Abstract:

CRYPTOCURRENCY MINING -A CENTRALISED EXCHANGE MODEL FOR THORNIEST ISSUES

Dr. RATHNAKAR GATLA
Associate Professor, Department of Management
Kakatiya Institute of Technology & Science, Warangal, TS.

ORCID: https://orcid.org/**0000-0001-6007-9636**

This paper is a modest attempt at cryptocurrency mining, its essence, and gives insights into the cryptocurrency trading mechanism process, and also explores the application of a centralized exchange model for the thorniest issues.

Have we ever wondered what it takes to mine Bitcoin and other cryptocurrencies, and how we may obtain crypto tokens without having to purchase them on an exchange? Many individuals were drawn to the crypto ecosystem by the fast rise in the values of cryptocurrencies such as Bitcoin, Ether, and Dogecoin. While most individuals purchase and trade them on exchanges, it is also feasible to 'mine' these tokens using a computer. The promise of getting paid with Bitcoin is a major lure for many miners. To be clear, do not need to be a miner to possess bitcoin tokens. We can buy cryptocurrencies with fiat currency, trade them on an exchange like Bitstamp with another cryptocurrency like Ethereum or NEO to buy Bitcoin, or earn them by shopping, writing blog posts on platforms that pay users in cryptocurrency, or even setting up interest-earning crypto accounts.

Keywords: Proof-of-work, Proof-of-stake, Proof-of-authority, contract for differences and OTC.

Introduction:

Over the past few years, cryptocurrencies have been rapidly gaining ground and redefining the finance market. The revolution brought forth by these digital assets has stimulated many businesses to capitalize on the crypto sphere by investing in cryptocurrency exchange and radically digitize the monetary transactions.

The first and most well-known application of mining involves Bitcoin, which was created by the pseudonymous Satoshi Nakamoto. While attempts at creating electronic currencies were nothing new even back in 2009, Bitcoin was notable because it was the first truly decentralized currency.

Prior to Bitcoin's inception, all currencies relied on a central authority of some sort. This approach is not ideal for a number of reasons, not least because you have to trust the issuer and everyone higher up in the hierarchy. Even a common service like PayPal, for instance, has complete autonomy over funds you store on the platform and could freeze them at any time. However, flattened this centralized hierarchy. Don't need permission from a central bank or intermediary to use it, nor required to sign anything. In fact, all need is an internet connection. And once you acquire some cryptocurrency, nobody can confiscate it behind back.

Bitcoin achieved this level of decentralization and security through an algorithm called Proof of Work. Mining is simply the real-world application of this algorithm.

Put simply, Bitcoin employs a system wherein anyone and everyone can propose new transactions. However, these transactions are only considered valid when other participants on the network reach an agreement on their legitimacy. The system also ensures that past transactions cannot be edited or reversed by anyone with malicious intent granting Bitcoin the property of immutability.

1. **The selected cryptocurrencies Appraisal:**

Sl. No.	Type of Crypto	Description	Leads	Confines
1.	**Bitcoin (BTC)**	The original, and (for now) the biggest by market capitalisation. It was launched in 2009 by Satoshi Nakamoto, a pseudonym for the mysterious person or group who created it, to secure payments across a peer-to-peer network. It aims to eliminate the need for a trusted third party, democratise money and ensure that transactions are anonymous.	Notorious cryptocurrency	Slow transaction speed and requires specialist mining equipment.
2.	**Bitcoin cash (BCH)**	Bitcoin Cash is a standalone digital currency, created as an offshoot of Bitcoin in August 2017 by a 'hard fork'. This was in response to the slowdown in bitcoin transaction speeds and the network's inability to reach consensus on proposed upgrades. Bitcoin Cash's maximum block size is 8mb, compared to 1mb for bitcoin, enabling it to process more transactions each second.	Faster transaction times than Bitcoin.	Requires specialist mining equipment
3.	**Ripple (XRP)**	Ripple is a cryptocurrency that underpins a payment network called RippleNet – used by major banks and financial institutions, including Santander and American Express. Ripple operates in a very different way to other digital currencies, which has led some to question its credentials as a true decentralised cryptocurrency.	Lightning-fast transaction speeds	RippleNet can be used without its underlying cryptocurrency.
4.	**Stellar (XLM)**	Stellar is a payment network that operates in a similar way to RippleNet	Integrates with the banks and used to	Cryptocurrency is not as widely

