iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** VI **Month of publication:** June 2023

DOI: https://doi.org/10.22214/ijraset.2023.53913

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VI Jun 2023- Available at www.ijraset.com

Blockchain Business Model and Security

Dharmik Gangani[1], Anuj Vaghani[2]
[1, 2]*Department of Information Technology, Sarvajanik College of Engineering & Technology, Surat Gujarat 305010 India*

Abstract: Blockchain has become the most mentioned or a trending topic on the internet. Today, it is used for many purposes such as smart contracts, keeping records of financial data for banks, data management for government agencies or services-based companies, etc. Blockchains are phlebotomizing money. Now a day there is a plethora of different networks or tokens available. Each and every token and network has its own pros and cons. You can use this cryptocurrency to purchase goods or services on the platform or transfer it to various exchanges. But the point is how this token or cryptocurrency generates revenue from providing different services. How are individual networks able to be upheld value in the blockchain market?
This research aims to know what are the different ways through which a blockchain company makes money and what things are important to run a profitable blockchain company and also researches what kind of vulnerability and problems occur in the blockchain. Blockchain networks are not immune to cyberattacks and fraud. Through this, we hope to increase the transparency of the Blockchain Business model to enhance the public's trust in blockchain networks and help to make a decision on which blockchain networks are profitable and good for future investments.
Keywords: Blockchain, Ethereum, Security, Vulnerability, Sustainable, Ethereum Virtual Machine(EVM), Taxonomy, Business Model.

I. INTRODUCTION

As the title proposes, a blockchain may be a developing chain of blocks(Transaction records) that holds information about transactions taking place over the web, or we can say networks and platforms. In the traditional database, all data is stored in a centralized form or structure and unstructured way. But, Blockchain does not store any data in a centralized form all data is stored in terms of the block. Blockchain is a highly secured system that records raw data such that it is complex to change or hack its content or data by cheating the system. All recorded transactions are visible to authorized persons or participants, traceable within the networks, immutable and irrevocable, which prompts the increasing usage of blockchains for data sharing and financial transactions in supply chains. These things make blockchain special compared to other technologies.
Now a day there are so many blockchain tokens or networks available The principal challenge associated with blockchain is a lack of awareness of the technology, especially in the banking sector, healthcare, insurance, financial services, P2P financial market, and a widespread lack of understanding of how it works. that is why every company makes sure its networks and smart contract are secure and fast. This is hampering investment and the exploration of ideas. But the big issue that emerges is how these businesses make profits. Well, in this research, we are going to try to address this question.

II. BLOCKCHAIN

As the name suggests, blockchain is nothing but a growing chain of blocks (records) that holds information about transactions taking place over the web. Every block (a record) contains data in the form of coding that is organized in a chronological manner. The main purpose of the blockchain is to allow fast, secure, immutable, and transparent end-to-end transactions. It is a trusted, decentralized network that allows for the transfer of digital money, flash loans, identity, and data.
As people understood the value of privacy and secure transaction. Modern consumers or clients have demanded concepts such that not storing any data or records on third-party servers and involvement of any government policy, it became a need of time to create a technology that will take the control of data from such organizations and give it to the people vis-à-vis network. Before we reach the main objective of writing this research paper. let understanding important of blockchain functionalities and elements will help to get a clear idea of how blockchain companies and networks generate revenue (in terms of financials).

A. Blocks

In short, the term block refers to the digital files that store transaction data and metadata. Blocks are data structures within the blockchain database.

So all information about blockchain transactions and financial records store inside these blocks, and every newly generated block is connected to the previous one through the use of cryptographic techniques its called secure hash using a hashing algorithm. There are a lot of things included in a block that is very important to how it works.

The blocks have three important components:

1) The transaction data
2) A unique cryptographic code called hash with timestamp
3) The hash of the previous block.

