Coins	21,299	1.74
Attributed (total)	896,550	73.2
Non-attributable blocks	327,984	26.8

Table 5. Dogecoin block attribution

Pool	Blocks	(%)
F2Pool	497,013	28.2
Other unknown miners	353,671	20.1
Clevermining	187,376	10.6
Smaller pools (share <1.5%)	186,348	10.6
Litecoin pool using LTm3aN5CbZ2Ns34...	160,644	9.11
litecoinpool.org.	113,283	6.42
BW Pool	91,265	5.18
LTC1BTC/LTC.BTC.TOP	65,228	3.70
yihaochi.com	35,745	2.03
Coinotron	34,694	1.97
GHash.IO	29,814	1.69
Attributed (total)	1,755,081	99.5
Non-attributable blocks	8,443	0.5

Table 6. Huntercoin block attribution

Pool	Blocks	(%)
F2Pool	1,142,821	63.9
litecoinpool.org.	282,136	15.8
HaoBTC	27,974	1.56
Smaller pools (share < 1.5%)	26,057	1.46
Attributed (total)	1,478,988	82.7
Non-attributable blocks	310,010	17.3

Table 7. Myriadcoin block attribution

Pool	Blocks	(%)
Smaller pools (share <1.5%)	587,986	28.1
Other unknown miners	423,684	20.3
nonce-pool	192,193	9.20
MiningPoolHub	181,168	8.67
Zpool	135,876	6.50
MJv9fLd7Qj...	64,720	3.10
LTC1BTC/LTC.BTC.TOP	48,132	2.30
Multipool	44,510	2.13
MWQVvPypce...	40,281	1.93
GHash.IO	37,916	1.81
wafflepool	33,605	1.61
Nut2Pools	31,359	1.50
Attributed (total)	1,821,430	87.2
Non-attributable blocks	268,544	12.8

additional expenditures for merge-mining another cryptocurrency exceed the expected rewards.

Resulting Mining Power Centralization Issues. The number of blocks found by a miner over a certain period indicate his actual hash rate (i.e., their mining power) during this period. Hence, we use the number of blocks generated by the largest miner or mining pool per day as an approximation for measuring the centralization of mining power[6]. Our findings are visualized as heatmaps in Fig. 4. Therein, each bar (column) represents the number of blocks mined by the largest entity on that day. We use the thresholds described in Sect. 2.1 as centralization indicators. If exceeded, the latter are known to introduce potential threats on the decentralization and security level of a PoW blockchain:

[6] We set the observation period to 24 hours to avoid extreme variance caused by lucky/unlucky streaks of miners since the time between found blocks is exponentially distributed, while still achieving accurate results.

- *Below 25%* (green) - Highest share is below the pessimistic threshold.
- *Greater 25%* (yellow) - Highest share is between 25% and one third.
- *Greater 33.33%* (orange) - Highest share is between one third and 50%.
- *Greater 50%* (red) - Highest share controls the majority of mining power.

In Bitcoin no single miner or mining pool has been able to aggregate and maintain more than 50% of the overall mining power for an extended period, since blocks became attributable[7]. (Table 8) However, the situation is quite different in Namecoin: here, *F2Pool* reached and maintained a majority of the mining power for prolonged periods.

Litecoin, despite being the largest Scrypt PoW blockchain, has experienced slight centralization since mid-2014, among others caused by *Clevermining* and lately *F2Pool*. Through merged mining, this situation is reflected and amplified in Dogecoin: *F2Pool* was responsible for generating more than 33% of the blocks per day for significant periods, even exceeding the 50% threshold around the end of 2016.

The effects of introducing merged mining have played out differently in the two multi-PoW cryptocurrencies we analyzed. While Huntercoin was instantly dominated by *F2Pool* and remained in this state until mid-2016, Myriadcoin appears to have experienced only a moderate impact. However, we note that so far none of the large mining pools that are active in other merge-mined chains have been observed to also operate in Myriadcoin.

Table 8. Distribution of overall percentage of days below/above the centralization indicator thresholds.