		and can process transactions in multiple currencies. It is underpinned by a cryptocurrency called lumens (XLM), which is commonly referred to as 'stellar' (including on the IG platform). Lumens can be used for payments on the network but also play an anti-spam role, as each transaction requires a small transaction fee, which is paid for in the cryptocurrency.	process transactions in multiple currency	recognized as some other.
5.	**Ether (ETH)**	Ether is the cryptocurrency of the Ethereum network, which enables users to code and release their own 'decentralised applications (dapps)' and create 'smart' contracts that automatically enforce their clauses. Small amounts of ether are destroyed as transactions are processed, preventing hackers from spamming the network.	Use beyond cryptocurrency on the Ethereum network, and transactions are fast.	Uncapped supply means it could be inflationary.
6.	**Litecoin (LTC)**	Litecoin is designed to be 'silver to bitcoin's gold', according to its founder Charlie Lee. And just as the supply of silver outstrips the supply of gold, Litecoin's maximum supply of 84 million coins is four times greater than bitcoin's. There is also some fundamental technological differences between the two.	Fast transaction speeds	Low market capitalization, when compared to the top/notorious bitcoin.
7.	**EOS**	EOS is the cryptocurrency of EOS IO, a blockchain platform that is said to replicate the key functionality of a computer's hardware and operating system. It provides tools and services for developers to build apps, including user accounts, authentication and databases. Responsibility for processing and other operations is distributed across the network, which its designers	Integrated with the EOSIO network, fast Transaction speeds	Uncapped supply means that it could be Inflationary

		claim will enable it to scale to millions of transactions per second in the future.		
8.	**NEO**	NEO is the name of both the cryptocurrency and the network it runs on. This network is like Ethereum in that it enables users to create decentralised apps and smart contracts. However, what sets NEO apart is that its network is currently tightly controlled by 'NEO Team', who require users to have a verifiable identity on the network.	integrated with the NEO network, compliant with regulations in many jurisdictions	may not be truly decentralised

The cryptocurrency mining will apparatus the above confines and plummeting the thorniest issues.

2. **Cryptocurrency Mining**

Cryptocurrency mining refers to the process of gaining cryptocurrencies by solving cryptographic equations with the use of high-power computers. The solving process comprises verifying data blocks and adding transaction records to a public record (ledger) known as a blockchain. That is secured by applying complex encryption techniques.

Cryptocurrencies use the decentralised method of distribution and for verification of transactions, it takes the help of cryptographic algorithms. Hence, there is no central authority, nor is there a centralised ledger.

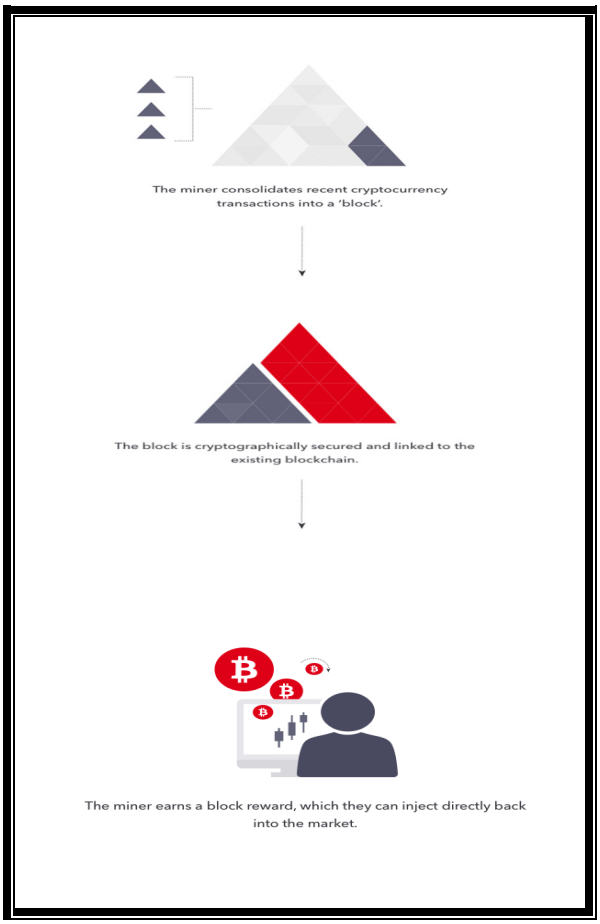
To get new coins on the ledger involves solving complicated mathematical puzzles that assist in verifying virtual currency transactions and then updating them on the decentralized blockchain ledger. As the outcome of this work, the miners receive pay with cryptocurrency.

