BRAIINS

Stratum V2 general overview

Daniela Brozzoni - Satoshi Spritz Live

A bit of history

- **getwork protocol**
  - First mining protocol
  - JSON-RPC method sent over a HTTP transport
  - Replaced by getblocktemplate RPC call
  - Used in solo mining

- **Stratum**
  - Developed by the creator of SlushPool, Marek "Slush" Palatinus
  - Used in pool mining
    - Miners didn’t get to decide which txs to include in blocks
  - JSON format
  - Messages between the pool and the miners are not encrypted

A bit of history

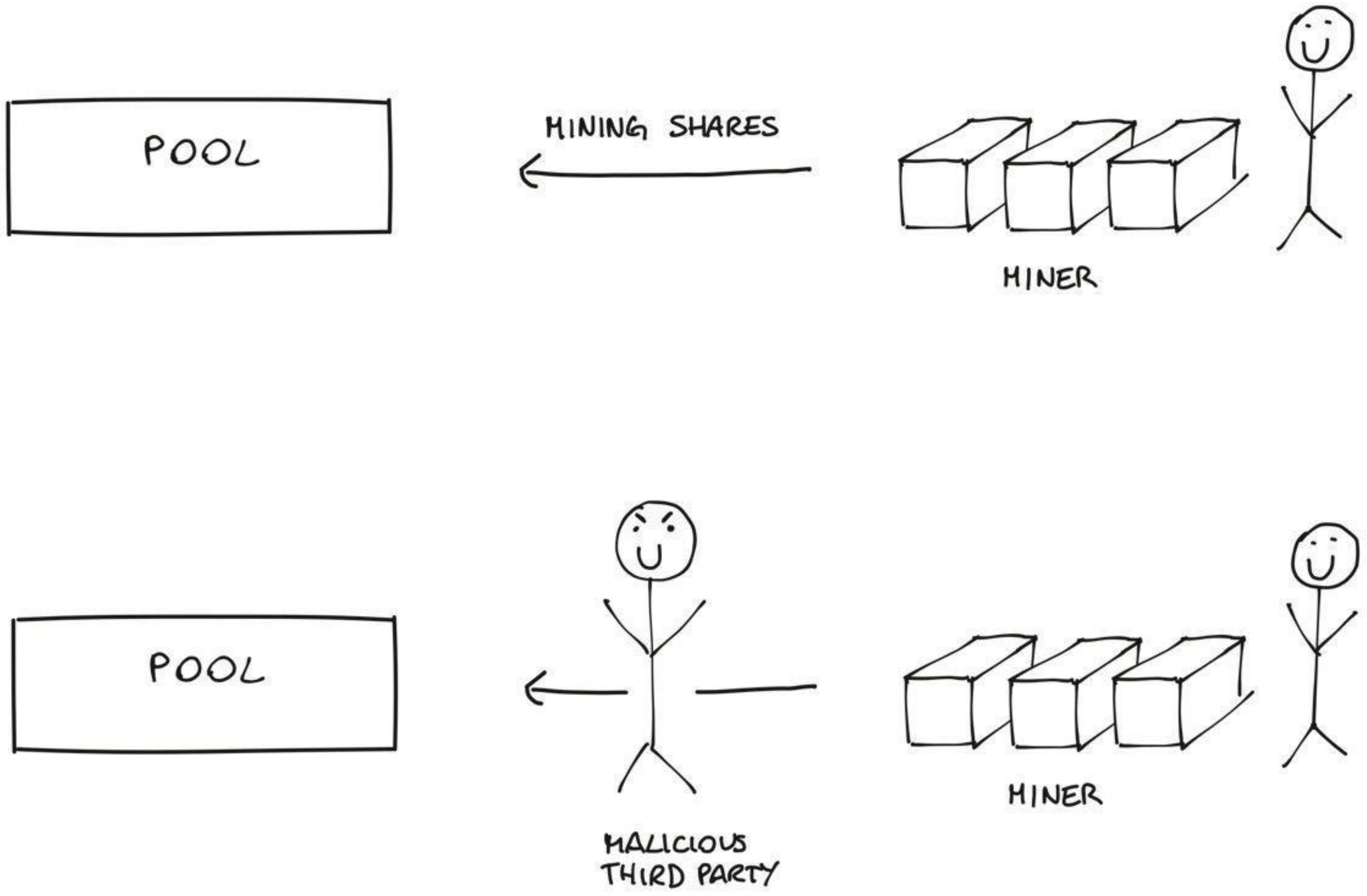
- **BetterHash**
  - Presented by Matt Corallo in 2018
  - Miners have the ability to construct their own block templates
  - Difficult to implement on the pool side

