Module 3: Bitcoin Mining

Aron Kondoro & Anthony Kigombola

Contents

- Overview of mining
- Mining vs Forging
- Design of a mining rig
- Problem of centralization
- Recent 51% attacks
- Hands-on: mining on a blockchain

Overview

- It is the mechanism to control and enable changes in blockchains
- In Bitcoin they use computing power to solve calculations
- Mining process
  - Grouping transactions
  - Validation
  - Spreading across network for validation by other nodes
  - If other nodes validate, they add in their ledgers
  - Once more than 50% verify blocks become permanent and irreversible
  - Miner who solved the puzzle receives reward/fee
- Validity depends on consensus

Transaction Confirmation

Transaction confirmation takes time (10 minutes in case of Bitcoin)

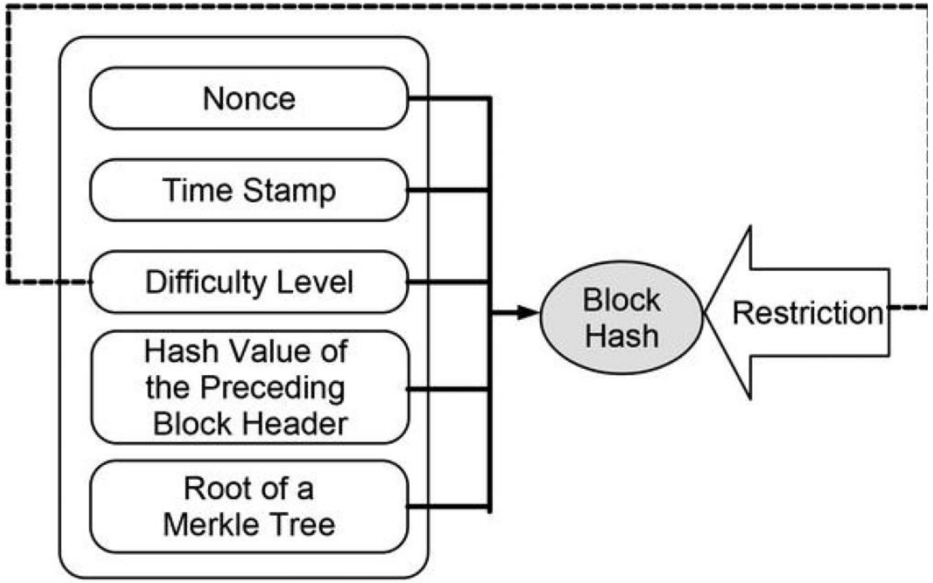
1. Transaction message is broadcasted
2. Miner selects batch of unconfirmed transactions (10,000 in case of Bitcoin)
3. Miner confirms validity i.e. sender has enough bitcoins
4. Miner groups them as one block
5. Miner broadcasts block back to the network
6. Other nodes add block to local database
7. Miners get rewarded i.e. in Bitcoin they get mining reward (pre-set number of new coins & transaction fees)

Validation Rules

- Transaction Data
  - Formal correctness: transaction contains all required data
  - Semantic correctness: transacation has meaning i.e. user has enough bitcoins
  - Authorization: signed by the owner
- Block Headers

Validation Rules

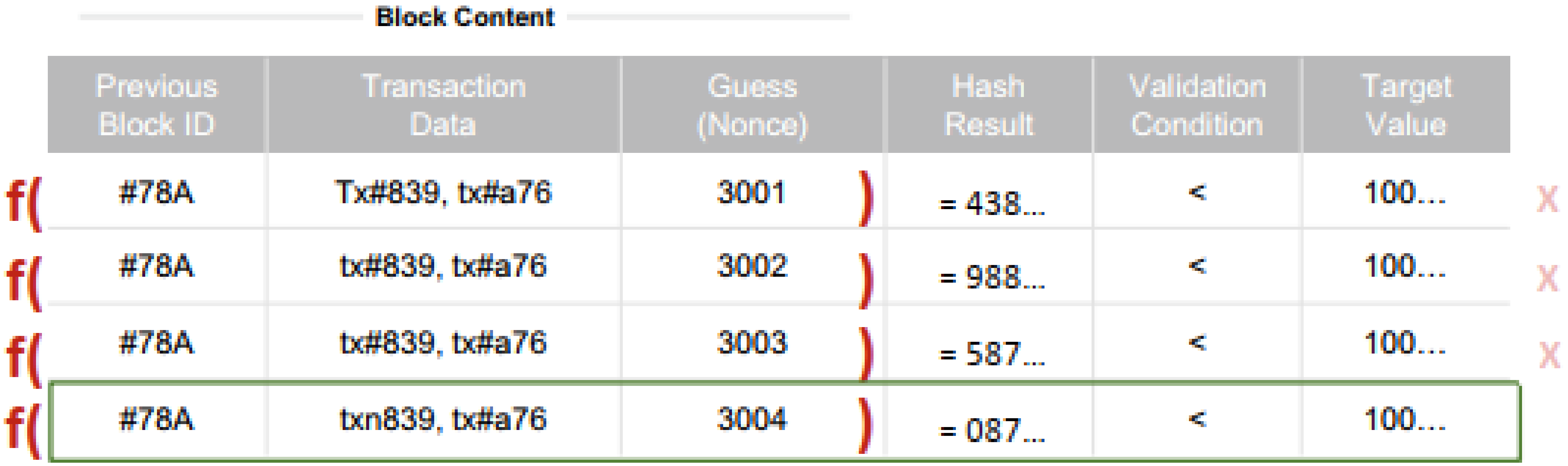
- Block Headers
  - Contain valid hash of previous block
  - Contain valid root of Merkle tree
  - Contain correct difficulty
  - Timestamp is after previous block
  - Contains a nonce
  - Hash value of all satisfy the difficulty level