3. **The process of Cryptocurrency mining**

The mining processes high-power computers (preferably) to solve complex mathematical equations. The first coder to crack all the code can authorise the transaction. As an outcome of the service, miners earn small amounts of cryptocurrency. Once the miner triumphantly solves the mathematical problem and verifies the transaction, they add the data to the public ledger, which is called a blockchain. The process broadly consists of three steps called transition inspection, creating a new block, and starting the mining.

3.1. Transactions inspection

Mining computers select pending transactions from a pool and check to ensure that the sender has sufficient funds to complete the transaction. This involves checking the transaction details against the transaction history stored in the blockchain. A second check confirms that the sender authorised the transfer of funds using their private key.



3.2. Creating a new block

Mining computers compile valid transactions into a new block and attempt to generate the cryptographic link to the previous block by finding a solution to a complex algorithm. When a computer succeeds in generating the link, it adds the block to its version of the blockchain file and broadcasts the update across the network.

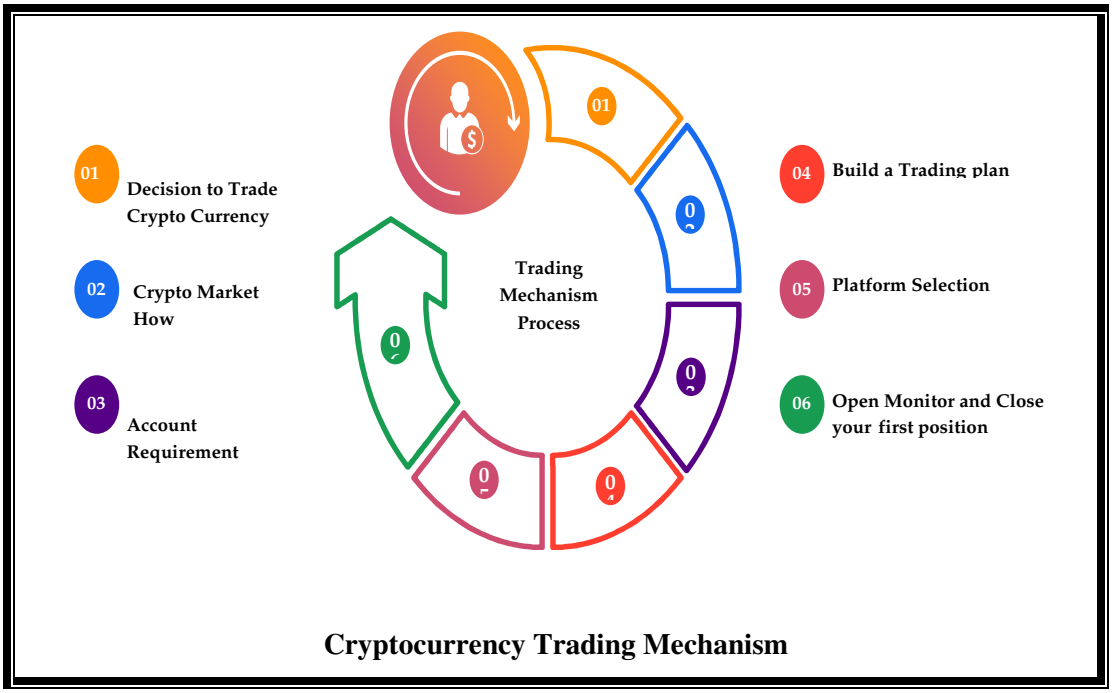
3.3. Start mining (how mining works)

Thinking of beginning mining, first require a high-performance computer. Also, create a wallet for popular cryptocurrencies such as Bitcoin and join a mining pool to accelerate profitability. These pools are groups of miners who join their resources to enhance their mining power. The profit created from mining is then distributed evenly to all members in the pool. Mining pools permit individuals to work together and fight more effectively.

