Options and Futures Imperil Bitcoin's Security

***Abstract*—A fundamental security assumption behind Bitcoin and all proof-of-work cryptocurrencies is that a majority of the mining power or hash rate is controlled by honest miners. It is well-known that if an adversary controls a majority of the mining power, they can perform a wide variety of malicious actions which are often called 51% attacks. Specifically, they can fork the blockchain and create a new longest chain that erases as many blocks as they wish from the current consensus chain, thus enabling double-spending.**

The conventional wisdom in the blockchain community is to assume that (i) having a majority of the hash power is a prerequisite for a successful attack, (ii) a majority attack is prohibitively expensive, and (iii) there is no real-world incentive for such an attack, i.e. even if a few mining pools have the majority hash rate, any such attack would effectively crash Bitcoin's price which would cause huge losses in revenue for the attacking miners. As such, it is widely believed that proof-of-work cryptocurrencies, and specifically Bitcoin, are immune to such attacks.

In this work, we refute all three of these assumptions: (i) We show that an adversary with a small percentage of the hash power can still reliably create forks that are six blocks deep, thus fracturing the public's trust in Bitcoin and most probably causing a crash in its price; (ii) We show that a majority attack on Bitcoin would cost only 6.43 billion USD, which is much lower than the community's expectation and only 0.85 percent of Bitcoin's market cap at the time of writing. Additionally, and more worryingly, an attack with only 30% of the total hash power, which would cost a mere 2.75 billion USD, will succeed with a probability of more than 95% within 34 days. Thus, such attacks are much more affordable than expected; (iii) Finally, and most importantly, we show that it is possible for an attacker to actually benefit from the resulting crash in the value of Bitcoin, due to the vast derivatives (options and futures) market that is currently in existence. Put simply, an attacker can first short Bitcoin using widely available derivative contracts and then intentionally perform an attack to crash the price and profit. Thus, there are real-world incentives for such attacks.

I. Introduction and Preliminaries

Bitcoin. Bitcoin [1] was the first working protocol for a decentralized cryptocurrency and currently holds the largest market cap among all such currencies, amounting to more than 756.69 billion USD at the time of writing [2][1]. There is also a huge derivatives market on Bitcoin with trade volumes that often exceed 1 trillion USD per calendar month (Section V).

Proof-of-Work [1]. In Bitcoin, transactions are grouped into *blocks* of a fixed maximum size. The blocks are then chained together in a singly-linked list using hash pointers with each block containing the hash of its parent (previous) block. This linked list is aptly named the *blockchain*. The blockchain is subject to consensus, i.e. all honest nodes on the network should eventually agree on its contents. Thus, adding a new block to the end of the blockchain is a deliberately hard task, called *mining*, that requires the solution of a computationally-intensive hash inversion puzzle. This scheme is called *proof-of-work* and ensures that a miner's chance of adding the next block to the blockchain is proportional to the miner's computational power, i.e. how many hashes she can compute per unit of time.

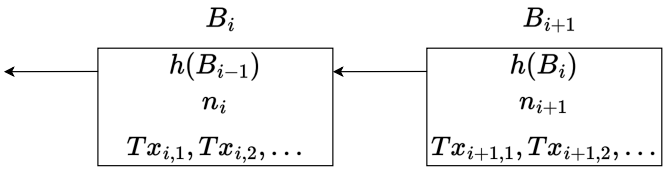


Fig. 1: A simplified view of the blockchain

Figure 1 shows an overview of this process. In this figure we have omitted implementation details that are not relevant to this work. Each block B_i contains the hash of the previous block B_{i-1}. This serves as a hash pointer in the linked list. It also contains a nonce n_i and a sequence of transactions $Tx_{i,1}, Tx_{i,2}, \ldots$. A miner who aims to add a new block B_{i+1} should first create the pointer to the previous block and populate a list of transactions that she intends to include. She should then choose the new nonce n_{i+1} such that the hash $h(B_{i+1})$ of her new block is below a certain predefined threshold[2]. Since the output of a hash function is unpredictable and an ideal cryptographic hash function can be modeled as a random oracle, the miner's only choice is to repeatedly try different nonces until she finds a valid block. Thus, her success probability is proportional to the number of hashes she can compute per unit of time.

Since mining is an expensive activity, due to both hardware and electricity costs, the miners should be financially incentivized to perform it. Bitcoin creates two incentives for the miners [1], [3]: (a) a block reward (currently 6.25 BTC $\approx$ 241,804 USD) is paid to each miner who successfully adds a new block, and (b) each transaction contains a transaction fee that is paid to the miner who adds it to the consensus chain.

Longest Chain Rule [1]. In the event that two miners find a valid block at approximately the same time, a temporary *fork* happens in which there are two valid blockchains known to the network. In such a scenario, the Bitcoin protocol allows miners to try to extend either branch. However, as soon as a branch becomes longer than the other(s), the shorter branch(es) are dropped by everyone who honestly follows the protocol. Thus, the protocol mandates that the longest chain is always the consensus chain and that every node on the network must always consider the longest chain known to them as the authoritative

[1]The time of writing is December 1st, 2023.

