Crypto Currencies & Consensus Mechanism in Finance

Abdul Shakeel [1] • Tariq Mahmood [2] • Hafiz Nasir Ali [3] • M. Iqbal khan [4]

[1] MPhil in mathematics, Punjab Education Department, District Vehari, Pakistan
[2] Ph.D. Affiliation in Punjab Education Department, District Vehari, Pakistan
[3] Postdoctoral fellows, I.I.University, Islamabad, Pakistan
[4] Punjab education department, district Multan, Pakistan
tmniazi2002@yahoo.com

Abstract. This paper is about digital currency and its ways to handle transactions in business matters. The purpose of this paper is to show how to minimize the risks of transactions and how to make the quickest transactions. And by which fake transactions or the slow process of transactions be avoided. The consensus mechanism is consisted of proof of stake and proof of work regarding security, validity, and verifying transactions in financial matters. Proof of work is considered more secure than proof of stake but proof of work is slow than proof of stake. Therefore, it may be stated there are some advantages and disadvantages of both ways of consensus mechanisms. As proof of Stake is a quick way but comparatively less secure than proof of work but proof of stake is the quickest way to make transactions. Anyhow, it may be stated that in the matter of digital transactions, for every person who wants to send or receive, directly or indirectly, the primary desire is the safety of the transaction and validity within the shortest period. So that proof of transaction can be provided to the other party and kept for record purposes also. In short, this paper guides cryptocurrency and its consensus mechanism for financial transactions.

1. Definition

Cryptocurrency is a digital currency that is used online to receive money and pay digital payments. It may be done through digital wallets. This transaction is made by banks but banks do not verify this transaction. The transaction system is actually peer to peer system; a person can send and receive it in a few seconds while sitting in any place. This is also used in trade and the transaction is made through a decentralized system after verifying different stages.

2. Beginning of Crypto Currency

This started as a BTC Bitcoin in the year 2009. The initial price was zero dollars. And after its mining, its price reached 6900 and its price depends upon the market. Cryptocurrency is just like software while the hard currency is just like the hardware of computers just for easy understanding. Or it may be considered a hard book/ paper book while crypto is just like a soft book.

3. Types of Crypto Currencies

From 2009 to up till 2022, there are 10397 cryptocurrencies are being used in the digital business, and day by day, this number is being increased. In the year 2014, 506 numbers of currencies were used reached 10397 in number. This means since 2014, it may be stated that more than the 20th fold, it has increased. This thing reflects the popularity of crypto or soft currency.

4. Cryptocurrency Exchanges

In all these cryptocurrencies, the operation is performed through exchanges. Near about 137 exchanges are working in the world now. These exchanges are being used to covert dollars into cryptocurrency and crypto into any other internationally acceptable currencies From these exchanges of the world, the top exchanges are Binance; Coin Base; Kraken; Crypto.com; Gemini; Gateio; Kucoin; Its temp; Bittrex; and Bit flyer.

The crypto exchange is a marketplace where cryptocurrency is being transacted. This is just like other exchanges used for trading. There are two types: one is called Centralized which is unsafe and invalid while the other is decentralized exchanges are valid and safe. The trading fee is applied to the transaction. Anyhow, it may be stated that the value of cryptocurrencies regarding dollars or pounds cannot be the same as it changes even within a day. This means sometimes its values decrease

and sometimes its values may increase. As concerned top cryptocurrencies are: Bitcoin, Cardano (ADA), Ethereum (ETH), Ripple (ZRP), Lite coin (LIT), Binance coin (BNB), Dogecoin (doge), Bitcoin cash. Tether (LISDT), Polkadot (DOT). Besides these cryptocurrencies, there are many other cryptocurrencies in thousands of numbers that are also dealing digitally in transactions and business.

5. Countries where digital currency is legal

The United States, Canada, Australia, El Salvador, Denmark, France, Germany, Iceland, Japan, Mexico, Spain, and the United Kingdom.

6. Countries where Bitcoin is being regularized

In these countries, Bahrain, Burundi, Cameron, Central African Republic, Gabon, Georgia, Ghana, Kuwait, Lesotho, Libya, Macao, and Maldives. As concerned the situation of cryptocurrency in India, it has been regularized since January of this year but a 30 percent tax has been levied on cryptocurrency transactions. This shows that in the above countries, crypto has been legalized because of its uses and its increasing business in the digital market.

7. Countries with absolute Ban

These are Algeria, Bangladesh, China, Egypt, Iraq, Morocco, Nepal, Qatar, and Tunisia. While In India, in January 2022, it has been legalized while the Case of Pakistan is in Court. It is expected that decision in Pakistan will also legalize. And the court has given them three months time period to Government concerned authorities for preparing its framework regarding its authenticity and legalization. In Pakistan, Waqar Zia is the name due to this personality, because of this person, the court has issued orders to legalize and regulated crypto as the digital currency. As concerned the consensus mechanism is used to validate the digital transaction.

