Basics of a monetary system:

1. Creation and production of money.
2. Storage of money.
3. Payment processing (authorization and verification).
4. Settlements (transfer of money – between banks in traditional system)
5. Record keeping.

In our traditional banking system, the banks control these five steps. The Federal Reserve creates the money. Banks control the ledger and the debits and credits entered to the ledger.

Money 1) facilitates trade, 2) stores excess wealth and 3) can be used to determine a common value of items or services for trade.

These bank-controlled centralized ledgers have many *advantages*:

1. They are controlled by a single entity, and access is controlled.
2. All data resides in a central location and is easy to control.
3. A centralized ledger is relatively cost effective.
4. A centralized ledger can be integrated to other systems.

These centralized ledgers also have *weaknesses*:

1. A centralized ledger is more prone to cyber attacks.
2. They lack transparency.
3. They present opportunities for a single point of failure.

Bitcoin and other digital currencies use DLT – Distributed Ledger Technology.

A distributed ledger is advantageous when you want to share a database with people that you don't trust. The technology keeps people from cheating. Bitcoin is a digital currency that uses a distributed ledger technology and puts all 5 steps of the monetary system outlined above into hands all around the world.

Decentralization of a digital monetary system:

1. **Creation and production of money.** It's done by the Bitcoin Miners. High-powered computers compete to be the first to validate a series of transactions, called a block, and add the block to the blockchain. Miners are paid transaction fees and 6.25 BTC per block for their efforts (if they solve the block correctly). That's around $349,000 at today's prices.

2. **Storage of money.** Digital wallets, either online (hot) or offline (cold). Public keys are your cryptographic address. A digital version of your mailbox. Your private key unlocks your mailbox and decrypts transactions.

3. **Payment processing.** Public keys allow you to receive Bitcoin, while private keys ensure that only you can receive and access your funds. Payments are made from your wallet. Bitcoin transactions are encoded into a block.

4. **Settlements, validation.** The transaction is broadcast on the Bitcoin network, where each participant validates and propagates the transaction until it reaches almost every node in the network. The transaction is verified by a mining node and included in a block of transactions that is recorded on the blockchain.

5. **Record keeping.** Once recorded on the blockchain and confirmed by sufficient subsequent blocks, the transaction becomes a permanent part of the Bitcoin open-distributed ledger and is accepted as valid by all participants.

Miners are essential to the process. By convention, the first transaction in a block is a special transaction that starts a new coin owned by the creator of the block. This adds an incentive for nodes to support the network and provides a way to initially distribute coins into circulation, since there is no central authority to issue them.

The steady addition of a constant of amount of new coins is analogous to gold miners expending resources to add gold to circulation. In our case, it is CPU time and electricity that is expended. The incentive can also be funded with transaction fees. If the output value of a transaction is less than its input value, the difference is a transaction fee that is added to the incentive value of the block containing the transaction.

Bitcoin mining is essential to the decentralized distributed ledger. Proof of work and proof of stake are the two most popular ways of processing cryptocurrency transactions. While they vary in crucial ways, proof of stake and proof of work are designed to assure users that payments will go through as expected.

Most of the established cryptocurrencies on the market use either proof of work or proof of stake. The most established proof-of-work cryptocurrency is Bitcoin, while the preeminent proof-of-stake asset is Ethereum.

The main difference between proof of work and proof of stake is that proof of stake relies on crypto staking, while proof of work relies on crypto mining. These methods add new "blocks" of transactions to the historical record, and both provide a way for users to earn additional crypto.

The bottom line: Proof-of-stake cryptocurrencies allow people to pledge or lock up some of their holdings as a way of vouching for the accuracy of newly added information. Meanwhile, proof-of-work cryptocurrencies require people to solve complex cryptographic puzzles — which can incur significant energy costs — before they're allowed to propose a new block.

Proof-of-work basics

Proof of work was the first widely used blockchain consensus mechanism (a term describing how users of a decentralized crypto network agree about who owns what).