[2]In Bitcoin, the threshold changes dynamically to ensure that a new block is mined roughly every 10 minutes.

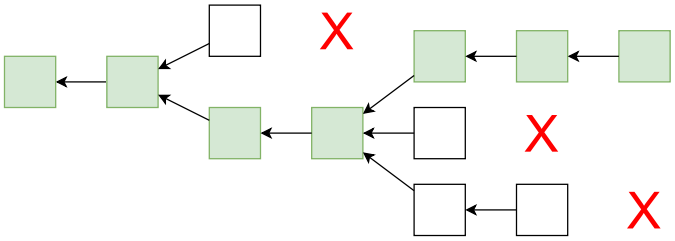


Fig. 2: An illustration of the longest chain rule in Bitcoin

blockchain[3]. This is illustrated in Figure 2. As long as a majority of the computational power on the network follows the protocol honestly, all honest participants are guaranteed to eventually reach a consensus about the blockchain.

DOUBLE-SPENDING [1], [4]. Preventing double-spending is arguably the main contribution of the Bitcoin protocol. A *double-spending* attack is when a Bitcoin user tries to use the same coin (transaction output) in two different transactions. In such cases, the two transactions will be in conflict [3] and at most one of them can be added to the consensus chain. Specifically, if Tx_1 and Tx_2 both spend the same coin, then any proposed block that contains Tx_1 can only be valid if neither it nor any of its ancestors (previous blocks) contain Tx_2. Suppose ALICE is selling an item to BOB and BOB is paying the price by a Bitcoin transaction Tx_1 that transfers part of his money to ALICE. In this case, it is not enough for ALICE to see Tx_1, since BOB might have created a conflicting transaction Tx_2 that double-spends the same coin. Thus, ALICE should wait for Tx_1 to be added to the consensus chain. However, even this does not guarantee that the payment is finalized, since it is possible that the miners eventually create a longer chain that contains Tx_2 and thus consensus switches from Tx_1 to Tx_2. In such cases, we would say that Tx_1 is *reverted*. In practice, this is unlikely to happen if Tx_1 is already in a block B_i and there are many blocks added after B_i. Such blocks are called *confirmation* blocks. The conventional wisdom and industrial standard practice is to wait for 6 confirmations before considering the transaction as irreversible, although some users take the risk of waiting for fewer confirmations [5].

MAJORITY ATTACK. If an adversary controls more than half of the hash power, she can create arbitrarily deep forks and revert as many blocks as she wishes. This is often called a 51% attack[4]. To fork the blockchain from block B_i onwards, she can simply create new alternative blocks $B'_{i+1}, B'_{i+2}, \ldots$ and continue mining on her own machine without disclosing the new alternative chain. She continues this until her alternative fork becomes longer than the network's current consensus chain, which is guaranteed to eventually happen with probability 1 since she holds a majority of the hash power. At that point, the adversary can simply publish the new chain which will immediately become the consensus chain and thus replace all the previous blocks after B_i and revert and potentially double-spend all the transactions therein. Not disclosing a valid block and instead continuing to mine to extend it is called *selfish mining* and is widely studied in the literature [6]. Specifically, it is now well-known that profiting from selfish mining is not limited to adversaries who have a majority of the hash power and can be done using a much smaller share [7]. The work [7] shows that an adversary that controls a minority stake (as a mining pool) can use selfish mining to increase its mining rewards and thus attract other miners to join it until it eventually controls a majority of the computational power.

In view of the discussion above, it is natural to wonder whether Bitcoin is actually vulnerable to majority attacks or any other attack that intentionally tries to revert multiple blocks. Given that the rule of thumb followed by most practitioners is to wait for 6 confirmations, a fork that goes 6 levels deep can very likely diminish the public's trust in Bitcoin and cause a crash in its market price. It is also widely accepted that a prolonged majority attack (if it happens) would be catastrophic to the cryptocurrency and can cause its downfall.

CONVENTIONAL WISDOM. The conventional wisdom in the blockchain community is to assume that such block-reverting attacks are highly unlikely to happen. The reasoning goes as follows:

1) Reverting multiple blocks and specifically double-spending a transaction that has 6 confirmations requires control of a majority of the mining power;
2) Having a majority of the mining power is prohibitively expensive and requires an outlandish investment in hardware;
3) Even if a miner, mining pool or group of pools does control a majority of the mining power, they have no incentive to act dishonestly and revert the blockchain, as that would crash the price of Bitcoin, which is ultimately not in their favor, since they rely on mining rewards denominated in BTC for their income.

