

# BITCOIN MINING

WHAT, WHY, HOW?

# What is purpose of mining?

Mining is the mechanism that underpins the decentralized clearing house that validate transactions and records them on the global blockchain ledger.

Mining secures the system and enables network-wide consensus without a 3rd party.



# Why is it called mining?

Bitcoin "mining" is called so because it draws an analogy to the process of mining precious metals like gold.

Just as physical mining involves extracting valuable resources from the earth, Bitcoin mining involves "extracting" new bitcoins from the Bitcoin network through a computational process.



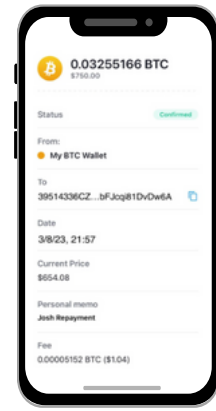
# Bitcoin Transaction Steps



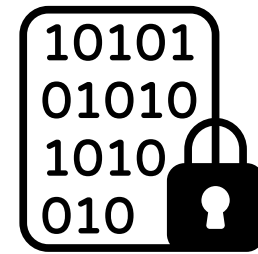
Betty wants to pay Jeff for a bike



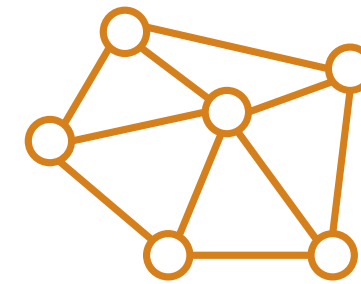
Jeff presents Bitcoin QR for Betty to scan.



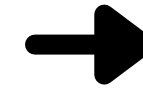
Betty enters amount & hits send.



Betty's wallet signs the transaction.



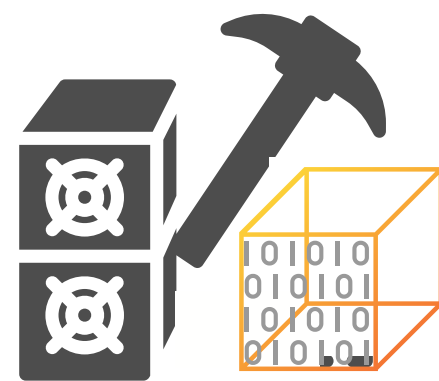
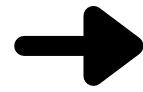
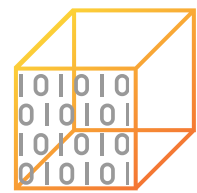
Transaction is broadcast to Bitcoin nodes for validation.



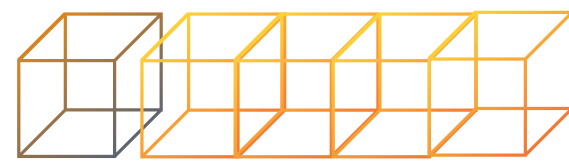
Transaction are added to the mempool



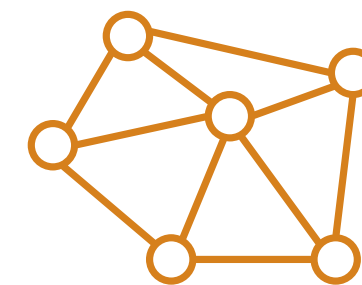
Miners combine transactions from mempool to form a block.



Once the block is formed, Miners compete to solve the encrypted puzzle.



Once solved, the miner is rewarded, the new block is added to the blockchain.



Nodes validate the block and propagate to the other nodes in the network



Jeff sees 1st transaction confirmation + New confirmations each new block.

# Bitcoin Full Node

- Run on a standard computer
- Store a complete, up-to-date version of the blockchain.
- Validate transaction against the rules
  - Ensuring digital signatures are valid
  - Determining authenticity
  - Confirming accuracy
  - Checking available balances and that transaction fees are paid
  - Preventing double-spending
- Place them into a mempool of unconfirmed transactions ready for miners.



# Bitcoin Mining Node

- Specialized computers called ASICs. Application Specific Integrated Circuits.
- Also validation nodes and transmit information to other nodes
- Verify blocks of transactions
- Compete with each other to complete proof-of-work consensus,
- Broadcast the new block to the network
- Receive the newly minted Bitcoin and transaction fees as a reward.
- This process takes substantial computing power and energy



# What is the mempool?

Every node builds a pool of valid but unconfirmed transactions known as the transaction pool, memory pool or mempool.

[mempool.space](https://mempool.space)



# Miner Rewards

Bitcoin miners receive two rewards in return for securing the network called the subsidy.

- 1) New coins created with each block.
- 2) Transactions fees from all the transactions in the block.

The surplus bitcoins between inputs and outputs. “Keep the change”

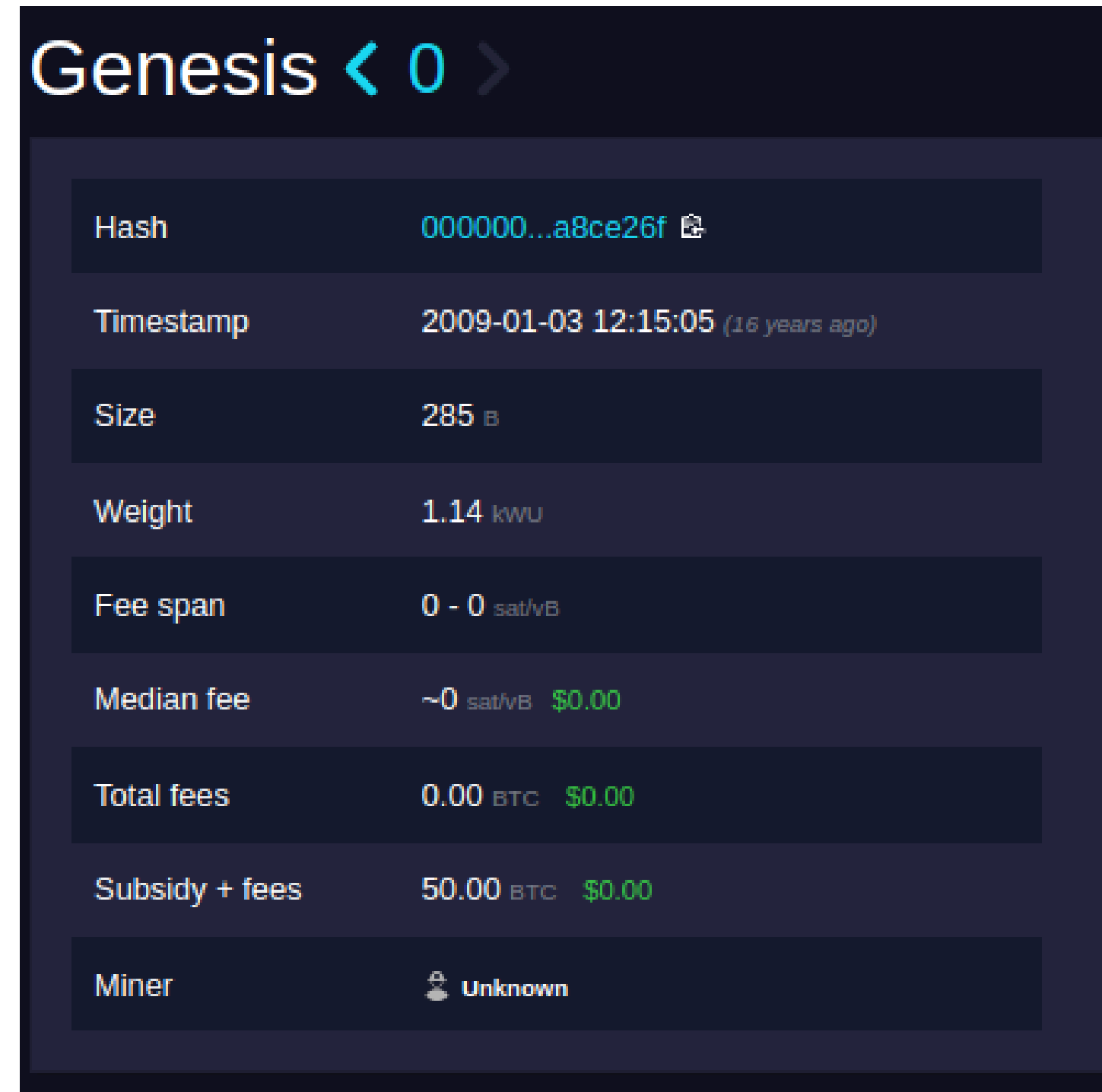


# Currency Creation


Bitcoin supply is created in similar process to how central banks create new currency except that it's fixed at 21 million bitcoins.