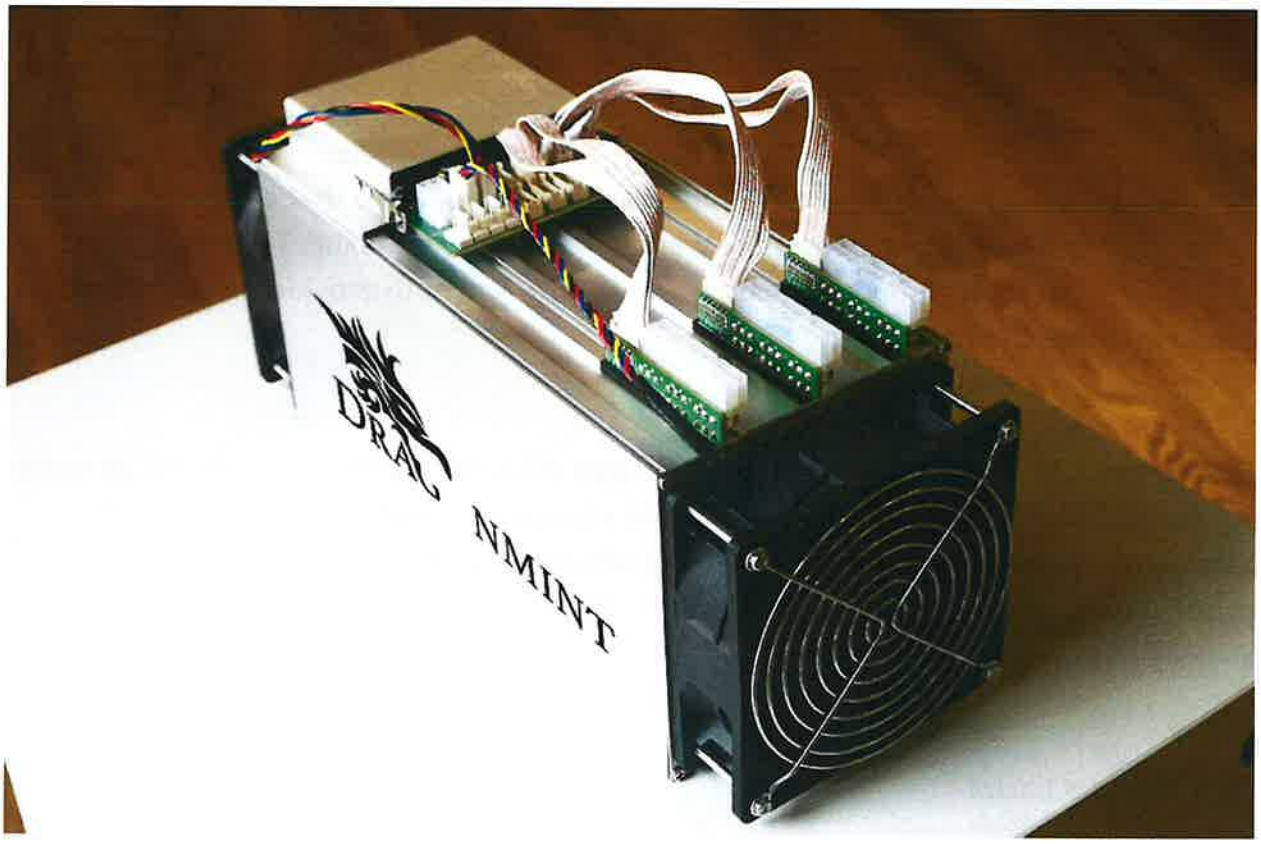
Proof of work requires users to mine or complete complex computational puzzles before submitting new transactions to the network. This expenditure of time, computing power and energy is intended to make the cost of fraud higher than the potential rewards of a dishonest action.

Supporters of proof-of-work cryptocurrencies argue that their methods are straightforward and time-tested. For instance, Bitcoin has been working properly 99.99% of the time since 2009, according to one analysis.

What is an ASIC Bitcoin Mining Machine?

Since it's now impossible to profitably mine Bitcoin with a standard computer or laptop, you'll need specialized hardware called ASICs.

Here's what an ASIC miner looks like up close:



The Dragonmint 16T miner.