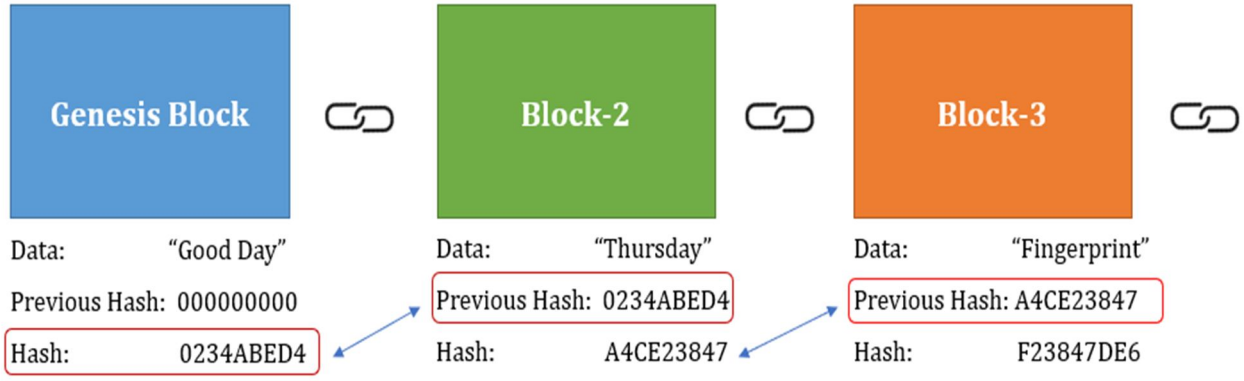


Fig. 1 Example of Cryptographic linking in blockchain

If I'm talking about block statistics, blockchain can generate one block every 10 minutes. In short, every 10 minutes, 2.4 terabytes of data will be added to the blockchain size. In one day, 350 GB is added in one day and 127 TB every year. This also means that there is no ledger limit. Block size can create issues in the future: The issue of block size limit brings new problems. Now it just starting of the blockchain era if this growth is continuous then we have to come up with a better solution. The block size will increase exponentially, it will require more time for crypto miners to solve a block. As a result, transactions become slower.

B. Transaction fees (Gas price)

Blockchain Transaction fees measure the average fee in USD when an Ethereum transaction is processed by a miner and confirmed with the transaction takes place. The reason gas is important is that it helps to require an appropriate fee is being paid by transactions submitted to the network. By ensuring that a transaction pays for each action it performs (or causes a smart contract to perform), we ensure that the network doesn't become bogged down with performing a lot of unwanted work that isn't valuable to the customer and sender. Which network requires less gas depends on how smart contract developers write functions and assign variables.

So if gas is basically a transaction fee, how do you pay it and gas is an actual token? This is where it gets a little complicated and problematic. gas prices vary from network to network. Although transaction fee (gas) is an element that things can be measured in, there isn't any actual token for gas. That is, you can't own 100 gas. Instead, gas exists only inside the Ethereum virtual machine (EVM)as a count of how much action is being performed by a smart contract. When it comes to actually pay for the gas or transaction fee, the gas is charged as an ether token, the built-in token on the Ethereum network, and the token with which miners are getting a bounty for producing blocks.

Providing too large amounts of gas is also different than providing too much ether. If you set a very high gas price, you will end up paying lots of ether for only a few actions, just like setting a super high transaction fee in Ethereum. You'll definitely be prioritized to the front of the line, but is to let your money is gone. If you provided a low gas price, however, and just attached more ether than was needed to pay for the gas that your transaction required, the left amount or gas will be refunded back to your wallets.

Miners only charge you for the assemble valid transactions into a block. You can think of the gas price as the hourly wage for the miner, and the gas cost as their timesheet of work performed. Miners set the price of gas based on supply and demand for the computational(Hardware) power of the network needed to process smart contracts and other transactions. You pay miners gas (in the form of ETH *consider token is ETh) to process your transactions and interactions with smart contracts.