There is some strong yet circumstantial evidence to support these, especially the latter claim. In 2014, the Ghash.io mining pool temporarily succeeded in breaching the 50% threshold and controlling more than half of the hash power [8]. However, no attack was observed. Currently, the top two mining pools, i.e. AntPool and Foundry USA, together control more than half of the computational power [9]. Indeed, centralization of hash power has been an ongoing issue and the top 2-3 mining pools have often controlled more than half of the hash rate in the past months (Figure 3), yet they have not attempted a majority attack. However, as we will outline in this work, all three assertions above are false and Bitcoin is indeed vulnerable to block reversion attacks.

II. OVERVIEW OF THE ATTACK

Each of the next sections in this work will focus on refuting one of the three claims above. We now provide an overview of these results and outline how they fit together to enable an attack on Bitcoin.

WHY 50% IS NOT NECESSARY. As mentioned, [7] shows that selfish mining can become profitable and help an attacker reach a majority of the mining power even when the attacker begins with a much smaller hash rate. Notwithstanding the clever attack in [7], an adversary who controls a portion q of the total hash

[3]In practice, the length of a chain is not just the number of blocks in it, but rather the total difficulty of mining these blocks. However, this minor detail does not change any of the analyses in this work.

[4]This naming is erroneous since one does not actually need 51% of the mining power. Thus, we prefer to use the term *majority attack*.

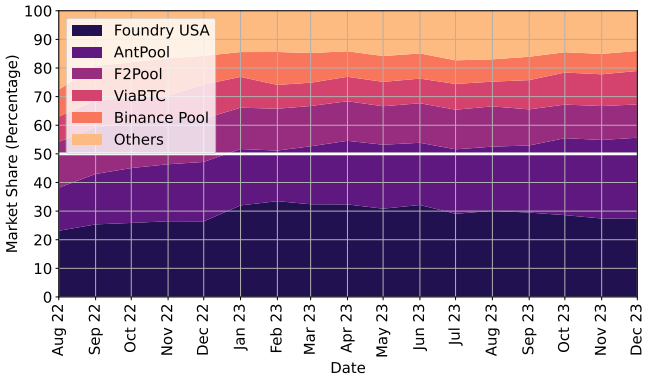


Fig. 3: Market shares of the largest Bitcoin mining pools over time [10].

rate, even when q is relatively small, can still attempt to perform selfish mining and create a fork that is several blocks deep. In such cases, the attacker's probability of success would be low and if she fails, she loses all the potential rewards she could have gained by honest mining. Nevertheless, if she does not care about such losses, e.g. if she has a larger incentive to act dishonestly, then she can repeat the attack until she reverts 6 blocks. Specifically, as we will see, relying on an analysis similar to that of [4] shows that an attacker who has merely 30% of the total hash rate has a success probability of more than 95% if she performs the attack for 33.7 days. An attacker with 40% of the hash rate can reach the same success probability within approximately 4.1 days and the time is reduced to only 1.9 days for an attacker with a 45% share.

THE COSTS OF AN ATTACK. The costs of an attack are also substantially smaller than one would expect. As we will see, a simple calculation shows that, at the time of writing, one can obtain the necessary hardware to have a majority of the hash power by spending approximately 6.43 billion USD. This is disregarding the potential discounts in bulk orders and assuming that the attacker buys the equipment rather than renting them. Crucially, although this number looks large, it is only 0.85 percent of the Bitcoin market cap at the time of writing and pales into insignificance in comparison with the trillion dollar monthly trade volume in Bitcoin derivatives. Similarly, we calculate that gaining a mining share of $20\%, 30\%$ and 40% costs only 1.61, 2.75 and 4.28 billion USD respectively. Thus, putting this together with the results mentioned in the previous paragraph, a patient attacker who is willing to wait for longer can dramatically reduce the costs of the attack[5].

INCENTIVES FOR AN ATTACK. Finally, and most importantly, the assumption that no attacker would have a financial incentive to perform such an attack is flatly wrong. It is not hard to imagine a state actor who has a vested interest in disrupting Bitcoin or crashing its market price. Currently, Bitcoin is banned in at least 10 countries, including some of the largest economies in the world [11]. The government of each of these countries can easily invest the amounts mentioned above into disrupting or destroying Bitcoin if they consider it as posing a real threat to their national currency. However, by far the biggest threat is posed by the often-unregulated Bitcoin derivative contracts such as options and futures. As we will see, the monthly trade volume in Bitcoin derivatives was above 500 billion USD in 15 of the past 16 months and even reached a trillion USD in several calendar months. Thus, an attacker can first short Bitcoin and then have the incentive to intentionally crash its price.

SUMMARY OF THE ATTACK. In short, an attacker can first use the Bitcoin derivatives market to short Bitcoin by purchasing a sufficient amount of put options or other equivalent financial instruments. She can then invest any of the amounts calculated above, depending on the timeline of the attack, to obtain the necessary hardware and hash power to perform the attack. If the attacker chooses to obtain a majority of the hash power, her success is guaranteed and she can revert the blocks as deeply as she wishes. However, she also has the option of a smaller upfront investment in hardware in exchange for longer wait times to achieve a high probability of success. In any case, as long as her earnings from shorting Bitcoin and then causing an intentional price crash outweighs her investments in hardware, there is a clear financial incentive to perform such an attack. The numbers above show that the annual trade volume in Bitcoin derivatives is more than three orders of magnitude larger than the required investment in hardware. Thus, it is possible and profitable to perform such an attack.

