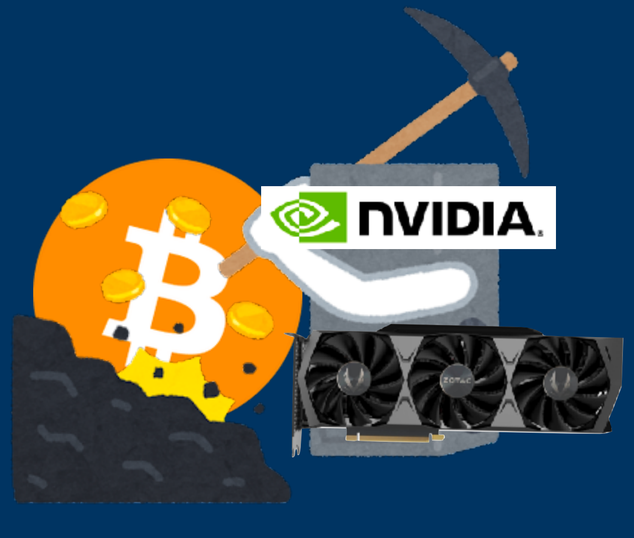
WIP

# Implement Bitcoin Miner with CUDA

Bcali B2 kekeho

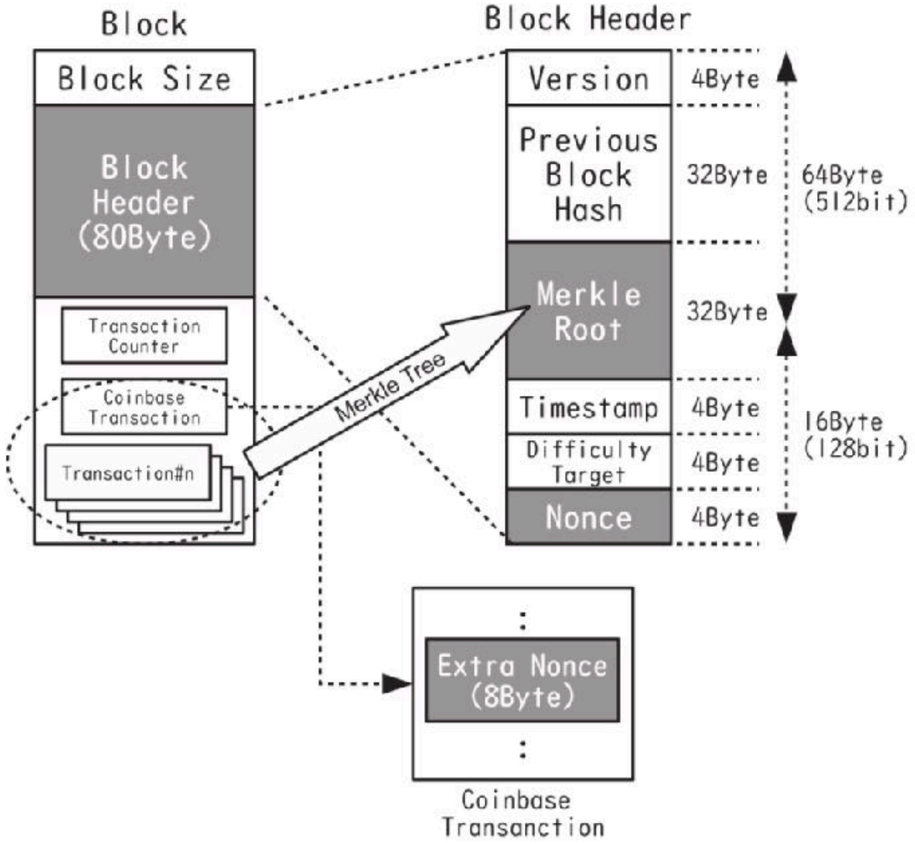
2022/07/14　kumo+bcali WIP



# How to mine bitcoin?

## Proof of Work

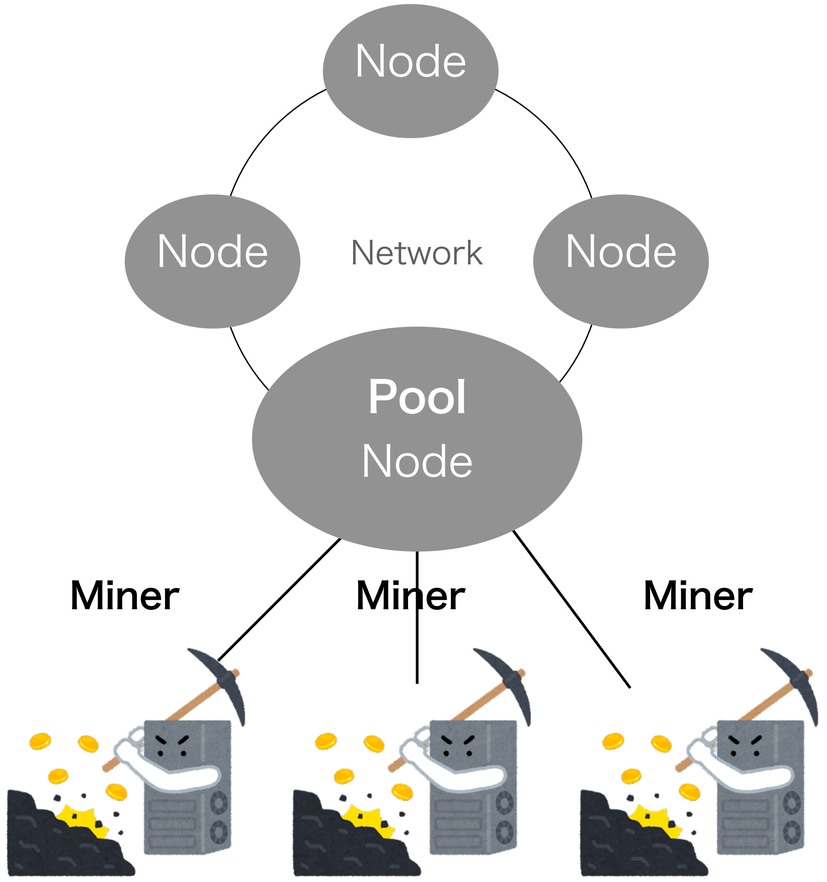
- sha256d(Block Header) < difficulty target
- Create a header that satisfies the above conditions by **trying various nonce fields of Block Header in a brute force**.




画像出典: FPGAx仮想通貨 ～FPGAで仮想通貨マイニング BOSUKE