Blockchain	$\leq 25\%$	$> 25\%$	$> 33.33\%$	$> 50\%$
Bitcoin	75.7	24.3	5.43	0.03
Namecoin	11.7	88.3	66.6	30.5
Litecoin	45.0	55.0	35.9	0.75
Dogecoin	16.3	83.7	60.7	2.45
Huntercoin	1.53	98.5	96.1	81.0
Myriadcoin	87.7	12.3	6.20	0.2

Mining Power Fluctuation. The operation of a mining pool requires extensive coordination effort in terms of recruiting miners or purchasing and installing the necessary infrastructure. Hence, it usually takes time until a mining pool is able to accumulate significant mining power shares. Merged mining, however, requires only minimal effort and can be described as a "software switch". Consequently, the observable high fluctuations of mining power in merge-mined cryptocurrencies may be attributed to mining pools being able to easily start

[7] It is in the realm of possibility that in the early days of Bitcoin individual miners, such as Satoshi Nakamoto himself have controlled large shares of the overall mining power.

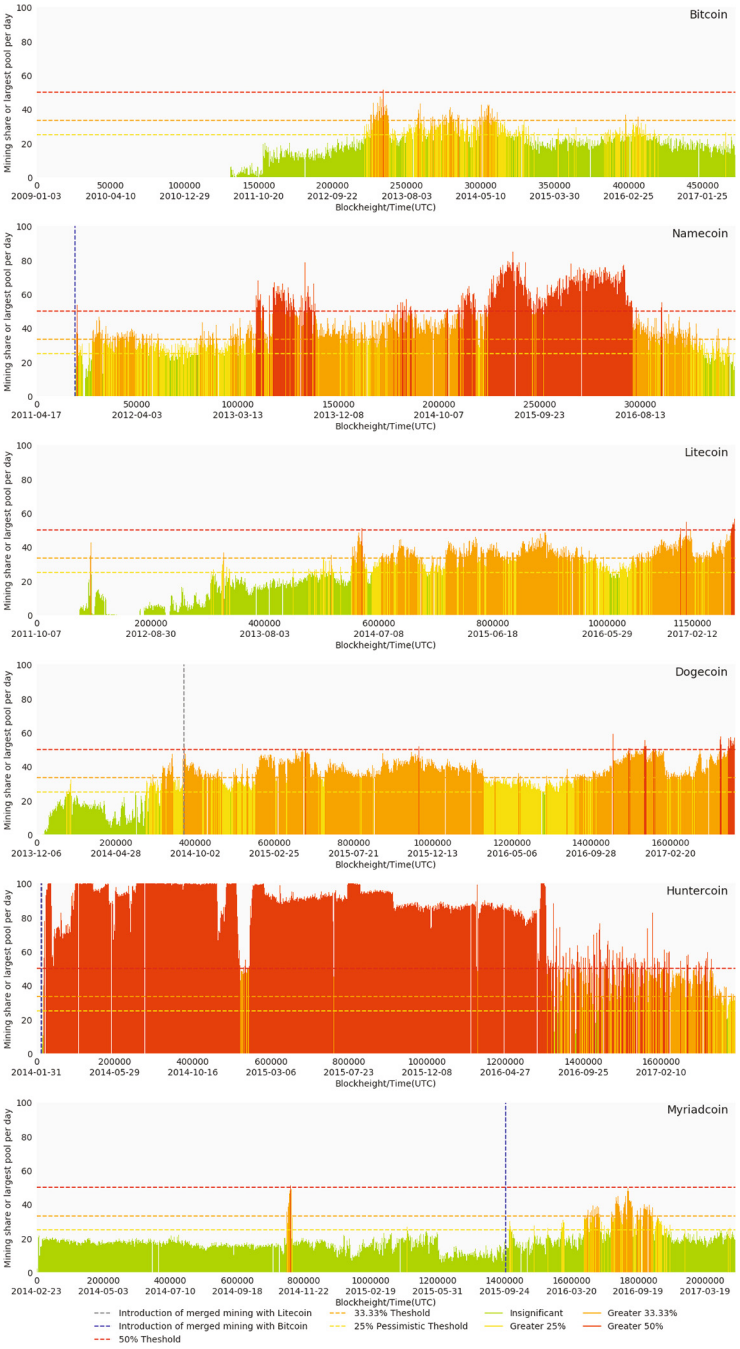

Fig. 4. Block share of largest miner/mining pool per day for Bitcoin (144 blocks), Litecoin (576 blocks), Namecoin (144 blocks), Dogecoin (1,440 blocks), Huntercoin (1,440 blocks) and Myriadcoin (1,440 blocks) since launch of the respective cryptocurrency. (Color figure online)

