Blockchain and Cryptocurrency

Shanaya Mehta

April 16, 2018

1 Introduction

A cryptocurrency is a digital asset that uses cryptography for securing the asset and for anti-counterfeiting purposes. According to *An Overview of Blockchain Technology: Architecture Consensus and Future Trends*[1], the blockchain is a technology that serves as a decentralized, immutable ledger for transactions that take place across a peer-to-peer network. Cryptocurrency and blockchain have been used reciprocally ever since the first cryptocurrency was developed. Presently, blockchain has found applications in many industries apart from cryptocurrencies. Blockchain and cryptography, combined, have changed how humans interact financially.

The paper, *Bitcoin: A peer-to-peer electronic cash system*[2], (Satoshi Nakamoto, 2008), describes the functioning and logic behind a cryptographic, trust-based payment system, a first of its kind of the cryptocurrency BITCOIN. Bitcoin uses decentralized blockchains for recording the transactions and maintains the complete anonymity of the person that has made the transaction. The transactions are entirely untraceable, however.

Today, many different cryptocurrencies have been developed which have various differentiating features; however, all of these cryptocurrencies use the blockchain technology to record the transactions. None of these cryptocurrencies is associated with any particular bank or nation, and hence anyone with a powerful computer and access to the internet can mine the cryptocurrency.

2 How Cryptocurrencies Work

Some terminologies common to all cryptocurrencies using blockchain include: "Block", "Blockchain", "Mining", "Hash", "Fork". A "block" is essentially a data structure which contains the transaction data. A "blockchain" is a public ledger containing a list of all transactions that have taken place. It is constantly growing as transactions occur and add to the ledger. The blocks comprise of transaction records from all previous transactions.

Mining refers to the verification step for making a cryptocurrency transaction and to add to the blockchain. It also introduces new cryptocurrency units on the system. A hash refers to a one-way function that takes as an input, data of variable size and outputs fixed length data. The hash function should be able to produce a unique output each time. A fork is a quantity generated when two blocks are created seconds apart. Forks are resolved by adding the block received first to the blockchain and subsequent blocks are added in new blocks.

A cryptocurrency uses distributed verification of transactions without a central authority monitoring the public ledger. As mentioned in *A Brief Survey of Cryptocurrency Systems*[3], cryptocurrencies work as follows:

- The user has a digital wallet with a generated address (a public key)

- This wallet contains a private key which is used to sign the transactions and serves to prove the ownership of the wallet
- The payer sends money to the payee's address and signs it using the payer's private key
- Mining verifies the transaction and the transaction record is then added to the blockchain ledger

The blockchain typically consists of fields as follows: a magic number, the block size, the block header, the transaction counter and the transaction itself. The first block of any cryptocurrency contains the first transactions. There is a unique path from each transaction record to the first record to minimize collision and access time, which serves as a security feature to avoid tampering by hackers.

3 Discussions

3.1 Some popular cryptocurrencies

There are plenty of cryptocurrencies available for use of which three of the more popular ones (apart from Bitcoin) are mentioned below:

- Litecoin, *Litecoin Hits an All-Time High*[4] [online]
  Launch year: 2011. It is based on a public global payment system, uncontrolled by any authority. As a proof of work, it uses "scrypt", which is decoded by a set of CPUs (Central Processing Units). It is said to have a faster block generation rate and hence an even faster transaction confirmation than Bitcoin. It is fast growing to be a widely accepted cryptocurrency amonst businesses and developers alike.
- Ethereum (Ether Gas tokens) *Ethereum: A secure decentralised generalised transaction ledger*[5]
  Launch year: 2015. Ethereum is a blockchain-based decentralized distributed system. Ethereum-based applications are run on its platform-specific cryptographic 'token' called "Ether". The Ether tokens are analogical to vehicles for moving around. The Ether token is used chiefly by developers.
- Ripple, *The ripple protocol consensus algorithm*[6]
  Launch year: 2012. Ripple, in its truest sense, does not make use of mining. It is typically a trust-based system to attain consensus whose goal is for each server to apply the same set of transactions to the current ledger. Hence, a new ledger is created every few seconds and a transaction is any proposed change to the ledger.

3.2 Drawbacks

As mentioned above, some of the cryptocurrencies allow complete anonymity in transactions and they are untraceable. This promotes illegal activity and since there is no regulatory body for cryptocurrency regulation, this is a significant demerit of the peer-to-peer electronic cash system.
The other drawback of such a system is scalability. The blockchains do not allow uploading of information that is huge in size and hence one cannot upload data such as images and videos.

3.3 The Bitcoin Bubble

In the recent years, cryptocurrencies saw a tremendous adoption rate since people started becoming aware of the existence of such a digital asset and a new technology. This led to the rise in the price of especially the Bitcoin, and the value peaked at almost three times the previous price. After this abnormal price surge, the price for Bitcoin fell considerably. This is known as the Bitcoin bubble.

4 Conclusion

In this article, the terms blockchain and cryptocurrency have been discussed at great length. The blockchain technology has indeed revolutionized the way transactions are conducted and stored, while cryptocurrencies have changed the mode of transactions and made it possible to conduct digital transactions. Blockchain will enable an increased number of people and businesses to trade much more freely and efficiently than before, which will significantly boost local as well as international trade.

While the merits of crytocurrencies continue to outweigh the demerits, it remains to be seen how many of these cryptocurrencies will withstand the competition and stay influential and relevant in the upcoming years.

References

[1] Z. Zheng S. Xie H. Dai X. Chen H. Wang "An Overview of Blockchain Technology: Architecture Consensus and Future Trends" 2017, IEEE International Congress on Big Data (BigData Congress) pp. 557-564 2017.

[2] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system", 2008, [online] Available: http://www.bitcoin.org/bitcoin.pdf.

[3] U. Mukhopadhyay, A. Skjellum, O. Hambolu, J. Oakley, L. Yu, R. Brooks, "A brief survey of cryptocurrency systems", 2016 14th Annual Conference on Privacy Security and Trust (PST), pp. 749-752, 2016.

[4] Litecoin Hits All-Time High — Investopedia. [online] Available: https://www.investopedia.com/news/litecoin-hits-alltime-high/

[5] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger", Ethereum Project Yellow Paper, vol. 151, 2014.

[6] D. Schwartz, N. Youngs, and Arthur Britto, "The ripple protocol consensus algorithm", Ripple Labs Inc White Paper, 2014.