# Mining Pool

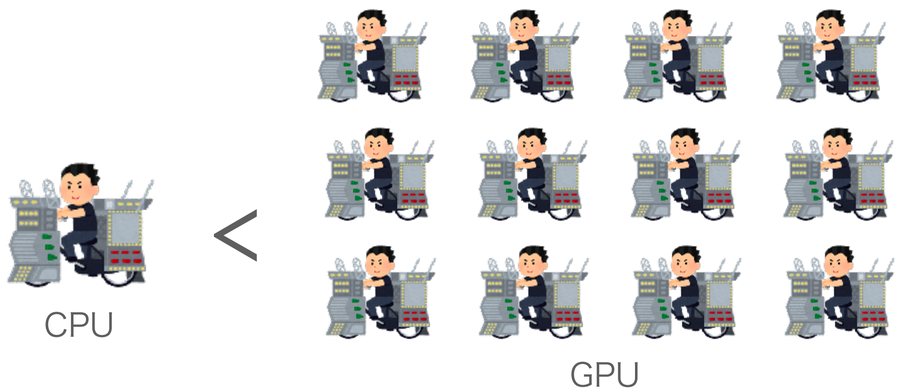
- Nowadays, **It is difficult to mine alone** because difficulty is too high
  - It looks like lottery
    In personal-level computer resources, you have to be very lucky to find them.
- So, **mining pools** are used to mine with the cooperation of several miner.
  - If someone in the pool finds it, each minor gets a modest reward based on the amount of work done.



