



# **santacroce tech**

## **opinion & insights**

**NOVEMBER 27, 2024**

# CONTENTS

03

Introduction

04

What is a Bitcoin mining pool?

05

How does a Bitcoin mining pool work?

06

What is a block template?

07

What is merged mining?

08

How Stratum v2 improves Bitcoin mining?

09

Data centers vs. solo mining

09

Are ASIC chip manufacturers a risk?

10

Is Bitcoin mining centralized?

11

Is Bitcoin mining a profitable business?

11

Santacroce's picks

12

About us | Contact info

# INTRODUCTION

*Our third newsletter focuses on the Bitcoin mining centralization issue, including the advantage of large operations, the reason behind the reduced number of machine suppliers, regulatory risks, and how block templates influence the network.*

*We all heard that the 3 largest mining pools control 70% of the Bitcoin mining—we'll circle that later on—but what exactly are those entities, how centralized are their operations and what is being implemented to improve this?*

*Don't worry, we'll keep it simple and short in this dip dive on how Bitcoin mining works and how decentralization is utopian. In all seriousness, stop listening to maxis, or any extremists in fact. Let's dig into it!*

**Roberto Santacroce Martins**

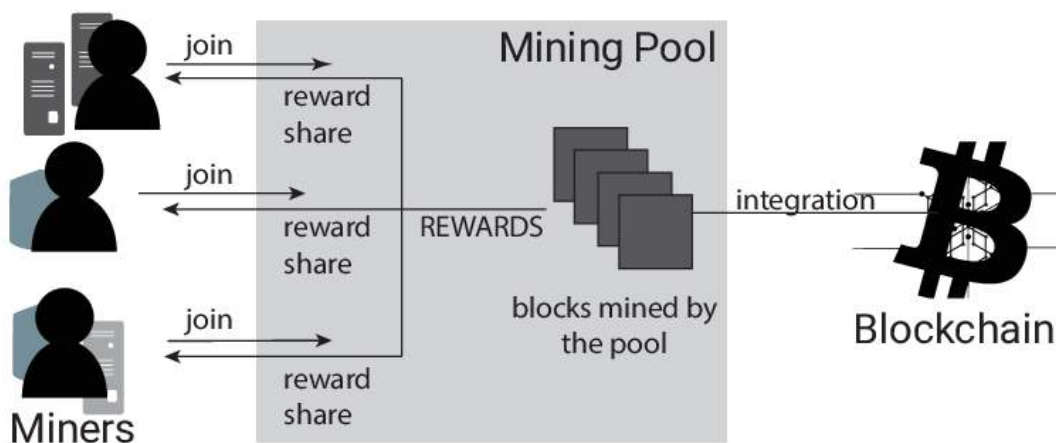
**Programmer, Santacroce Tech Founder**



# WHAT IS A BITCOIN MINING POOL?


A Bitcoin mining pool is a collective of miners who combine their computing power to increase their chances of solving the Proof-of-Work puzzle and earning rewards. Bitcoin mining resembles a lottery: each miner generates random hashes, thus having more tickets improves your odds. By joining a mining pool, participants share resources, effectively multiplying their chances of finding a block.

When a mining pool successfully mines a block, the reward is distributed among participants based on their contributed computational power. This collaboration helps individual miners compete against large-scale operations, ensuring a more equitable mining environment. While pools increase the likelihood of consistent rewards, they should (in principle) not compromise Bitcoin's decentralization, as pool members retain control over their own hardware.



Basics of the Bitcoin mining pool process.

# HOW DOES A BITCOIN MINING POOL WORK?



A Bitcoin mining pool operates by coordinating the efforts of multiple miners, directing them to focus on solving smaller, manageable portions of the Proof-of-Work puzzle. The pool operator assigns miners specific tasks, ensuring no overlap in their efforts. Miners submit their completed work (shares) to the pool, which monitors their contributions. The pool combines these shares to collectively solve the block puzzle, increasing efficiency.

