Cryptocurrency

Dilpreet Singh Bajwa

POST 5: 8-7-18/Cryptocurrency

Crypto-Currency: A cryptocurrency or crypto currency is a digital or virtual currency that uses strong cryptography for financial transactions and it is difficult to counterfeit the cryptocurrency. Cryptocurrency is not issued by any central authority like banks, making it theoretically immune to government interference or manipulation. The decentralized control of each cryptocurrency implements with the help of technology called **blockchain**.

Block Chain: A blockchain is a continuously growing list of records, called **blocks**, which are linked and secured using cryptography and are added to the blockchain in chronological order. By design, blockchains are inherently resistant to modification of the data. It is "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way. The validity of each cryptocurrency's coins is provided by a blockchain.

Block: A block is the 'current' part of a blockchain, which records some or all of the recent transactions. Each block typically contains a hash pointer as a link to a previous block, a timestamp and transaction data. Once completed, a block goes into the blockchain as a permanent database. Each time a block gets completed, a new one is generated. There are countless number of such blocks in the blockchain, connected to each other (like links in a chain) in proper linear, chronological order. Every block contains a hash of the previous block. The blockchain has complete information about different user addresses and their balances right from the genesis block to the most recently completed block.

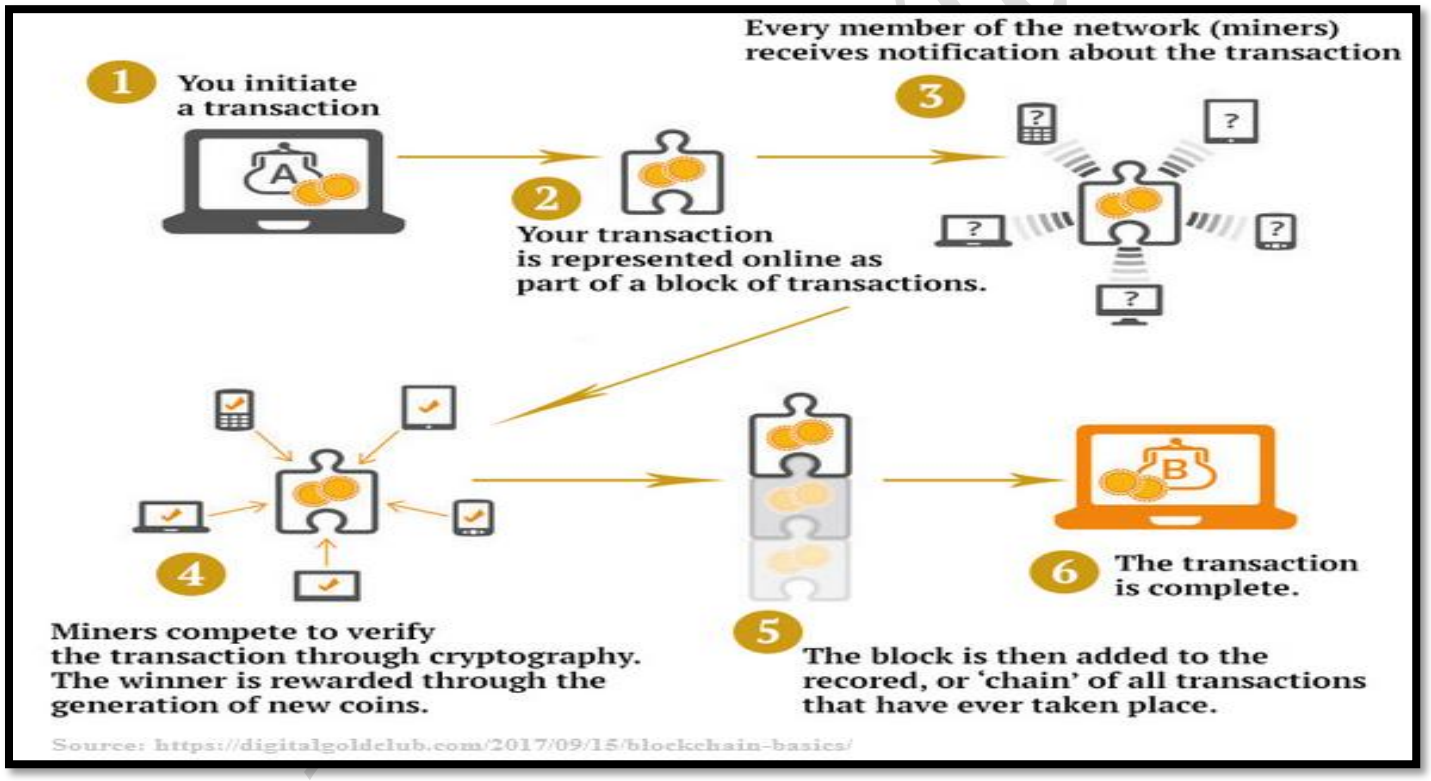
Advantage: With blockchain, every time someone makes a transaction, that transaction is recorded in a block so that it remains permanently available. When the next block is created, it will contain a cryptographic record of the previous block, essentially holding that previous' block transaction history. As more and more people send money, more and more blocks are created and linked to one another into the blockchain. If someone wanted to hack a transaction or duplicate it, they'd have to attack the entire blockchain.

Miners: *In case of cryptocurrencies, everyone using the coin/crptocurrency contribute to linkage of blocks. The people or machines on behalf of users of cryptocurrency link these transactions or blocks are called as* ***miners.*** Miners compete against one another to solve a complex mathematical equations using their computer's processor or graphics card. When a miner finds a solution, the transactions

within the block are considered to be confirmed and the miner is rewarded. In exchange for a small fee, they link together the transactions and create the blocks to be added to the blockchain. In some cases, there are special computers designed specifically for mining cryptocurrency, called ASICs.

How it all Works: Suppose you want to send coin (cryptocurrency) to someone, you initiate an transaction for it. Your transaction is represented online as part of block of transactions and forwarded to network of computers for verification/validation. This network is a network of miners, They got notification about transaction now and compete with each other to verify the transaction through cryptography. Once miners verify the transaction, the transactions combined to form a block and then this block is added to the existing blockchain. The miners whose machines are first to verify transactions and maintain a blockchain are rewarded by allocating them new cryptocurrency/coins. At last the updated block chain is distributed to entire network and used for future verification.

Below is a blockchain diagram to better explain the concept:



Bitcoin is generally considered the first decentralized cryptocurrency launched in 2009 by some unknown group or person under the pseudonym Satoshi Nakamoto. As of May 2018, there were over 17 million bitcoins in circulation with a total market value of over $140 billion.

Sources:
https://www.investopedia.com/terms/b/blockchain.asp
https://www.investopedia.com/terms/c/cryptocurrency.asp
https://blockgeeks.com/guides/what-is-cryptocurrency/
https://en.wikipedia.org/wiki/Cryptocurrency
https://globalcoinreport.com/why-monero-xmr-should-be-preferred-over-bitcoin-btc/
https://heimdalsecurity.com/blog/posts/page/3/
https://www.bloomberg.com/news/articles/2018-01-02/criminal-underworld-is-dropping-bitcoin-for-another-currencymarkets
https://learnblockchainfast.org/blog-1/2018/3/30/mining
https://learnblockchainfast.org/blog-1/2018/3/30/mining
https://digitalgoldclub.com/2017/09/15/blockchain-basics/

Google Drive Link: https://drive.google.com/file/d/17MAUZ1A3TjSUO9vbnYIjc3GGderD3uBh/view?usp=sharing