CRYPTOCURRENCY MINING

Our definitive guide to cryptocurrency mining

C[®]IN RIVET

Independent British blockchain and crypto news

PREVIOUS

CONTENTS

CRYPTOCURRENCY MINING EXPLAINED

Cryptographic hash functions	
The ideal cryptographic hash function has five main properties	
What do you need to get started with mining?	

CRYPTOCURRENCY MINING STRATEGIES

General strategies	
Hardware mining	
Hardware mining terms	
Cloud-based mining	
Pros of cloud-based mining	
Cons of cloud-based mining	
Types of cloud-based mining	
Mining contracts	
Software	

THE REAL COST OF MINING7Operation costs7How to mine Bitcoin71. Bitcoin mining hardware – a processor72. Get a Bitcoin wallet73. Find a mining pool84. Get a mining programme8

HOW TO MINE ALTCOINS9Litecoin9Dogecoin9Ethereum9

CRYPTOCURRENCY MINING EXPLAINED

Cryptocurrency mining is the process of verifying transactions on a blockchain ledger. Anyone with access to the internet and suitable hardware can participate in mining.

The participant who first solves the problem gets to place the next block on the blockchain and claim the rewards. The rewards are transaction fees (from the transactions in the block) as well as the newly released cryptocurrency e.g. Bitcoins.

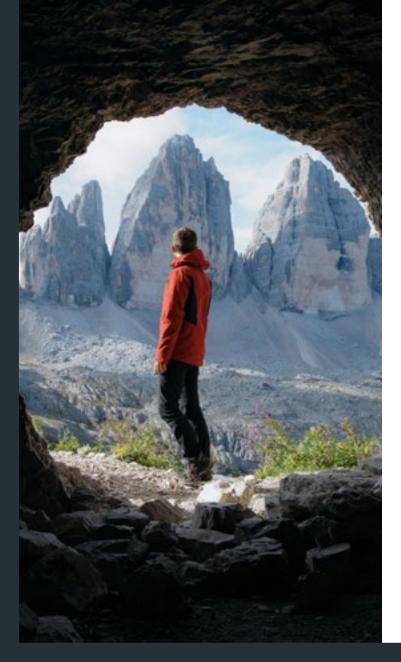
Cryptographic hash functions

The way mining works is primarily centred on what is known as cryptographic hash functions.

In short, a cryptographic hash function is a mathematical algorithm that maps data of arbitrary size to a bit string of a fixed size. They are designed so that they only work as a one-way function, meaning it's infeasible to invert them. The sole way to attempt to recreate the input data from a cryptographic hash function's output is to attempt a brute force search of possible inputs and hope they produce a match.

One of the biggest examples of this is SHA-256. SHA stands for Secure Hash Algorithm. This particular one-way function converts text of any length into a string of 256 bits. The text (input data) is often called the message, whereas the hash value (output) is known as the message digest.





If any change occurs within the input data, even just a single character, it will in turn change the output so extensively that the two hash values would seemingly appear uncorrelated.

The ideal cryptographic hash function has five main properties

- Deterministic; the same message always results in the same hash
- Quick to compute the hash value for any given message
- It is infeasible to generate a message from its hash value except by trying all possible messages
- A small change to a message should change the hash value so drastically that the new hash value appears uncorrelated with the old hash value
- It is infeasible to find two different messages with the same hash value

These hash functions are used to write new transactions into the blockchain as a result of the mining process.

What do you need to get started with mining?

- A cyptocurrency wallet: Without one of these, you'll have no location to store your newly acquired tokens.
- Mining software: For mining altcoins, you'll want to do some research to work out which software is best for the altcoin you intend to mine.
- Access to a mining pool: A pool is where a group of miners get together to combine their computers/devices to bolster their chances of cracking the cryptographic puzzles to add a fresh transaction to the blockchain, thereby granting them the reward tokens and the transaction fee.
- Access to an online currency exchange: This is where you will exchange or trade your cryptocurrency.
- The right hardware setup located in an air-conditioned space: There is a wide range of hardware available, such as the DragonMint T1, Pangolin Whatsminer M3X, Bitmain Antminer S9i, and so on. Again, the right hardware will vary depending on which altcoin you intend to mine.
- **A powerful desktop:** Or a custom-built one that is specifically designed for mining.
- **Mining ASIC chip** or a special GPU mining rig.

CRYPTOCURRENCY MINING STRATEGIES

The prospect of mining cryptocurrency can be daunting, but it doesn't have to be. The three biggest methods of mining are as follows: software mining, hardware mining, and cloud-based mining.