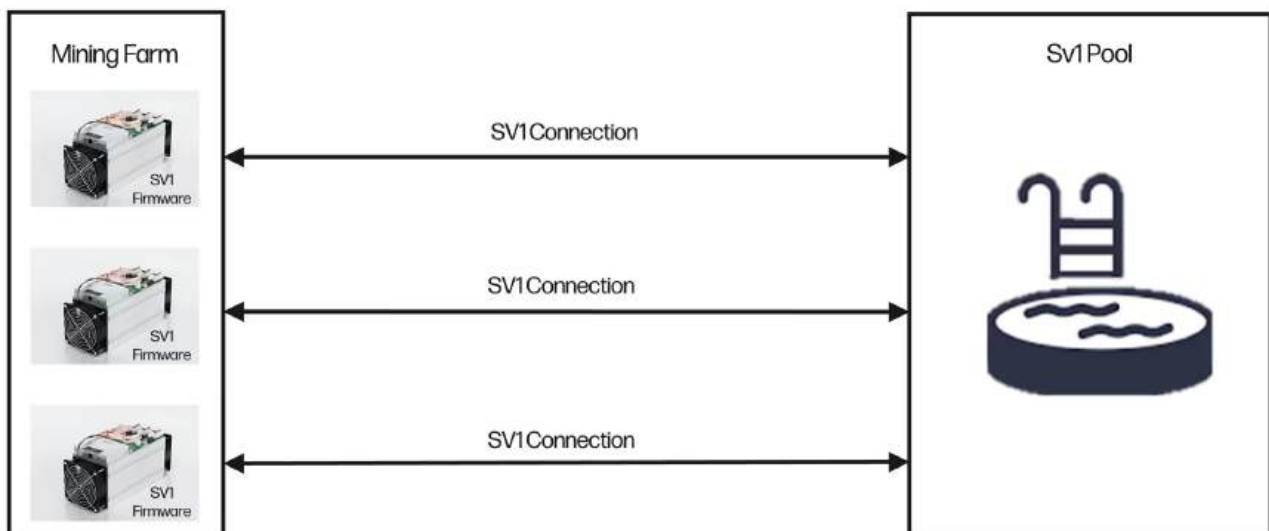
Pool owners decide which transactions to prioritize—more on this later—collect fees (usually 1-3% of rewards) and determine payout structures. Payouts typically follow proportional or pay-per-share (PPS) models, rewarding miners based on their contribution. Mining pools are better than solo mining for most because they offer more consistent earnings, even if smaller, reducing the volatility of waiting for a solo block reward.

# WHAT IS A BLOCK TEMPLATE?



A Bitcoin block template is a blueprint created by mining pools that defines the transactions to include in a new block. The pool operator has significant control, as they select which transactions to prioritize or exclude. Operators can accept "bribes" in the form of private transaction fees (via out-of-band payments) to bypass or include specific transactions, potentially undermining the network's neutrality.

Stratum V1 Miner to Pool Direct Connection  
Source: Galaxy Digital Research



Layout of basic ASIC connection to a mining pool.

Most mining pools use software like [Stratum](#) or similar protocols to distribute block templates and manage miner communication. Generally, the higher the fee, the more likely a transaction is included. This method gives pool operators too much power, emphasizing the importance of decentralization and ethical practices in maintaining network fairness.