Bitcoins are issues with every block reward roughly every 10 minutes.

The block reward started at 50 bitcoin reward per block in 2009 and then halves continually every 4 years until it reaches 0 (approximately by year 2140)



The image shows a screenshot of a Bitcoin block explorer interface for the Genesis block. The title is "Genesis < 0 >". The data is presented in a list of key-value pairs:

Hash	000000...a8ce26f 
Timestamp	2009-01-03 12:15:05 (16 years ago)
Size	285 B
Weight	1.14 kWU
Fee span	0 - 0 sat/vB
Median fee	~0 sat/vB \$0.00
Total fees	0.00 BTC \$0.00
Subsidy + fees	50.00 BTC \$0.00
Miner	 Unknown

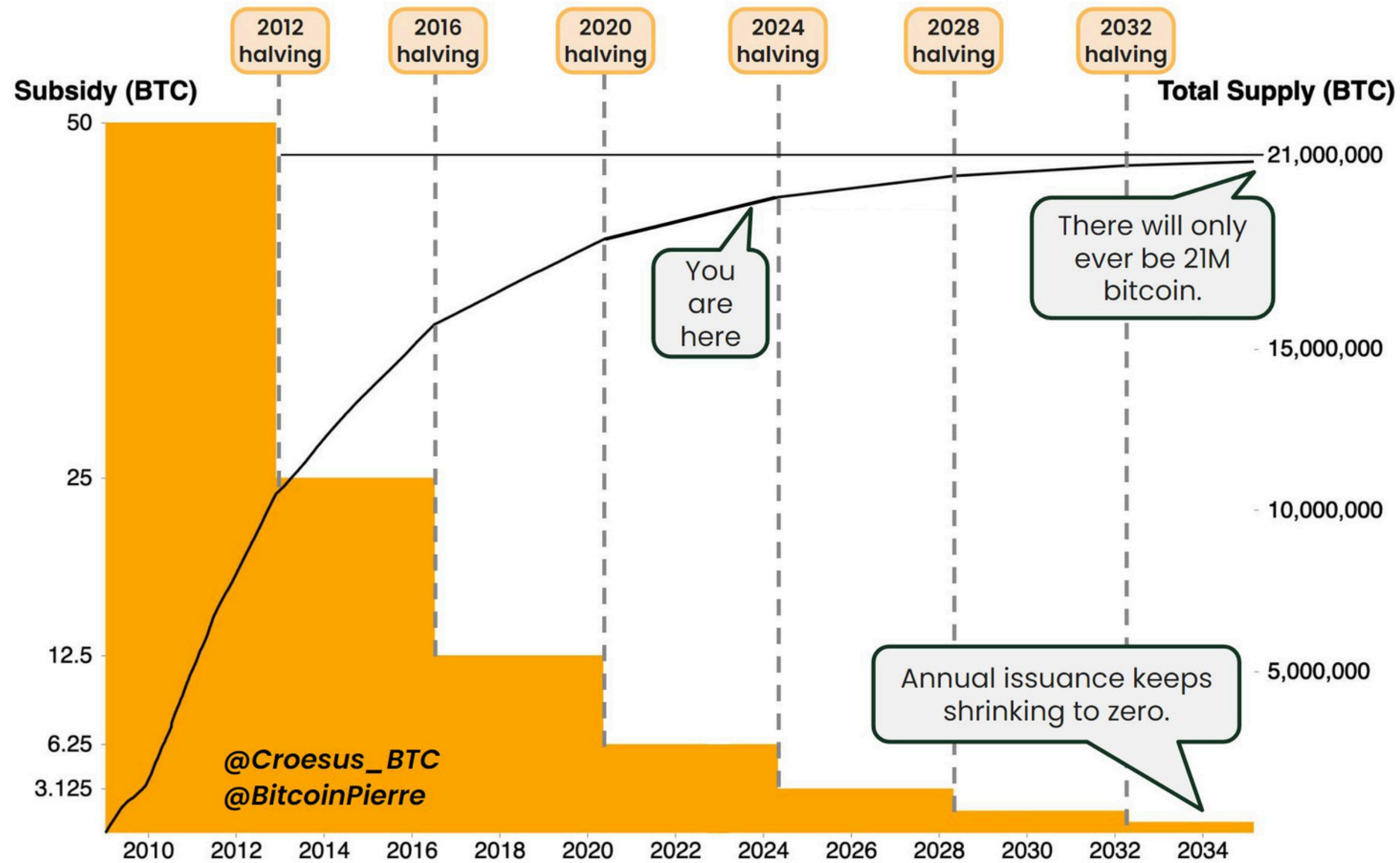


# Bitcoin Halving

The rate of new bitcoins decreases exponentially over 32 halvings until block 6,930,000.

20,999,999,876,900,000 sats

Halving Year (Estimated)	Block Number	Block Reward	BTC Circulating Supply	Circulating Supply Percentage
2009	0	50.00000000	10,500,000.00000000	0%
2012	210,000	25.00000000	15,750,000.00000000	50.00000006%
2016	420,000	12.50000000	18,375,000.00000000	75.00000008%
2020	630,000	6.25000000	19,687,500.00000000	87.50000010%
2024	840,000	3.12500000	20,343,750.00000000	93.75000010%
2028	1,050,000	1.56250000	20,671,875.00000000	96.87500011%
2032	1,260,000	0.78125000	20,835,937.50000000	98.43750011%
2036	1,470,000	0.39062500	20,917,968.75000000	99.21875011%
2040	1,680,000	0.19531250	20,958,984.37500000	99.60937511%
2044	1,890,000	0.09765625	20,979,492.18750000	99.80468761%
2048	2,100,000	0.04882812	20,989,746.09270000	99.90234386%
2052	2,310,000	0.02441406	20,994,873.04530000	99.95117198%
2056	2,520,000	0.01220703	20,997,436.52160000	99.97558604%
2060	2,730,000	0.00610351	20,998,718.25870000	99.98779307%
2064	2,940,000	0.00305175	20,999,359.12620000	99.99389658%
2068	3,150,000	0.00152587	20,999,679.55890000	99.99694833%
2072	3,360,000	0.00076293	20,999,839.77420000	99.99847420%
2076	3,570,000	0.00038146	20,999,919.88080000	99.99923713%
2080	3,780,000	0.00019073	20,999,959.93410000	99.99961859%
2084	3,990,000	0.00009536	20,999,979.95970000	99.99980932%
2088	4,200,000	0.00004768	20,999,989.97250000	99.99990468%
2092	4,410,000	0.00002384	20,999,994.97890000	99.99995236%
2096	4,620,000	0.00001192	20,999,997.48210000	99.99997620%
2100	4,830,000	0.00000596	20,999,998.73370000	99.99998812%
2104	5,040,000	0.00000298	20,999,999.35950000	99.99999408%
2108	5,250,000	0.00000149	20,999,999.67240000	99.99999706%
2112	5,460,000	0.00000074	20,999,999.82780000	99.99999855%
2116	5,670,000	0.00000037	20,999,999.90550000	99.99999929%
2120	5,880,000	0.00000018	20,999,999.94330000	99.99999966%
2124	6,090,000	0.00000009	20,999,999.96220000	99.99999984%
2128	6,300,000	0.00000004	20,999,999.97060000	99.99999993%
2132	6,510,000	0.00000002	20,999,999.97480000	99.99999997%
2136	6,720,000	0.00000001	20,999,999.97690000	99.99999999%
2140	6,930,000	0.00000000	20,999,999.97690000	100.00000000%



Predictable and unchangeable supply amount and rate of change.