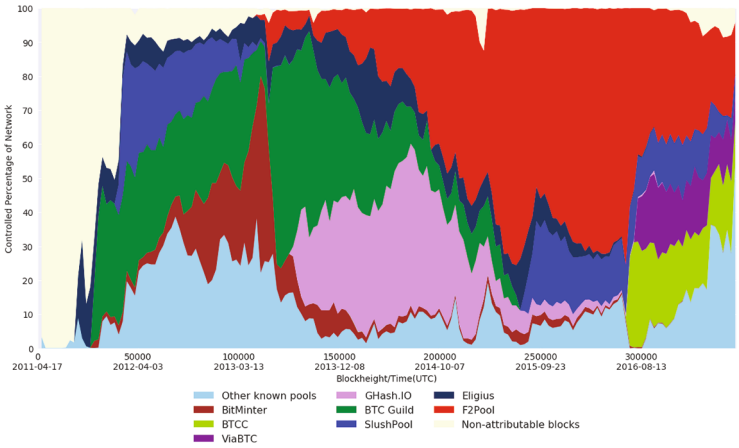

Fig. 5. Distribution of blocks in Namecoin per pool over time. Each data point resembles the share among 2,016 blocks ($\sim$2 weeks), i.e., the difficulty adjustment period.

or end their operation without major preparations (cf. Fig. 5, e.g. around block 300,000).

A further interesting observation is the increase of non-attributable blocks occurring simultaneously to drops of mined blocks that are attributable to large mining pools. Such behavior is observed in Litecoin, Huntercoin and Namecoin (cf. Fig. 5 approximately at block 250,000). Further analysis and investigation into such events is necessary to rule out that these are attempts of pools to conceal their total mining power when operating near or beyond the security guarantees offered by Nakamoto consensus

5 Discussion

In this section we discuss the security implications of merged mining on the ecosystem of cryptocurrencies and study how current theoretic arguments relate to our findings.

Introduction of New Attack Vectors. The advantage of merged mining is that miners are no longer forced to choose between mining one cryptocurrency or another. However, its biggest strength can also be viewed as a potential attack vector [27]. The ability to generate blocks for the merge-mined child blockchains at almost no additional cost, apart from maintaining a client node, allows misbehaving miners to carry out attacks without risking financial losses in both the parent and other child blockchains. Such an attack was carried out by the Eligius mining pool in 2012. Without their explicit consent, its miners were coerced to participate in an attack led by the pool operator, ultimately stalling the operation of the fledgling cryptocurrency CoiledCoin by mining empty blocks[8].

[8] cf. https://bitcointalk.org/index.php?topic=56675.msg678006#msg678006.

This attack serves as the predominant example for highlighting threats posed by merged mining on child cryptocurrencies: the miners of the pool did not suffer any financial loss and, as it appears, were not even aware of the attack, as all actions were performed solely by the operator.

However, to the best of our knowledge, it was never explicitly stated that merged mining may also facilitate attacks against a parent cryptocurrency. Consider for example a miner who is highly invested in a multi-merge-mined cryptocurrency. Due to merged mining this miner can perform attacks on one of the supported parent blockchains (e.g. selfish mining or DoS through mining empty blocks) at no additional mining cost. While such scenarios previously seemed far-fetched, as the PoW difficulty of a parent blockchain was generally considered to exceed that of a merge-mined child, this is no longer the case for multi-merge-mined cryptocurrencies (see Sect. 4.2). This highlights that *merged mining as an attack vector works both ways*. Such attacks are particularly interesting because parent cryptocurrencies cannot easily prevent being merge-mined by child blockchains.

Furthermore, we describe a *reputation attack* as a noteworthy adversarial strategy in the context of merged mining. Since block attribution to pools is currently based on markers and addresses, rather than cryptographic signatures, an adversary can fake attribution of parent blocks while still earning revenue in the child chains. We consider a scenario where a targeted mining pool $\mathcal{P}$ holds a 24% mining power share of a parent chain C_{parent}, which can be used to merge-mine a child chain C_{child}. We assume a malicious merged mining entity $\mathcal{M}$ holds only 10% share of C_{parent} and uses the C_{child} (and not C_{parent}) as its main revenue channel. In such a scenario, it would be possible for $\mathcal{M}$ to create $\approx 10\%$ of the blocks in C_{parent}. $\mathcal{M}$ could now fake the attribution of its blocks in C_{parent} by using the (public) reward address and/or coinbase marker of $\mathcal{P}$. Due to the false flag blocks attributed to $\mathcal{P}$, this pool would appear to hold 34% of the share for C_{parent}. As a result, $\mathcal{P}$ might be regarded as too large or nefarious for the parent cryptocurrency, which could in turn undermine the integrity of the parent chain as a whole. While $\mathcal{M}$ will lose all revenue in C_{parent}, it will still gain revenue in C_{child}.