The algorithm acquires several cryptocurrencies, including Bitcoin, Ethereum, and Dogecoin. It guarantees that no single authority becomes so powerful that it starts to run the show. This process done by miners is a crucial part of adding new blocks of transaction data to the blockchain. A fresh block is only added to the blockchain system if a miner appears with a new winning proof-of-work. (PoW). This occur after every ten minutes in the network. Proof-of-work aims to prevent users from printing extra coins they didn't earn, or double-spending. Proof-of-stake (PoS) depends on the community's actual stake in the currency instead of consuming energy in a race to be the first to solve computations. The more currency a "forger" (i.e., the PoS term in lieu of the PoW term "miner") holds, the more transactions can be validated. Proof-of-authority

(PoA) is another method of validating transactions as it relates to cryptocurrency has validators curating their own reputation in order to achieve payout. Validators earn their reputation by running software to put transactions into blocks that require a link to properly identify that validator. This method places every person in the network on equal footing everyone only has one identity.

4. Cryptocurrency Trading Mechanism Steps:



Cryptocurrency Trading Mechanism

4.1. Decision to Trade Crypto Currency

There are two routes to trading cryptocurrencies called speculating on their prices using contract for differences (CFD) or buying the digital currencies in the hope they increase in value.

4.1.1. Trading cryptocurrencies using CFDs

A CFD is a contract in which agree to exchange the difference in the price of a cryptocurrency from when first open the position to when close it. Speculating on the price of the market, rather than taking ownership of the cryptocurrency. If open a long position and the cryptocurrency does increase in value, make a profit, but if it falls in price, make a loss the opposite is true for a short position.

4.1.2. Buying cryptocurrencies via an exchange

Alternatively, might decide to buy a cryptocurrency, which means that you take ownership of a portion of the digital currency outright, with the intention of holding it in a digital wallet and profiting if it increases in value.

Before starting, you will need to open a cryptocurrency wallet and an account with a cryptocurrency exchange. There can be steps to this process, and you might have to join a waiting list for an account.

4.2. Cryptocurrency market works

The cryptocurrency market operates in a different way from other financial markets, which makes it vital to learn how it works, and understand the jargon used to describe it, before start trading.

The cryptocurrency market is a decentralised digital currency network, which means that it operates through a system of peer-to-peer transaction checks, rather than a central server. When cryptocurrencies are bought and sold, the transactions are added to the blockchain a shared digital ledger which records data through a process called ‘mining’.

Cryptocurrencies are also famously volatile, which makes it important to know what is likely to move the market this could be anything from ICOs and blockchain forks, to breaking news and government regulation.

4.3. Open an account

When trade on cryptocurrencies, instead of buying them, you can be ready to open a position much faster. Need not a digital wallet or an account with an exchange. In fact, all need to trade via CFDs is an account with a leveraged trading provider.

4.4. Build a trading plan

Having a trading plan is crucial to success for any trader but even more so for cryptocurrency traders because the market can see high amounts of volatility. This is a double-edged sword volatility makes the market extremely attractive, but difficult to trade. This is why trading plan should include risk management tools, as well as an outline of goals, which cryptocurrency want to trade, and a methodology for entering and exiting trades known as a trading strategy.

A plan should also include the way to analyse the cryptocurrency market either through technical or fundamental analysis. Technical analysis focuses on the price movement of a cryptocurrency and its historical patterns, while fundamental analysis looks at the external factors and macroeconomic data that impact the digital asset. Whichever the method chooses, it is important to remain up to date with any news that could impact the market, as cryptocurrencies are especially sensitive to market sentiment.

4.5. Choose cryptocurrency trading platform

Trading platforms can provide with a smarter and faster way to trade cryptocurrencies CFDs with personalised alerts, interactive charts and built in risk management tools.