# Finite Supply: Clever Features

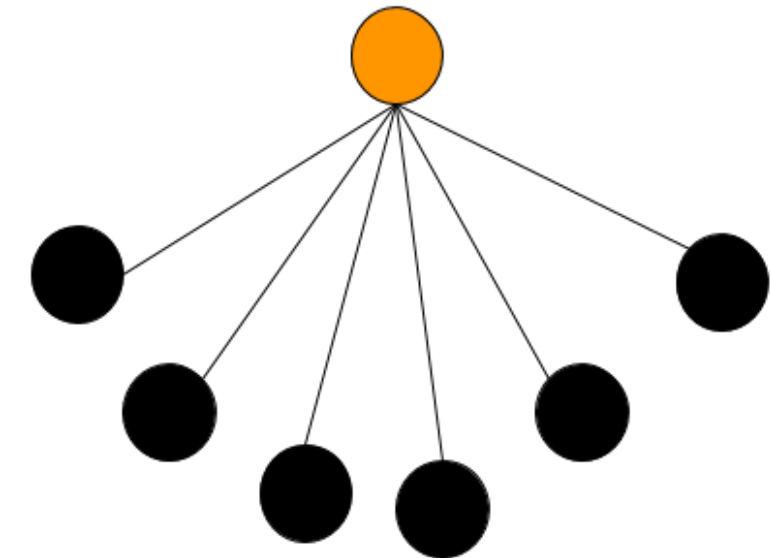
- Predefined Distribution Schedule:  
Block rewards
- Halvings
- Difficulty Adjustment

# Decentralized Consensus

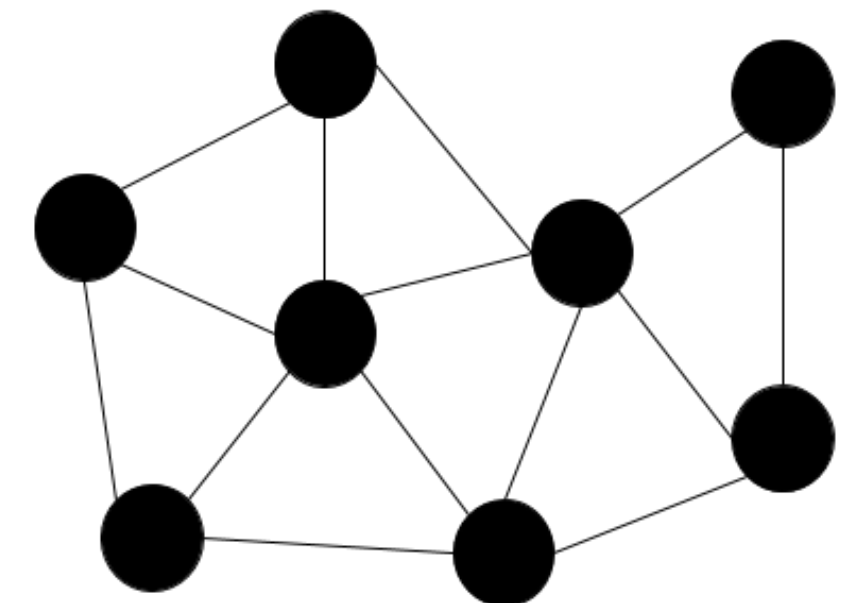
Consensus emerges from these 4 processes.

- 1) independent verification of each transaction by every full node on the network.
- 2) independent aggregation of those transactions into new blocks by mining nodes through proof of work algorithm.
- 3) independent verification of new blocks by every node and assembly into a chain.
- 4) Independent selection by every node of the chain with the most cumulative computation demonstrated through proof of work.

**Centralized**



**Decentralized**



# Proof of Work Algorithm

- Bitcoin miners ASSEMBLE proposed blocks of transactions.
- Then they COMPETE rapidly trying random inputs over quadrillion times before finding an input that is lower than the target.
- The miners do this for the CHANCE to RECORD their block onto the ledger and win bitcoin as a REWARD.
- When the algorithm is based on a deterministic function (SHA256), the input itself constitutes proof that a certain amount of work was done to produce the result.

# ASIC - Application Specific Integrated Circuit



Bitmain  
Antminer S9  
~14th/s



Bitmain  
Antminer S19 pro  
~140th/s



Bitmain  
Antminer S21 pro  
~234th/s



Bitmain  
Antminer S21e Hyd  
430Th/s



MicroBT  
WhatsMiner M10S  
~55Th/s



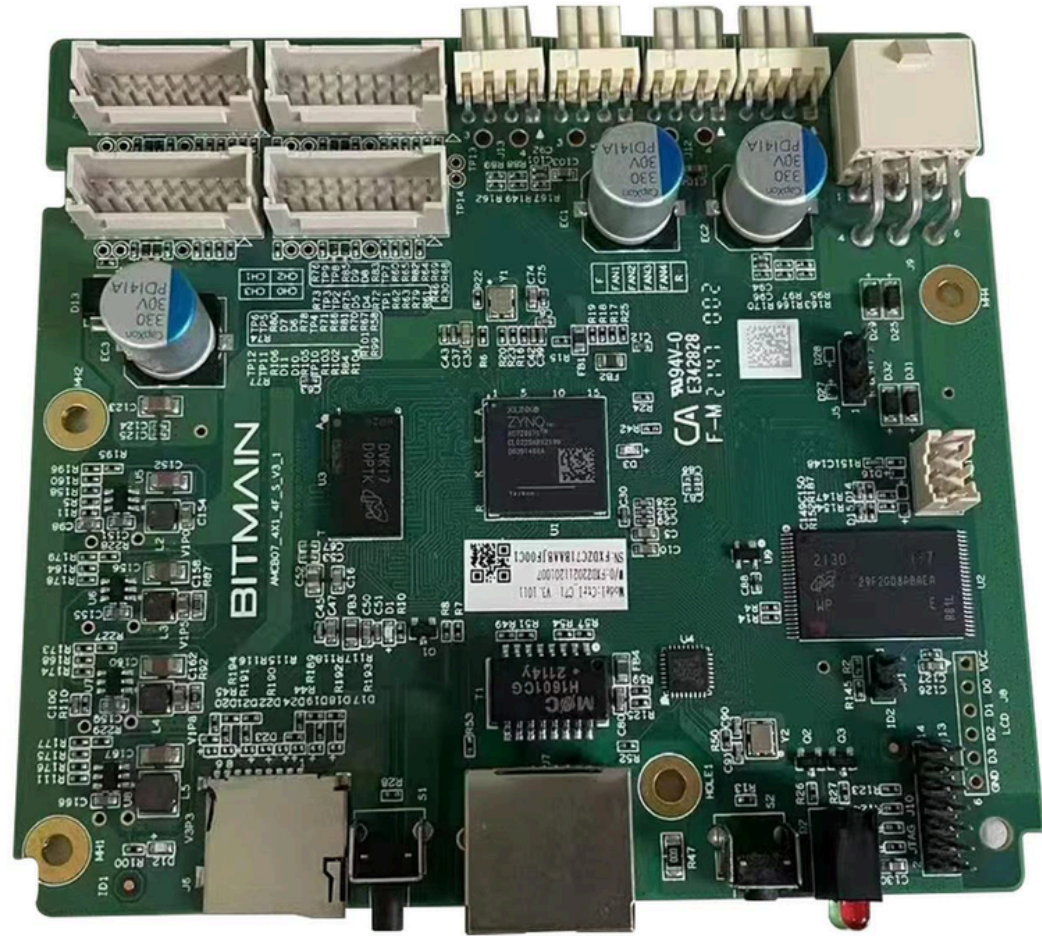
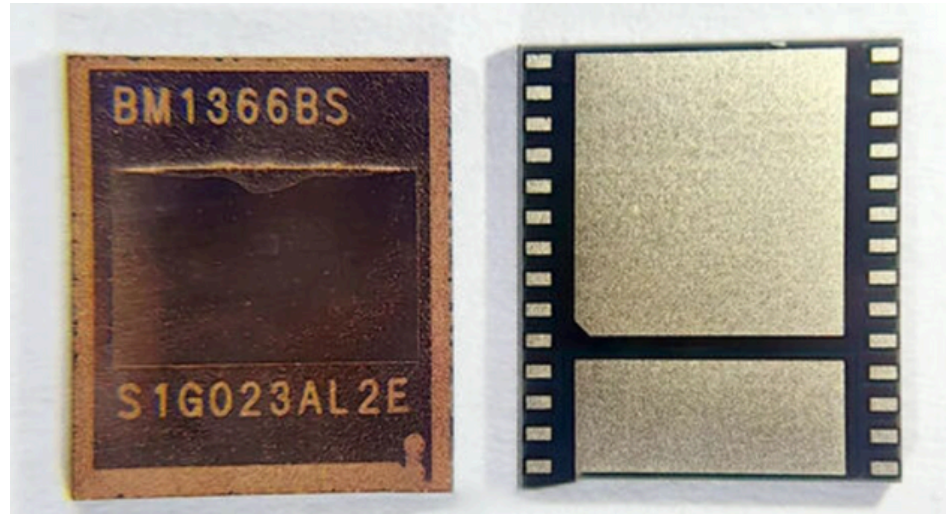
MicroBT  
WhatsMiner M50S  
~126Th/s



