Cryptocurrency Primer

A brief history of Cryptocurrency and how it evolved from its dark roots to coming out into the light and being a respectable business.

When computers first became mainstream in the early 1980's many consumers were interested in getting software for their computers. Software made the computers more versatile and useful. Many consumers began forming computer clubs to share in computer software since quality computer programs were expensive. It was not uncommon for users to pool their funds to buy software and make copies for each of them. Computer clubs were really an excuse to copy software.

Software companies soon began making copy protection schemes to try to prevent copying and hackers were people who tried to circumvent those copy protections.

Soon computers were connecting to each other over modems and phone lines and bulletin board services were set up that allowed people to download software or engage in discussions. People began to download software on these systems.

One problem with downloading software is that sometimes noise on the line could cause the data to be corrupted. So hashing was a method of testing the download file was the same as the original file. I found this definition online:

> **Hashing is the process of converting an input of any length into a fixed size string of text, using a mathematical function.**

I hashed the above text to get this SHA-256 hash example:

731eea0d902f8cb05884998bb9d4785f092749919e6114c76185a915561d60b6

It doesn't matter how big the file you hash, the output is the same length.

Crypto wallets were inspired by the copying example above. When certain websites would be online offering software to be downloaded, authorities could shut them down. Therefore users came up with a decentralized method. The idea was that instead of having a server and peers connected to the server, where the server was vulnerable, they created a peer to peer system also known as P2P. Each peer would run on a computer and connect to other peers forming a network. If one peer was shut down the network would continue. Also Bitcoin was created **Open Source** which means that the

source code was posted publicly so that people could look at the code to make sure there wasn't anything dishonest about it.

The original Bitcoin wallet worked this way. A user could download the wallet application and it would connect to the network. Once a peer was found it would receive a list of other peers from it. Once a minimum number of peers were found the program would then download the database in what is called synchronizing. As the blocks are downloaded the transactions are verified by the hash method above to verify that the database transactions are valid. This chain of blocks being verified by hashing is called **Blockchain Technology**. It's a trusted way to verify that the database is accurate and cannot be manipulated. Each new block is built on top of the other.

Bitcoin was developed when connection to the internet was slow and not very reliable. Therefore it was designed to have 10 minutes between each block, giving the wallets time to build consensus and verify blocks. When I developed Paccoin, I chose a 1 minute block time as by 2013 we had higher internet connection speeds. However over time I realized that one minute block time also meant longer synchronization times and larger database sizes for new wallets coming online, so when I developed Kema Coin I decided to go with 5 minute block times.

Bitcoin was developed by Satoshi Nakamoto, probably a pseudonym for the original developer. Because it was posted online in open source format people began to copy it and make different cryptocurrencies and improving it along the way.

Originally people used Bitcoin as a method of payments on the Dark Web. Users could make payments that were semi-anonymous. For example people used a website called Silk Road that allowed users to pay for drugs or contraband online with bitcoin.

However Bitcoin has come out of the dark and is being used for legitimate business purposes including buying computers or mining equipment. Many websites are beginning to accept payment for products online with cryptocurrencies. Even big companies like JPMorgan and Facebook are talking about creating their own cryptocurrencies, and states are putting forth legislation to accept tax payments in the form of cryptocurrencies.

The time for cryptocurrencies has finally arrived, we think an exchange that is available in all 50 states has a potential for real growth.

Bill Corless