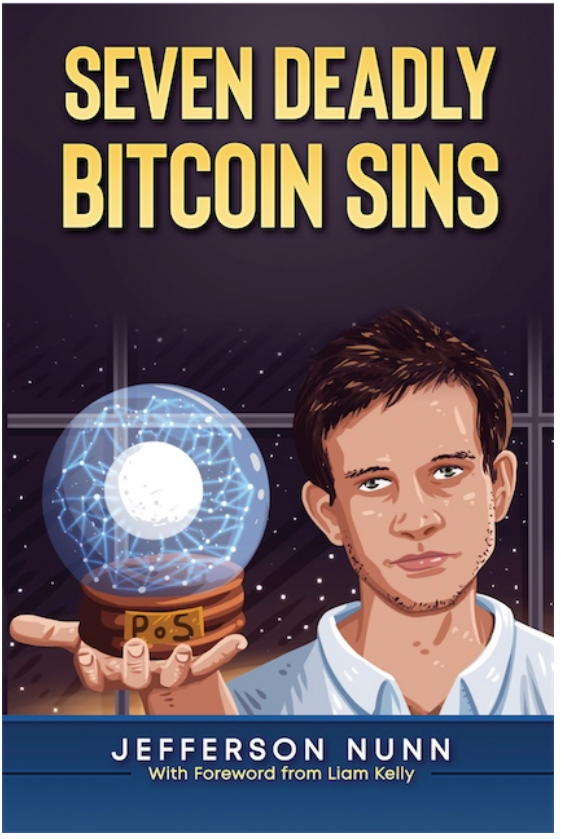


In the following book, Jefferson Nunn will be walking through, in detail, seven questions posed by the co-creator of Ethereum. These seven questions are some of the most relevant features of this booming ecosystem. From mining, to governance and everything in between.

SEVEN DEADLY BITCOIN SINS

by Jefferson Nunn

SEVEN DEADLY BITCOIN SINS

JEFFERSON NUNN
With Foreword from Liam Kelly

Seven Deadly Bitcoin Sins
Jefferson Nunn Consulting
www.jeffersonnunn.com

Cover Designed by Pixel Studio
Arranged by Eswari Kamireddy
Edits by Lisa Bowman
Foreword by Liam Kelly
Published by BookLocker.com, Inc., St. Petersburg, Florida.

Author's Note: I do not recommend the purchase, sale or holding of any stock or cryptocurrency. I am a holder of Bitcoin.

Library of Congress Cataloging-in-Publication Data Control Number: 2019900459

1. COMPUTERS | BUSINESS & ECONOMICS| SCIENCE COM060000
2. COMPUTERS / Internet / General BUS027000
3. BUSINESS & ECONOMICS / Finance / General BUS069000

ISBN: 978-1-64438-534-0

First Edition

In the following chapters, *we* will explore, in detail, seven questions posed by the co-creator of Ethereum, Vitalik Buterin. The series was inspired by a discussion between Buterin and a WeChat group called "Mars Finance Global Family."[1] The seven questions address some of the most relevant features of this booming ecosystem, from mining, as in this chapter, to governance, and everything in between.

DEADLY SIN #1: FEAR OF 51% ATTACKS

Of all the potential attacks on cryptocurrencies, one of the most dreaded is known as a 51 percent attack [2]. A 51% attack occurs when miners launch an assault on a given blockchain to take over the approval process for transactions currently being processed. A successful attack would not allow for complete control over the cryptocurrency, but it could significantly alter how the cryptocurrency is used.

This type of attack, for instance, would not allow this group of miners to arbitrarily create new coins or to alter historical transactions, but the malicious miners could double spend transactions over which they currently have control or halt the transaction altogether.

Bitcoin Gold: Successfully Attacked

The largest example of this attack is with Bitcoin Gold.[3] In May 2018, over a period of four days, malicious miners controlled a vast amount of hash power on Bitcoin Gold's network, such that they were able to double-spend transactions, eventually stealing more than $18 million worth of Bitcoin Gold. Despite creating updates to the wallet, reversing entire blocks, and increasing confirmation times, the cryptocurrency still experienced a significant failure (Malwa, 2018).