Centralization Risks. Merged mining does not increase the costs to the miner in regards to solving the Proof-of-Work puzzle, which is considered to be the primary cost factor in PoW cryptocurrencies. However additional costs regarding bandwidth, storage and validation of the merge-mined blockchain's blocks/transactions are incurred regardless of the relative size or hash rate of the miner. Therefore, according to [27] merge-mined cryptocurrencies have a greater risk of centralization or concentration of mining power (economies of scale).

Our analysis indicates that merge-mined child blockchains experienced prolonged periods where individual mining pools have held shares beyond the theoretical bounds that guarantee the security of the cryptocurrency. We conclude that *current merge-mined currencies have a trend towards centralization.*

However, it is too early to tell if the centralization trend also applies to multi-merged-mining in cryptocurrencies such as Myriadcoin. Multi-merge-mined blockchains allow for more than one parent cryptocurrency and have a greater chance to acquire a higher difficulty per PoW algorithm, in comparison to the respective parent blockchain. This, in fact, may change the underlying (crypto)economic assumptions with regards to merged mining and introduces new directions for research in this field.

The theoretic implications of a dishonest miner holding a large share of the network hash rate are well known [3,12,17,28]. However, we are not aware of any recent case where such an attack has been carried out in one of the analyzed cryptocurrencies, as such evidence cannot easily be derived solely by analyzing the blockchain data structures. Rather, active measurements within the P2P network of the cryptocurrency are necessary [17]. Our analysis serves as a cautionary note – the impact of such an attack on the cryptocurrency market and the mining ecosystem are unclear. The apparent lack of cryptographically verifiable attribution information regarding the hash rate of mining pools only renders the situation worse. This bares additional risks of intended or unintended misattribution of non negligible fractions of the overall hash rate.

Furthermore, we want to point out that through the alternative use-cases of some of the merge-mined cryptocurrencies, certain attacks may also have additional implications. Namecoin for example, can be used to register and update arbitrary name-value pairs, such as DNS entries. In this case, every registered domain expires after a certain number of blocks (i.e., amount of time). Should a mining pool hold a large block share at that time, it can take over a domain name by blocking the required update (refresh) transaction to enter the blockchain in time. Once the domain name has expired, the misbehaving pool can register the domain himself.

Validation Disincentive. Not only the detection of misbehaving pools with large hash rates requires active network monitoring, but also the verification of the *validation disincentive* assumption: In [27] the authors propose that miners which participate in merged mining have an incentive to skimp on (transaction) validation, since it becomes the main (computational) cost driver in merged mining. Although not mentioned explicitly in [27], the rate of blockchain forks, i.e., stale block rate of merged mined cryptocurrencies, could be an indicator for relaxed transaction validation of miners. Since stale blocks are not directly recorded in the blockchain, the only way to acquire the required measurements is through active monitoring of the involved peer-to-peer networks, as demonstrated in [6,7]. Conducting these measurements for multiple merge-mined cryptocurrencies is topic for future work. In addition, it might be necessary to actively trigger those conditions by broadcasting incorrect transactions/blocks. However, we stress that performing such tests in live networks raises ethical and financial questions.

Long-Term Dependency. Merged mining was originally conceived as a bootstrapping technique for alternative cryptocurrencies [27,33]. To the best of our knowledge, once introduced, no cryptocurrency has abandoned merged mining – not even the child cryptocurrencies which our analysis in Sect. 4 has shown to suffer from centralization issues. Hence, we argue that although merged mining can increase the hash rate of child blockchains, *it is not conclusively successful as a bootstrapping technique.*

Results presented in [29] indicate that even if a PoW blockchain should just be used in a bootstrapping phase before switching to a different consensus algorithm, it is theoretically necessary to keep on mining infinitely long. Otherwise it would be impossible for new nodes joining the network to distinguish between the original bootstrapping chain and a longer, but malicious counterpart. In theory, this might pose a new use case for merged mining in scenarios where a blockchain is bootstrapped using PoW and then switches to a different consensus algorithm. In this case the PoW bootstrapping chain can be continued relatively cheap through merged mining by appending empty blocks.