MicroBT  
WhatsMiner M60S  
~186Th/s



MicroBT  
WhatsMiner M63S  
~424Th/s



# ASIC MINER HASHRATE

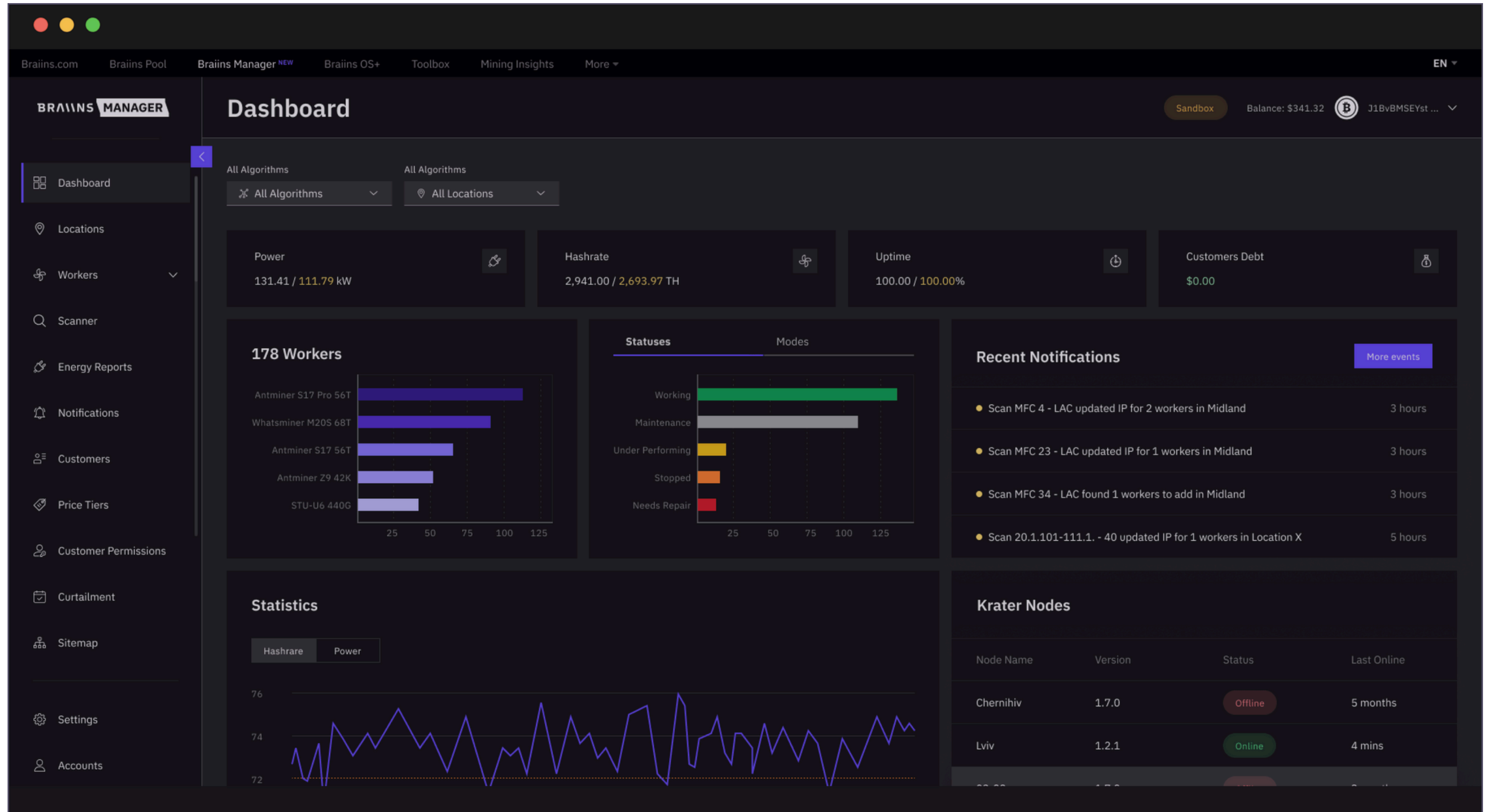
**Hashrate** is the estimated rate of total hashes completed per second.

Hashrate Unit	Hash	Hashes Per Second
H/s (Hash)	1	One
kH/s (KiloHash)	1,000	One Thousand
MH/s (MegaHash)	1,000,000	One Million
GH/s (GigaHash)	1,000,000,000	One Billion
TH/s (TeraHash)	1,000,000,000,000	One Trillion
PH/s (PetaHash)	1,000,000,000,000,000	One Quadrillion
EH/s (ExaHash)	1,000,000,000,000,000,000	One Quintillion
ZH/s (ZettaHash)	1,000,000,000,000,000,000,000	One Sextillion
YH/s (YottaHash)	1,000,000,000,000,000,000,000,000	One Septillion



**S19Pro miner has  
a hashrate of  
~120 TH/s**

# ASIC Miner Firmware





# ASIC BITCOIN MINER MANUFACTURERS

**BITMAIN**



**MicroBT**



**iPollo**



**思创优**  
StrongU

**INNOSILICON**



**Canaan**

# Basic Parts in a **Bitcoin** Mining operation



Transformer from source to supply electricity to the panel



Electrical Panel with 240V electricity + breakers



PDU Power Distribution Unit and cables supply power from panel to miner



ASIC Bitcoin mining computer



Internet router, network switch and network cabling to each miner



Ventilation system to move cold air in and hot air out.

# Bitcoin mining costs

## Hardware costs

- ASIC computers can cost anywhere between \$500 for used to over \$15,000 for the latest miners.

## Energy expenses

- Each miner uses around 3500watts and 220-240 volt supply

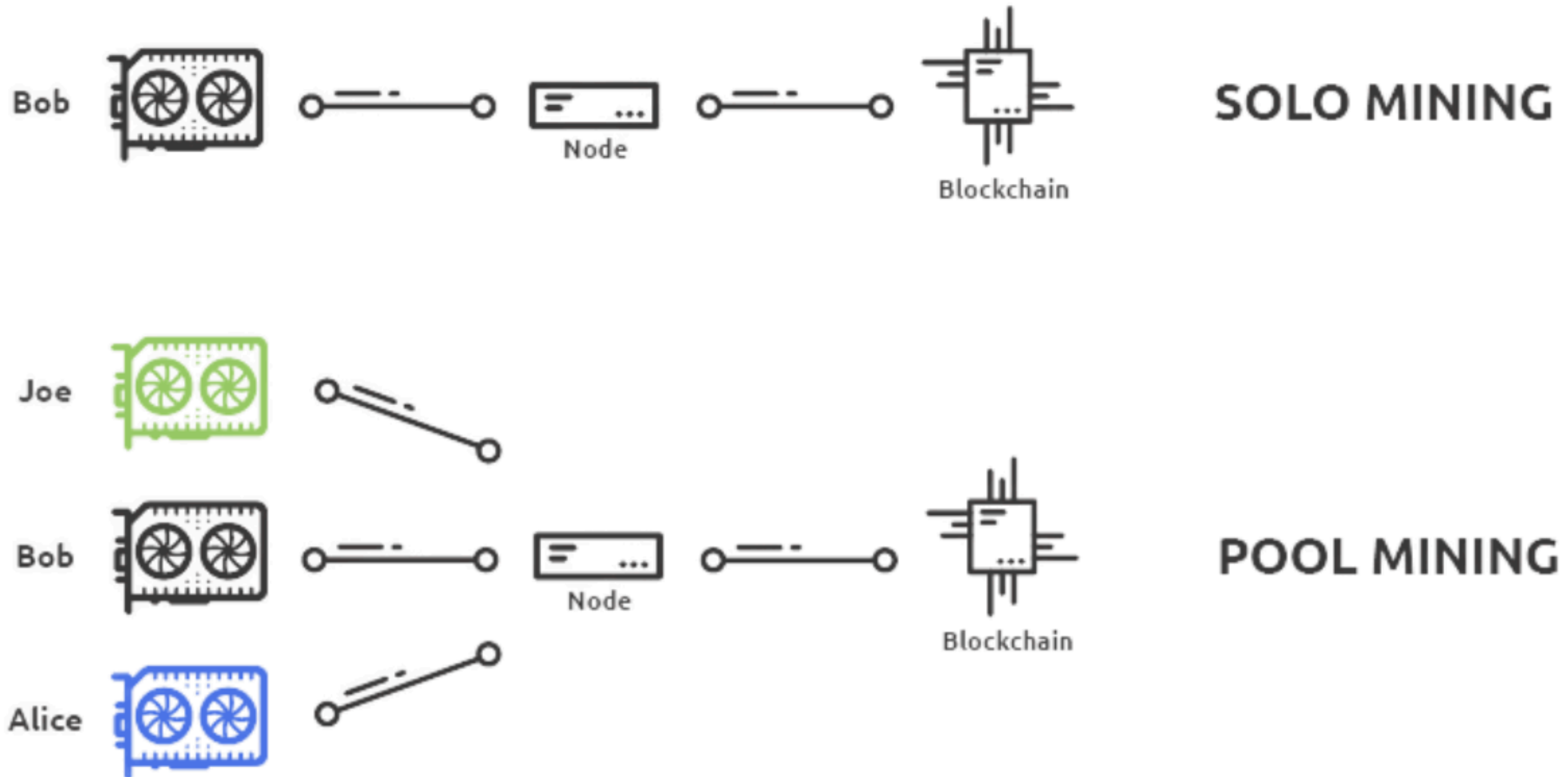
## Cooling costs

- ASICs produce a lot of heat that needs to be dispersed to keep the miners in good condition.