# CUDA

- The more cores, the more nonce attempts
  - It can run many sha256 in parallel!
- My GPU: RTX 3090
  **10496 core**, 24GB memory
  - It can run sha256 x 10496 in parallel
  - I bought this gpu for Machine Learning, but I'll use it for mining

自宅のRTX 3090😎

# CUDA

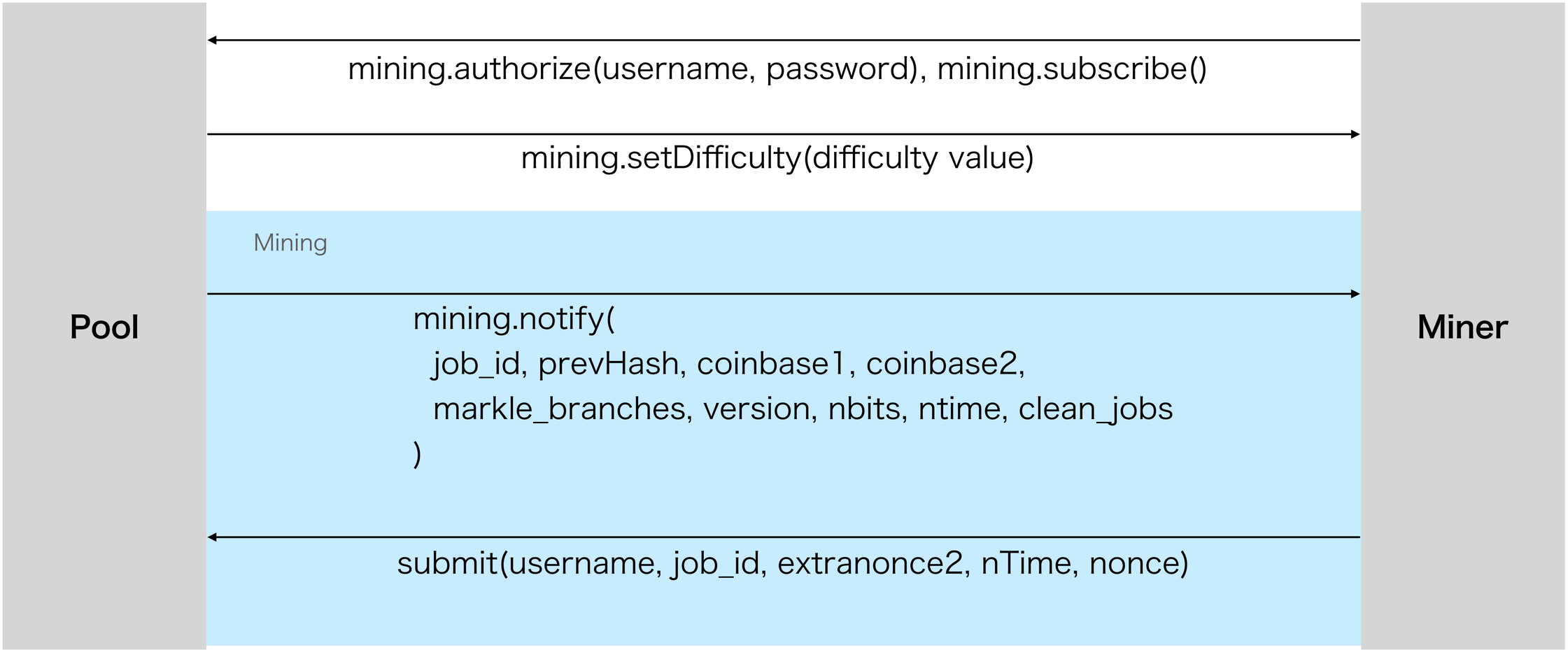
- **GPGPU**: General-Purpose computing on GPU
- **CUDA**: Platform for GPGPU provided by NVIDIA
- Functions written in C-lang can be executed in parallel on NVIDIA GPUs.