Mining Process

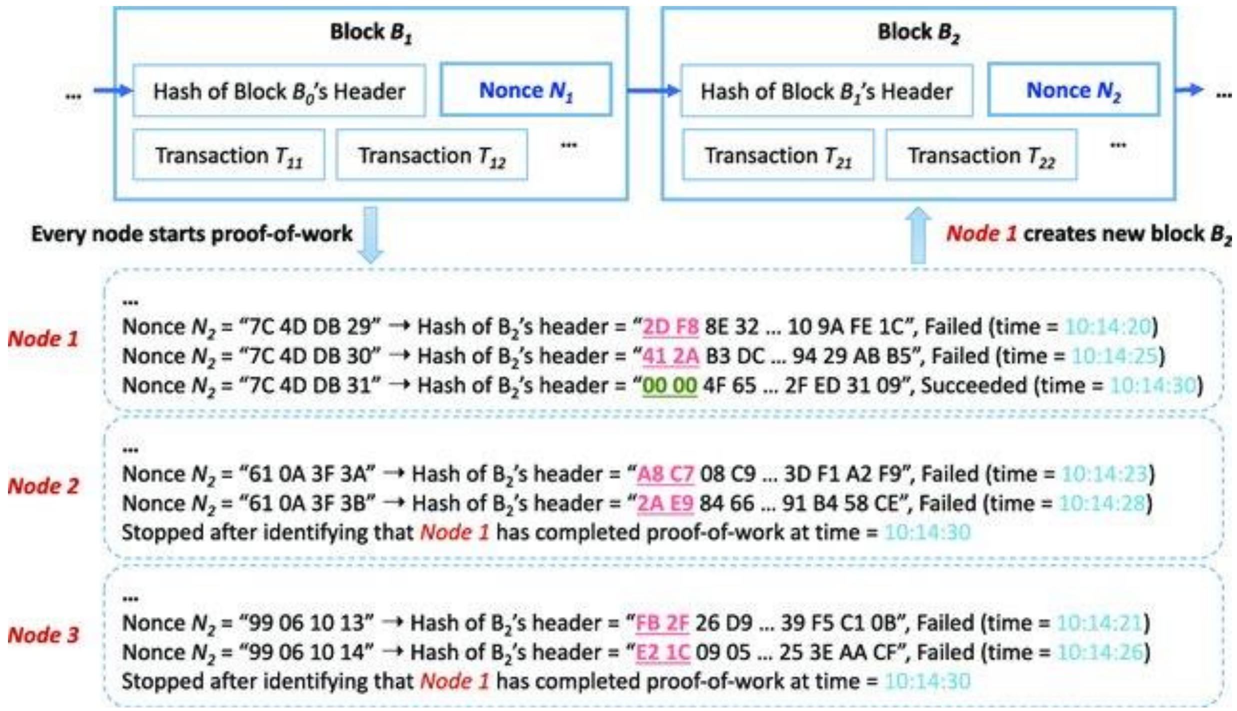
- Any node can be a miner
- Miners are the critical component that enforce the rules of the network
- Miners invest in computing capacity to perform validation
- Bitcoin uses Proof-of-Work (PoW) where they solve cryptographic challenges
- Difficulty of this puzzle changes proportional to the amount of computer power

Hash Validation



	Block Content							
	Previous Block ID	Transaction Data	Guess (Nonce)		Hash Result	Validation Condition	Target Value	
f(	#78A	Tx#839, tx#a76	3001	)	= 438...	<	100...	X
f(	#78A	tx#839, tx#a76	3002	)	= 988...	<	100...	X
f(	#78A	tx#839, tx#a76	3003	)	= 587...	<	100...	X
f(	#78A	txn839, tx#a76	3004	)	= 087...	<	100...	

The Nonce



Node 1

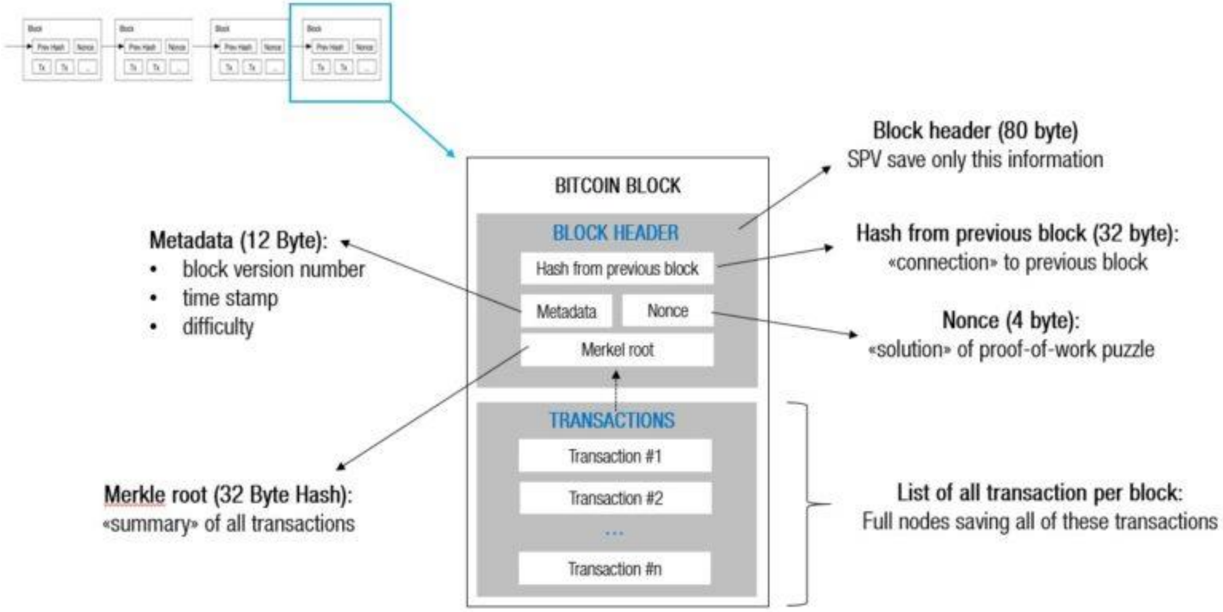
...
Nonce N_2 = "7C 4D DB 29" → Hash of B_2's header = "2D F8 8E 32 ... 10 9A FE 1C", Failed (time = 10:14:20)
Nonce N_2 = "7C 4D DB 30" → Hash of B_2's header = "41 2A B3 DC ... 94 29 AB B5", Failed (time = 10:14:25)
Nonce N_2 = "7C 4D DB 31" → Hash of B_2's header = "00 00 4F 65 ... 2F ED 31 09", Succeeded (time = 10:14:30)

Node 2

...
Nonce N_2 = "61 0A 3F 3A" → Hash of B_2's header = "A8 C7 08 C9 ... 3D F1 A2 F9", Failed (time = 10:14:23)
Nonce N_2 = "61 0A 3F 3B" → Hash of B_2's header = "2A E9 84 66 ... 91 B4 58 CE", Failed (time = 10:14:28)
Stopped after identifying that *Node 1* has completed proof-of-work at time = 10:14:30

Node 3

...
Nonce N_2 = "99 06 10 13" → Hash of B_2's header = "FB 2F 26 D9 ... 39 F5 C1 0B", Failed (time = 10:14:21)
Nonce N_2 = "99 06 10 14" → Hash of B_2's header = "E2 1C 09 05 ... 25 3E AA CF", Failed (time = 10:14:26)
Stopped after identifying that *Node 1* has completed proof-of-work at time = 10:14:30