# WHAT IS MERGED MINING?

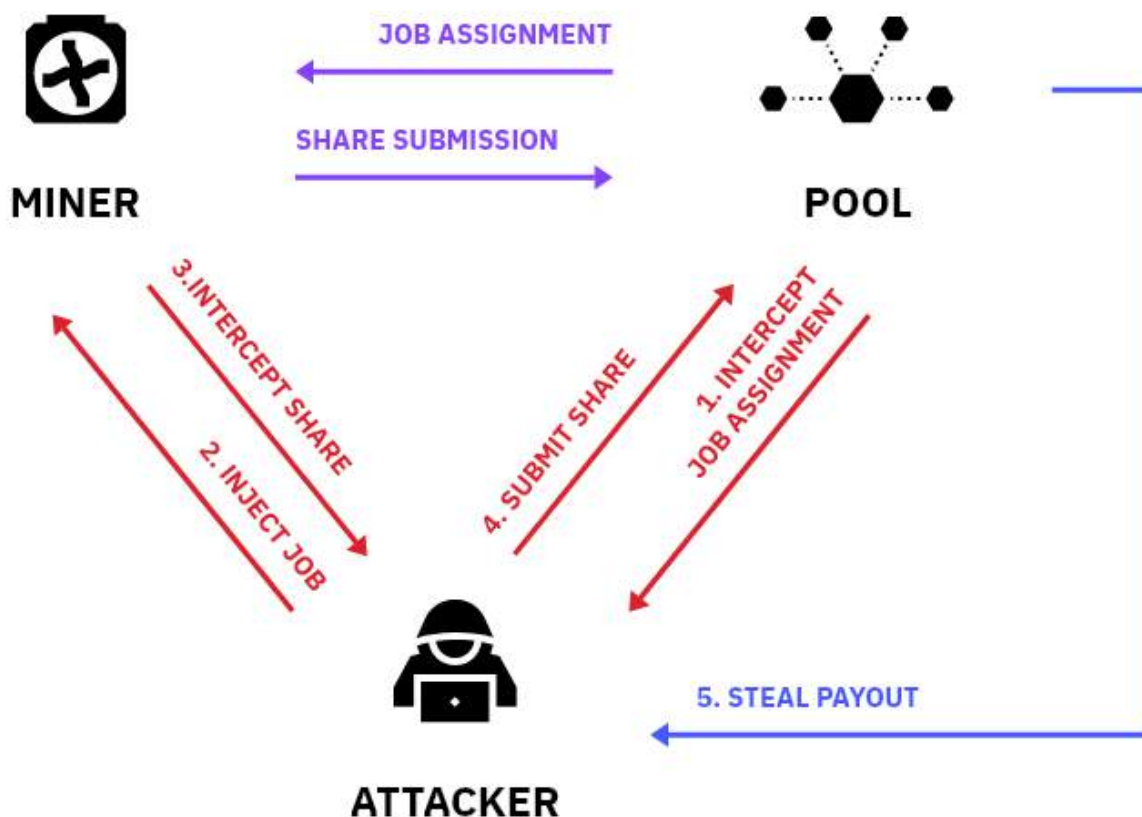


Merged mining allows miners to validate two or more blockchain networks simultaneously using the same computational work. In this process, miners create a block for the primary blockchain and reuse the proof-of-work (PoW) hash to secure an auxiliary chain (e.g., Namecoin). The mining pool acts as an intermediary, combining miner contributions and submitting valid shares to both chains, simplifying coordination.

When mining, if a hash meets the difficulty of the auxiliary chain but not the primary chain, it can still be submitted as a valid block for the auxiliary chain, achieving dual benefits from the same computational work. While energy-efficient, merged mining requires additional setup and heightened technical complexity. Chains like Dogecoin utilize Scrypt, but they can't share work with Bitcoin unless a compatible auxiliary blockchain exists.

# HOW STRATUM V2 IMPROVES BITCOIN MINING?

Stratum v1 is susceptible to man-in-the-middle attacks, particularly through 'hashrate hijacking', where attackers can intercept and misuse proof of work data. [Stratum v2](#) improves Bitcoin mining by reducing inefficiencies in communication between miners and pools and enhancing security, positively impacting the speed and performance of mining operations.



Attack vector known as 'hashrate robbery'

Instead of relying on mining pools to dictate block templates, miners can run local software to select their own, increasing decentralization and giving miners more control over what transactions are included in blocks. While it doesn't directly incentivize solo miners to join pools, the protocol makes it more appealing to participate in pooled setups, especially for those with limited resources or smaller operations.



## DATA CENTERS VS. SOLO MINING



Data centers often benefit from access to better energy sources, particularly in remote locations where energy might have been previously wasted or underutilized, like near hydroelectric dams or wind farms, which can significantly reduce operational costs.

Regulatory clarity in some regions provides a more stable legal environment for mining operations, reducing the operational risk. Additionally, data centers provide professional management, which includes maintenance, security, and connectivity, ensuring higher uptime and efficiency. Furthermore, data centers can leverage economies of scale, making it easier to manage and upgrade equipment.