6 Conclusion

In this paper, we assessed current theories regarding merged mining from an empirical point of view and contributed to the discussion by raising new questions and directions for future work.

We derived a simple attribution scheme and achieved to map a significant portion of the mining pool ecosystem of the analyzed cryptocurrencies, beyond what was publicly known until now. The collected information sheds some light on the long-term evolution of merged mining in different cryptocurrencies. While merged mining is a common practice in the cryptocurrency space, the empirical evidence suggests that only a small number of mining pools is involved in merged mining. These pools enjoy block shares beyond the desired security and decentralization goals. It is currently unclear and topic of future research whether new constructs, such as multi-merged mining, will succeed in resolving the outlined issues.

The multi-purpose usage of PoW in merged mining is an interesting application, not only from a resource consumption point-of-view, but also in the context of future sharding and scalability discussions. Therefore, further research and analysis regarding merged mining is required as a basis for developing and building solutions, which will be able to stand the test of time.

Acknowledgments. We want to thank Philipp Schindler and Georg Merzdovnik for valuable discussions and feedback. This research was funded by FFG - Austrian Research Promotion Agency Bridge Early Stage 846573 A2Bit, FFG Bridge 1 858561 SESC and COMET K1.

References

1. Ali, M., Nelson, J., Shea, R., Freedman, M.J.: Blockstack: a global naming and storage system secured by blockchains. In: 2016 USENIX Annual Technical Conference (USENIX ATC 2016), pp. 181–194. USENIX Association, Denver (2016)
2. Anderson, L., Holz, R., Ponomarev, A., Rimba, P., Weber, I.: New kids on the block: an analysis of modern blockchains (2016). http://arxiv.org/pdf/1606.06530.pdf. Accessed 10 Nov 2016
3. Androulaki, E., Capkun, S., Karame, G.O.: Two bitcoins at the price of one? double-spending attacks on fast payments in bitcoin. In: CCS (2012)
4. Back, A., Corallo, M., Dashjr, L., Friedenbach, M., Maxwell, G., Miller, A., Poelstra, A., Timón, J., Wuille, P.: Enabling blockchain innovations with pegged sidechains (2014). http://newspaper23.com/ripped/2014/11/http:www-blockstream-com-sidechains.pdf. Accessed 10 Nov 2016
5. Bentov, I., Pass, R., Shi, E.: Snow white: provably secure proofs of stake (2016). https://eprint.iacr.org/2016/919.pdf
6. Decker, C., Wattenhofer, R.: Information propagation in the bitcoin network. In: 2013 IEEE Thirteenth International Conference on Peer-to-Peer Computing (P2P), pp. 1–10. IEEE (2013)
7. Decker, C., Wattenhofer, R.: Bitcoin transaction malleability and MtGox. In: Kutyłowski, M., Vaidya, J. (eds.) ESORICS 2014. LNCS, vol. 8713, pp. 313–326. Springer, Cham (2014). doi:10.1007/978-3-319-11212-1_18
8. Dogecoin community. Dogecoin reference implementation. github.com/dogecoin/dogecoin. Accessed 10 Nov 2016
9. Eyal, I.: The miner's dilemma. In: 2015 IEEE Symposium on Security and Privacy (SP), pp. 89–103. IEEE (2015)
10. Eyal, I., Sirer, E.G.: Majority is not enough: bitcoin mining is vulnerable. In: Christin, N., Safavi-Naini, R. (eds.) FC 2014. LNCS, vol. 8437, pp. 436–454. Springer, Heidelberg (2014). doi:10.1007/978-3-662-45472-5_28
11. Franco, P., Bitcoin, U.: Cryptography, Engineering and Economics. Wiley, New York (2014)
12. Gervais, A., Karame, G.O., Wüst, K., Glykantzis, V., Ritzdorf, H., Capkun, S.: On the security and performance of proof of work blockchains. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, CCS 2016, pp. 3–16. ACM, New York (2016)
13. Heilman, E., Kendler, A., Zohar, A., Goldberg, S.: Eclipse attacks on bitcoin's peer-to-peer network. In: 24th USENIX Security Symposium (USENIX Security 2015), pp. 129–144 (2015)
14. Huntercoin developers. Huntercoin reference implementation. https://github.com/chronokings/huntercoin. Accessed 05 Jun 2017
15. Jakobsson, M., Juels, A.: Proofs of work and bread pudding protocols (extended abstract). In: Preneel, B. (ed.) Secure Information Networks. IFIP, vol. 23, pp. 258–272. Springer, Boston (1999). doi:10.1007/978-0-387-35568-9_18
16. Kalodner, H., Carlsten, M., Ellenbogen, P., Bonneau, J., Narayanan, A.: An empirical study of namecoin and lessons for decentralized namespace design. In: WEIS (2015)
17. Karame, G.O., Androulaki, E., Roeschlin, M., Gervais, A., Čapkun, S.: Misbehavior in bitcoin: a study of double-spending and accountability. ACM Trans. Inf. Syst. Secur. **18**(1), 2:1–2:32 (2015). doi:10.1145/2732196. Article no 2

