



# **santacroce tech**

## **visão de mercado**

**27/NOVEMBRO/2024**

# ÍNDICE

03

Introdução

04

O que é uma cooperativa de mineração de Bitcoin?

05

Como funciona uma cooperativa de mineração?

06

O que é um modelo de bloco?

07

O que é mineração combinada?

08

Como o Stratum v2 melhora a mineração de Bitcoin?

09

Data centers vs. mineração solo

09

Os fabricantes de chips ASIC representam um risco?

10

A mineração de Bitcoin é centralizada?

11

A mineração de Bitcoin é um negócio lucrativo?

12

Recomendação

12

Sobre nós | Contato

# INTRODUÇÃO

*Nossa terceira newsletter foca no problema da centralização da mineração de Bitcoin, incluindo a vantagem das grandes operações, a razão por trás da redução do número de fornecedores de máquinas, riscos regulatórios, e como os modelos de bloco influenciam a rede.*

*Todos ouvimos que as 3 maiores cooperativas de mineração controlam 70% da mineração de Bitcoin – voltaremos a isso mais tarde – mas o que exatamente são essas entidades, quão centralizadas são suas operações e o que está sendo implementado para melhorar isso?*

*Não se preocupe, manteremos isso simples e breve nesta imersão sobre como funciona a mineração de Bitcoin e como a descentralização é utópica. Falando sério, pare de ouvir os maximalistas, ou quaisquer extremistas. Vamos nos aprofundar nisso!*

**Roberto Santacroce Martins**

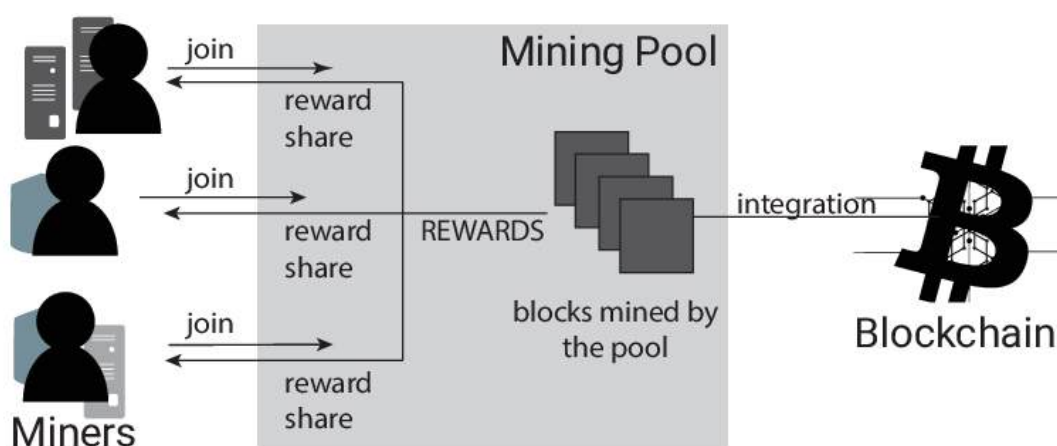
**Programador, Fundador @ Santacroce Tech**



# O QUE É UMA COOPERATIVA DE MINERAÇÃO?


Uma cooperativa de mineração de Bitcoin é um grupo de mineradores que combinam seu poder computacional para aumentar suas chances de resolver o quebra-cabeça da Prova de Trabalho e ganhar recompensas. Minerar Bitcoin assemelha-se a uma loteria: cada minerador gera hashes aleatórios, portanto, ter mais 'ingressos' melhora suas chances. Ao ingressar em uma cooperativa de mineração, os participantes compartilham recursos, multiplicando efetivamente suas chances de encontrar um bloco.

Quando uma cooperativa de mineração encontra com sucesso um bloco, a recompensa é distribuída entre os participantes com base no poder computacional contribuído. Essa colaboração ajuda mineradores individuais a competir contra operações em grande escala, garantindo um ambiente de mineração mais equitativo. Embora as cooperativas aumentem a probabilidade de recompensas consistentes, elas não deveriam, em princípio, comprometer a descentralização do Bitcoin, já que os membros da cooperativa mantêm o controle sobre seu próprio hardware.



Fundamentos do processo de cooperativa de mineração de Bitcoin.