- **Stratum V2**
  - Introduced in November 2019 by Pavel Moravec, Jan Čapek, Matt Corallo
  - Adopts BetterHash idea for job distribution

Main improvements with Stratum V2

- Prevents man-in-the-middle attacks
- Reduces bandwidth consumption
- Improves decentralization
- Improves job distribution latency

Prevents man in the middle attacks



BRAIINS

Prevents man in the middle attacks

- **In V1 messages are exchanged in plaintext**
  - Privacy leaks
  - Hashrate hijacking attack

- **Stratum V2 uses AEAD encryption scheme**
  - Provides confidentiality and integrity for the messages exchanged between pools/proxies and miners

Reduces bandwidth consumption

- **Completely binary instead of JSON-based**
- **Eliminates some redundant messages**
- **Size of a share submission message:**
  - V2: 32 bytes without encryption, 48 with encryption
  - V1: ~100 bytes

Improves decentralization

- **In V1 miners didn’t choose the transactions to include in blocks**
  - A pool could decide to censor certain transactions!
  - Signaling

- **Optional in Stratum V2: Job negotiation protocol**
  - Miners can choose the jobs to work on, then send them to the pool to validate that they are well constructed

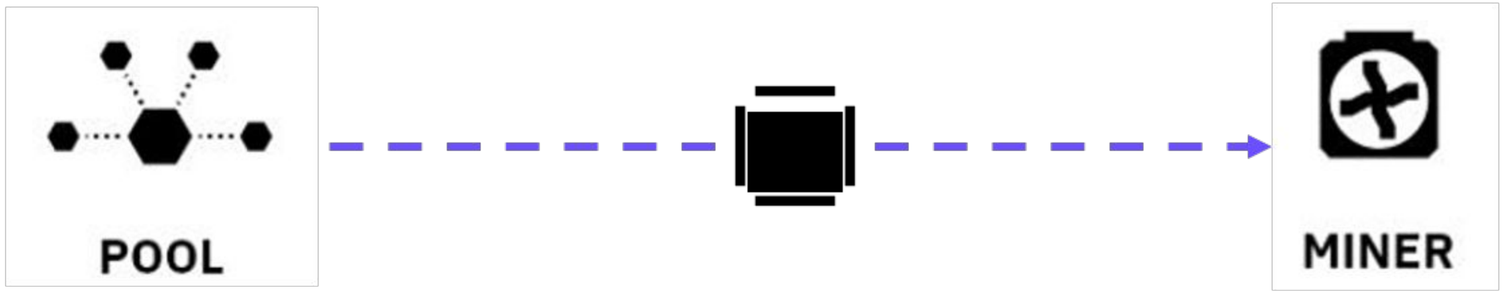
- **In V2 miners submit their own blocks**

Improve job distribution latency

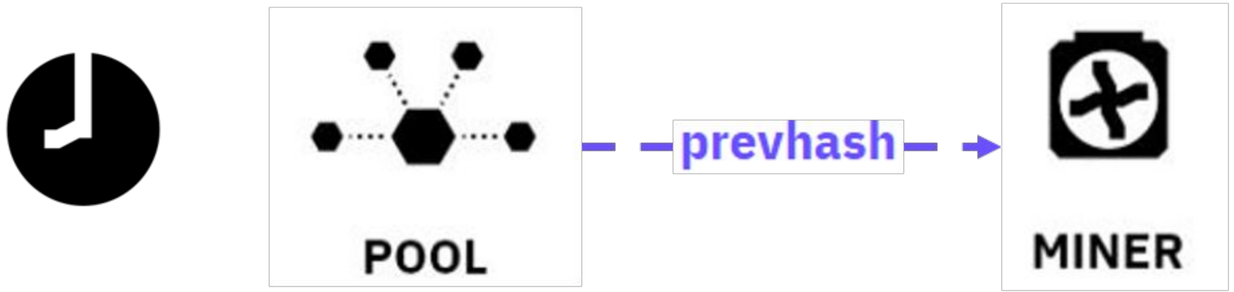
- **When a block is found, pools need to send new jobs to the miners to work on**
  - It has to be quick: miners don’t want to waste time working on the previous block!
  - In V1, the new job message included the prevhash and the merkle path from the coinbase
    - The full merkle path is needed if you manipulate the coinbase to enlarge your search space
    - Incentive to send empty blocks
  - In V2, merkle path message and prevhash are sent separately

Improve job distribution latency

1. Send full block template(s) before the previous block has been found



2. Send the prevhash message separately after a block has been found



BRAIINS

Questions?

BRAINS