Block header (80 byte)
SPV save only this information

Hash from previous block (32 byte):
«connection» to previous block

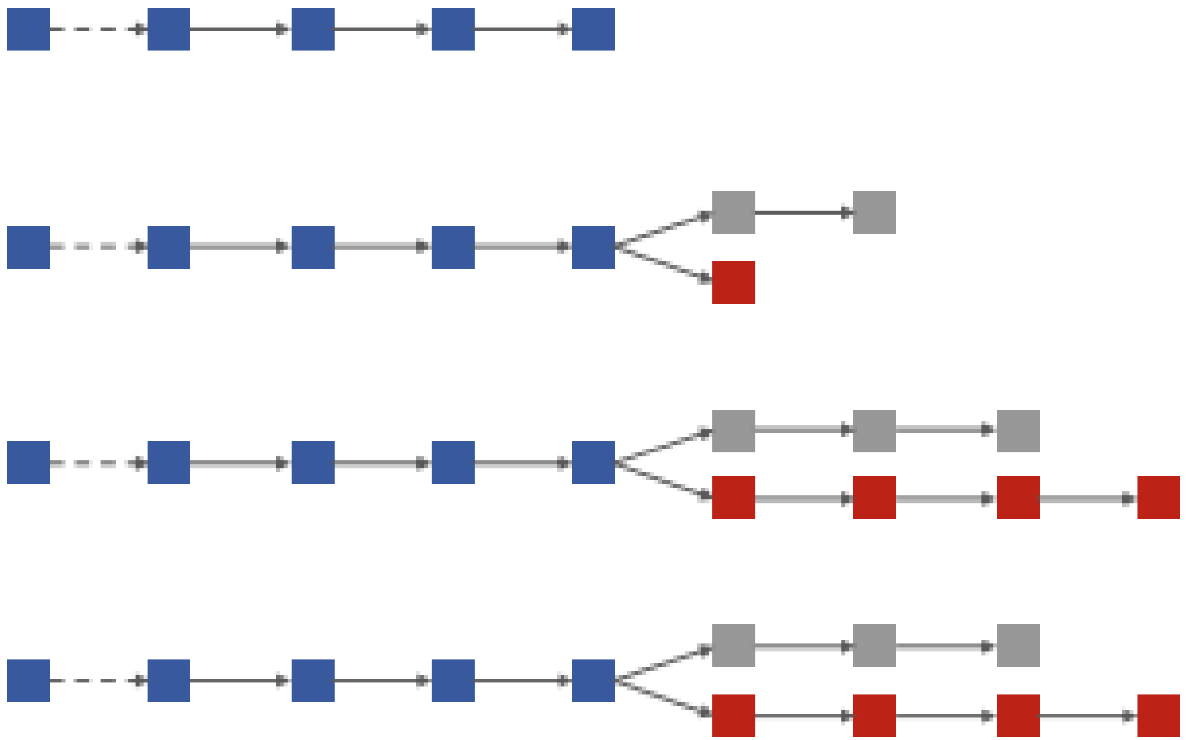
Nonce (4 byte):
«solution» of proof-of-work puzzle

List of all transaction per block:
Full nodes saving all of these transactions

Metadata (12 Byte):
- block version number
- time stamp
- difficulty

Merkle root (32 Byte Hash):
«summary» of all transactions

51% Attack



(a) Initial state of the blockchain in which all transactions are considered valid.

(b) Honest nodes continue to extend the valid chain by adding grey blocks, while the attacker secretly starts mining a fraudulent branch.

(c) The attacker succeeds in making the fraudulent branch longer than the honest one.

(d) The branch of the attacker is published and is now considered the valid one.

Mining Software

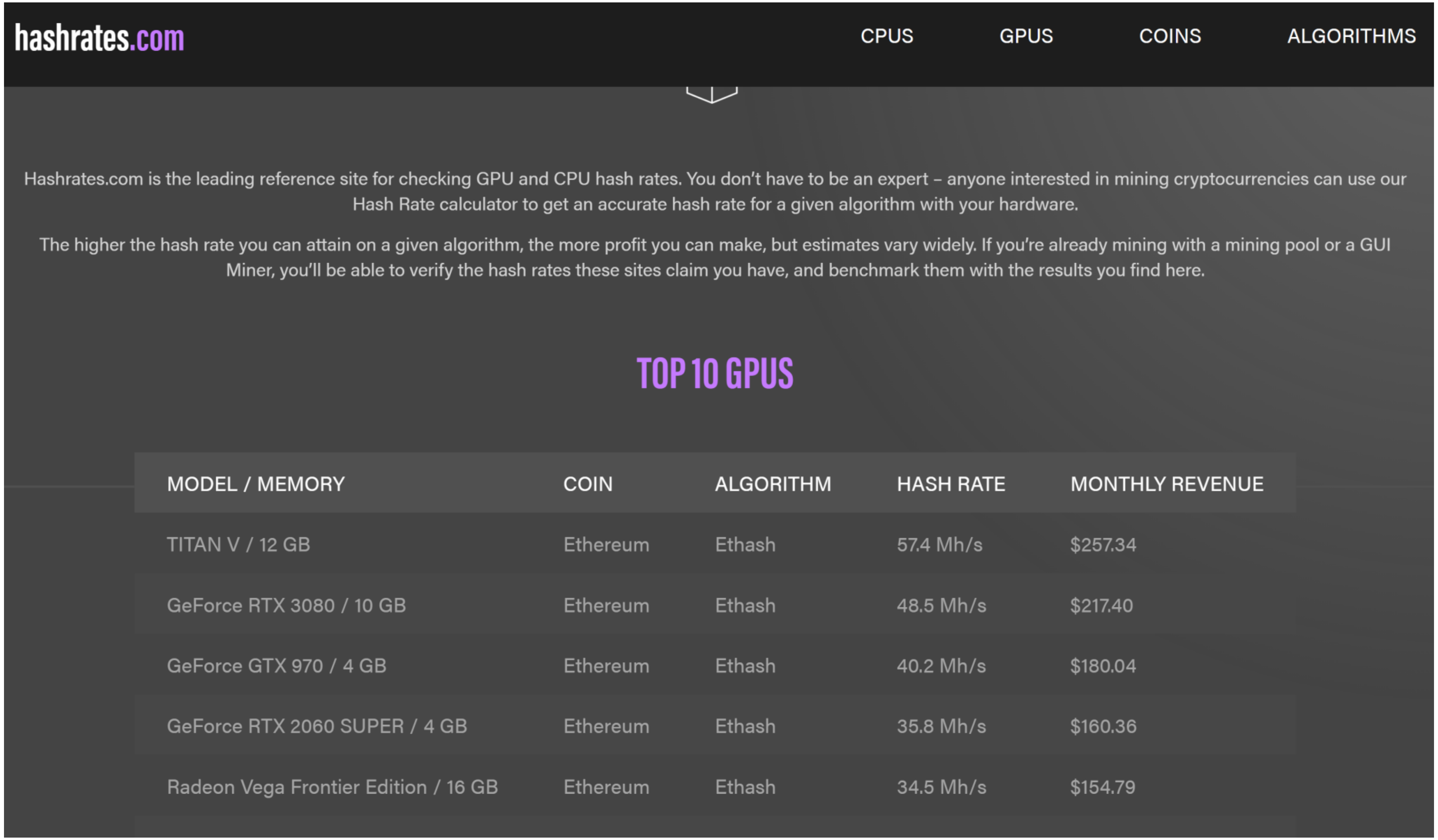
- Most are GPU and ASIC based
  - Ethminer - https://github.com/ethereum-mining/ethminer