The gas calculation formula is:

Gas limit * base free + tip

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VI Jun 2023- Available at www.ijraset.com

III. BLOCKCHAIN BUSINESS MODEL

Since Satoshi Nakamoto published the proposal to make a virtual currency system that will take the control of data from such organizations and give it to the people vis-à-vis the network. After that Blockchain technology seems to have gained life in businesses and it creates more and more value. a lot of companies have started operating with blockchain in their business. Blockchain is an emerging and highly disruptive technology that is poorly understood and in its beginning phase. Cryptocurrency get attention after Bitcoin prices soared suddenly in 2017, reaching an all-time high of $19,783 the same year. How it can create value in cryptocurrencies and in many other practical applications like a token exchange and flash loans?

A business model describes a plan or strategy of a company to sell a product or service and generate revenue from there. Each company will create its ways of handling business and take necessary decisions to increase the growth of the company. let's understand how the blockchain business model works and generates profit.

The formula of generate profit is simple: Profit=Total Revenue-Total Expenses (consumes < sells)

A. CEX

Cryptocurrency exchanges are platforms that open the door for the trading of cryptocurrencies for other assets, including digital and stable currencies. In effect, cryptocurrency exchanges act as an intermediary between a buyer and an owner and generate revenue from commissions and transaction fees. Exchanges enable you to buy and sell cryptocurrency in several ways. You can place a market order and buy or sell cryptocurrency at the market base price.

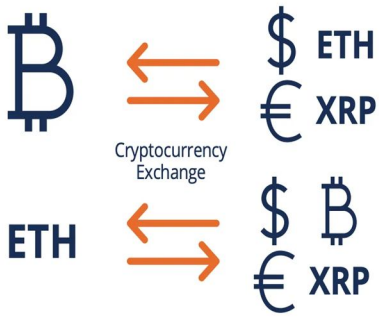


Fig. 2 Cryptocurrency Exchanges

On common cryptocurrency exchanges, $10 can be exchanged for an Ethereum of equivalent value, and vice-versa. Similarly, Ethereum worth $10 can be exchanged for solona of equivalent value. The same concept can be applied to different assets or networks based on what is offered by the exchange.

So, how do cryptocurrency exchanges (CEX) make money?

For a cryptocurrency exchange to make money, it needs to attach to some of the financial momentum flowing through it. In most cases, that means assessing fees for common transactions, such as:

1) Trading Fees
2) Deposits made when moving crypto to online storage spaces, like digital wallets
3) Withdrawals and liquidations
4) Flash Loans

Well, crypto exchanges make money off trading fees: When you buy or sell something, you pay the exchange a cut. These vary exceptionally. by the size of the trade and often by the trader's monthly volume and, of course, there are withdrawal fees for coins or tokens. Clients also pay blockchain trading fees, but those don't go to exchanges. there are transaction fees any time you move Bitcoin from one wallet to another, or from an exchange to a wallet. The fees are determined by the number of transactions that are in the mempool waiting to be confirmed. As I'm typing this, the bitcoin mempool is empty so your transaction costs are at a 6+ month low. In May 2021, Ethereum's Highest transaction fee was over $71.72!!!

The cost of a flash loan depends on the platform providing it. A 0.09% fee is collected from the Flash Loan amount, 70% of which is redirected as extra income for depositors and 30% of which is split using the same 20%/80% model of the origination fee. There are also additional fees for transactions on the Ethereum Blockchain, and these fees depend on the network status and transaction complexity.

B. Block space

Block space is probably the second biggest market in crypto by revenue (behind CEX) but might be one of the least understood. To be sustainable over the long run and maintain market valuation a network has to sell more than it consumes. But what can network or blockchain sell to generate revenue? blockchain actually sells blocks. A “block,” refers to the storage space or slot in a blockchain. In order to use a blockchain on his network, investors and crypto projects need to buy that slot on the chain to store their information or transaction records. Applications buy blocks in blockchains to help operate their own blockchains or networks like polygon(Matic). A "transaction fee" is money paid to crypto miners in exchange for the transaction process. Ethereum sells block space primarily to other applications like Axis Infinite and Audius. Blockchains achieve this by selling blocks, which can settle a plethora number of transactions in each block, at certain intervals. Project owners buy blocks in blockchains to help operate their own blockchains or network. Ethereum’s massive profit comes from the transaction fees paid for transactions on the Ethereum blockchain. For example:

1) Bitcoin sells blocks every 10 minutes that can fit 1 MB worth of transactions.