8. Consensus Mechanism

A consensus mechanism is a methodology that is used to validate online transactions. Anyhow, it has been tried to eliminate the risk or decrease the chances of risk. A higher risk will notify about lower validity. But in economics, it is considered that the higher the risk, the higher the profit will be while if there is a low level of risk in investment the lower will profit from the concerned investment.

A consensus Mechanism is a fault-tolerant mechanism that is used in computer and blockchain systems to achieve the necessary agreement on a single data value or a single state of the network among distributed processes or multi-agent systems such as with cryptocurrencies. It is useful in record keeping among other things. The consensus mechanism is known as

proof of work (POS) which requires the exertion of computational power to solve a different but arbitrary puzzle to keep all nodes in the network honest. A consensus mechanism refers to any number of methodologies used to achieve agreement, trust, and security across a decentralized computer network. In the context of blockchain & cryptocurrencies proof of stake (Pos) is two of the most prevalent consensus mechanism. (Mansa, 2021).

For improvement in online business, it is necessary that validity of online transactions can be adopted only by ending the risks measures, and deficiencies. The matter of fact is that with the change of currencies, and transaction methodologies, many types of new frauds are also being adopted.

Proof of Stake is a cryptocurrency consensus mechanism for processing transactions and creating new blocks in a blockchain. A consensus mechanism is a method for validating entries into a distributed database and keeping the database secure. While proof of work is a competitive approach to verifying transactions which naturally encourages people to look for ways to gain an advantage, especially since the monetary value is involved (Field 2021).

Both are approaches used to verify transactions regarding process and validity and period also. Both are competitive with each other.

Proof of Work (POW) & Proof of Stake (POS) is the two main ways cryptocurrency transactions are verified. Proof of work is more secure than proof of stake but it is slower and consumes more energy. Proof of Stake requires participants to put cryptocurrency as collateral for the opportunity to successfully approve transactions (Chandler, 2021).

The success of the transaction may be verified from the approaches. Similarly approaches also inform about the level of transaction whether it is quick or slow.

9. Advantages & disadvantages of Proof of Work (POW)

The advantages are as under:

High level of security, provides a decentralized method of verifying transactions and allows minors to earn a crypto reward.

The disadvantages are as under:

Inefficient with slow transaction speeds and expensive fees, High energy usage, Mining often requires expensive equipment; (Editor, 2022)

Through proof of work, minor investors can earn income from their investments. In this small investors can invest money to earn profit like the big investment. It has advantages as well as disadvantages.

10. The advantages & disadvantages of Proof of Stake

The advantages of proof of stake are as under:

Effectively communicate messages, Navigate customers & clients around your business, Entice people into your store, Discount in store without having to lift a finger, Creativity, imagination & personality in displaying products & services, The ability to retain customers and leads by encouraging them to interact with business, Promote any usual or photography campaigns, Cross marketing with other brands & companies (Editor, 2021a).

Through this proof of stake, communication becomes easier with increasing creativity and imagination but the problem lies with the currency which is comparatively more costly, and the chances of destruction.

Disadvantages/Cons of Proof of Stake:

It can be costly, React to competitors, There is potential to offend, and Vandalism (wreckage).

Disadvantages of not having Proof of Stake

You need manpower, People may not understand your business, Offers & information about brands may not be communicated, You may lose customers, and Competitors may have stronger branding (Editor, 2021b).

In absence of a P.o.S, personal customers may be shifted to another place. Furthermore, you have to hire a labor force for work.

11. Properties of Consensus Mechanism

A consensus mechanism protocol has the following few key properties which determine its applicability & efficacy:

I. Safety; According to the rules of protocol, if all nodes produce the same output and the output produced is valid, the consensus protocol is determined to be safe.

II. Liveness: To liveness of a consensus protocol is guaranteed if all the faulty nodes participating in the consensus eventually produce a value.

III. Tolerance: A consensus protocol provides fault tolerance if it can recover from the failure often or participate in a consensus. Tolerance is the value that is considered valuable in social, and political life.

IV. Non-repudiation: This provides the means to verify that the supposed sender sent the message.

12. Proof of Random Trust

The anti-tempering, transparency, and immutability of blockchain technology provide good support for the realization of a power resource-sharing transaction network. However, the original blockchain's slow transaction confirmation, huge resource consumption, and transaction data leakage have restricted its application in the power grid. To solve deficiencies The proof of Random Trust (PoRT) consensus algorithm, algorithm uses random trust values to solve the shortcomings of the original consensus algorithm consumes a lot of energy and solves the phenomenon of unfair power. It also uses the SSSS encryption algorithm to achieve the privacy of transaction data (Zhang et al., 2021).

By Zhang & et al. (2021) performance analysis can be done through liveness, security, and scalability.

The fact is that many Scholars prefers to analyze the performance of transaction from safety and validity. The further shorter period in verifying the transactions is also considered well.

For analysis of portfolio investment in Bitcoin versus in the S & P Index, gauging for price volatility of the assets, we have constructed a Value at Risk (VaR) Model. This VaR Model constructed only takes into account one of the few investments risk aspect, i.e. risk attributed to Volatility in Price (Barjaktarović et. al. 2014).