- There are few CPU based for selected coins
  - CPU Miner - https://sourceforge.net/projects/cpuminer/
  - XMRig - https://github.com/xmrig/xmrig

Mining Hardware

- Companies
  - Bitmain
  - MicroBT
  - Canaan
- Components
  - GPU/ASIC
  - Power supply
  - Cooling fans
  - Backup generator

Hashrate and revenue calculation



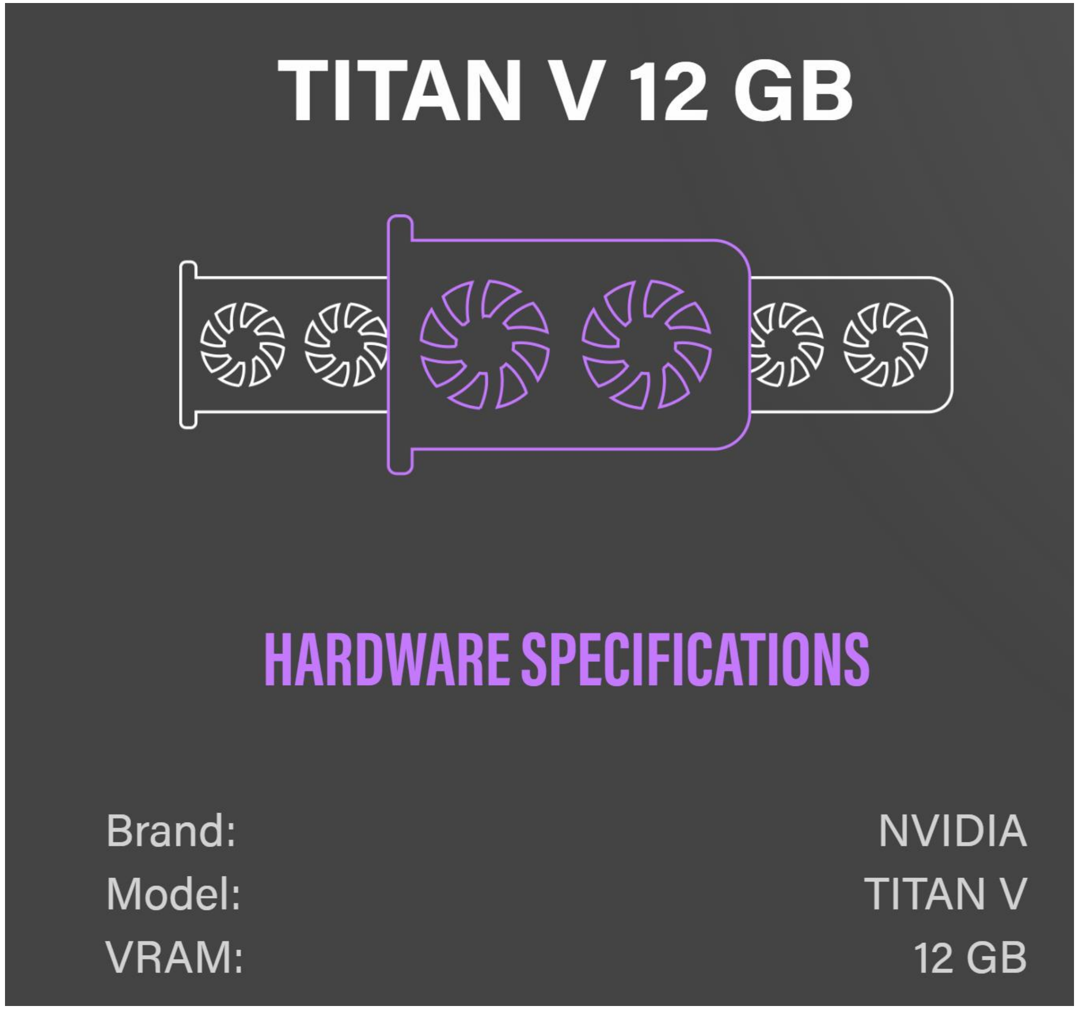
Hashrates.com is the leading reference site for checking GPU and CPU hash rates. You don't have to be an expert – anyone interested in mining cryptocurrencies can use our Hash Rate calculator to get an accurate hash rate for a given algorithm with your hardware.

The higher the hash rate you can attain on a given algorithm, the more profit you can make, but estimates vary widely. If you're already mining with a mining pool or a GUI Miner, you'll be able to verify the hash rates these sites claim you have, and benchmark them with the results you find here.

TOP 10 GPUS

MODEL / MEMORY	COIN	ALGORITHM	HASH RATE	MONTHLY REVENUE
TITAN V / 12 GB	Ethereum	Ethash	57.4 Mh/s	$257.34
GeForce RTX 3080 / 10 GB	Ethereum	Ethash	48.5 Mh/s	$217.40
GeForce GTX 970 / 4 GB	Ethereum	Ethash	40.2 Mh/s	$180.04
GeForce RTX 2060 SUPER / 4 GB	Ethereum	Ethash	35.8 Mh/s	$160.36
Radeon Vega Frontier Edition / 16 GB	Ethereum	Ethash	34.5 Mh/s	$154.79