Based on the argument above, Bitcoin options and futures imperil Bitcoin's security and its core consensus protocol. We believe there is a complete lack of awareness on the part of financial players who are issuing such derivative contracts as to their potentially destructive effect on Bitcoin. We are hoping to raise awareness about this issue so that (i) the financial institutions realize the risk that issuing Bitcoin derivatives, especially shorting vehicles such as put options, poses to their earnings, and (ii) the regulators step up to reign in the unregulated derivatives market and enforce sensible caps on these trades.

We also note that this vulnerability is, at its core, due to a disconnect between the financial players in the cryptocurrency markets on the one hand, who treat Bitcoin and other similar currencies as if they are publicly-traded stocks, and the decentralized design of proof-of-work on the other hand. If Bitcoin were a stock, the attack we are describing would be tantamount to an investor first shorting the stock using leveraged contracts for differences whose value far exceeds the company's market cap and then buying enough shares to take control of the company and intentionally crashing it. This would of course be illegal due to a wide variety of insider trading regulations. However, since Bitcoin does not follow a proof-of-stake protocol, one only needs to control mining power, which is much cheaper. Moreover, mining is decentralized and largely unregulated and not subject to insider trading laws.

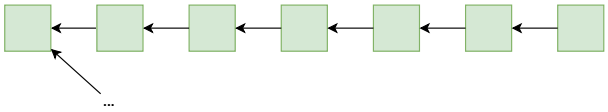
In the following sections, we will explain the calculations that went into each part of the argument above in more detail.

[5]We are not considering electricity costs since they vary significantly in different countries. Nevertheless, we are intentionally grossly over-approximating the cost of the hardware, e.g. by considering a purchase instead of renting. Moreover, the cost of electricity would not realistically surpass the hardware costs. Additionally, one can double all of our cost estimates and the analysis and vulnerabilities still stand.

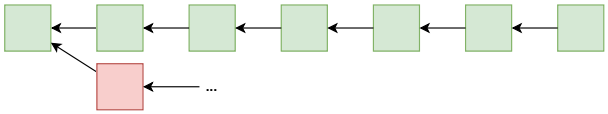
III. Block-reverting as a Minority Miner

Setting. In this section, we consider a malicious miner who wishes to intentionally create a fork that is 6 blocks deep, thus reverting 6 blocks of the previously-established consensus chain, in order to diminish the public's trust in Bitcoin and crash its price. Note that there is nothing special about the number 6 other than the fact that it is often used as a rule-of-thumb by the community. Our analysis below can be trivially extended to any number of blocks. We suppose that the attacker has a portion $0 < q < 1$ of the total hash power on the network. The problem is trivial if $q \geq 0.5$ since an attacker with a majority of the hash power is guaranteed to succeed in reverting any number of blocks. Thus, we focus on the case where the attacker is a minority miner, i.e. $q < 0.5$.

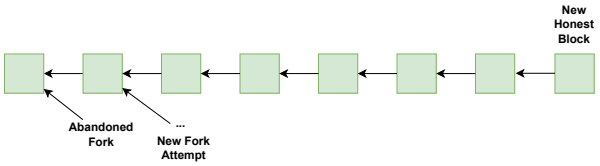
The Attack. The attack begins in the following blockchain state, where the green squares denote the current (honest) consensus chain and the dots show where the attacker is trying to add a new block to create a fork. In this state, the attacker's fork is 6 blocks behind the honest chain. Thus, we call this a -6 state.



As the attack progresses, there is a probability q that the attacker succeeds first in adding a new block, thus taking us to the -5 state below, where the attacker's chain is only 5 blocks behind the consensus chain.



On the other hand, with probability $1 - q$, the honest miners will form a new block. However, in this case, the attacker will simply abandon the previous fork and attempt a new fork that is 6 blocks deep, so we will remain at a -6 state.



Markov Chain. In general, let us model the attack by creating a Markov chain with states $\{-6, -5, -4, -3, -2, -1, 0, 1\}$, where a state $-i$ denotes that the attacker's fork is i blocks behind the consensus chain. The analysis above shows that the state -6 should have a transition to -5 with probability q and another transition to itself with probability $1 - q$. Similarly, it is easy to see that -5 should have a transition to -4 with probability q, corresponding to the case where the attacker finds the next block and reduces the distance between the two chains, and another transition to -6 with probability $1 - q$ corresponding to the case where the honest miners mine a new block.