In economics, it is considered that the level: of risk identifies the earning level. If there is a lower risk in the matter, the profit will be lower. Higher risk will identify a high level of earnings. Anyhow, forensic accounting may be used for better and long-term results. Forensic accounting is a combination of accounting and investigative techniques used to detect discrepancies and irregularities in financial data (Agarwal, 2019).

Irregularities in currency rates create some dissatisfaction about the status of currency in the eyes of investors. The stable exchange rate is considered favorable for those who do not want to indulge or who do not want to take the risk or who do not play tricks or who want to take a profit with abnormal.

Companies with strong financial statements, low risk of bankruptcy, and earnings manipulation were considered Forensic Positive by V & M, whereas the ones with weak financial statements, high risk of bankruptcy, and earnings manipulation (all directly/ indirectly indicative of fraud) were taken to be Forensic Negative (Mraović, 2008) This is the advantage which is gained especially to the large scale business companies because they can survive in long term. Therefore, they have more possibilities to earn economies of scale on a long scale.

It is fact that with the quickest transactions through digital currencies, now through digital currencies many people or companies invest money in digital currencies and sometimes they earn, and sometimes who do not care about market rates, they may lose or decrease their digital currency investment. Besides this, online fraud or fake transactions or fake accounts or temporary accounts, different frauds, and hacking systems are challenges for validity and online business.

For analysis of portfolio investment in Bitcoin gauging for financial fraud crimes, an Econometric Model has been constructed with variables – Monthly Bitcoin prices and Reported Monthly Bitcoin Hacks. Regression of Bitcoin prices (monthly) on the Reported Bitcoin Hacks of the previous periods (rather than regression of Bitcoin prices (monthly) on Reported Bitcoin Hacks of the same period) has been performed, as it is obvious that financial frauds occurring on the current period will most likely affect the prices of stocks in the following Nonperiod. (Dutta et. al. 2012)

No doubt, due to online transactions and digital currencies, many types of fraud and my practices are being seen and reported. This is why now cybercrime laws are being formulated in different countries of the world to control online and digital frauds.

13. Concluding Remarks

In recap, it may be stated that consensus mechanism guides to do safer and more valid transactions. But this mechanism has approached with some advantages and disadvantages regarding period and validity. Anyhow, the safer and quickest way is through online transactions. The fact is that digital currency and its uses are not the same for all countries because of the status of digital currency and the ATMs of cryptocurrencies. But still, there is required to legalize cryptocurrency, where it has been necessary to establish ATMs and exchanges of cryptocurrencies so that people could be aware of safer payments. Through exchanges, people will be able to exchange the cryptocurrency into dollars or pounds and with dollars or pounds, they will be able to buy certain cryptocurrencies. It is hoped that in the future, like soft books, soft currencies will prevail over hard currencies. Briefly, it may be stated that cryptocurrency will not only save the central bank resources for issuing paper or plastic money but in this way online or digital new types of business and the transaction will be promoted without establishing large premises of the financial institution. In short, new rules to keep citizens safe and fearless from the dangers of soft currency will be mandatory regarding cyber crimes and fake identity or hacking. We all should keep in mind that technology is also being used by criminals as investigation agencies adopt new technology.

Corresponding Author:
Tariq Mahmood, Ph.D.
Affiliation in Punjab Education Department, District Vehari, Pakistan.
E-mail: tmniazi2002@yahoo.com

References:
1. Mansa J., (2021), "Consensus Mechanism", retrieved from www.investopedia.com, updated on November 30, 2021.
2. Field J. F., (2021), "Proof of Stake (POS), retrieved from www.proofofstake.com, updated on December 17, 2021.
   Chandler S., (2021), "Proof of stake versus proof work, retrieved from www.businessinsider.com, December 22, 2021.
3. Editor (2022), "Advantages & disadvantages of Proof of Work", retrieved from www.fool.com, posted on January 21, 2022.
4. Editor (2021a), "The advantages & disadvantages of POS", retrieved from www.peerlessassigns.com, retrieved on February 2, 2021.
5. Editor (2021b), "Properties of consensus mechanism", retrieved from www.oreilly.com, retrieved on December 25, 2021.
6. Zhang, Y., Yan, B., Yao, Y., & Yu, J. (2021). Proof of random trust consensus mechanism for power resource sharing system. Procedia Computer Science, 187, 402-407.
7. Barjaktarović, L., Terzić, I., & Milojević, M. (2014). Testing Applicability of Value at Risk Models in Stocks Markets. Mediterranean Journal of Social Sciences, 5(9), 297.
8. Agarwal, A. (2022). Traditional Stock Market or Cryptocurrency?–Inspecting for a Better Risk-Minimising Investment Portfolio. Asian Journal of Economics, Finance and Management, 9-16.
9. Mraović, B. (2008). Relevance of data mining for accounting: social implications. Social Responsibility Journal, 4(4), 439-455.