# Stratum Mining Protocol

- **Protocol for communication between pools and miners**
- Communication over TCP sockets, using JSON-RPC
  - RPC: Remote Procedure Call
- Send the method name and arguments to be called in JSON

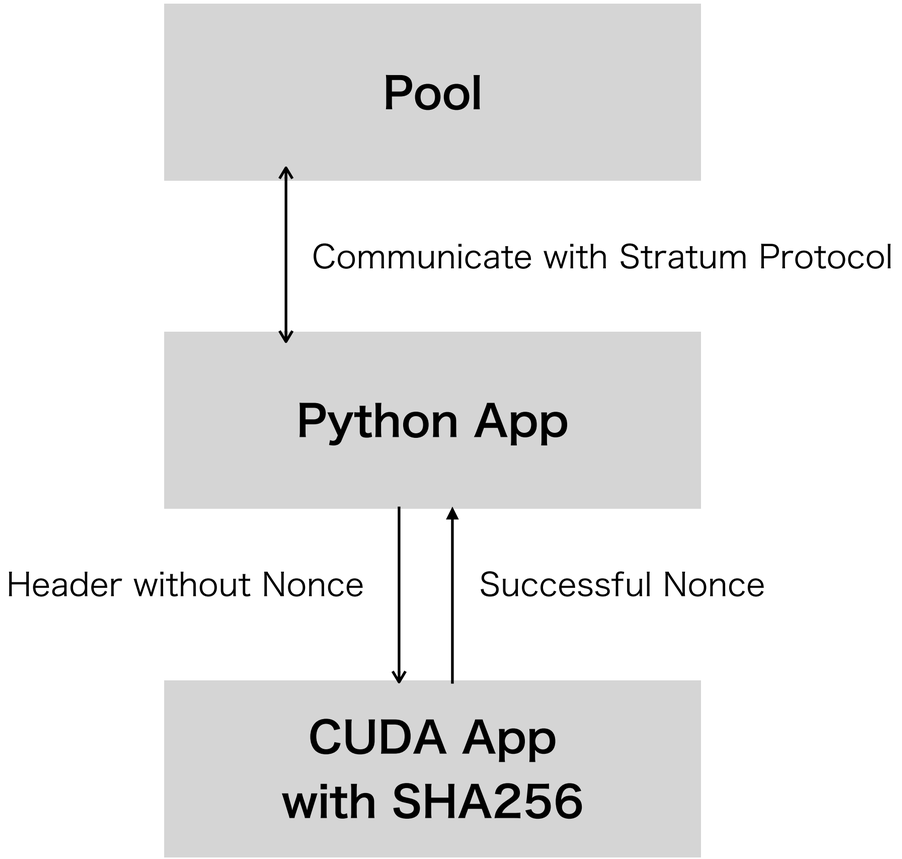
# Stratum Mining Protocol

## Protocol Details



# Implement

- Communication with Pool is implemented in Python
- Hash calculation part is implemented in CUDA
- I just finished the implementation. Evaluation is not yet...



# My thoughts

- It was fun!
- Stratum protocol is a plaintext communication, so I would like to try the Man in the Middle attack.
- I would learn Stratum V2 Protocol which use Noise protocol for encryption
- (I thought Pool is a centralized point, which is not good.)

# References


- S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf
- braiins, Stratum v1 docs — mining protocol, https://braiins.com/stratum-v1/docs
- braiins, Stratum v2 — the next generation protocol for pooled mining, https://braiins.com/stratum-v2