In general, most mining is done through speculation, because you need to calculate your profitability when mining cryptocurrency.

As with any investment, there's always risk. One minute the value of your desired cryptocurrency could be high, but the next minute it could plummet. Miners typically have a rough idea of whether they believe a cryptocurrency will increase in value, and it is these cryptos they will opt to mine.

General strategies

- Mine the most profitable token.
- Mine coins that start with a low hash rate and acquire a lot of them then hope they are added to an exchange.
- Mine the most profitable coin, sell it, and then buy other coins (that may or may not be mineable) that you believe to be the best investment. This is a form of speculative mining.
- Use a mining profitability calculator to determine whether or not you will turn a profit on your desired token.

Hardware mining

Hardware mining is incredibly popular, though its initial start-up cost will set you back financially. When looking into mining hardware, it's important to take note of your chosen hardware's hash rate and power consumption.

Below is a brief list of possible hardware options:

- Halong Mining DragonMint T1: The T1 has an impressive 16 TH per second hash rate, making it one of the most efficient pieces of hardware on the market. However, it does have a consumption of 1,480 Watts, so you will end up using a lot of power.
- **Pangolin Whatsminer M3X:** The M3X is an intensive piece of hardware that uses a large amount of power, ranging between 1800-2100 Watts. This does come with a 12.5 TH per second hash rate, which is good, if still lower than the T1. However, the M3X does cost a lot less than the T1.

Bitmain Antminer S9i: The S9i utilises a Dual ARM Cortex-A9 microprocessor with support for Gigabit Ethernet. This powerful processor enables the hardware to mine blocks that are submitted instantly. The S9i has a hash rate of 14 TH per second, as well as boasting a lower consumption rate than both the T1 and M3X, clocking in at roughly 1,320 Watts.

Whilst these three pieces of hardware are amongst the most popular on the market, they are by no means the only ones available. For instance, the Avalon6 is another cheap option, but it is unlikely to turn you a profit. Make sure to do research into your desired hardware to ensure you make the correct purchase for your needs.

Hardware mining terms

- **Hash rate:** The hash rate refers to the amount of power a miner uses to solve a mathematical algorithm that mines the cryptocurrency.
- **Power consumption:** The power consumption informs the user how much electricity the mining hardware will use when operating. Power consumption is measured in Watts. To avoid using up huge amounts of power, you'll want to find hardware that uses a low number of Watts.
- Energy efficiency: Energy efficiency is measured in Joules. Similar to power consumption, the lower the amount of energy a miner uses, the better. For instance, if the number of Joules is low, it tends to suggest that the miner will consume less power and still put out the same amount of work.

Cloud-based mining

In simple terms, cloud-based mining refers to mining using the shared power run from remote data centres. The only thing you need to start cloud-based mining is a home computer, a cryptocurrency wallet, and a few other basic essentials.

Pros of cloud-based mining

- You can do it at home without the need for an air-conditioned space to run a mining setup.
- No added electricity costs.
- You don't need to offload equipment if mining ever stops being profitable.
- No risk of being let down by your mining equipment, which can cost a lot of money.

Cons of cloud-based mining

- High risk of fraud
- Lower profits since it will be split with the operator
- Lack of control and flexibility

Types of cloud-based mining

- Hosted mining: This type of cloudmining is when you are leased a mining machine that is hosted by the provider.
- Virtual hosted mining: This type creates a general purpose, virtual private server. You need to install mining software for this method.
- **Renting hash power:** This is where you rent an amount of hashing power from a provider without having a dedicated physical or virtual computer. This method is quite popular.

Mining contracts

- **Genesis-mining:** This is a popular company where users are able to buy hash rates for Bitcoin, Ethereum, and Monero mining.
- **Hashflar.io:** This is another popular site offering some of the better rates in the industry. You can mine based on hash algorithms such as SHA-256, Scrypt, Ethash, and X-11.
- **Hashing24:** This site offers a free demo, so users are able to test the waters if they are unsure about which contract to pick.
- NiceHash: This site offers cloud-mining, hash rental services, and multipool. They offer hashing power without contracts on a pay-as-you-go basis.

Note: It is worth knowing which hash algorithms belong to which cryptocurrency. For example, Bitcoin works with SHA-256, Ethereum with Ethminer/Minergate, and Litecoin with Scrypt. Make sure to do your research before jumping to a decision.

Software

Choosing the correct software is also a vital aspect in this space. The way cryptocurrencies are mined is based upon proof-of-work algorithms. These algorithms enable miners to process data and sort them into blocks. However, the more people that mine on a network in turn increases the difficulty for the miners.

