SUBMITED TO

MR. BINUMON JOSEPH

SUBMITED BY

ALEENA THERESA GEORGE

S9 INT MCA

ASSIGNMENT

**CRYPTOCURRENCY**

A cryptocurrency is a digital or virtual currency that is secured by cryptography, which makes it nearly impossible to counterfeit or double-spend. Many cryptocurrencies are decentralized networks based on blockchain technology—a distributed ledger enforced by a disparate network of computers. A defining feature of cryptocurrencies is that they are generally not issued by any central authority, rendering them theoretically immune to government interference or manipulation.

* A cryptocurrency is a new form of digital asset based on a network that is distributed across a large number of computers. This decentralized structure allows them to exist outside the control of governments and central authorities.
* The word “cryptocurrency” is derived from the encryption techniques which are used to secure the network.
* Blockchains, which are organizational methods for ensuring the integrity of transactional data, is an essential component of many cryptocurrencies.
* Many experts believe that blockchain and related technology will disrupt many industries, including finance and law.
* Cryptocurrencies face criticism for a number of reasons, including their use for illegal activities, exchange rate volatility, and vulnerabilities of the infrastructure underlying them. However, they also have been praised for their portability, divisibility, inflation resistance, and transparency.

**1. Bitcoin**

Bitcoin is the original cryptocurrency and it remains the go-to leader of the space. As of this writing, the market capitalization of the world's top digital currency is more than $125 billion, with a price per coin of more than $7,305.

There are roughly 17.1 million BTC in circulation, according to coinmarketcap.com. This is all in spite of earlier speculation about a Flippening, in which other digital currencies would permanently take over the No. 1 spot. That has yet to transpire. (See more: "The Flippening": Will Ethereum Take Bitcoin's Place?)

**2. Ethereum**

Ethereum, the digital token which prompted the rise of the initial coin offering (ICO), comes in second on our list of cryptocurrencies by market cap. It is significantly smaller than bitcoin; the current market cap is just shy of $50 billion, with a trading price of about $500 per token. There are just over 100.7 million ETH tokens in circulation as of this writing.

**3. Ripple**

The No. 3 slot goes to the much-hyped Ripple, with a total market capitalization of more than $19.8 billion. Unlike the top two digital currencies (as well as the one directly following it), the price of each XRP token is very small. As of this writing, it's just over 50 cents per token. On the other hand, the total number of XRP in circulation is quite high. There are over 39 billion tokens in circulation now.

**4. Bitcoin Cash**

Bitcoin cash, the spin-off of bitcoin which launched as a result of a hard fork, comes in fourth in our ranking. The total market cap of this digital currency is about $14.5 billion, with a market price of $843 per coin and a total circulation of just over 17.2 million BCH.

**5. EOS**

Rounding out the top five is EOS, with a market cap of $7.83 billion and a total circulation of more than 896 million tokens.

Compete Risk Free with $100,000 in Virtual Cash

Put your trading skills to the test with our FREE Stock Simulator. Compete with thousands of Investopedia traders and trade your way to the top! Submit trades in a virtual environment before you start risking your own money. Practice trading strategies so that when you're ready to enter the real market, you've had the practice you need. Try our Stock Simulator today .

**How cryptocurrency works**

The source codes and technical controls that support and secure cryptocurrencies are highly complex. However, laypeople are more than capable of understanding the basic concepts and becoming informed cryptocurrency users.

Functionally, most cryptocurrencies are variations on Bitcoin, the first widely used cryptocurrency. Like traditional currencies, cryptocurrencies’ express value in units – for instance, you can say “I have 2.5 Bitcoin,” just as you’d say, “I have $2.50.”

Several concepts govern cryptocurrencies’ values, security, and integrity.

### **Blockchain**

A cryptocurrency’s blockchain (sometimes written “block chain”) is the master ledger that records and stores all prior transactions and activity, validating ownership of all units of the currency at any given point in time. As the record of a cryptocurrency’s entire transaction history to date, a blockchain has a finite length – containing a finite number of transactions – that increases over time.

Identical copies of the blockchain are stored in every node of the cryptocurrency’s software network – the network of decentralized server farms, run by computer-savvy individuals or groups of individuals known as miners, that continually record and authenticate cryptocurrency transactions.

A cryptocurrency transaction technically isn’t finalized until it’s added to the blockchain, which usually occurs within minutes. Once the transaction is finalized, it’s usually irreversible. Unlike traditional payment processors, such as PayPal and credit cards, most cryptocurrencies have no built-in refund or chargeback functions, though some newer cryptocurrencies have rudimentary refund features.