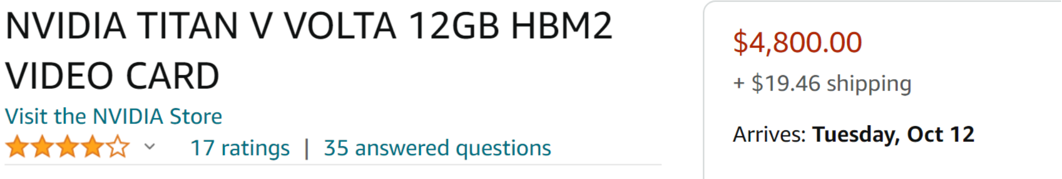
Example of top GPU



TITAN V 12 GB

HARDWARE SPECIFICATIONS

Brand:	NVIDIA
Model:	TITAN V
VRAM:	12 GB



NVIDIA TITAN V VOLTA 12GB HBM2 VIDEO CARD

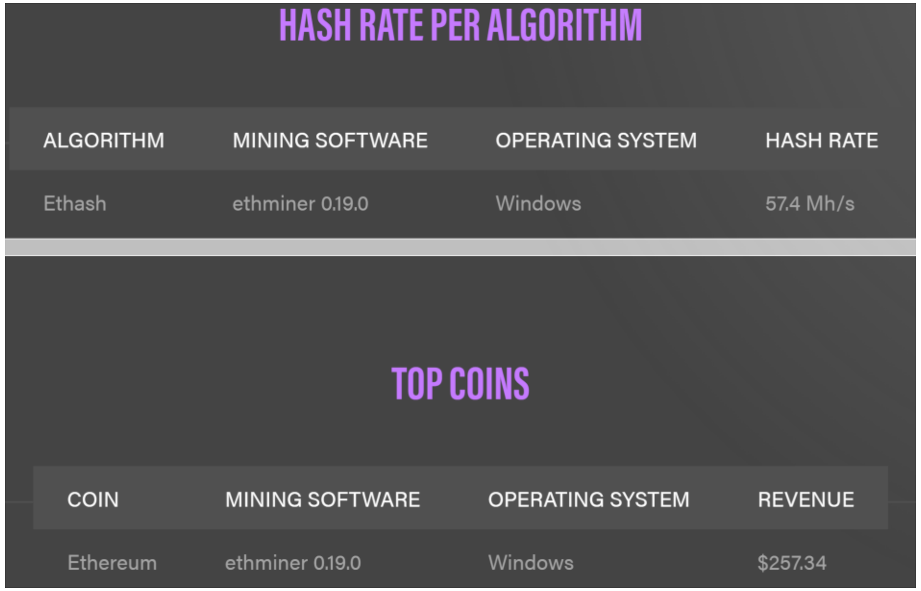
Visit the NVIDIA Store

★★★★☆ 17 ratings | 35 answered questions

$4,800.00

+ $19.46 shipping

Arrives: **Tuesday, Oct 12**



HASH RATE PER ALGORITHM

ALGORITHM	MINING SOFTWARE	OPERATING SYSTEM	HASH RATE
Ethash	ethminer 0.19.0	Windows	57.4 Mh/s

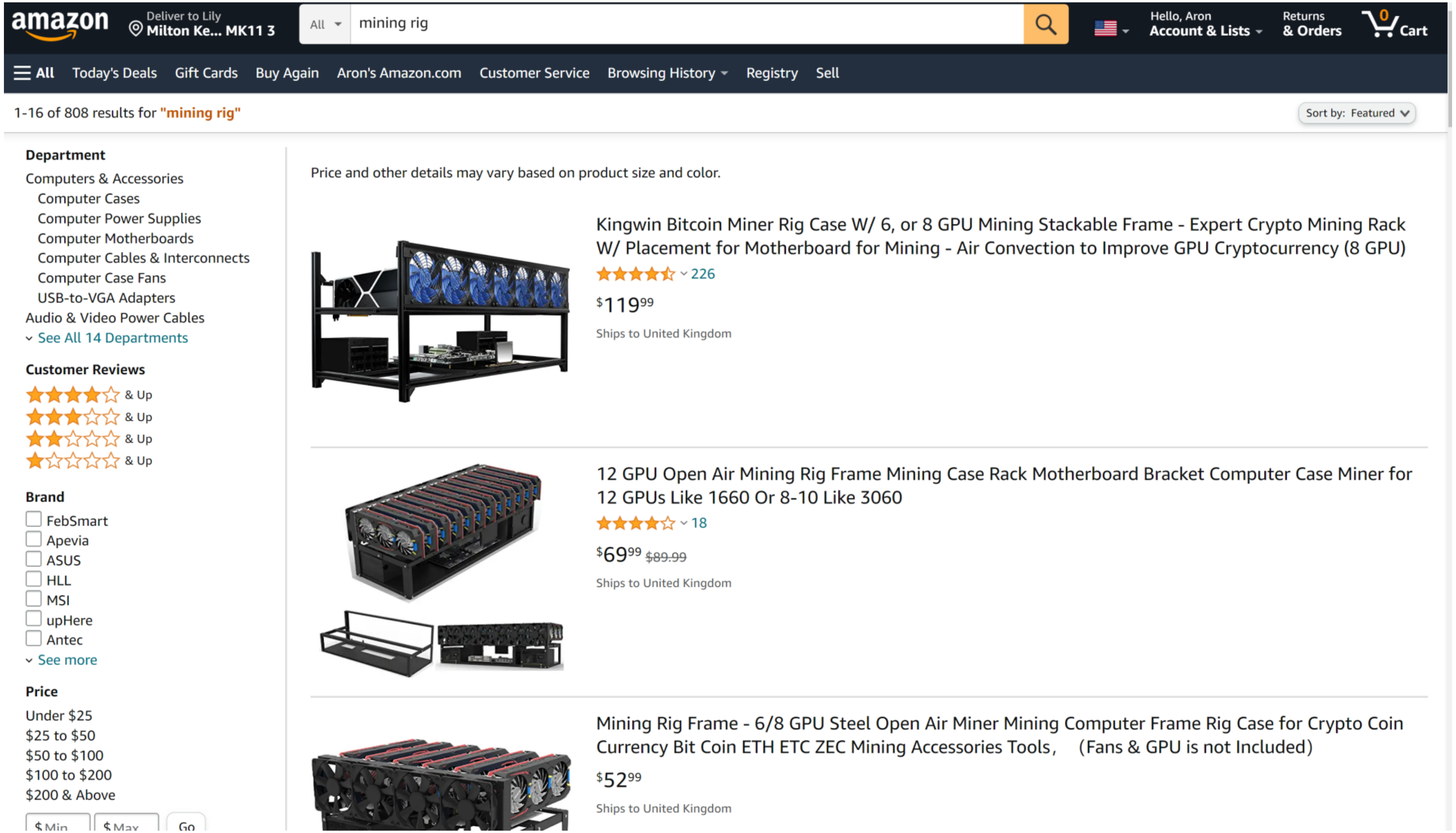
TOP COINS

COIN	MINING SOFTWARE	OPERATING SYSTEM	REVENUE
Ethereum	ethminer 0.19.0	Windows	$257.34

Mining Rigs

- Ethereum has proven to be the most profitable crypto to mine per wattage.
  - 8 AMD RX580's generate $20 per day before electricity.
- Typical Rig uses **1000 watts**

Mining rigs online



1-16 of 808 results for "mining rig"

Department

Computers & Accessories
Computer Cases
Computer Power Supplies
Computer Motherboards
Computer Cables & Interconnects
Computer Case Fans
USB-to-VGA Adapters
Audio & Video Power Cables
See All 14 Departments

Customer Reviews

★★★★☆ & Up
★★★☆☆ & Up
★★☆☆☆ & Up
★☆☆☆☆ & Up

Brand

☐ FebSmart
☐ Apevia
☐ ASUS
☐ HLL
☐ MSI
☐ upHere
☐ Antec
See more

Price

Under $25
$25 to $50
$50 to $100
$100 to $200
$200 & Above
$ Min $ Max Go

Price and other details may vary based on product size and color.