18. Kiayias, A., Russell, A., David, B., Oliynykov, R.: Ouroboros: a provably secure proof-of-stake blockchain protocol (2016). https://pdfs.semanticscholar.org/1c14/549f7ba7d6a000d79a7d12255eb11113e6fa.pdf. Accessed 20 Feb 2017
19. Lerner, S.D.: Rootstock platform. http://www.the-blockchain.com/docs/Rootstock-WhitePaper-Overview.pdf. Accessed 5 Jun 2017
20. Lewenberg, Y., Bachrach, Y., Sompolinsky, Y., Zohar, A., Rosenschein, J.S.: Bitcoin mining pools: a cooperative game theoretic analysis. In: Proceedings of the 2015 International Conference on Autonomous Agents and Multiagent Systems, pp. 919–927. International Foundation for Autonomous Agents and Multiagent Systems (2015)
21. Litecoin community. Litecoin reference implementation. github.com/litecoin-project/litecoin. Accessed 10 Nov 2016
22. Micali, S.: Algorand: The efficient and democratic ledger (2016). http://arxiv.org/abs/1607.01341. Accessed 9 Feb 2017
23. Myriad core developers. Myriadcoin reference implementation. https://github.com/myriadcoin/myriadcoin. Accessed 05 Jun 2017
24. Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system, December 2008. https://bitcoin.org/bitcoin.pdf. Accessed 10 Nov 2016
25. Nakamoto, S.: Merged mining specification, April 2011. en.bitcoin.it/wiki/Merged_mining_specification. Accessed 10 Nov 2016
26. Namecoin community. Namecoin reference implementation. https://github.com/namecoin/namecoin. Accessed 10 Nov 2016
27. Narayanan, A., Bonneau, J., Felten, E., Miller, A., Goldfeder, S.: Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton University Press, Princeton (2016)
28. Nayak, K., Kumar, S., Miller, A., Shi, E.: Stubborn mining: generalizing selfish mining and combining with an eclipse attack. In: 1st IEEE European Symposium on Security and Privacy. IEEE (2016)
29. Pass, R., Shi, E.: Hybrid consensus: Scalable permissionless consensus, September 2016. https://eprint.iacr.org/2016/917.pdf. Accessed 10 Nov 2016
30. Rosenfeld, M.: Analysis of bitcoin pooled mining reward systems. arXiv preprint arXiv:1112.4980 (2011)
31. Rosenfeld, M.: Analysis of hashrate-based double spending (2014). http://arxiv.org/abs/1402.2009. Accessed 10 Nov 2016
32. Sapirshtein, A., Sompolinsky, Y., Zohar, A.: Optimal selfish mining strategies in bitcoin. In: Grossklags, J., Preneel, B. (eds.) FC 2016. LNCS, vol. 9603, pp. 515–532. Springer, Heidelberg (2017). doi:10.1007/978-3-662-54970-4_30
33. Nakamoto, S.: Comment in "bitdns and generalizing bitcoin" bitcointalk thread. https://bitcointalk.org/index.php?topic=1790.msg28696#msg28696. Accessed 05 Jun 2017
34. Schrijvers, O., Bonneau, J., Boneh, D., Roughgarden, T.: Incentive compatibility of bitcoin mining pool reward functions. In: Grossklags, J., Preneel, B. (eds.) FC 2016. LNCS, vol. 9603, pp. 477–498. Springer, Heidelberg (2017). doi:10.1007/978-3-662-54970-4_28
35. Taylor, M.B.: Bitcoin and the age of bespoke silicon. In: Proceedings of the 2013 International Conference on Compilers, Architectures and Synthesis for Embedded Systems, p. 16. IEEE Press (2013)