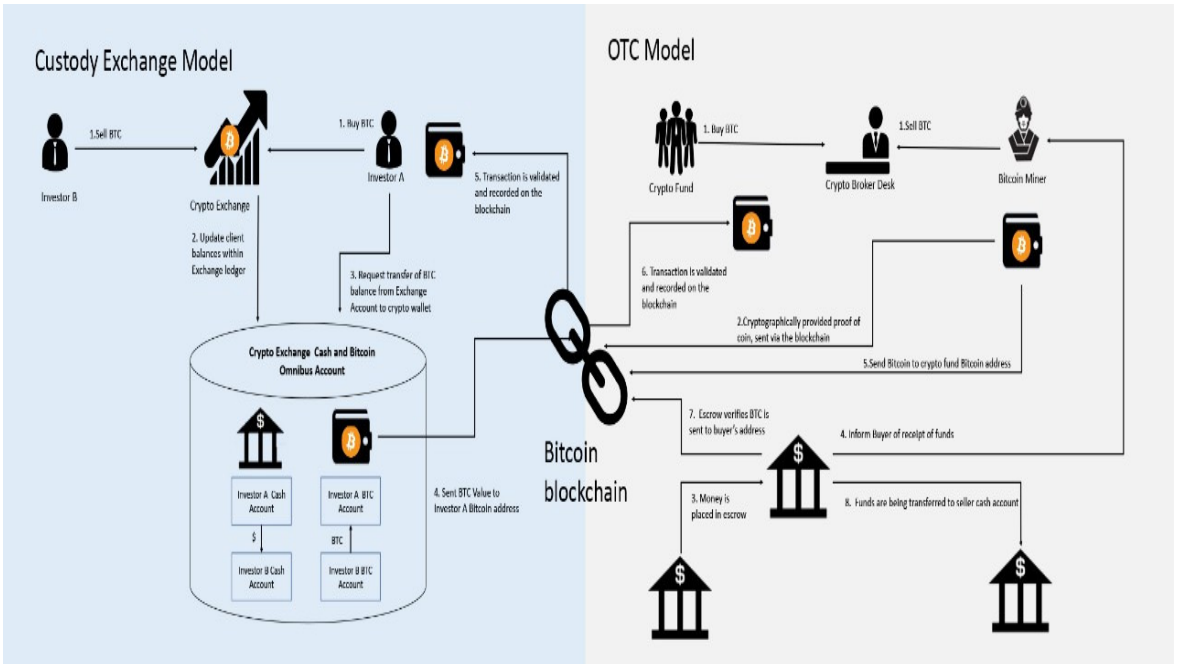
4.6. Open, monitor and close first position

As there is no need to own a digital wallet, once opened an account and chosen the platform, can start trading cryptocurrencies straight away.

Whether decided to trade bitcoin, ether, litecoin or another cryptocurrency, all need to do is open the deal ticket for the chosen market, and see both a buy and a sell price listed. be able to decide the size of the position, and then select buy to open a long position or sell to open a short position. Remember, add stops or limits to close the trade once it hits a certain level and protect the trade from unnecessary risks. Monitor the profit or loss of the position in the 'open positions' section of the dealing platform. And when decided that it's time to close the position, just need to place an equivalent trade in the opposite direction.

5. Centralized Exchange Model (Hi-tech Trading Mechanism)

The centralized exchange model is the dominant approach for trading digital assets and cryptocurrencies in public blockchains because it solves the limitations of numerous blockchain protocols relating to trading speed and settlement fees. (Mining fees as per transaction rather than the traded value.) However, this poses significant issues for the market in that parties to a trade are exposed to the security of the crypto exchange during the transaction process. As a result, there is growing scepticism about the relevance of the centralized exchange model, and most institutional participants are utilizing OTC mechanisms to facilitate trading and settlement of crypto assets. The vast majority of transactions conducted on cryptocurrency exchanges are "off-chain" transactions.



Centralized Exchange Model

The custody and OTC models being utilized and the challenges surrounding delivery-versus-payment mechanisms reveal that as the crypto market evolves, so, too, are solutions to address the thorniest issues.

6. Factors that have a significant impact on their prices at the cryptocurrency market

Cryptocurrency markets move according to supply and demand. However, as they are decentralized, they tend to remain free from many of the economic and political concerns that affect traditional currencies. While there is still a lot of uncertainty surrounding cryptocurrencies.

a. **Supply:** The total number of coins and the rate at which they are released, destroyed or lost.
b. **Market capitalisation:** The value of all the coins in existence and how users perceive this to be developing.
c. **Press:** The way the cryptocurrency is portrayed in the media and how much coverage it is getting.
d. **Integration:** The extent to which the cryptocurrency easily integrates into existing infrastructure such as e-commerce payment systems.
e. **Key events:** Major events such as regulatory updates, security breaches and economic setbacks.