Kingwin Bitcoin Miner Rig Case W/ 6, or 8 GPU Mining Stackable Frame - Expert Crypto Mining Rack W/ Placement for Motherboard for Mining - Air Convection to Improve GPU Cryptocurrency (8 GPU)
★★★★☆ 226
$119.99
Ships to United Kingdom

12 GPU Open Air Mining Rig Frame Mining Case Rack Motherboard Bracket Computer Case Miner for 12 GPUs Like 1660 Or 8-10 Like 3060
★★★★☆ 18
$69.99 ~~$89.99~~
Ships to United Kingdom

Mining Rig Frame - 6/8 GPU Steel Open Air Miner Mining Computer Frame Rig Case for Crypto Coin Currency Bit Coin ETH ETC ZEC Mining Accessories Tools， (Fans & GPU is not Included)
$52.99
Ships to United Kingdom

Profitability

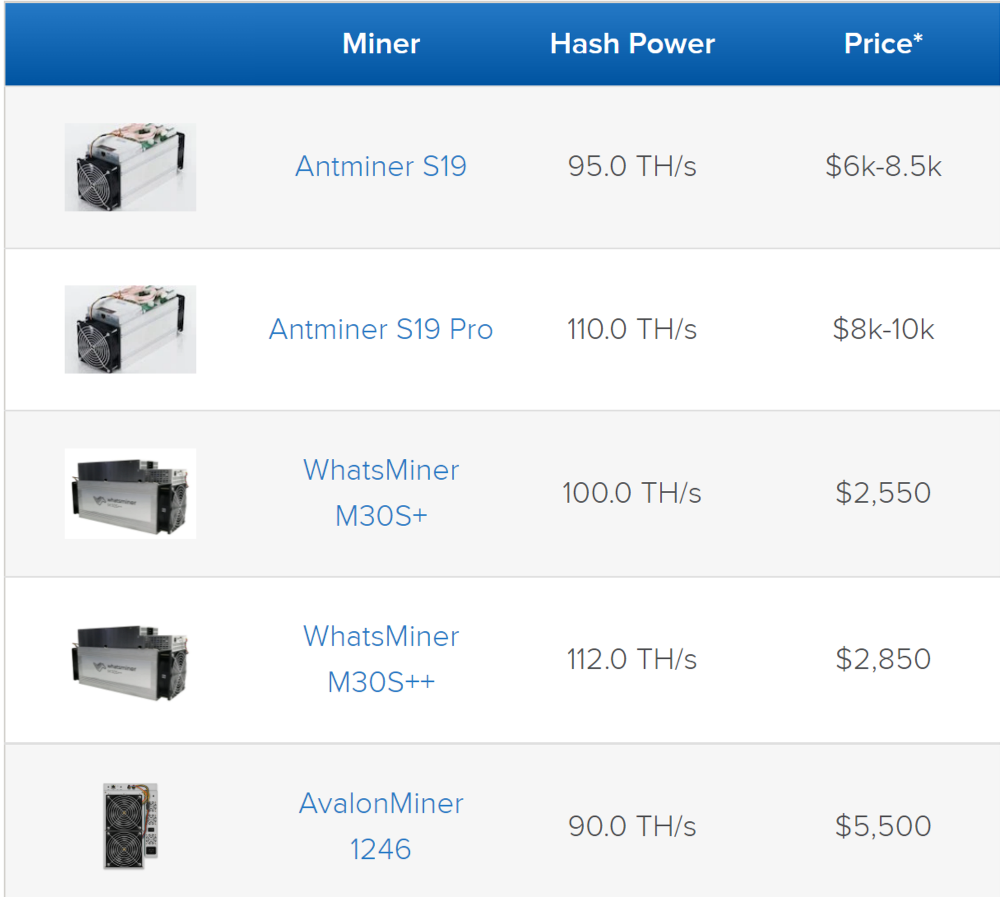
- Market price of the coin
  - High volatile
- Cost of electricity
  - Higher hashrate more electricity usage

Application-Specific Integrated Circuit (ASIC) Miner

- Designed for the sole purpose of mining bitcoins or other cryptocurrencies
  - Powerful
  - Efficient