## Maintenance and repair costs

- Constant maintenance and repairs are needed to keep miners running optimally.

# Solo Mining vs Mining Pools

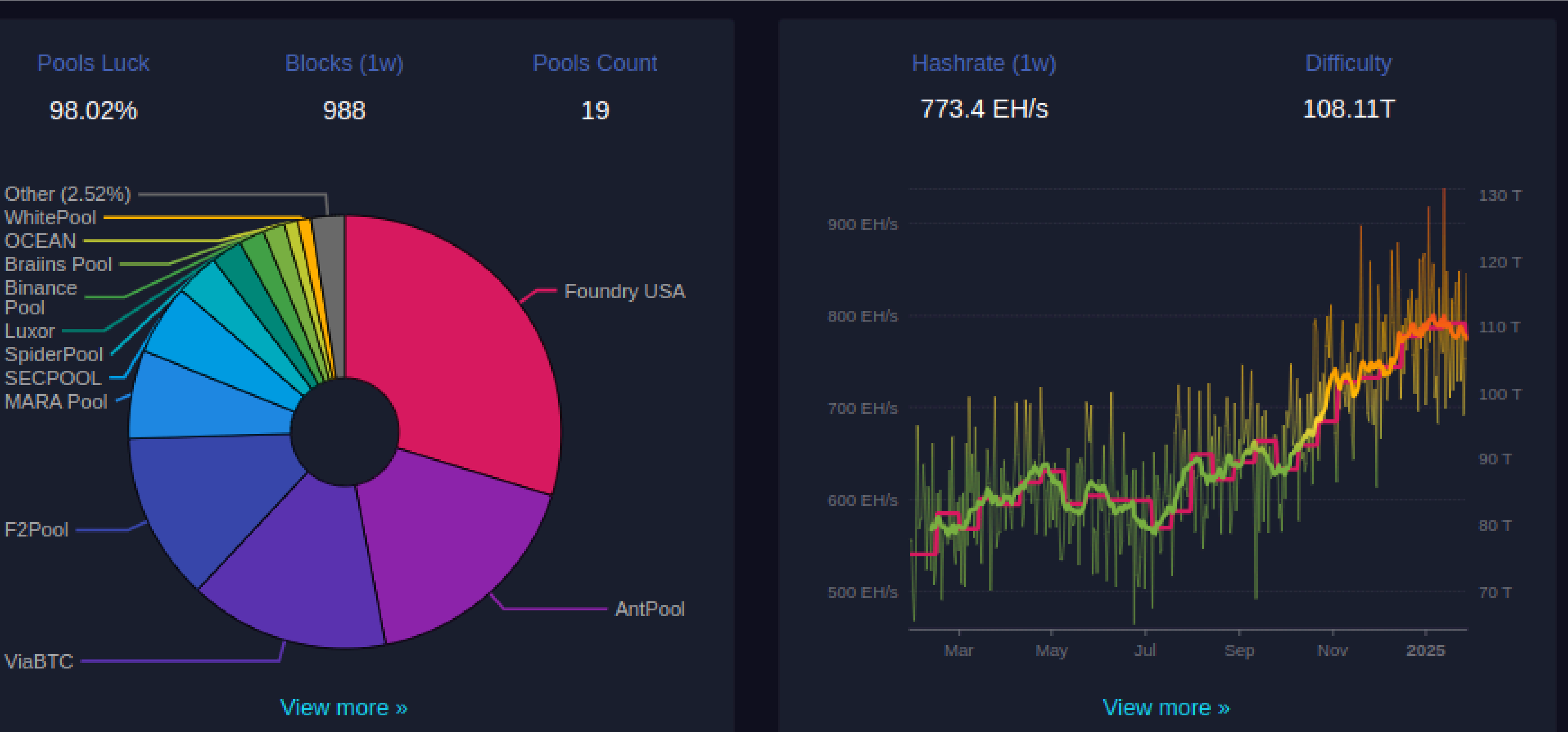


# Mining Pools

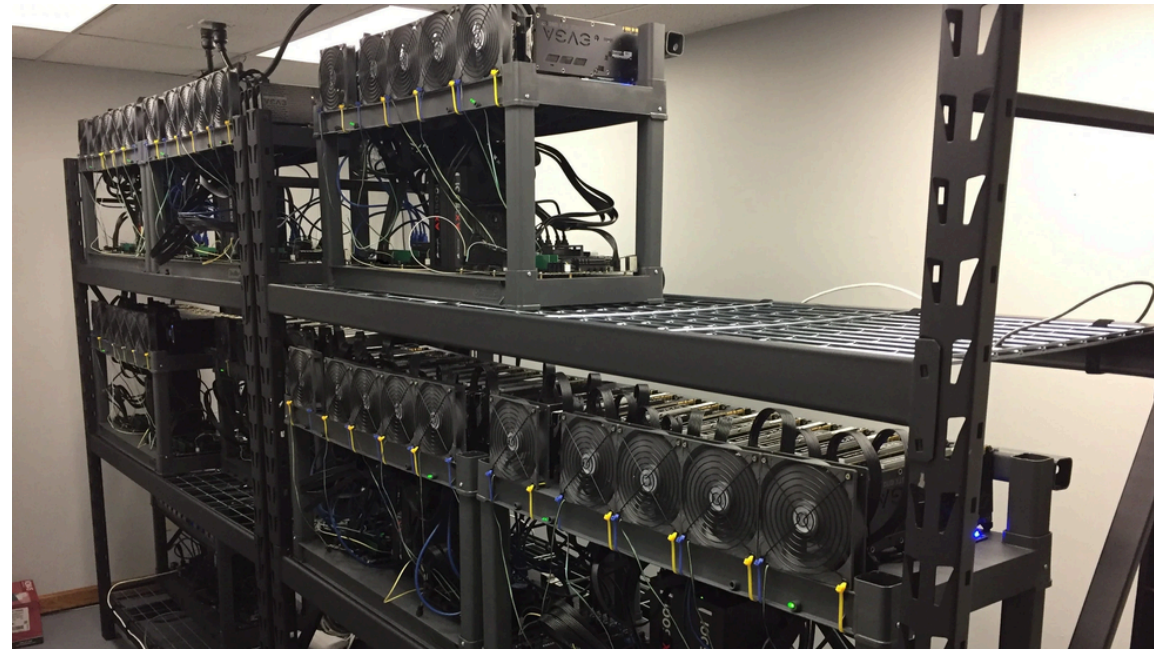
- Mining pools coordinate thousands of miners “pooling” their hashrate together and sharing the rewards among all participants.
- Open to any miner, big or small.
- There are numerous payment systems (over 15), but the vast majority of mining pools operate on a PPS, FPPS, PPS+, and PPLNS basis.