Variant A. We consider two variants of the attack. In variant A, the attacker only publishes her chain when it becomes strictly longer than the consensus chain, i.e. when the Markov chain reaches state 1. At this point, the attack is successful. Thus, this variant can be modeled by the Markov chain in Figure 4. From each state, there is a probability q that the attacker finds the new block and thus we move right in the Markov chain and a probability $1 - q$ that the honest miners add a new block and thus we move left. The only exceptions are states -6 and 1. As shown above, at state -6, we will remain at the same state even if the honest miners find a new block since the attacker would simply restart the attack at a new forking point. At state 1, the attacker succeeds and thus there is no need to continue the analysis. Hence, we assume the Markov chain never leaves state 1 after reaching it. Our goal is to compute the probability that the Markov chain reaches state 1 in a fixed number k of steps. This is the same as the probability of the attacker's success in reverting a continuous sequence of 6 blocks if she performs the attack for k blocks' time.

We note that our Markov chain is similar to the one in [4] but not identical to it. The difference is that the attacker modeled in [4] aims to perform a successful double-spending so she has to revert a particular block. In contrast, our attacker is only interested in reverting 6 consecutive blocks and does not care which 6 blocks are reverted.

Variant B. The attacker does not necessarily need to wait until her chain becomes strictly longer (state 1). She can already publish her chain when it has the same length as the other (honest) chain, which corresponds to state 0. At this point, since there are two chains of the same length, the honest miners are free to choose which chain to extend. Assuming they have no bias, half of the honest mining power will then be used in extending the attackers chain. This variant of the attack can be modeled by the Markov chain in Figure 5 and is slightly more likely to succeed.

Value Iteration [12]. In both variants of the attack, our goal is to find the probability that starting at vertex -6 and taking k steps, we end up in state 1. This is the same as the attacker's success probability if she continues the attack for k blocks' time. It is easy to compute this probability using a classical value iteration algorithm. Let $p[u, k]$ be the probability of being at state u after k steps. We have $p[-6, 0] = 1$ and $p[u, 0] = 0$ for all $u \neq -6$. Let $v_1, v_2, \ldots, v_r$ be the predecessors of u in the Markov chain and the edge from v_j to u have probability $\pi(v_j, u)$. It is easy to see that for all $k \geq 1$, we have

$$p[u, k] = \sum_{j=1}^{r} p[v_j, k-1] \cdot \pi(v_j, u).$$

Intuitively, if we want to be at state u after k steps, we have to first get to one of its successors v_j in $k-1$ steps and then take the edge from v_j to u.

Success Probabilities in Bitcoin. We consider attackers with between 10% and 45% of the hash power in 5% increments. In Bitcoin, a block is mined roughly every 10 minutes. Figure 6 shows the attacker's success probability if she employs variant A and Figure 7 provides the same results for variant B. Specifically, an attacker who has only 30% of the hash power will have a success probability of more than 95% using variant A if she persists on the attack for 33.7 days. The attack duration

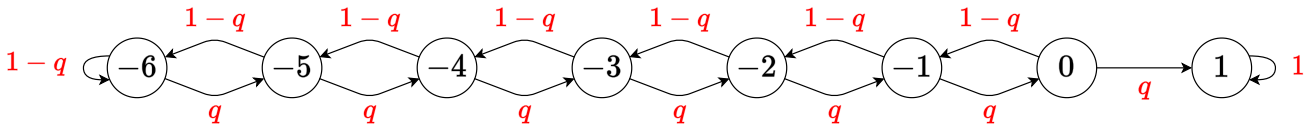


Fig. 4: The Markov chain modeling variant A of the attack.

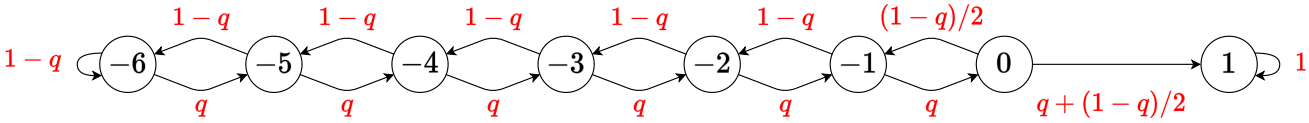


Fig. 5: The Markov chain modeling variant B of the attack.