Application-Specific Integrated Circuit (ASIC) Miner

- Considerations
  - Hash rate: Hashes per sec
  - Efficiency: watts
  - Price

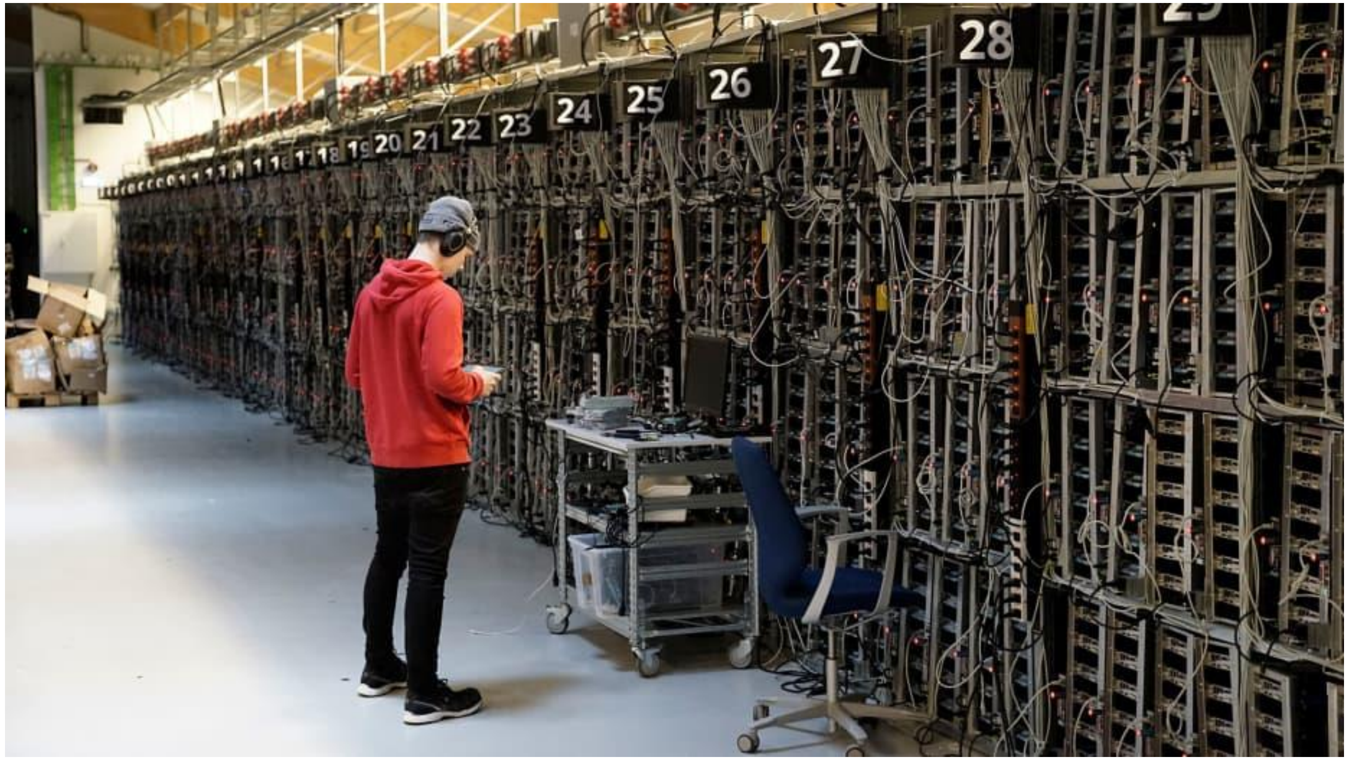


	Miner	Hash Power	Price*
	Antminer S19	95.0 TH/s	$6k-8.5k
	Antminer S19 Pro	110.0 TH/s	$8k-10k
	WhatsMiner M30S+	100.0 TH/s	$2,550
	WhatsMiner M30S++	112.0 TH/s	$2,850
	AvalonMiner 1246	90.0 TH/s	$5,500

Large Scale Mining

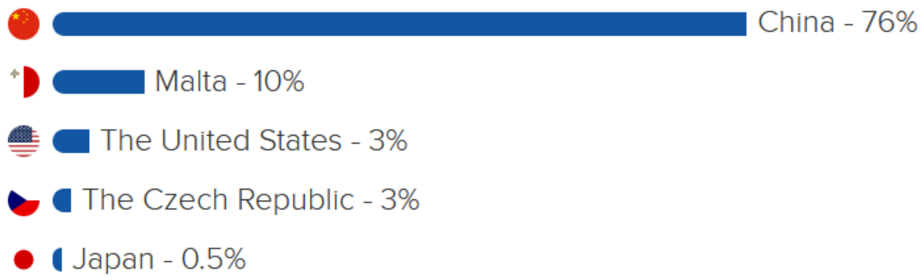
✓ Bitcoin can be efficiently mined with: ASIC (SHA-256 algorithm)

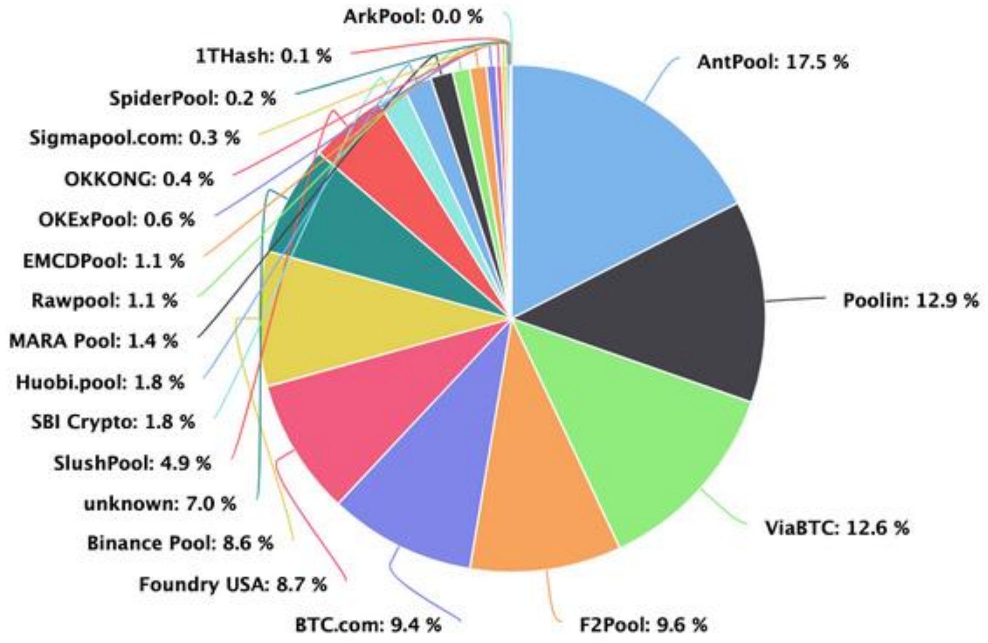
✗ Bitcoin cannot be efficiently mined with (unsupported): GPU, CPU, mobile phone



Mining Pools

- Group of miners who consolidate computing resources to increase of success
- Profits are distributed evenly to all members