2) Ethereum sells blocks every 15 seconds that can fit 80 KB worth of transactions (*which is equivalent to 4 MB every 10 mins*).

On the other hand, blockchains don’t sell any block or block space, but they give backspace on lease for a certain timestamp. Kusama slot winners are locking up 100,000 to 200,000 KSM ($35-70 million) for 48 weeks to lease a para chain slot for the 48-week max. Each slot is leased for a certain timestamp, broken into 6-week segments, with a max of 48 weeks. The Kusama block locked up to gain control of a para chain is returned to the team once the lease expires. Auctions for Kusama are done by developers, and teams bid using two pieces of information their bid amount and slot lease time. Slot time is determined in six-month (26 weeks) segments, with two years being the maximum allowed duration. Smaller teams tend to bid for smaller slot durations, while larger projects with more long-term goals will bid for the maximum duration. To renew their slots, teams have two options. The most obvious one is to host another auction to source funds to re-lease the para chain, and teams can also shift to a 'part thread' model, which uses a pay-as-you-go model. However, larger teams with more sophisticated functionality can create their own wealth funds to build funds specifically to fund para-chain auctions, making the network self-sustaining.

Fig. 3 How much do crypto projects charge to use their services?

These projects generate enormous income from their blockchains, their daily fee income is relatively decent. with the above proof, It's clear that Ethereum blocks are worth the most in the present as well as in future investment. It’s also evident that low-fee networks like Solana and Cardano struggle to generate significant fee income.

C. DEX

Decentralized exchanges, also known as DEXs, are peer-to-peer marketplaces where cryptocurrency Buyers and sellers make transactions directly without handing over management of their funds to an intermediary or third party. These transactions are open doors for the use of self-executing agreements written in code called smart contracts (Written in solidity or rust lang etc). Decentralized exchanges rely on smart contracts to allow traders to execute orders without an intermediary. On the other hand, centralized exchanges are managed by a harge fees centralized organization or private organization, they are involved because looking to make a profit. Decentralized exchanges usually cto people who want to trade more than one token at once.

Traditional crypto exchanges charge commissions for every trade, but you never know what those amounts are for decentralized ones. This is because the charges will depend on how many tokens were traded and which blockchain platform they're on.
Uniswap is a decentralized exchange (DEX) that allows users to swap tokens using liquidity provided by other users. Uniswap charges users a small fee whenever a trade is made.

1) Staking
2) Become a liquidity provider
3) Yield farming
4) Lending

D. NFT MarketPlaces

The key source of revenue for an NFT Marketplace is its pricing structure. Every marketplace platform levies a fee for each action that occurs on the site. Let us now look into the fees that are required in numerous major NFT Marketplace platforms.

1) NFT Minting
2) Listing Fees
3) Transaction Fees
4) Subscription Fees
5) NFT T-bond