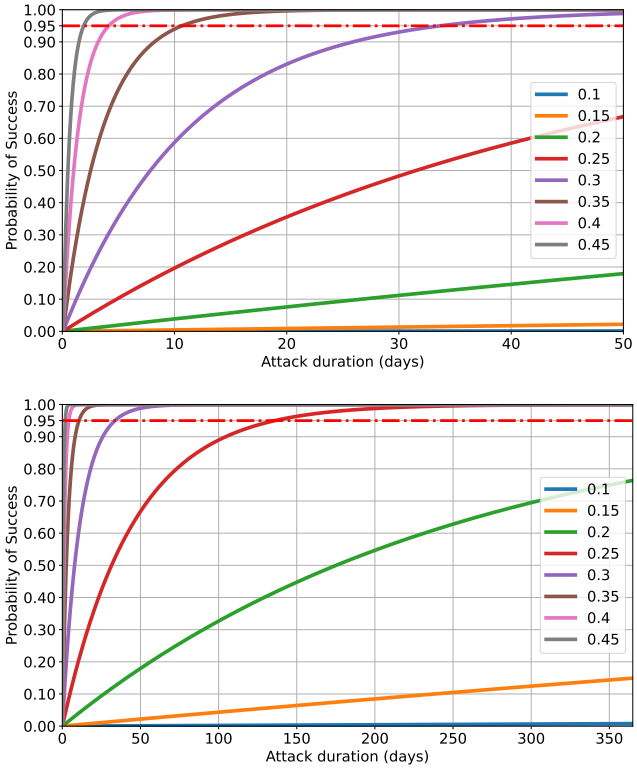


Fig. 6: Attacker's success probability for variant A within 50 days (top) and a year (bottom). Each line corresponds to a different portion q of the hash power controlled by the attacker.

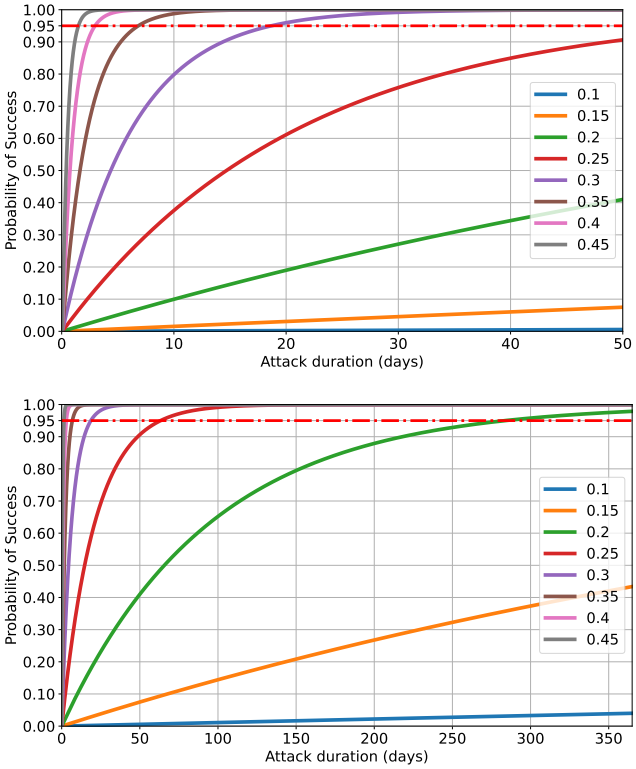


Fig. 7: Attacker's success probability for variant B within 50 days (top) and a year (bottom). Each line corresponds to a different portion q of the hash power controlled by the attacker.

to obtain a 95% success rate is reduced to 4.1 days for an attacker with 40% of the hash power and 1.9 days for one with 45%.

The attack duration can be further improved with variant B. Specifically, with regards to a situation where the attack controls 30%, 40%, and 45% of the total hash power, the attack duration would be reduced to 18.7, 2.97, and 1.5 days, respectively.

IV. Cost of the Attack

In the previous section, we showed that an attacker with a minority of the hash power can still succeed in reverting 6 blocks with high probability. Of course, an attacker who has a majority of the hash power will succeed in reverting any number of blocks with probability 1. In this section, we consider the costs of a block reverting attack. Specifically, we ask the following question: *How much does it cost to obtain a portion q of the hash power?* Our goal is not to obtain an exact number, but a ballpark estimate and upper-bound on the cost. Thus, we make the following simplifying assumptions:

- We only consider the cost of hardware at the time of writing. We assume the attacker is buying the hardware, rather than renting it and do not consider potential discounts on bulk orders.
- We ignore electricity costs as they vary widely based on

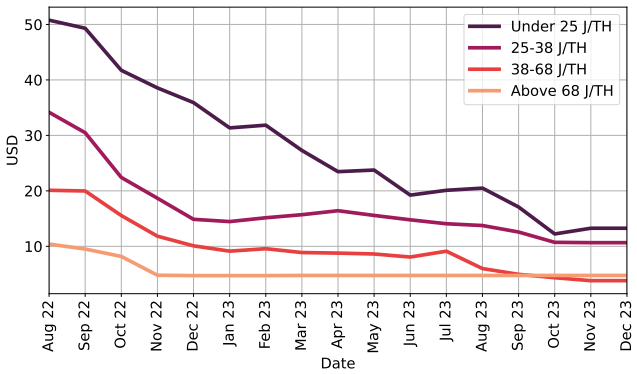


Fig. 8: historical price per TH of different Bitcoin mining ASICs grouped by four efficiency tiers.

location.