# COMO FUNCIONA UMA COOPERATIVA DE MINERAÇÃO?



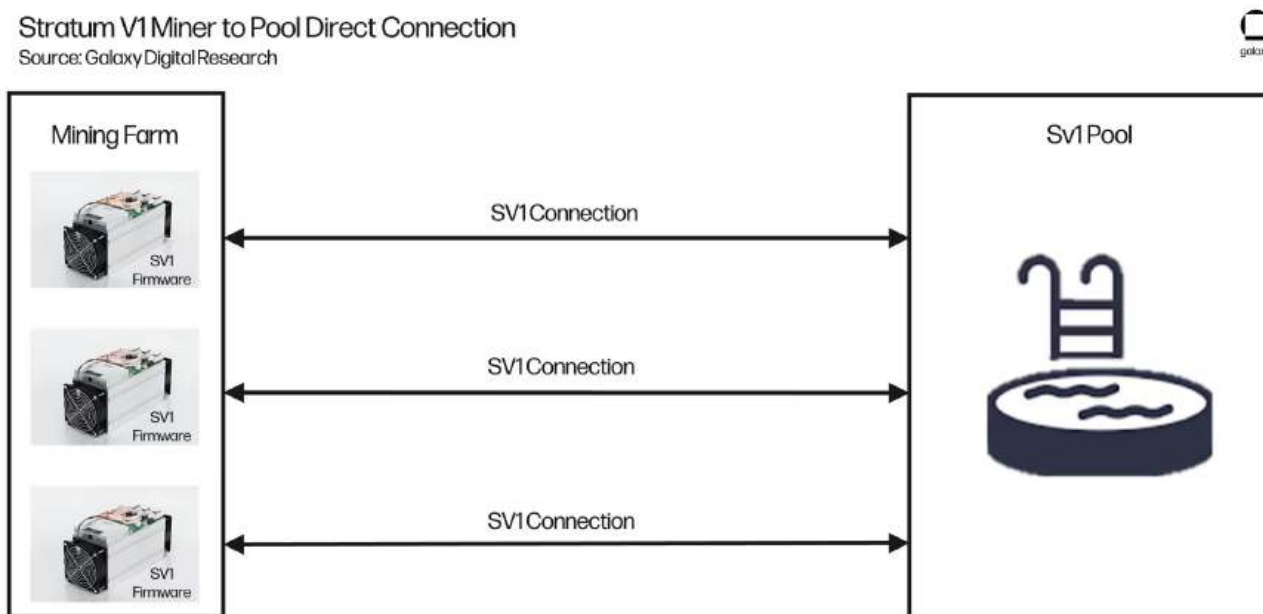
Uma cooperativa de mineração de Bitcoin funciona coordenando os esforços de vários mineradores, direcionando-os a se concentrarem na resolução de porções menores e gerenciáveis do quebra-cabeça de Prova de Trabalho. O operador da cooperativa atribui tarefas específicas aos mineradores, garantindo que não haja sobreposição nos esforços. Os mineradores enviam seu trabalho concluído (ações) para a cooperativa, que monitora suas contribuições. A cooperativa combina essas ações para resolver coletivamente o quebra-cabeça do bloco, aumentando a eficiência.

Os proprietários da cooperativa decidem quais transações priorizar – falaremos mais sobre isso mais tarde – coletam taxas (normalmente de 1-3% das recompensas) e determinam as estruturas de pagamento. Os pagamentos geralmente seguem modelos proporcionais ou pay-per-share (PPS), recompensando os mineradores com base na sua contribuição. Cooperativas de mineração são melhores do que minerar sozinho para a maioria, pois oferecem ganhos mais consistentes, mesmo que menores, reduzindo a volatilidade de esperar pela recompensa de um bloco solo.



# O QUE É UM MODELO DE BLOCO?

Um modelo de bloco de Bitcoin é uma planta criada pelas cooperativas de mineração que define quais transações incluir em um novo bloco. O operador da cooperativa tem um controle significativo, já que eles selecionam quais transações priorizar ou excluir. Operadores podem aceitar "subornos" na forma de taxas de transação privadas (via pagamentos fora da rede) para contornar ou incluir transações específicas, potencialmente minando a neutralidade da rede.



Disposição básica da conexão de um ASIC a uma cooperativa de mineração.