7. Conclusion

Cryptocurrency mining is an interesting alternative to the traditional centralized systems that currently operate throughout the world. However, it's very taxing in terms of computer and power resources and isn't feasible for many users as a result. Led by the success of Bitcoin, other cryptocurrencies such as Ethereum, Ripple, or Dogecoin, to name a few, have emerged and have experienced rapid growth and expansion. Mining is necessary for the operation of these decentralized virtual currencies.

A number of crypto startups admit that the centralized model of crypto-exchanges was a necessary first step to develop the market, but that the next evolution will come from decentralized exchanges. While this type of venue currently represents trivial volumes, it is gaining significant attention and might represent the next evolution and/or addition in the cryptocurrency exchange landscape. new trading mechanisms would certainly blur the line between exchange and OTC trading.

References

1. Antoon Spithoven (2019). Theory and Reality of Cryptocurrency Governance, *Journal of Economic Issues*, 53:2, 385-393, DOI: 10.1080/00213624.2019.1594518.
2. Chen, Yan, Igor Pereira, and Pankaj C. Patel (2020), Decentralized Governance of Digital Platforms, *Journal of Management*, 20, 1-33.
3. Evans, David S. (2014). "Economic Aspects of Bitcoin and Other Decentralized Public-Ledger Currency Platforms."Working Paper No. 685 (2nd series), *Coase-Sandor Institute for Law and Economics, University of Chicago*, April 2014
4. Gilbert, Scott and Hio Loi. 2018. "Digital currency risk." *International Journal of Economics and Finance* 10 (2):108.
5. Hayes, A. Cryptocurrency value formation: An empirical study leading to a cost of production model for valuing bitcoin. *Telemat. Inform.* 2017, 34, 1308–1321.
6. Hileman, Garrick and Michel Rauchs. 2017. Global Cryptocurrency Benchmarking Study. *Cambridge: University of Cambridge, Judge Business School.*
7. Hughes, Scott D. 2017. "Cryptocurrency Regulations and Enforcement in the U.S." *Western State University Law Review* 45 (1): 1–28.
8. Le Khac, N.A.; Kechadi, M.T. Application of data mining for anti-money laundering detection: A case study. In Proceedings of the 2010 IEEE *International Conference on Data Mining Workshops*, Sydney, Australia, 13 December 2010; pp. 577–584.

9. Loi Luu, Yaron Velner, Jason Teutsch, and Prateek Saxena. 2017. Smartpool: Practical decentralized pooled mining. *In 26th {USENIX} Security Symposium*pages 1409–1426.
10. Luu L, Velner Y, Teutsch J, Smartpool: Practical decentralized pooled mining[C] in 26th {*USENIX} Security Symposium ({USENIX} Security 17*). 2017: 1409-1426.
11. Munoz, J.Z.I.; Suarez-Varela, J.; Barlet-Ros, P. Detecting cryptocurrency miners with NetFlow/IPFIX network measurements. *In Proceedings of the 2019 IEEE International Symposium on Measurements and Networking*, Catania, Italy, 8–10 July 2019.
12. P. McCorry, C. F. Shahandashti, and F. Hao, "A smart contract for boardroom voting with maximum voter privacy," in *International Conference on Financial Cryptography and Data Security*, Malta, 2017, pp. 357-375.
13. Sanz-Bas, D.; del Rosal, C.; Alonso, S.N.; Fernández, M.E. Cryptocurrencies and Fraudulent Transactions: Risks, Practices, and Legislation for Their Prevention in Europe and Spain. Laws 2021, 10, 57.
14. Xiaopeng Li, Zhuo Li 2020A Performance Measurement and Optimization Mechanism for Blockchain Mining Pool System ICBTA 2020: 2020 the 3rd International Conference on Blockchain Technology and Applications December 2020 Pages 27–33 https://doi.org/10.1145/3446983.3446991.