The justification for the first assumption is that it keeps our analysis sound, i.e. we can only over-approximate the cost by making this assumption. As for the second assumption, we note that electricity costs are often negligible in comparison to hardware costs and that our main argument, i.e. the vulnerability of Bitcoin to majority attacks and block-reverting attacks, remains intact even if the estimates we obtain here are doubled. Indeed, as we will soon see, the trade volume of Bitcoin derivatives is more than three orders of magnitude larger than the numbers obtained here.

At the time of writing, the total hash rate of the Bitcoin network is 484.59 EH/s [13]. Furthermore, [14] categorized Bitcoin mining ASICs into four efficiency tiers based on their energy consumption: Under 25 J/TH, 25-38 J/TH, 38-68 J/TH, and Above 68 J/TH. Figure 8 shows the historical price in USD per TH for each tier. To ensure the soundness of our analysis, we have estimated attack costs using the most expensive efficiency tier, i.e. Under 25 J/TH. This tier incorporates the most advanced generation of ASIC hardware that consumes the least amount of electricity. Table I summarizes the costs of obtaining various portions q of the total hash power at the time of writing. Note that if the current hash power is x, it is not enough for the attacker to purchase a hash power of $q \cdot x$, since her hash power will also be added to the network's total. Instead, she should buy y units of hash power where $\frac{y}{y+x} = q$ or equivalently $y = -\frac{q \cdot x}{q-1}$. Moreover, Figure 9 shows the historical price of obtaining various portions q of the total hash power based on the data from [2], [13], [14]. As Table I and Figure 9 show, it is easy to obtain a majority of the hash power, or a sizable minority that allows an attack as per the previous section, using an investment that is a tiny percentage of the Bitcoin's current market cap and, as we will see, three orders of magnitude smaller than the annual trade volume of Bitcoin derivatives.

V. Bitcoin Derivatives

In the previous section, we have already established a rough upper-bound on the costs of block-reverting attacks and argued that this cost is less than one percent of the current market cap of Bitcoin. Nevertheless, the required investment is substantial. Thus, the only remaining piece of the puzzle is to argue why

q	Required EH/s	Cost (Billion USD)	$\frac{\text{Cost}}{\text{Bitcoin Market Cap}}$
0.10	53.84	0.71	0.0009
0.15	85.52	1.13	0.0015
0.20	121.15	1.61	0.0021
0.25	161.53	2.14	0.0028
0.30	207.68	2.75	0.0036
0.35	260.93	3.46	0.0046
0.40	323.06	4.28	0.0057
0.45	396.48	5.26	0.0069
0.50	484.59	6.43	0.0085

TABLE I: The required hash power and hardware cost for an attacker who wishes to control a portion q of the total hash power.

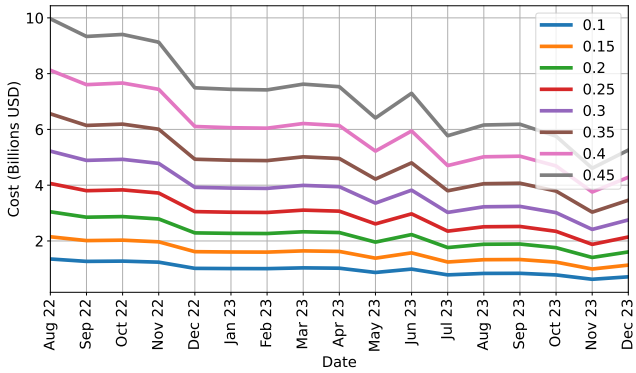


Fig. 9: The historical cost of obtaining a portion q of the hash power for various values of q.

anyone would be incentivized to invest such huge sums with the hope of crashing Bitcoin's price. In other words, how can an attacker profit from a price crash?

Bitcoin Derivatives. There is a huge and mostly unregulated Bitcoin derivatives market whose trade volumes often exceed 750 billion or even 1 trillion USD in a calendar month. Cryptocurrency exchanges such as Binance, OKX and ByBit offer future contracts and options on a wide variety of coins. Figure 10 shows the monthly trade volume of these largely unregulated markets between August 2022 and November 2023 [15]. As evident in this figure, the annual trade volume of Bitcoin derivatives is an order of magnitude larger than Bitcoin's market cap, which was itself two orders of magnitude larger than the cost of an attack. Thus, it is clearly feasible to buy enough put options, or other shorting vehicles, to benefit from a price crash that is induced by the block-reverting attacks explained above.

Regulated Derivatives. There is also a much smaller regulated market that offers futures and option contracts through the Chicago Mercantile Market (CME), which is overseen by the Commodity Futures Trading Commission (CFTC). Figure 11 shows the monthly CME trade volumes of Bitcoin derivatives during August 2022–November 2023 [16]. As evident from this figure, the regulated market is much smaller and does not pose the same level of risk to Bitcoin as the unregulated market.