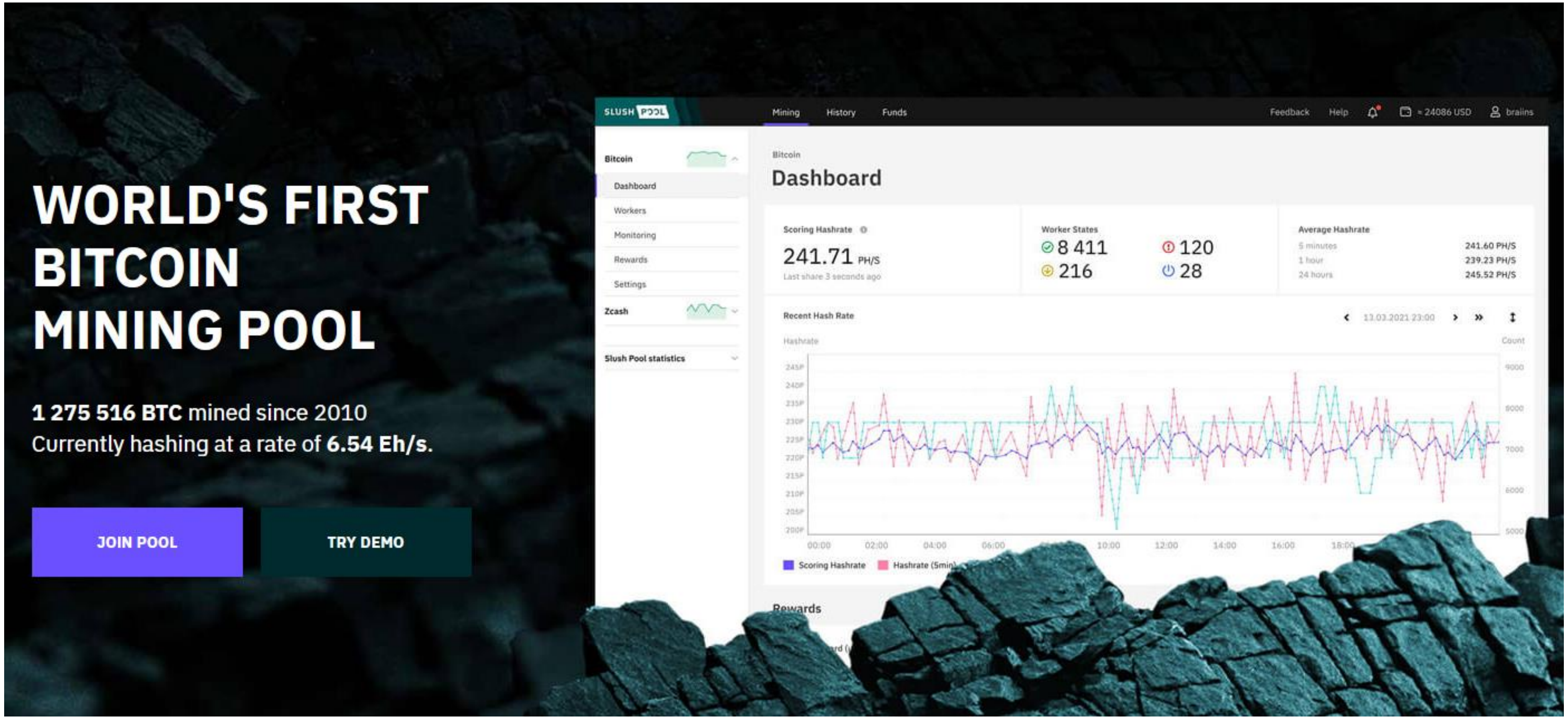




Mining Pool Functions

- Managing the pool members’ hashes
- Looking for rewards through pooled efforts of available processing power
- Recording work performed by each pool member
- Assigning reward shares to each pool member in proportion to the work performed after suitable verification.

www.slushpool.com



WORLD'S FIRST BITCOIN MINING POOL

1 275 516 BTC mined since 2010
Currently hashing at a rate of **6.54 Eh/s.**

Bitcoin

Dashboard

Scoring Hashrate: 241.71 PH/S
Last share 3 seconds ago

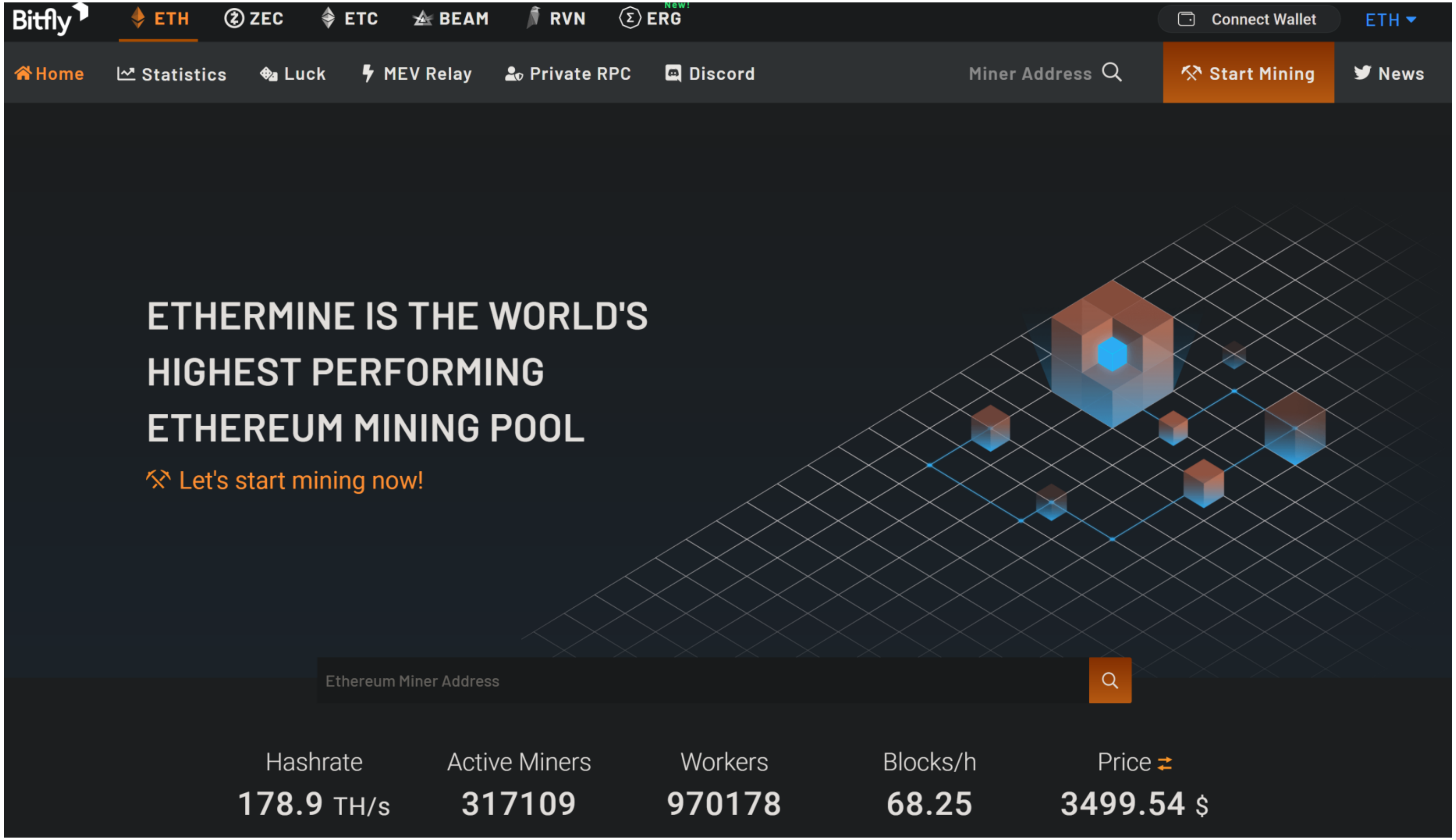
Worker States: 8 411, 216, 120, 28

Average Hashrate
5 minutes 241.60 PH/S
1 hour 239.23 PH/S
24 hours 245.52 PH/S

Recent Hash Rate 13.03.2021 23:00

Rewards

ethermine.org



ETHERMINE IS THE WORLD'S HIGHEST PERFORMING ETHEREUM MINING POOL

Let's start mining now!

Ethereum Miner Address

Hashrate	Active Miners	Workers	Blocks/h	Price ⇄
178.9 TH/s	317109	970178	68.25	3499.54 $

Local Mining Pool

- Master Server
  - geth --http --http.addr "IP ADDRESS" --http.port PORT
- Clients/Miners
  - ethminer.exe -P http://[IP ADDRESS:PORT]