Payout Method	Description	Advantages	Disadvantages
Pay-Per-Share (PPS)	Miners receive a fixed payout for each share they solve, regardless of whether a block is found. Payout is calculated based on the share's difficulty.	<ul style="list-style-type: none"> <li>- Stable and predictable income.</li> <li>- Lucrative in bearish markets.</li> </ul>	<ul style="list-style-type: none"> <li>- Miners do not receive transaction fees.</li> <li>- Higher pool fees due to the guaranteed payout.</li> </ul>
Pay-Per-Last-N-Shares (PPLNS)	Profits are distributed based on the number of shares contributed to the last N shares before a block was found. Reward fluctuates with pool luck.	<ul style="list-style-type: none"> <li>- Potentially higher rewards if the pool finds blocks frequently.</li> <li>- Fair distribution based on recent contribution.</li> </ul>	<ul style="list-style-type: none"> <li>- Income can be zero if no blocks are found.</li> <li>- Short-term volatility due to pool luck.</li> </ul>
Pay Per Share + (PPS+)	Combines aspects of PPS and PPLNS. Block reward follows PPS, while transaction fees and pool fees are handled like PPLNS.	<ul style="list-style-type: none"> <li>- Miners gain from transaction fees, unlike pure PPS.</li> <li>- More balanced exposure to pool luck.</li> </ul>	<ul style="list-style-type: none"> <li>- Complexity in understanding payment structure.</li> <li>- Still subject to some pool luck for fee distribution.</li> </ul>
Full Pay Per Share (FPPS)	Both block rewards and transaction fees are paid out based on theoretical profit, with miners receiving payment for all shares submitted, not contingent on block discovery.	<ul style="list-style-type: none"> <li>- Guaranteed payment for shares, including transaction fees.</li> <li>- No trust needed for income validation.</li> <li>- Revenue independent of pool luck.</li> </ul>	<ul style="list-style-type: none"> <li>- Higher operational costs for the pool.</li> <li>- Might result in lower net payout due to fee structure.</li> </ul>
Datum (Ocean Mining)	A unique payout method where miners are paid based on the actual value they add to the network, which includes not just block rewards but also considers network security and decentralization. It uses a dynamic pricing model where the payout rate adjusts according to market conditions and pool performance.	<ul style="list-style-type: none"> <li>- Rewards for contributing to network health.</li> <li>- Adaptive to market changes.</li> <li>- Encourages long-term participation.</li> </ul>	<ul style="list-style-type: none"> <li>- Complex to understand and predict earnings.</li> <li>- Potential for variable income based on external factors.</li> </ul>