NFT Minting - NFT minting is the process of transforming any type of asset into a new digital asset in the form of non-fungible tokens. Only in this manner can an asset be exchanged on an NFT Marketplace.To do so, the user must first take their desired asset and convert it into an NFT using NFT Marketplace. The user will be charged a fee by the marketplace platform for this activity.
Listing Fees - After converting any type of assets, such as a photo, artwork, video, or music, into an NFT, the user must advertise their NFT on the marketplace platform so that interested purchasers may bid on that item. The platform would charge the user a listing fee to list that NFT.
Transaction Fees - Once an NFT is posted and available for purchase, multiple potential buyers will place bids on it. When the owner of the NFT decides to trade the NFT to a specific offer and the buyer plans to complete the payment, the platform will impose a transaction fee of 2 to 2.5 percent of the NFT's final sale price.
Subscription Fees - While this is not a necessary charge model, numerous big platforms use it to generate money. This membership cost is simply an additional price to give certain extra advantages for platform users such as having a particular preference in listing an NFT or having access to the liquidity pool dashboard, among other things. Users who choose to hold a premium membership can pay the additional costs and benefit from the platform's exclusive benefits.
NFT T-bond - The NFT T-bond is another successful revenue-generating concept that functions similarly to US Treasury bonds. This bond will enable users to sell tokens that are locked until their maturity date. It may also be used for staking to gain rewards and is exchanged on a number of secondary marketplaces.

IV. RISKS (VULNERABILITY) AND CONCERNS IN THE BLOCKCHAIN ERA

A. 51% Attack

A 51% assault is a cryptocurrency blockchain attack carried out by a group of miners who control more than 50% of the network's mining hash rate. Controlling parties have the ability to change the blockchain by owning 51% of the network's nodes.
The attackers might prevent fresh transactions from receiving confirmations, halting payments between some or all users. They would also be able to undo transactions that were carried out while they were in command. Reversing transactions might allow them to double-spend coins, which is one of the difficulties that consensus systems like proof-of-work were designed to avoid.A blockchain is a distributed ledger, or database, that records transactions and information about them before encrypting the data. Through a validation procedure, the blockchain network establishes a majority consensus on transactions, and the blocks containing the information are sealed.
Cryptographic techniques are used to connect the blocks, and prior block information is saved in each block. Once validated enough times, the blocks are virtually hard to change.
The 51% assault is a blockchain attack in which a group controls more than 50% of the hashing power—the computer power that solves the network's cryptographic puzzle. This gang then presents a revised blockchain to the network at a very particular place in the blockchain, which the network theoretically accepts because the attackers possess the majority of it.

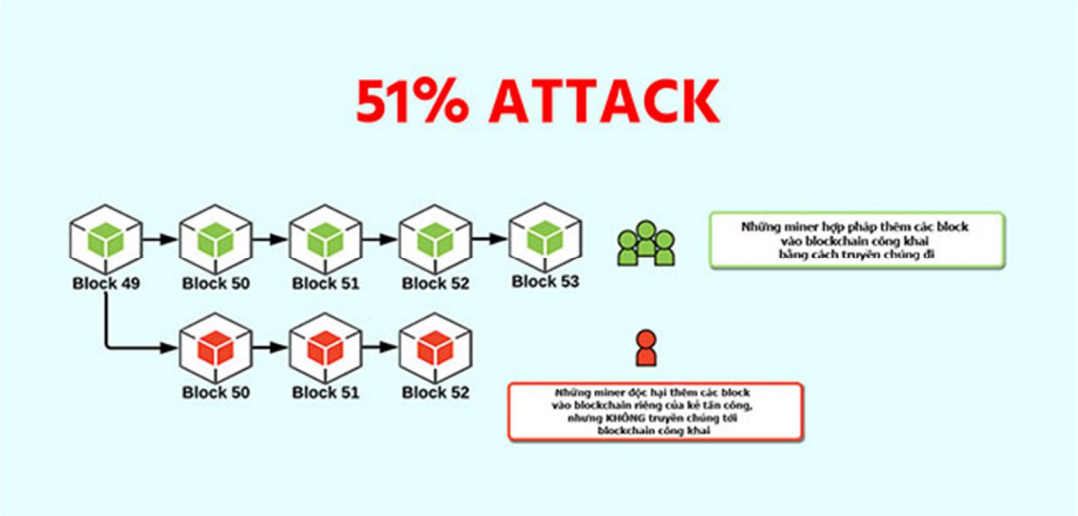


Fig. 4 51% attack evolution

Even in the case of a 51% assault, changing past block transactions locked in prior to the commencement of the attack would be exceedingly difficult. The more recent the transactions, the more difficult it is to modify them. It would be hard to modify transactions before a checkpoint in Bitcoin's blockchain, where transactions became permanent.

