Jeanine Woody

MA 400

Senior Thesis

Cryptocurrencies and Real-World Applications

Cryptocurrencies are a form of electronic commerce that is created through crypto systems. These systems tend to create a chain, which is known as a blockchain, and is compiled through encryption and decryption techniques. These techniques have evolved through many practices specifically through the creation and application of theories from Euclid, Fermat, Mersenne, Euler, Gauss, and Fibonacci. Their respective theories led to developments in Number Theory—the properties of positive integers and its reliance on factoring and testing prime numbers. Number Theory has been a key aspect in developing computer algorithms. Their respective findings helped to curate one of the most widely used cryptosystem known as Rivest-Shamir-Adleman (RSA) Cryptosystem. RSA Cryptosystems rely on encryption and decryption techniques based on Number Theory. There are two distinct types, public and private, which each have specific characteristics. In a public key, also known as an Asymmetric Cryptograph, anyone is able to encrypt messages using the receiver's public key, but only those with a private key could decrypt the message. For those who use RSA systems, a digital signature is created at the end of the message to show the connection to the sender.

The most well-known form of Cryptocurrency, Bitcoin, was created by the anonymous Satoshi Nakamoto in 2008. His paper called "Bitcoin - A Peer-to-Peer Electronic Cash System" presented the idea that electronic cash should be shared through online payments via a peer-to-peer system that would function without an intermediary third party. The purpose of the paper

was to prove that electronic commerce should rely more on cryptographic systems instead of trust. This would ultimately allow for transactions to occur directly between two individuals.

Cryptocurrencies are prominent in a few industries, specifically Financial Technology and Machine Learning. The Financial Technology (Fin Tech) section normally uses cryptocurrency blockchain protocols in what is known as a Distributed-Ledger Technology (DLT). The application of DLT to different aspects of the Fin Tech industry allows for cost savings because an outside third party is not needed to verify transactions. According to this protocol, no single entity or government body could determine the inflation rate of the transactions, instead they would be determined by an algorithm. Machine Learning is based on pattern recognition and the theory that computers can learn specific tasks without being programmed to do so. Researchers of this topic attempt to observe the correlation between data sets and artificial intelligence. In the United States, regulatory agencies like the U.S. Commodity Futures Trading Commission (CETC) view cryptocurrencies as commodities, while the Internal Revenue Service (IRS) views them as properties. On the other hand, the Securities and Exchange Commission (SEC) does not recognize cryptocurrencies as securities despite the fact that they stress that types of e-currency in the market need surveillance to monitor their application. These differences make it difficult for regulation policies to be put into effect to monitor cryptocurrencies. The real-world application shows how different industries rely on aspects of the exchange to perform certain tasks within their designated spheres.