# Prominent Mining Pools



# Types of **Bitcoin** mining operations



> .2 Megawatt home mine



15 Megawatt Mine



300 Megawatt Industrial Mine



.5 Megawatt  
Wind powered off-Grid mine



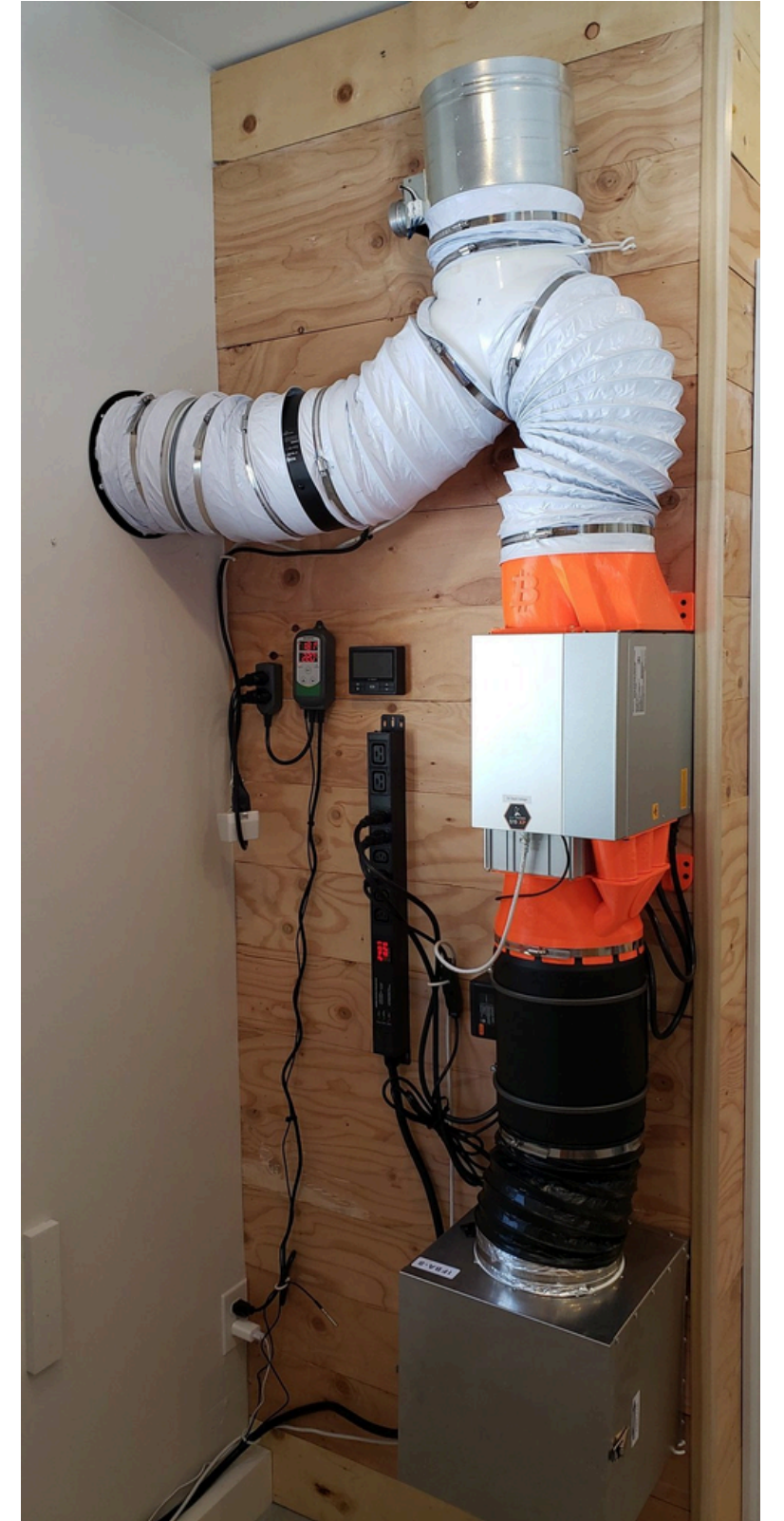
1 Megawatt  
Natural Gas off-Grid mine



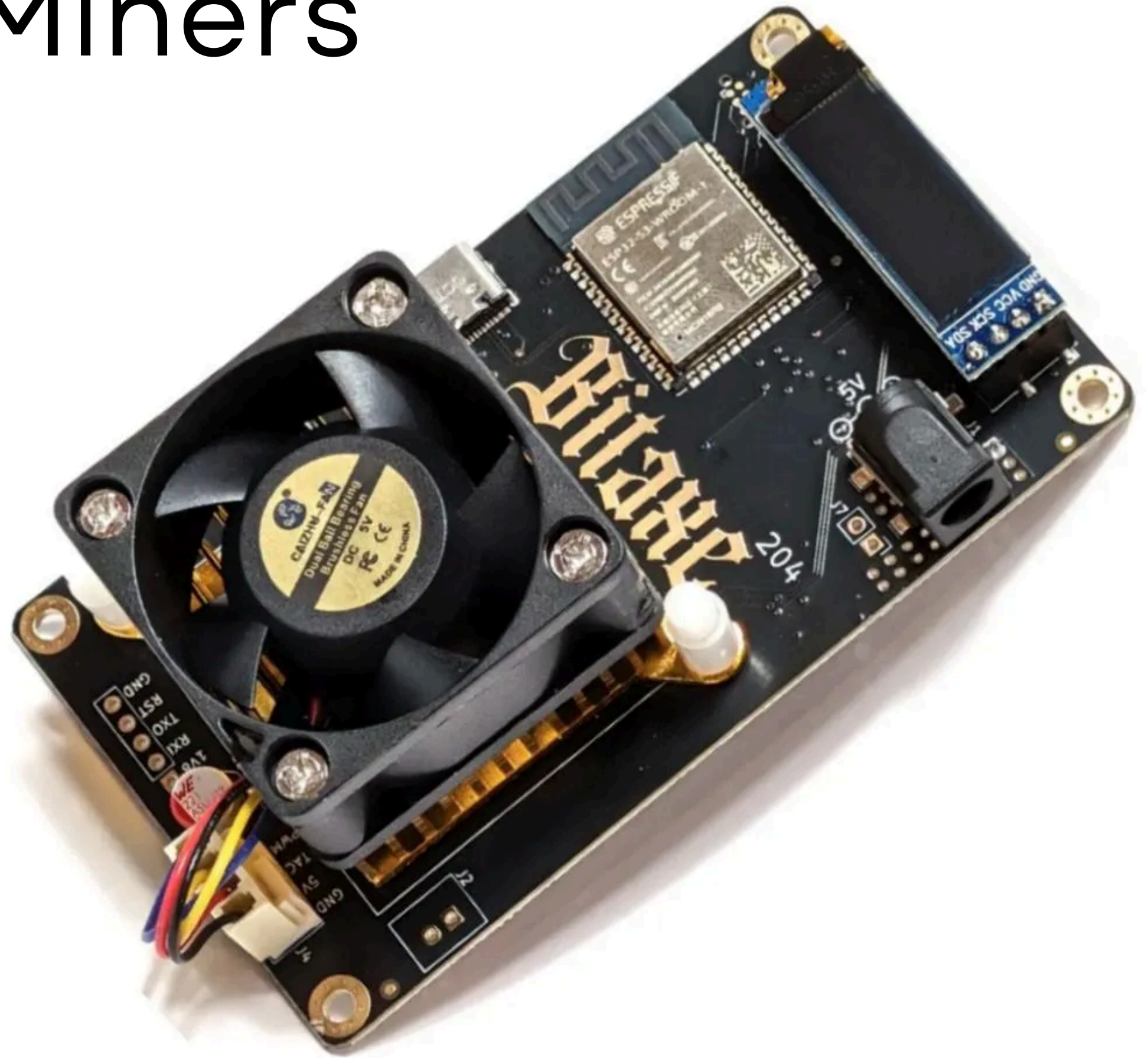
Liquid cooled immersion mine



# Bitcoin Heaters



# Lottery **Bitcoin** Miners



# WHY IMMERSION COOLING FOR **BITCOIN** MINING?

## More performance

Less energy use - 30% less electricity with fans removed. Reduced heat allows for overclocking for 20% more hashrate.



## Silent operation

One air cooled aisc miner generates the noise of 75dB 24/7, 365. With immersion cooling their is very little noise

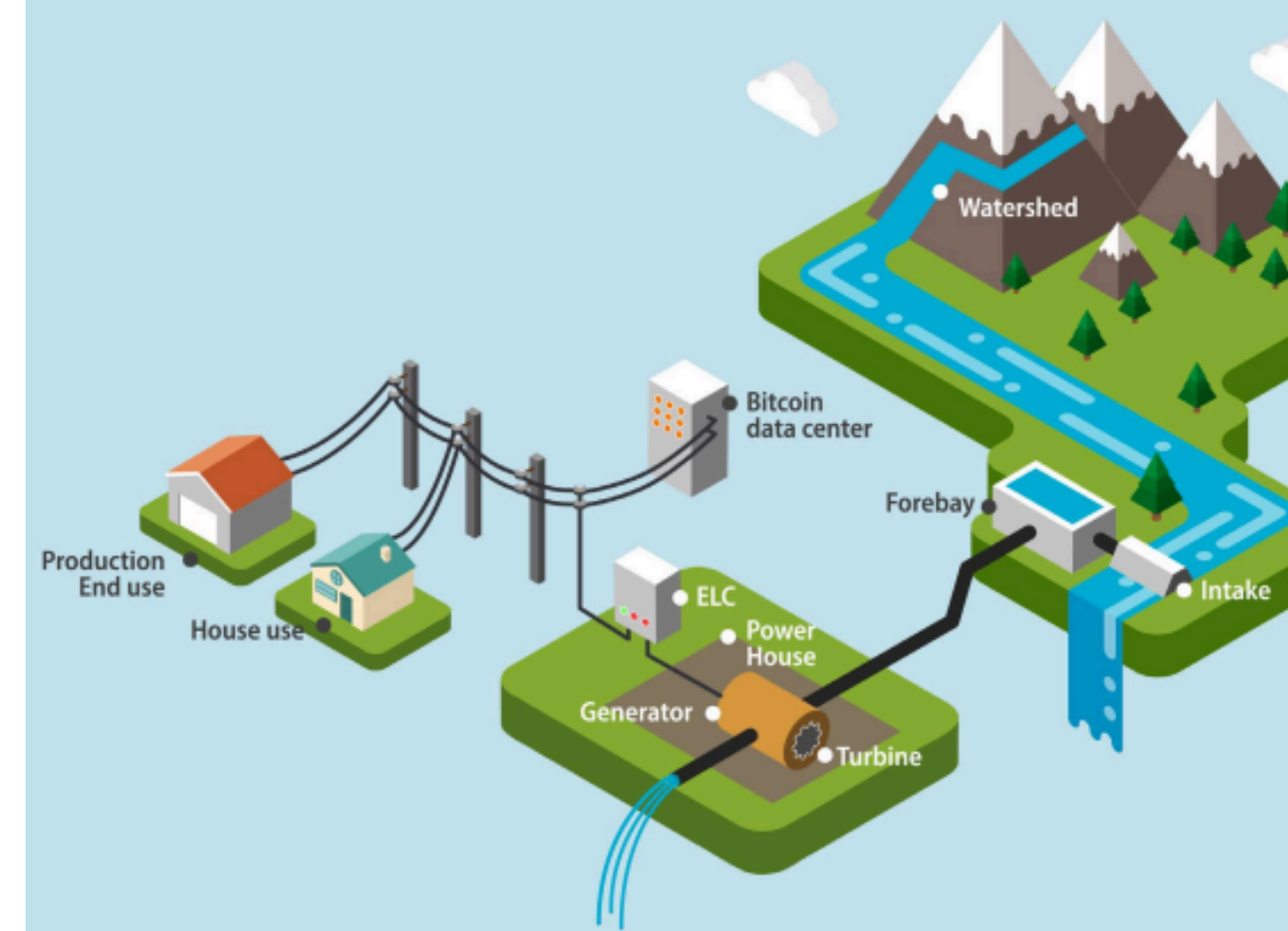


## Less repairs, More uptime, more earning

Asic miners immersed in the liquid are completely protected from high temperature, humidity, dust and vibration. All that results in immediate increase in miners time between failures and elimination of a majority of scheduled maintenance.

# Bitcoin Use case: Bringing Clean Power to Underserved Communities

- In the Kenyan countryside, 500 families are now receiving uninterrupted, off-grid power for the first time - made possible and affordable because of bitcoin mining.
- This community is leveraging bitcoin mining to help fund their electricity grid development. The problem is that without an anchor tenant for the energy to be built, then it won't be built (or will not be sustainable). Bitcoin mining serves as the location agnostic, variable power, buyer of last resort.
- This is a small scale example of how Bitcoin mining can help build the world's electricity infrastructure.
- Gridless Compute in Kenya empowers communities by providing off-grid power solutions, thereby improving livelihoods and fostering economic growth.