During the lag time between the transaction’s initiation and finalization, the units aren’t available for use by either party. Instead, they’re held in a sort of escrow – limbo, for all intents and purposes. The blockchain thus prevents double-spending, or the manipulation of cryptocurrency code to allow the same currency units to be duplicated and sent to multiple recipients.

### **Private Keys**

Every cryptocurrency holder has a private key that authenticates their identity and allows them to exchange units. Users can make up their own private keys, which are formatted as whole numbers between 1 and 78 digits long, or use a random number generator to create one. Once they have a key, they can obtain and spend cryptocurrency. Without the key, the holder can’t spend or convert their cryptocurrency – rendering their holdings worthless unless and until the key is recovered.

While this is a critical security feature that reduces theft and unauthorized use, it’s also draconian. Losing your private key is the digital equivalent of throwing a wad of cash into a trash incinerator. While you can create another private key and start accumulating cryptocurrency again, you can’t recover the holdings protected by your old, lost key. Savvy cryptocurrency users are therefore maniacally protective of their private keys, typically storing them in multiple digital (though generally not Internet-connected, for security purposes) and analog (i.e., paper) locations.

### Wallets

Cryptocurrency users have “wallets” with unique information that confirms them as the temporary owners of their units. Whereas private keys confirm the authenticity of a cryptocurrency transaction, wallets lessen the risk of theft for units that aren’t being used. Wallets used by cryptocurrency exchanges are somewhat vulnerable to hacking. For instance, Japan-based Bitcoin exchange Mt. Gox shut down and declared bankruptcy a few years back after hackers systematically relieved it of more than $450 million in Bitcoin exchanged over its servers.

Wallets can be stored on the cloud, an internal hard drive, or an external storage device. Regardless of how a wallet is stored, at least one backup is strongly recommended. Note that backing up a wallet doesn’t duplicate the actual cryptocurrency units, merely the record of their existence and current ownership.

### **Miners**

Miners serve as record-keepers for cryptocurrency communities, and indirect arbiters of the currencies’ value. Using vast amounts of computing power, often manifested in private server farms owned by mining collectives comprised of dozens of individuals, miners use highly technical methods to verify the completeness, accuracy, and security of currencies’ block chains. The scope of the operation is not unlike the search for new prime numbers, which also requires tremendous amounts of computing power.

Miners’ work periodically creates new copies of the blockchain, adding recent, previously unverified transactions that aren’t included in any previous blockchain copy – effectively completing those transactions. Each addition is known as a block. Blocks consist of all transactions executed since the last new copy of the blockchain was created.

The term “miners” relates to the fact that miners’ work literally creates wealth in the form of brand-new cryptocurrency units. In fact, every newly created blockchain copy comes with a two-part monetary reward: a fixed number of newly minted (“mined”) cryptocurrency units, and a variable number of existing units collected from optional transaction fees (typically less than 1% of the transaction value) paid by buyers.

Worth noting: Once upon a time, cryptocurrency mining was a potentially lucrative side business for those with the resources to invest in power- and hardware-intensive  mining operations. Today, it’s impractical for hobbyists without thousands of dollars to invest in professional-grade mining equipment. If your aim is simply to supplement your regular income, plenty of freelance gigs offer better returns.

Though transaction fees don’t accrue to sellers, miners are permitted to prioritize fee-loaded transactions ahead of fee-free transactions when creating new blockchains, even if the fee-free transactions came first in time. This gives sellers an incentive to charge transaction fees, since they get paid faster by doing so, and so it’s fairly common for transactions to come with fees. While it’s theoretically possible for a new blockchain copy’s previously unverified transactions to be entirely fee-free, this almost never happens in practice.

Through instructions in their source codes, cryptocurrencies automatically adjust to the amount of mining power working to create new blockchain copies – copies become more difficult to create as mining power increases, and easier to create as mining power decreases. The goal is to keep the average interval between new blockchain creations steady at a predetermined level. Bitcoin’s is 10 minutes, for instance.

### **Finite Supply**

Although mining periodically produces new cryptocurrency units, most cryptocurrencies are designed to have a finite supply – a key guarantor of value. Generally, this means that miners receive fewer new units per new blockchain as time goes on. Eventually, miners will only receive transaction fees for their work, though this has yet to happen in practice and may not for some time. If current trends continue, observers predict that the last Bitcoin unit will be mined sometime in the mid-22nd century, for instance – not exactly around the corner.

Finite-supply cryptocurrencies are thus more similar to precious metals, like gold, than to fiat currencies – of which, theoretically, unlimited supplies exist.