What Is Bitcoin, and How Is It Mined?

Bitcoin is the most recognizable and popular cryptocurrency, and it is mined, or discovered, in the same way as other digital currencies such as Ethereum or Litecoin, although there are variations in the mining process.

A defining characteristic of a cryptocurrency is that it is not fiat money, meaning there is no central issuing authority.

Digital currencies exist only as a series of ones and zeroes and are distributed across computer net- works, much like other information on the internet. Cryptocurrencies are governed by an algorithm that compiles and tracks digital transactions. The transactions are assembled in inalterable blocks that are linked together to form the blockchain, which is the underlying, enabling technology behind all crypto- currencies.

The series of networked computers on which cryptocurrencies live are known as nodes. The nodes store and disseminate the transaction blocks. Some nodes on the network are also miners: spe- cialized computers designed to perform a phenomenal number of calculations. The speed of those computers is indicated by their hashrate, which is measured in trillions or even quadrillions of hashes per second. The higher the hashrate and the more calculations needed to mine a digital currency, the more secure it is.

Inside a digital currency miner, a high-speed computer is trying to guess a random number generated by the cryptocurrency system that, when combined with data in a pending transaction and passed through a hash function, converts input data of any size to output data of a fixed length, like fitting a key into a lock.

Solving the equation verifies the transaction and adds that block to the chain. The first miner to solve the equation is rewarded in cryptocurrency. The more equations a miner can solve, the more money that miner can earn. If it were that simple, however, huge banks of computers might be able to corner the market. So creators of digital currencies built another level of complexity into their governing algo- rithms by regularly raising the difficulty level of the equations needed to add a block to the chain.

For Bitcoin, it takes 10 minutes on average to process a block because that is the pace the developers of the currency determined is necessary to reach the cap they placed on the total number of bitcoins that will ever be created, 21 million, which is expected to be reached some time in 2140. There are currently about 18.5 million bitcoins in circulation. SOURCE: Engineering News-Record