In the case of Bitcoin Gold, the attack was made possible by a confluence of events. Since Bitcoin Gold used the Equihash mining algorithm,[4] the mining platform is very similar to ZCash,[5] so there is a large supply of hash power available—around 500 Megahash in May[6] 2018, according to Coinwarz. A second significant factor was the high value of the coin at the time, which was around $75 per

coin[7] (Live Coin Watch, 2018). Another factor was the low amount of total hash rate on the coin, which was around 40 mega-hash.[8]

To attack Bitcoin Gold, the malicious miner simply had to create a custom mining script and deploy it to around 40 mega-hash worth of miners. At a cost of about one bitcoin per mega-hash per 100 hours, the 40 mega-hash system would only cost approximately 40 BTC for the 100-hour time.[9]

Can Bitcoin Be Attacked by Bitmain?

Larger currencies, such as Bitcoin[10] and Ethereum,[11] point to their large hash power as proof that the 51 percent attack cannot occur to their respective cryptocurrencies. Bitcoin is currently at approximately 40 Petahash, and Ethereum is at 288 Terahash. Based on this, there would only be two ways to attack either cryptocurrency using this style of hack: attempt to double the hash rate overnight or attempt to compromise more than 51 percent of the miners via collusion and monopolization.

In light of this, the bitcoin protocol is vulnerable to such a threat by Bitmain[12] and related pools as they have more than enough hash power to compromise the cryptocurrency at any time. And Vitalik Buterin asks, **"Isn't this a big problem?"**

The principle point is that most bitcoin miners run on rigs manufactured by Bitmain, or they mine in pools controlled by Bitmain or their affiliates.[13] This means that at any time, malicious code can be injected into the pools or potentially into the miners by a software update, to affect how the miners are mining.

Could Antbleed Have Caused a 51% Attack?

Bitmain was directly responsible for the "Antbleed"[14] vulnerability, as revealed in April 2017. This problem was hard coded into a large majority of miners and would allow either Bitmain or malicious hackers to shut down all miners running this system, making a majority attack less costly for someone to implement. Bitmain's response at

the time was that this was never intended to be a bug but rather a feature:

"We never intended to use this feature on any Antminer without authorization from its owner. This is similar to the remote erase or shutdown feature provided by most famous smartphone manufacturers."

Although the source code for Bitmain's miners is public source, the software that runs their pools is kept confidential and out of the public's view. According to Blockchain.com in 2018, the following five pools control more than 50 percent of bitcoin's hash rate:[15]

- BTC.com 19.1 percent
- ViaBTC 12.4 percent
- AntPool 12.2 percent
- BTC.TOP 10.7 percent
- SlushPool 10.7 percent

This totals 65.1 percent of the entire hash rate of the bitcoin network. If these five pool owners were to collaborate on any combined update to their pool, it could have a disastrous impact on mining.

Matt Odell on the 51% Attack

Speaking to these issues, bitcoin developer Matt Odell[16] told *BTC-Manager*:

"[We] don't know the makeup of the individual pools. How much is controlled directly by Bitmain in their server farms versus how much are independent miners who use Bitmain's pools because they are solid reliable pools with low variance."

The only check on a mining pool's power is for the individual miners. To that, Odell offers:

"Pool operators have a lot of power, but those individual miners can change their pools if they don't like how they are being operated, which provides a soft check on that power. In the future if Matt Coral-

lo's betterhash works and gets adopted, those pool operators will have much less power."

Betterhash—Will it Really Be Better?

Betterhash[17] would solve this issue by affecting how individual miners operate within mining pools (Corallo, 2018). The "Stratum" protocol requires that pool operators, such as Bitmain, create the template for the block, and then the protocol requires the miners to build on that template.

This means pool operators can censor what miners can work on. Since the pool can select which transactions to include in a block, the pool could potentially reject transactions as well.

The most dramatic effect of the pool's censorship power was most visibly seen in the "block accelerator" systems that all pools were offering during the "full blocks" period of bitcoin prior to the introduction of Segwit[18] and the Lightning Network.[19]

The Betterhash proposal Matt Corallo submitted in March 2018 is still pending on the standards track. The other members of the committee are concerned about how this proposal would interact with the rest of the system. This proposal would move the building of block templates to individual miners and allow miners to select for themselves which transactions to include in blocks.

Attack on Stratum

For a period of almost 12 months and during the rise of bitcoin to $20,000, just about every block mined by bitcoin was a full 1MB block.[20] During this time, the debate regarding the block size increase reached a fevered pitch between bitcoin and Segwit supporters as well as the 8MB block supporters. Ultimately, the battle ended with the fork of Bitcoin Cash[21] (BCH) on August 16, 2017.

During this time, ViaBTC and BTC.com both offered "transaction accelerators"[22] and required miners to mine blocks with those accelerated transactions while keeping the payments for accelerated transactions to themselves (Bergmann, March 2017).

