menugem®
27 Wildwood Rd Springfield, IL 62704-4359
(217) 836-0276 www.menugem.com

Ryan Fernandez – Writing Sample 1 – Blockchain and Bitcoin

Blockchain
Blockchain is a data structure used to store information securely by linking blocks of information together and recording the data in multiple places simultaneously. The strength of blockchain lies within its ability to hold data not in one central database but on many computer servers across the world on a peer-to-peer (P2P) network. The information stored in a blockchain can be easily verified and is theoretically so authentic that it can be treated as a definitive system of record.

Using the blockchain technology as a platform, software developers can create applications that run on the blockchain. The most popular application using this technology is the virtual currency Bitcoin.

In 2008 an anonymous technology expert using the pseudonym Satoshi Nakamoto wrote a paper introducing the idea of Bitcoin. His paper outlined how the underlying technology, the blockchain, would work. Although the author did not explicitly use the term blockchain in the 2008 paper, the writing describes linking information together in a "chain of blocks" (Nakamoto 7). The existing term blockchain has since been used when referring to the concepts described by Nakamoto.

Smart Contracts
The software and logic used on top of a blockchain are called smart contracts. In the case of Bitcoin and other virtual currencies, smart contracts could include transaction approval, the amount to transfer for a transaction, and which account numbers are involved in the transaction. But smart contracts are not limited only to uses involving currency.

An individual or organization could use smart contracts to store dental records. Smart contracts could be used for storing tax filing information, driver information, or whatever kind of information would benefit from being in a ledger.

Virtual currencies happen to be prevalent in the news during the current time, but virtual currencies are just one of many applications that can be made using the blockchain and smart contracts.

Bitcoin Miners
As stated in Rob Marvin's PC Mag article the essential parts of a block on a blockchain consist of:

- Unique cryptographic signature (hash ID)
- The asset or transaction data (the thing of value)
- A timestamp
- The hash ID of the previous block

Bitcoin miners verify the world's Bitcoin transactions, put them into blocks, and add them to the Bitcoin blockchain. Since the hash ID is a non-numeric, encrypted ID, the challenge lies within

finding the hash ID of the next block to go on the blockchain. It has to be a value that, when hashed, begins with a number of zero bits, and that is within a "hash limit" defined by the logic of the virtual currency. Bitcoin miners use computing power to find an appropriate value for the hash ID. Doing so will "win" them the right to hash the next block. When a miner successfully adds a block to the ledger he or she is rewarded in Bitcoin.

Banks and Bitcoin
The way to purchase Bitcoin is through a digital currency exchange. Of these, Coinbase is the most popular at the moment. Bitcoin can be purchased through Coinbase using PayPal, a credit or debit card, or a bank account. Bitcoin sellers can receive money by connecting a bank account to their Coinbase account. Alternatively, Coinbase users can deposit funds into their own Coinbase account to buy and sell Bitcoin.

Local vendors and Bitcoin
It's up to each business that accepts Bitcoin to administer its own method of accepting payment. According to website Bitcoin Wiki there is no centralized way of accepting payment, although with various software platforms such as Bitpay, customers can pay in Bitcoin using smartphones and QR codes to exchange such information as the Bitcoin wallet address and transaction amount.

Bitcoin Summary
Because of the structure of Bitcoin's hash ID, the creation of new Bitcoins is said to be finite. According to website Bitcoin Wiki the final Bitcoin will be mined in the year 2140.

As for crypto-currencies in general, I believe more time is needed to see how central banks of the world continue to react, how major financial firms react, and how investors behave. I believe more time is needed to develop a long- term strategy on the subject.

Among the crypto-currencies in existence, Bitcoin is the most established because it has the longest blockchain, which has been in existence for the longest time and therefore is a more dependable system of record.

Security
So far, events of hacking involving crypto-currencies are attacks to the software (such as apps using virtual currency wallets). In these cases, amounts of currency are illegally moved between accounts, which is unfortunate for the hacked account holders, but the currency itself still exists. In these cases, the applications being hacked are running on top of the currency blockchain, but the blockchain data structure itself is a sound one. The data stored in the blockchain is always secure.

Works Cited

“Controlled Supply.” Bitcoin Wiki. Website Publisher, 7 December 2017 Published. Web. 11 December 2017 Accessed.

“In-store Transactions.” Bitcoin Wiki. Website Publisher, 1 November 2014 Published. Web. 11 December 2017 Accessed.

Marvin, Rob. "Blockchain: The Invisible Technology That's Changing the World." PC Magazine 29 August 2017

Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System." 2008.