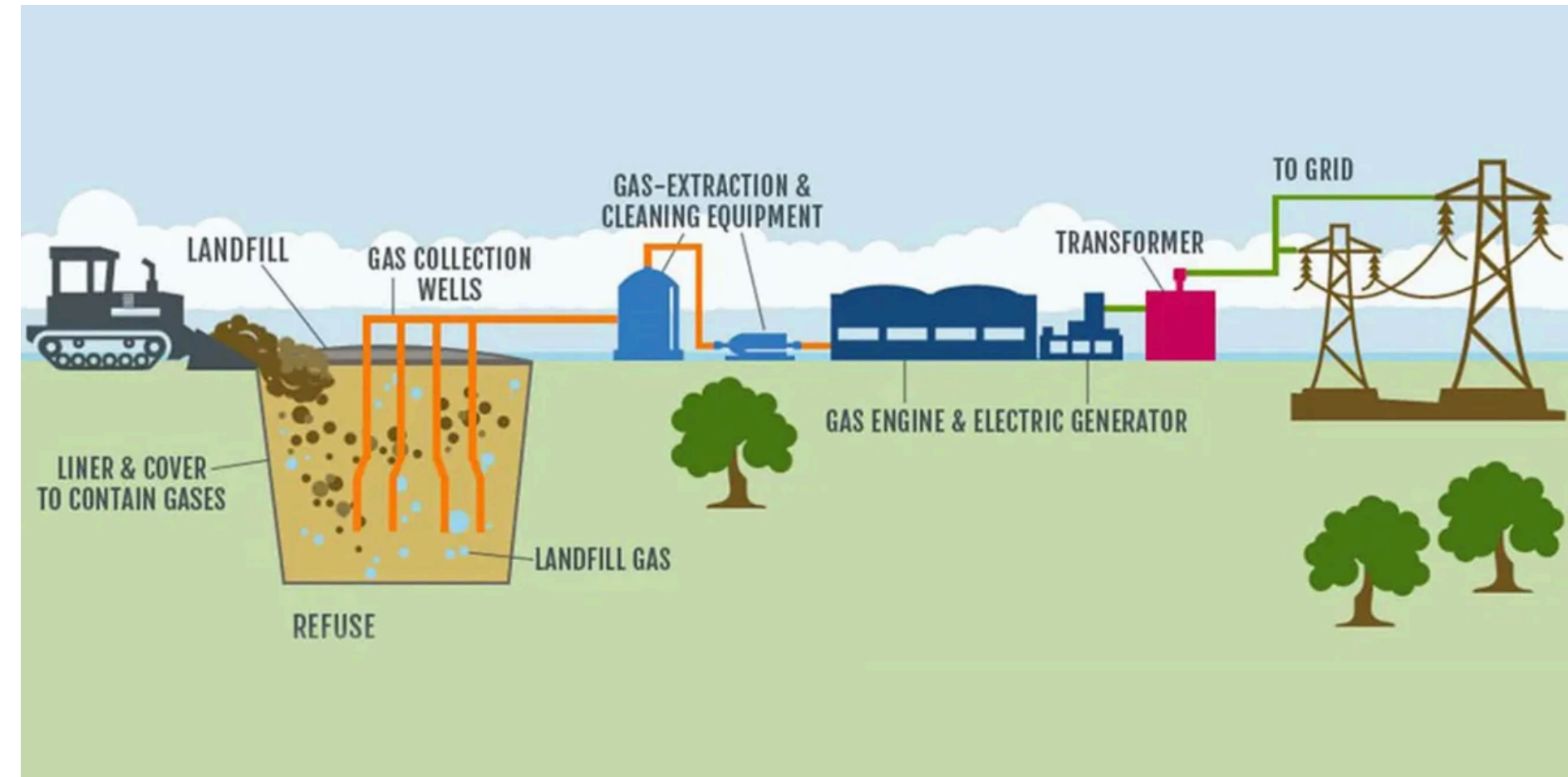


# Recapturing Landfill Methane for **Bitcoin** Mining

Vespene Energy recently launched a 1.6MW landfill gas-powered Bitcoin mining operation in Marathon County. This project is expected to mitigate 20,000 tonnes of CO2 equivalent per year, which is akin to taking 4,300 cars off the road for an entire year.

NodalPower, which began its operations in 2022, has a total of 4.8 MW of projects.

Together, these two companies produce 6.4 MW of power from previously flared methane gas, mitigating a total of 80,000 tonnes of CO2 equivalent.



# Heating a car & truck wash with **Bitcoin** miners

*“Bays and TC Car/ Truck/ RV/ ATV Wash has both self serve bays open 24 hours everyday. **Bays and hot water are now heated with Bitcoin.** Stop by and check it out. Water are now heated with Bitcoin.”*



This hydronic snow melt system used to cost \$25 per day in propane costs and is now running at a \$24/day profit. What was once a business expense has become a new profit center by using the heat generated by the bitcoin ASIC miners.

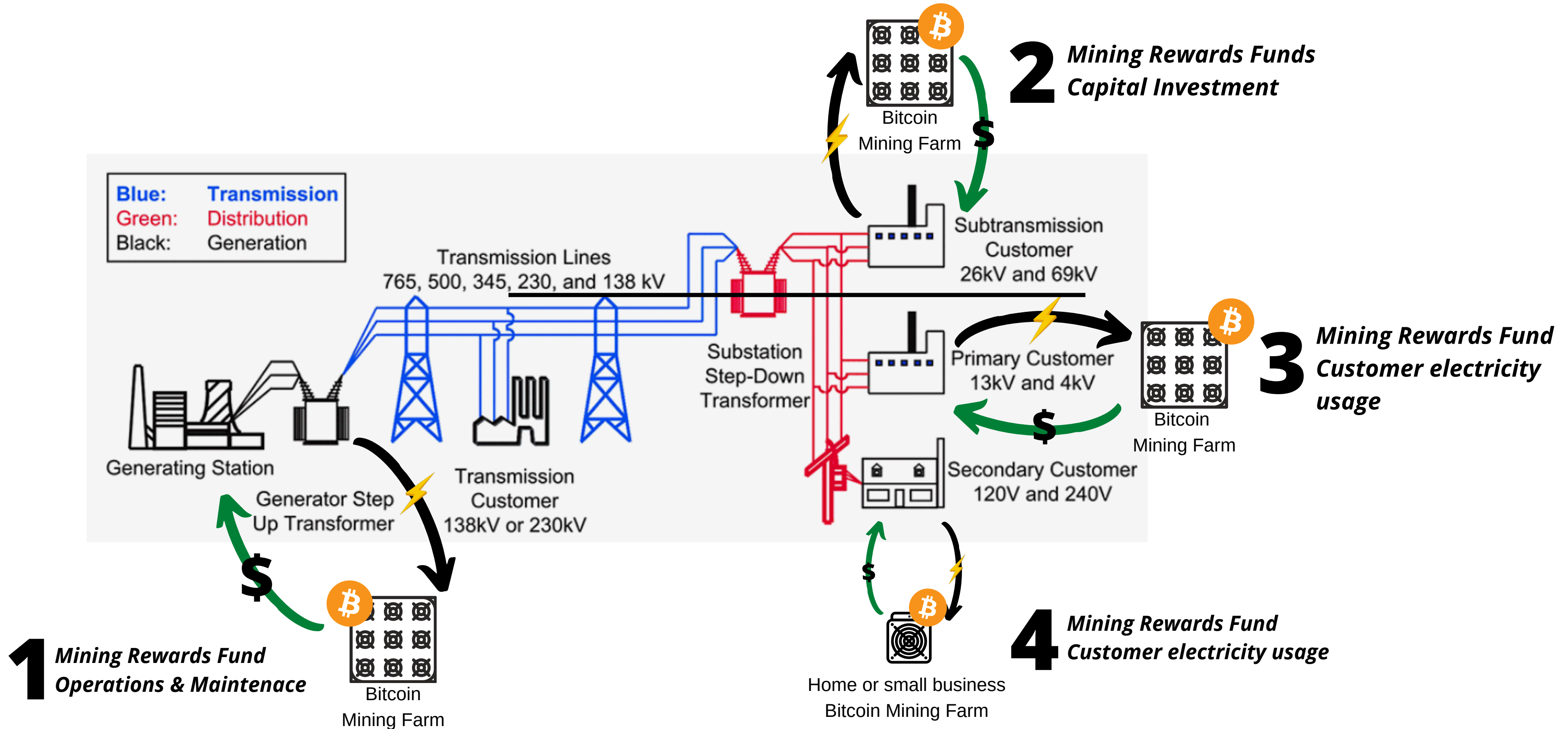


**6 ASIC miners in immersion tank**

Monetizing  
stranded natural  
gas by mining  
**bitcoin** in the  
oilfield.



# Bitcoin can fund electricity grid development





There are now 70 Bitcoin mining companies producing net zero, or neg-negative emissions

41 use 99%+ sustainable-energy based operations

29 reduce emissions by using flared or vented methane as a power source (see image)

<b>Flaring Company</b>	<b>MW</b>		<b>Venting Co</b>	<b>kW</b>
<a href="#">Crusoe Energy</a>	123.4		Anonymous	2000
<a href="#">Unblock</a>	15		Cryptotherm - Ven	2000
<a href="#">jaienergy.com</a>	3.15		Blue Hills - site 2	1000
<a href="#">Nakamotor Partners</a>	3		Scilling Mining	224.25
Green Mining Capital	6		AmityAge Mining	438.75
<a href="#">Arthur Mining</a>	8		Chainergy	75
BitRam	3		Biomining	0
Giga Energy	12		EasyCryptoHunter	0
<a href="#">Wild Rose Mining</a>	1.1			
<a href="#">Plexus (Flared. GP &amp; Sas</a>	6			
<a href="#">Imperium Digital</a>	0			
Anonymous #1	12			
Anonymous #2	9			
Blue Hills (Site 1)	1			
Vespene Energy	1.6			
Spur	1			
<a href="#">CryptoTherm - Flared</a>	9			
NodalPower	4.8			
LMS/DC Two (Aus)	0.8			
Marathon	0.28			
GDA (ARG)	3.5			
<b>Total MW</b>	<b>223.63</b>		<b>Total MW</b>	<b>5.738</b>

# Bitcoin Security Model