A maioria das cooperativas de mineração usa softwares como o [Stratum](#) ou protocolos similares para distribuir modelos de bloco e gerenciar a comunicação com os mineradores. Geralmente, quanto maior a taxa, maior a probabilidade de uma transação ser incluída. Esse método confere aos operadores das cooperativas demasiado poder, destacando a importância da descentralização e de práticas éticas para manter a justiça na rede.

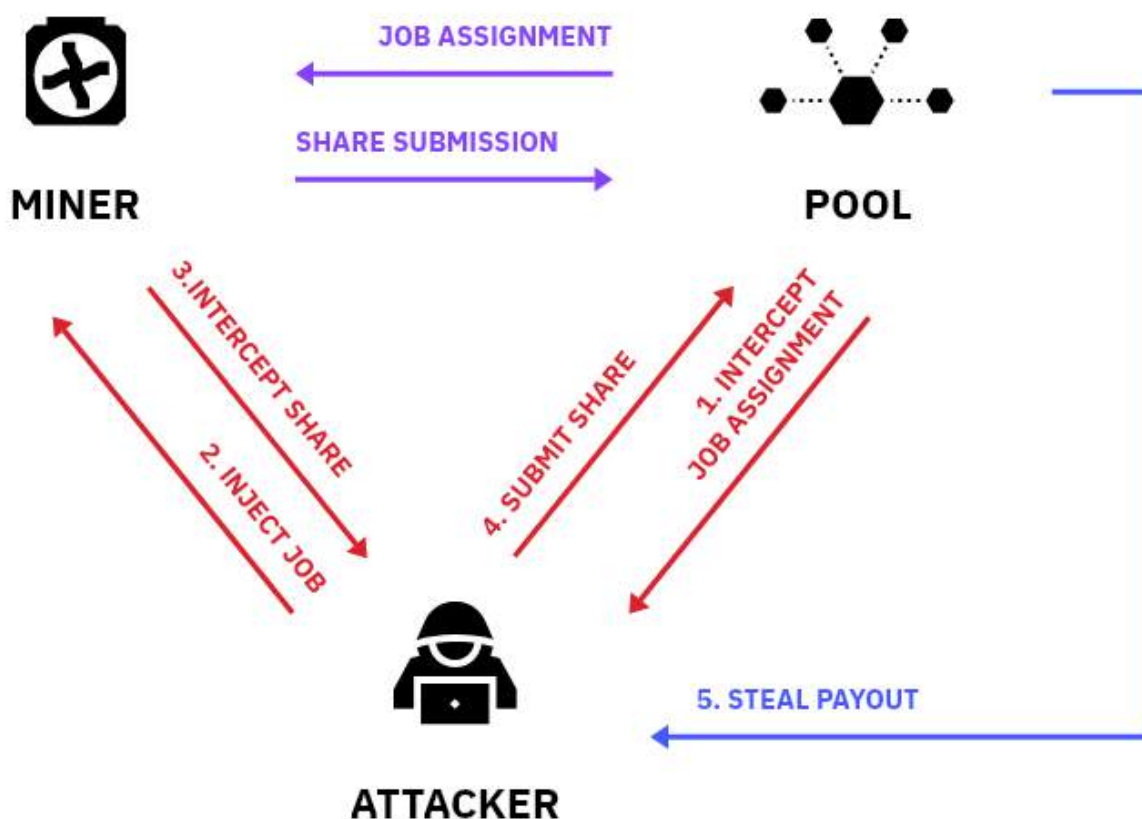
# O QUE É MINERAÇÃO COMBINADA?

A mineração combinada permite que os mineradores validem duas ou mais redes de blockchain simultaneamente usando o mesmo trabalho computacional. Nesse processo, os mineradores criam um bloco para a blockchain principal e reutilizam o hash de prova de trabalho (PoW) para garantir uma cadeia auxiliar (por exemplo, Namecoin). A cooperativa de mineração atua como intermediária, combinando as contribuições dos mineradores e submetendo ações válidas para ambas as cadeias, simplificando a coordenação.

Ao minerar, se um hash atende à dificuldade da cadeia auxiliar, mas não da cadeia principal, ele ainda pode ser submetido como um bloco válido para a cadeia auxiliar, obtendo benefícios duplos do mesmo trabalho computacional. Embora seja eficiente em termos de energia, a mineração combinada requer configuração adicional e uma complexidade técnica aumentada. Cadeias como Dogecoin utilizam Scrypt, mas não podem compartilhar trabalho com o Bitcoin a menos que exista uma blockchain auxiliar compatível.