## ARE ASIC CHIP MANUFACTURERS A RISK?

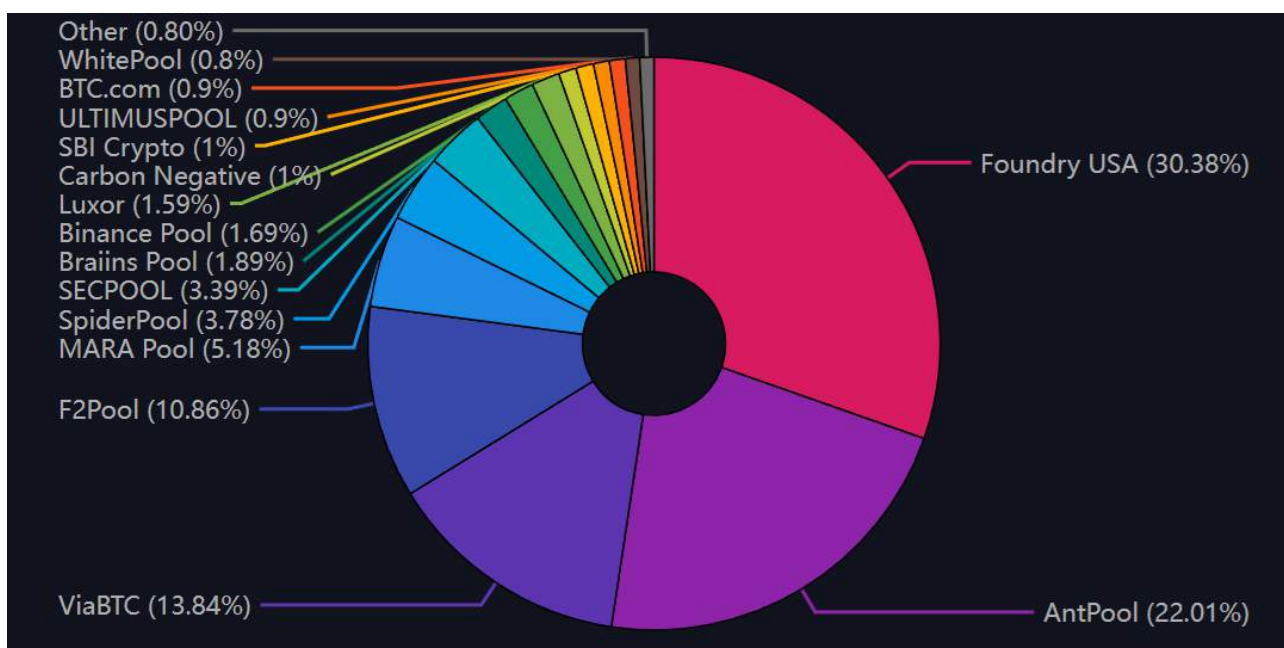


The reduced number in ASIC machine suppliers can be attributed to market consolidation, high entry barriers, and the complexity of manufacturing. This concentration might pose a risk concerning supply chain security and potential duopolies. However, the software aspect can be mitigated by rewriting the entire OS and software to eliminate most known backdoors, enhancing security.

Yet, the risk of unknown hardware vulnerabilities persists. To address this, one could implement monitoring via tools like firmware analysis software or hardware security modules (HSMs), which scan for unusual chip behavior or unauthorized access attempts, thus potentially detecting new types of hardware-based attacks.

# IS BITCOIN MINING CENTRALIZED?

Currently, Bitcoin mining does exhibit centralization, with a few large pools controlling a significant portion of the network's hashrate. However, this centralization is mitigated by the potential for migration to protocols like Stratum v2, which decentralizes transaction selection back to individual miners, reducing the influence of pool operators.



Weekly BTC mining pools ranking on Nov. 27.

The Bitcoin price above \$90k incentivizes home mining with reused ASIC chips, exemplified by devices like BitAxe, making mining accessible to smaller operators. This trend suggests that while the concentration of hashrate in a few pools exists, the underlying dynamics are shifting towards greater decentralization, as individual miners gain more autonomy.

# IS BITCOIN MINING A PROFITABLE BUSINESS?



Bitcoin mining can indeed be profitable, especially at \$90k, given the favorable energy prices medium-to-large miners secure. However, the industry faces challenges, such as competition growth. More miners enter the market, increasing mining difficulty and compressing profit margins.

Setting up mining operations involves significant initial capital for hardware, infrastructure, and energy solutions. While these factors mean there's no 'free money', miners with competitive edges such as lower operational costs, access to renewable or wasted energy sources, and efficient technology can continue to be profitable even during market downturns or when capital costs rise.

## SANTACROCE'S PICKS



### State of Stratum V2 | Plan B Forum 2023 | Lugano

State of Stratum V2 with Kristian Csepсар.



<https://www.youtube.com/watch?v=KQs7kUbU09g>

## ABOUT US

Santacroce Tech is a company dedicated to blockchain technology, focusing on scalability and decentralization. We are actively involved in open-source development around Bitcoin, contributing to initiatives like Stratum V2 and Drivechain, which aim to enhance efficiency, flexibility, and innovation within the ecosystem.

Our expertise is bolstered by decades of experience in the technology industry and established relationships within the sector. We actively participate in initiatives like the Bitcoin Center NY and contribute to notable projects such as BRZ, Brazil's first stablecoin, and Alkimiya, which focuses on the tokenization of financial streams related to cryptocurrency mining.

These experiences position us as strategic partners, equipped to offer valuable insights and act as advisors to executive teams in making critical technological decisions..

## CONTACT INFO



Count on Santacroce Tech's content to guide you through the dynamic digital asset and blockchain industry. Subscribe now for invaluable insights! For business inquiries or general questions, please don't hesitate to contact us at [info@santacroce.xyz](mailto:info@santacroce.xyz)

==--==--== block 872,257 ==--==--==