The important thing to note about software is that because cryptocurrencies run with different algorithms, they require different software. For Bitcoin, it is recommended to use the official BitCore client, whereas Ethereum would require something like Ethminer or Minergate.



C[®]IN RIVET

Independent British blockchain and crypto news

THE REAL COST OF MINING

When you are setting out to mine for`cryptocurrencies,`you have to think through the various factors that will impact your overall`profitability. Operational and environmental costs are arguably the highest expense when it comes to cryptocurrency mining.

Operation costs

The major operational cost to mine for cryptocurrencies will be, of course, electricity. The electricity cost will also be a key factor to determine the hardware you chose. If your electricity cost is high then it may be worth waiting for the 'latest generation' equipment to reduce overall payback times for the hardware you need to buy (for example, wait two months for a more efficient miner to arrive that will pay back in 200 days vs another immediate delivery miner that pays back in 300 days).

Another key aspect is the operational cost it takes to keep your mining operation running 24 hours a day with minimal downtime. Any time you aren't hashing away will be discounted from the payback time you calculated on your initial capital investment.

Environmental costs are the final area that shouldn't be overlooked. It's easy to mine in a spare bit of space (a loft, for example) but not thinking about aspects like heat management or even general logistics may lead to significantly shortening the lifespan of your miner. There have been examples of people tripping over wires and bringing down a whole stack of miners (with this leading to the end of a particular operation). Nonetheless, mining for cryptocurrencies is still a popular way to get involved in the community. Below, we take a look at how you can successfully mine specific types of coins.

How to mine Bitcoin

In the early days it was possible to mine Bitcoin using a desktop PC. Now specialised hardware is required, otherwise the cost of electricity to power a PC would exceed the potential earnings of Bitcoin from the operation.

These are the things you will need to start mining.

1. Bitcoin mining hardware - a processor

You can buy the hardware to mine Bitcoin on Amazon. In addition there are lots of other pieces of supporting hardware available – cooling fans, s tacking racks (allowing more than one miner to be conveniently set up), processing boards, cards and chips.

The basic way to maximise returns is to have your hardware running for as long as possible every day and as efficiently as possible. Before starting, you may want to know if you're likely to make any money so it's worth using a Bitcoin mining calculator.

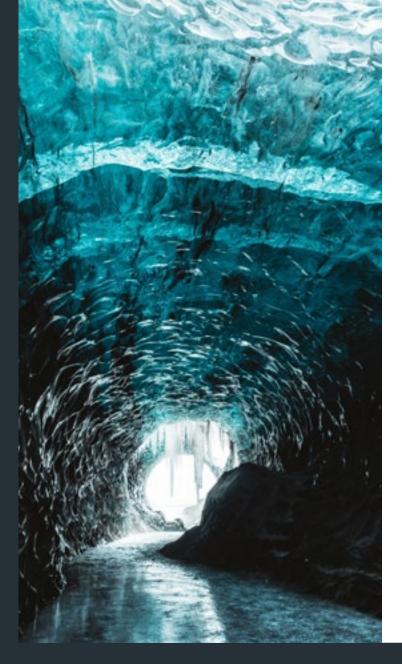
To use the calculator you need to know the hashing power of the miner, power consumption, price of electricity in your country and the mining pool fee. In return you pay the mining pool a fee (usually a percentage). The difficulty (in terms of computer effort) means realistically this is the most practical option to mine Bitcoin. The hashing power and power consumption will be included in the miner specs.

2. Get a Bitcoin wallet

Selecting the right cryptocurrency wallet will depend on your particular circumstances. If you hold one currency then using that currency's official wallet is probably the easiest option.

If you hold more than one currency (or are planning to own more than one) then you will need a wallet that can hold more than one type of currency.

These are the three main single currency Bitcoin wallets with a quick overview.



Bitcoin Core is the software that runs the entire Bitcoin network. A secure digital wallet is included in the software and it can be used to send and receive Bitcoin. Storing your Bitcoin in the wallet will allow users to contribute to the Bitcoin network by validating transactions and storing a copy of the blockchain.

Mycelium is a mobile only wallet (so it cannot be accessed via desktop) and users are able to switch between Bitcoin and standard fiat currency. So essentially users are able to buy and sell Bitcoins for fiat. It can also accept Bitcoin stored on other wallets so can help if users are consolidating Bitcoins stored across multiple wallets.

Electrum is a desktop wallet and has been around since the early days of Bitcoin. It is widely used by Bitcoin holders and it's able to integrate with the major hardware wallets.