# COMO O STRATUM V2 MELHORA A MINERAÇÃO?

O Stratum v1 é suscetível a ataques de homem no meio, particularmente através do 'roubo de hashrate', onde atacantes podem interceptar e mal usar dados de prova de trabalho. O [Stratum v2](#) melhora a mineração de Bitcoin ao reduzir ineficiências na comunicação entre mineradores e cooperativas e ao aprimorar a segurança, impactando positivamente a velocidade e o desempenho das operações de mineração.



Vetor de ataque conhecido como 'roubo de hashrate'

Em vez de depender das cooperativas de mineração para ditar os modelos de bloco, os mineradores podem executar softwares locais para selecionar os seus próprios, aumentando a descentralização e dando aos mineradores mais controle sobre quais transações são incluídas nos blocos. Embora não incentive diretamente mineradores individuais a ingressarem em cooperativas, o protocolo torna mais atraente participar de configurações de mineração cooperativa, especialmente para aqueles com recursos limitados ou operações menores.



## DATA CENTER VS. MINERAÇÃO INDIVIDUAL

Os Data Centers geralmente se beneficiam do acesso a melhores fontes de energia, especialmente em locais remotos onde a energia poderia ter sido previamente desperdiçada ou subutilizada, como próximo a hidrelétricas ou parques eólicos, o que pode reduzir significativamente os custos operacionais.

A clareza regulatória em algumas regiões oferece um ambiente legal mais estável para operações de mineração, diminuindo o risco operacional. Além disso, os Data Centers oferecem gerenciamento profissional, incluindo manutenção, segurança e conectividade, garantindo maior tempo de atividade e eficiência. Além disso, os Data Centers podem aproveitar economias de escala, facilitando a gestão e atualização de equipamentos.

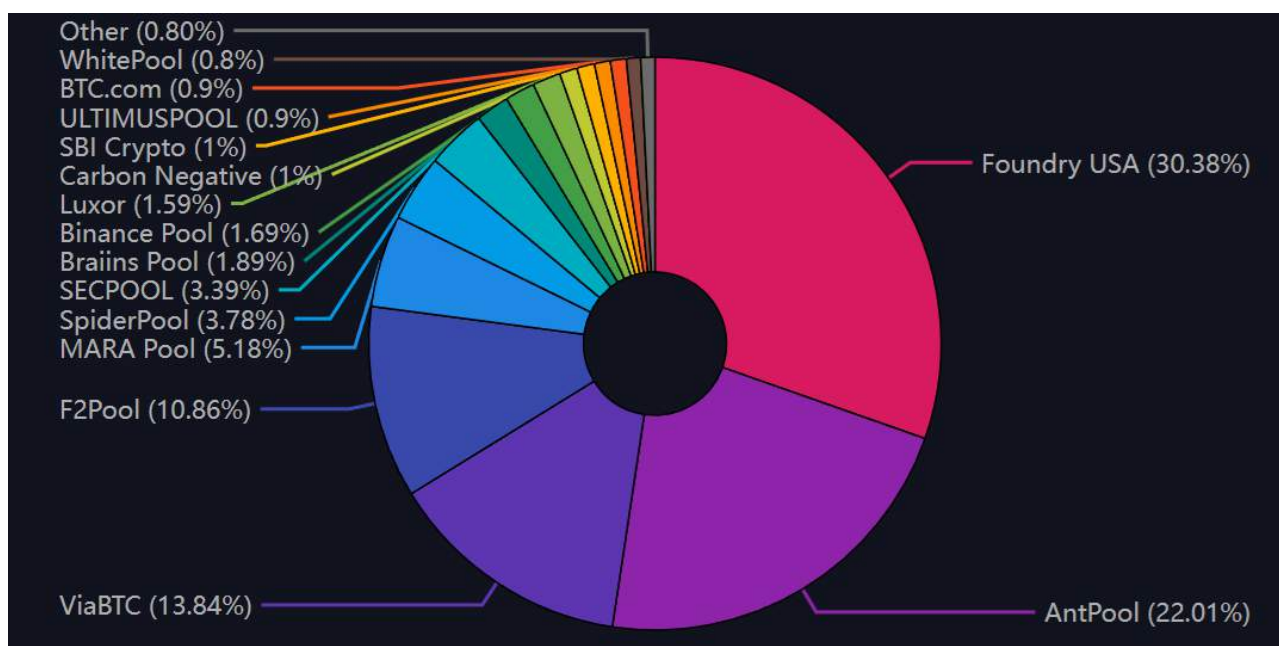
## OS FABRICANTES DE ASIC REPRESENTAM UM RISCO?

