Cryptocurrency

Bitcoin is an amazing evolution of currency. Learn why this new form of money will be the currency of the future.

To understand what cryptocurrency is, you have to start at revisiting the concept of currency itself.

Currency is a system of money. The rules of how the money is created, distributed, valued, and stored is normally set forth by the institution that is issuing the currency. For instance, the US dollar is issued by the federal government. The government determines when and how much to print, what denominations to use, and how to introduce the currency into circulation. This is considered a **centrally controlled system**. That means that the government has control over the currency. In the US, the dollar value is allowed to adjust based on supply and demand. However, the government could print a lot of dollars and devalue the currency all by itself. The value of our dollar could plummet and it would have nothing to do with economic factors but solely due to the centralized controller determining that it is going to flood the market with newly printed notes.

A good example of this currency manipulation was when President Nixon's administration took America off the "gold standard." Before this time, the dollar actually could be redeemed for a given amount of gold held by the government. Unfortunately, by having currency that is tied to gold it meant that there was a real limit to the amount of money that would be available for circulation. This has the ability to cripple the growth of an economy. Because of this, the US dollar was devalued and no longer represented an amount of gold held by the government. Today, the dollar only has value because we believe it does. That sounds frightening, but it is the very basis of currency. If the world was plunged tomorrow into a cataclysm of epic proportions, your dollars and your gold would mean nothing and food and fuel would become the new currency.

The government manipulation of the currency in this example is one of the major drawbacks of many centralized currencies. Wouldn't it be amazing to have a reliable currency that was not centralized, didn't allow anyone to print new currency with impunity, and could be universally accepted and exchanged? Enter **cryptocurrency**.

Everyone has the Ledger

Decentralizing currency is not an easy task. When you have a bank, they are in charge of keeping track of all of the transactions and balances of their clients. If you do not have a centralized control system, then who is tracking the currency? For cryptocurrency the answer is everyone. If you want, you can download the ledger of every single transaction that has occurred in the life of a cryptocurrency.

Let's say you were part of a group of people that started a bank. In order that no one person could steal from the bank by manipulating the bank ledger, you made everyone keep the same ledger. On top of that, before you added anything to the ledger, all members have to agree that the new transaction is valid and authentic. And the ledger is kept in ink, so no one could change the ledger once it had been written to. This would be a very safe and reliable system of tracking money. This is a lot like the system

of cryptocurrency. The ledger is what is known as the **Block Chain**. The members of this bank would be considered cryptocurrency **miners**.

Can I be a Miner? Yes you can!

One of the benefits of a currency that is de-centralized is that anyone can engage in it. There is no account to set up. Cryptocurrencies do not have your name or account information attached to them. To mine a currency, you just need to load software on a computer. This software will down load the ledger and start to act like the bankers in our example. It will take pending transactions, use mathematical processes to validate their authenticity, and then send out their findings to be verified with other miners and then accepted and written to the register. The more powerful your computing power, the more transactions you can verify.

So why should you consider mining? It seems like you are just lending your computer to a system to increase its reliability and security.

As discussed before, centralized agencies determine when and how much currency to print and move into circulation. For cryptocurrency, the new currency is generated by mining and awarded to the miners. That means that as your computer is maintaining the integrity and security of the system, it is also generating income in the form of cryptocurrency. Cryptocurrencies have a built in maximum number of currency units that they will generate. This is like the gold standard in that there is a set amount of the currency that will be mined. For Bitcoin, this value is 21 million Bitcoins. Once that level is reached, there will be no more newly minted Bitcoins. So why will people still mine at that time? When this happens, the miners will still profit from transaction charges they can receive from verifying new currency transactions.

Wallets

Wallets are computer programs or hardware devices that allow people to store and transact their cryptocurrency. Many wallets are available for desktops and mobile devices. They will install on your device and setup a special security key. When you want to receive some Bitcoins, your wallet generates an address (a long alphanumeric string of characters) and you send it to the person sending you the currency. They will input the address into their wallet, assign the amount of currency to transfer, and send it into the system. The miners will see this transaction and start mathematically verifying it. Once done, they will add it to the Block Chain and the transaction is complete. Your wallet will receive notification that the transaction is verified and the new currency is yours to spend.

The mathematics involved is complicated and performs many functions to protect the system and to keep the transactions anonymous. One of the more important things is to prevent double spending of currency. If you have a centralized currency system, this is easy. If you write two $100 checks on your checking account with only $100 of cash deposited, the first check that arrives will be cashed. There is not enough cash for the second check so it will be declined. One of the more difficult problems in decentralized systems is determining the order of transactions so that the correct sequence of payments is recorded and currency isn't allowed to be spent twice. This is one of the reasons for the miner's concurrence on the transaction and the timing of the transaction.

This has been a very basic introduction to the concept of cryptocurrency. Bitcoin was a pioneering currency, but it is not the only cryptocurrency out there. Whether you are excited about the concept of a stable, non-government regulated form of currency or you think the whole thing is just bunk, there is little chance that this new form of buying and selling is going to go away anytime soon.