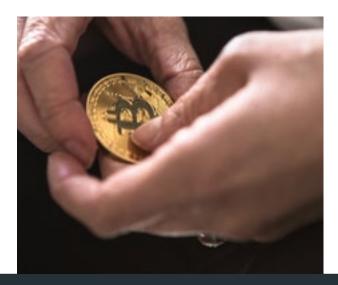
3. Find a mining pool

The reason why joining a mining pool is the most realistic option for **Bitcoin mining** (particularly if you're just starting out) is straightforward. Bitcoins are awarded in blocks and unless you are very lucky you are unlikely to get any of the coins (usually 12.5 coins per block). Bitcoin mining pools began when the mining difficulty increased to the extent that a solo miner could take months or years to generate a block. In a pool blocks can be generated more quickly and the miners can receive a portion of the Bitcoin block reward on a consistent basis rather than more randomly over a long time period. The kind of things you should be looking at when considering your pool is the reward method (e.g. proportional, pay per share); any fees charged for withdrawal; how frequently is a block mined; how stable is the pool and how easy is it to withdraw money. There are many comparison sites and blogs which talk about the different pools.

Once you've selected your pool, it's normally straightforward to sign up and add a worker that will have its own ID so the pool can keep track of your miner and its mining efforts.

4. Get a mining programme

Your miner will already have the appropriate software loaded but you will need a programme for your computer to measure, control and monitor your miner. Once you've chosen your programme, you're ready to mine!



HOW TO MINE ALTCOINS

For those looking to mine new altcoins, you should know that it's significantly easier than mining Bitcoin. This is because the current network hash rate for mining Bitcoin is exceedingly higher than many altcoins.

With a lower network hash rate, the mining process tends to be quicker and more cost effective. Below, we take a look at how you can mine some of the most popular altcoins.

Litecoin

Certain altcoins function differently than Bitcoin in the mining process, such as Litecoin. Litecoin, at its core, is similar to Bitcoin in its code. Bitcoin allows transactions to be approved every 10 minutes, whereas Litecoin allows them to be approved every $2^{1/2}$ minutes. Litecoin also allows for a grand total of 84 million coins to be minted, which is exactly four times higher than Bitcoin. Immediately, you can see that the odds of mining Litecoin are greater than the odds for mining Bitcoin.

Whereas Bitcoin relies on SHA-256, Litecoin relies on scrypt technology, which is more memory intensive than other proof-of-work algorithms. The use of scrypt demands that mining hardware like a GPU mining rig is required, which uses significantly greater processing power. So, while Litecoin is faster and easier to acquire than Bitcoin, it comes at the cost of needing huge amounts of processing power.

Dogecoin

Dogecoin is another altcoin that loosely follows the Litecoin protocol. It similarly makes use of scrypt technology as its proof-of-work scheme and bears a block time of a single minute. To add to its speedy acquisition rates, there is no limit to how many coins can be produced. This naturally brings about negatives. For instance, because it deals with large numbers of coins, their individual value is incredibly low. This can prove beneficial in its accessibility and creates a vacuum for smaller transactions to be enacted, but it would be hard to turn a profit dependent on how expensive your mining setup is.

Ethereum

One of the more well-known altcoins is Ethereum. This coin relies on its own platform-specific cryptographic token, Ether. In essence, Ether can function in multiple ways – it can be traded like any other digital currency and it can even run applications within it and monetise work. It is noticeably quicker for new transactions and coins to be created due to the fact new blocks of data are approved every 15-20 seconds. This guide is certainly not an exhaustive list of altcoins. There are so many out there today with more and more popping up as time goes on.

Litecoin, Dogecoin, and Ethereum are some of the more well-known altcoins, but that does not necessarily guarantee they are the best. As always, cryptocurrency is an investment, and there is a huge risk that your tokens won't increase in value but rather decrease.

Do keep in mind that the hardware you require can vary and that there is no certainty that you won't end up losing money.

Whether you want to know the latest news about mining, equipment or the next best token to focus on, we've got you covered. At Coin Rivet, we deliver the latest news, insights and knowledge in the cryptocurrency industry.

Bringing you news, analysis, opinion and insight from the fast-moving blockchain world. Our team of journalists and contributors cover the likes of cryptocurrencies, wallets, exchanges and ICOs across a wide range of sectors including retail, fintech, banking and gaming. We go beyond the press releases and marketing hype to tackle all the industry topics that matter.

Featured in



FOX AEXPRESS COINGEEK

coinrivet.com 🄰 💿 in 🖻

< 10 >



Independent British blockchain and crypto news