A diminuição no número de fornecedores de máquinas ASIC pode ser atribuída à consolidação do mercado, altas barreiras de entrada e à complexidade da fabricação. Tal concentração pode representar um risco em termos de segurança da cadeia de suprimentos e potencial formação de duopólios. No entanto, o aspecto de software pode ser mitigado ao reescrever todo o sistema operacional e software para eliminar a maioria das portas dos fundos conhecidas, aumentando a segurança.

Ainda assim, o risco de vulnerabilidades de hardware desconhecidas persiste. Para lidar com isso, pode-se empregar monitoramento através de ferramentas como softwares de análise de firmware ou módulos de segurança de hardware (HSMs), que detectam comportamentos incomuns no chip ou tentativas de acesso não autorizado, podendo assim identificar novos tipos de ataques baseados em hardware.

# A MINERAÇÃO DE BITCOIN É CENTRALIZADA?

Atualmente, a mineração de Bitcoin realmente exibe centralização, com poucas grandes cooperativas controlando uma porção significativa do hashrate da rede. No entanto, essa centralização é mitigada pelo potencial de migração para protocolos como o Stratum v2, que devolve a seleção de transações aos mineradores individuais, reduzindo a influência dos operadores de cooperativas.



Ranking semanal das cooperativas de mineração de BTC em 27 de novembro.

O preço do Bitcoin acima de \$90 mil incentiva a mineração doméstica com chips ASIC reutilizados, exemplificado por dispositivos como o BitAxe, tornando a mineração acessível a operadores menores. Essa tendência sugere que, embora haja concentração de hashrate em algumas cooperativas, a dinâmica subjacente está mudando para uma maior descentralização, à medida que os mineradores individuais ganham mais autonomia.

# MINERAÇÃO DE BITCOIN É UM NEGÓCIO LUCRATIVO?

A mineração de Bitcoin pode de fato ser lucrativa, especialmente com o preço acima de \$90 mil, dado os preços de energia favoráveis que mineradores de médio a grande porte conseguem. No entanto, o setor enfrenta desafios como o aumento da competição. Mais mineradores entram no mercado, aumentando a dificuldade de mineração e comprimindo margens de lucro.

A configuração de operações de mineração envolve um capital inicial significativo para hardware, infraestrutura e soluções de energia. Embora esses fatores signifiquem que não há 'dinheiro fácil', mineradores com vantagens competitivas como custos operacionais mais baixos, acesso a fontes de energia renovável ou desperdiçada, e tecnologia eficiente podem continuar a ser lucrativos mesmo durante quedas de mercado ou quando os custos de capital aumentam.

## RECOMENDAÇÃO

### State of Stratum V2 | Plan B Forum 2023 | Lugano (inglês)

State of Stratum V2 com Kristian Csepсар.



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

# SOBRE NÓS

Santacroce Tech é uma empresa dedicada à tecnologia blockchain, com foco em escalabilidade e descentralização. Estamos ativamente envolvidos no desenvolvimento open source ao redor do Bitcoin, contribuindo para iniciativas como o Stratum V2 e o Drivechain, que visam aprimorar a eficiência, flexibilidade e inovação no ecossistema.

Nossa expertise é reforçada por décadas de atuação na indústria tecnológica e por relacionamentos consolidados no setor. Participamos ativamente de iniciativas como o Bitcoin Center NY e contribuímos para projetos de destaque, como o BRZ, a primeira stablecoin brasileira, e o Alkimiya, focado na tokenização de fluxos financeiros ligados à mineração de criptomoedas.

Essas experiências nos posicionam como parceiros estratégicos, capacitados a oferecer insights valiosos e a atuar como conselheiros para equipes executivas em decisões tecnológicas críticas.

## CONTATO



Conte com o conteúdo da Santacroce Tech para guiá-lo através da dinâmica indústria de ativos digitais e blockchain. Inscreva-se agora para receber insights valiosos! Para contatos comerciais ou perguntas gerais: [info@santacroce.xyz](mailto:info@santacroce.xyz)

===== bloco 872,257 =====