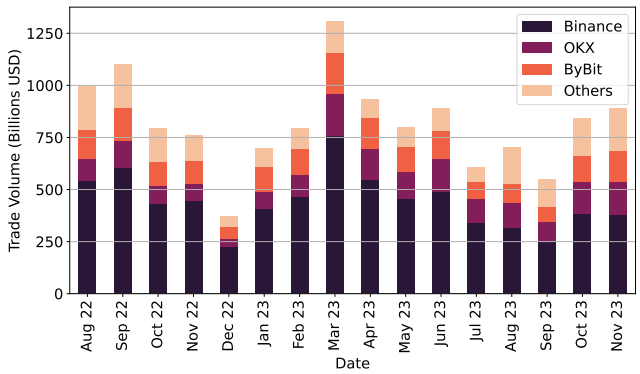


Fig. 10: Total trade volume of unregulated Bitcoin derivatives [15].

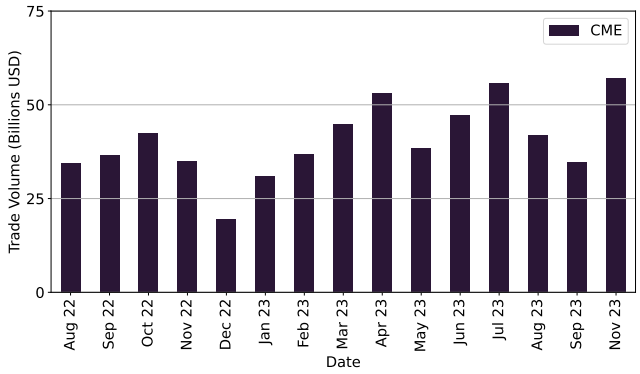


Fig. 11: Total trade volume of regulated (CME) Bitcoin derivatives [16].

VI. Conclusion

In this work, we refuted several common misconceptions regarding Bitcoin's security against block-reverting attacks. Specifically, we showed that (i) a successful block-reverting attack does not necessarily require (even close to) a majority of the hash power; (ii) obtaining a majority of the hash power or a minority that is sufficient for a block-reverting attack costs roughly 6.43 billion or 2.75 billion USD, respectively, which are much lower numbers than what the community seems to expect and two orders of magnitude smaller than the Bitcoin market cap; and (iii) Bitcoin derivatives, i.e. options and futures, imperil Bitcoin's security by creating an incentive for a block-reverting/majority attack. The annual trade volume of these derivatives over several unregulated markets is more than three orders of magnitude larger than the hardware cost of such attacks. Thus, an attacker can first obtain derivatives that short Bitcoin and allow her to benefit from a crash in Bitcoin's price and then intentionally perform a block-reverting attack with the goal of crashing the price.

Acknowledgment

Removed to preserve anonymity in review.

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.
[2] "Cryptocurrency prices, charts and market capitalizations." [Online]. Available: https://coinmarketcap.com/
[3] M. A. Meybodi, A. K. Goharshady, M. R. Hooshmandasl, and A. Shakiba, "Optimal mining: Maximizing bitcoin miners' revenues from transaction fees," in *Blockchain*, 2022, pp. 266–273.
[4] M. Rosenfeld, "Analysis of hashrate-based double spending," *arXiv preprint arXiv:1402.2009*, 2014.
[5] B. Hou and F. Chen, "A study on nine years of bitcoin transactions: Understanding real-world behaviors of bitcoin miners and users," in *ICDCS*, 2020, pp. 1031–1043.
[6] K. A. Negy, P. R. Rizun, and E. G. Sirer, "Selfish mining re-examined," in *FC*, 2020, pp. 61–78.
[7] I. Eyal and E. G. Sirer, "Majority is not enough: bitcoin mining is vulnerable," *Commun. ACM*, vol. 61, no. 7, pp. 95–102, 2018.
[8] A. Hern, "Bitcoin currency could have been destroyed by 51% attack," 2014. [Online]. Available: https://www.theguardian.com/technology/2014/jun/16/bitcoin-currency-destroyed-51-attack-ghash-io
[9] "Bitcoin hashrate distribution," 2023. [Online]. Available: https://www.blockchain.com/explorer/charts/pools
[10] "Bitcoin mining pools." [Online]. Available: https://hashrateindex.com/hashrate/pools
[11] P. BAJPAI, "Countries where bitcoin is legal and illegal." [Online]. Available: https://www.investopedia.com/articles/forex/041515/countries-where-bitcoin-legal-illegal.asp
[12] R. Bellman, "A markovian decision process," *Journal of Mathematics and Mechanics*, pp. 679–684, 1957.
[13] "Total hash rate." [Online]. Available: https://www.blockchain.com/explorer/charts/hash-rate
[14] "Bitcoin asic price index." [Online]. Available: https://data.hashrateindex.com/chart/asic-price-index
[15] "Volume of bitcoin futures." [Online]. Available: https://www.theblock.co/data/crypto-markets/futures/volume-of-bitcoin-futures-monthly
[16] "Volume of cme bitcoin futures." [Online]. Available: https://www.theblock.co/data/crypto-markets/futures/average-daily-volume-of-cme-bitcoin-futures-monthly