This opens up another related attack vector. Using this same power, governments or other malicious groups could require pools to block transactions and keep quiet about those transactions they block.

Audit of Bitmain

Bryan Bishop,[23] a cryptocurrency expert, recently offered to provide an independent third-party audit of Bitmain's hash rate. On Twitter, he told *BTCManager*:

"An independent, outsider audit of Bitmain hash rate is possible. I think their move towards greater transparency is a huge win for bitcoin, if they follow through. A good audit would combine both the technical expertise of a bitcoin developer with forensic accounting" (Bishop, 2018).

BTCManager reached out to Bryan to follow up with a few questions of our own. When asked about the Betterhash proposal, Bryan said:

"I think the Betterhash proposal from Matt Corallo is going to help a lot. In the meantime, I'm left wondering about Bitmain's control of many of the large bitcoin mining pools."

Bitmain's Silence

When confronted by the bitcoin community about these concerns, Bitmain (2018) only offered the transparency policy[24] on their website, excerpted below:

1. Every 30 days Bitmain will publish data on self-mining.
2. There is a zero-tolerance policy on secret mining.
3. They will never seek to mine empty blocks.
4. They will provide shipping and volume information of new miners to the public.

There is nothing in the disclosure about their cooperation with other pools or about how they select which transactions to mine or even how their mining pools operate. *BTCmanager* asked Bitmain

these questions on their support forum and by email, and we have not received a response. We will update this article should we hear back from the firm.

Is Ethereum Protected?

Ethereum has proven to be more resistant to attacks than bitcoin; however, it suffers from the same Stratum protocol difficulty as the pioneer cryptocurrency. That said, Ethereum has been moving to a Proof of Stake (PoS)[25] implementation.

This would require some major changes to the entire Ethereum system. Ethereum "Serenity"[26] is the code name for this system that includes the Casper[27] Proof of Stake. The next major step will be Ethereum's "Constantinople"[28] and will provide the building blocks for this. Implementation has been delayed until sometime between 2019 and 2020,[29] according to Ethereum developers.

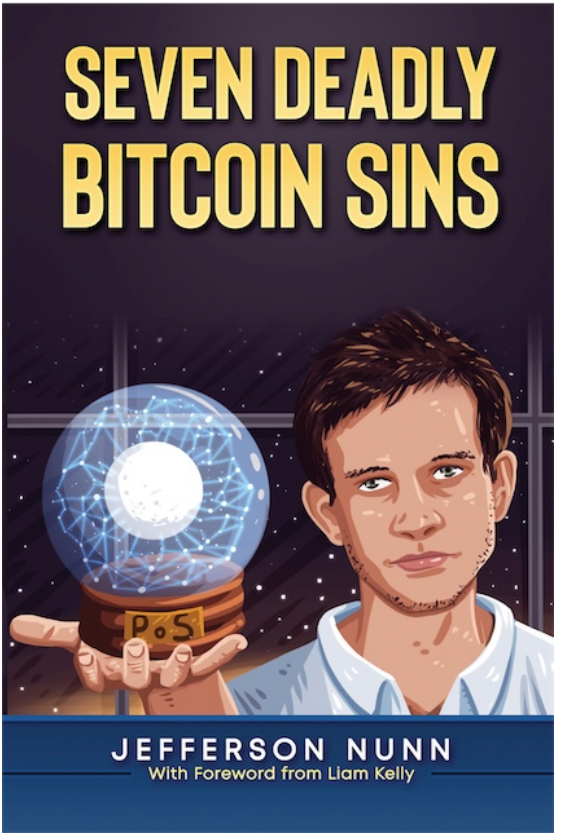
This means that, right now, the top four Ethereum pools[30] can collaborate in a malicious way. According to GasTracker (2018), the top four pools are:

- Ethpool / Ethermine - 43.88 percent
- Nanopool - 20.91 percent
- MiningPoolHub - 10.12 percent
- 2miners - 8.6 percent

BTCManager also attempted to reach out to Ethermine and Nanopool through their support system and email. To date, we have not received a response to our inquiries. We will update this article should we hear back from either pool operator.

Stopping the Attacks

A 51 percent attack is a very real threat. The threats are not only from external state-sponsored forces but also from malicious attackers. Cryptocurrency developers are continuing to review proposals and propose multi-year development plans while attackers are crafting plans of their own.



In the following book, Jefferson Nunn will be walking through, in detail, seven questions posed by the co-creator of Ethereum. These seven questions are some of the most relevant features of this booming ecosystem. From mining, to governance and everything in between.

SEVEN DEADLY BITCOIN SINS

by Jefferson Nunn