To avoid 51% attacks:

1) Increase the supervision of mining pools.
2) Ensure that the hash rate is greater.
3) Avoid utilising consensus processes based on proof-of-work (PoW).

B. Phishing Attacks

Phishing assaults on blockchain networks are becoming more common, causing major problems. Phishing efforts usually target individuals or corporate personnel. Phishing is a sort of bitcoin fraud in which victims are duped into handing up their private keys or personal information. To acquire the victim's trust, the attacker usually disguises himself as a reputable institution or person. After the victim has been duped, the attacker utilises their personal information to steal their bitcoin funds.

As hackers and cyber assaults get more sophisticated, phishing schemes are becoming more widespread. Many of attacks are directed at wallets, cryptocurrency exchanges, and initial coin offerings (ICOs). As a result, crypto users must be informed of how they operate in order to safeguard themselves and their cash.

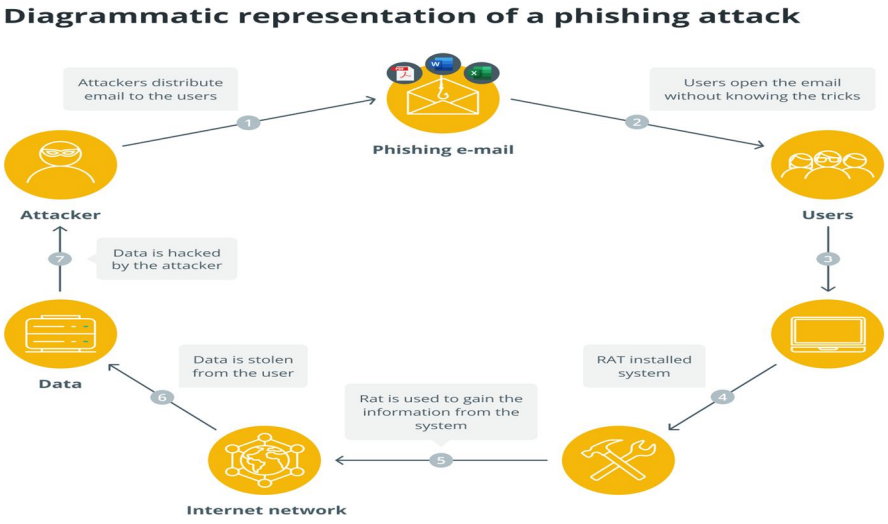


Fig. 5 Phishing Attack

In a phishing attack, the hacker's purpose is to steal the user's credentials. They have the ability to send legitimate-looking emails to the owner of the wallet key. The user must submit login information via an associated bogus hyperlink. Access to a user's credentials and other sensitive information might cause harm to both the person and the blockchain network. They are also vulnerable to further attacks.

To avoid phishing attacks:

1) Increase browser security by installing a trusted add-on that alerts you to dangerous websites.
2) Boost device security by installing harmful link detection software as well as trustworthy antivirus software.
3) If you receive an email seeking login information related to the issue, reconfirm with the partner.
4) Don't click on the link until you've read it completely. Enter the address into your browser instead of clicking on the links.
5) Avoid utilising open Wi-Fi networks when using an electronic wallet or doing other critical financial operations.

C. Routing Attacks

Routing attacks are the next key problem for blockchain technology's security and privacy.The real-time flow of enormous volumes of data is essential to a blockchain network and application.Using routing assaults, an attacker can separate a network into two (or more) different components. The attacker prevents communication between nodes within a chain and those outside of it. The attacker establishes rival blockchains in this manner. When the attack is over, all blocks mined along the smaller chain are discarded. Any transactions and miners' profits are also deleted. Hackers can leverage the anonymity of an account to intercept data while it is delivered to internet service providers.

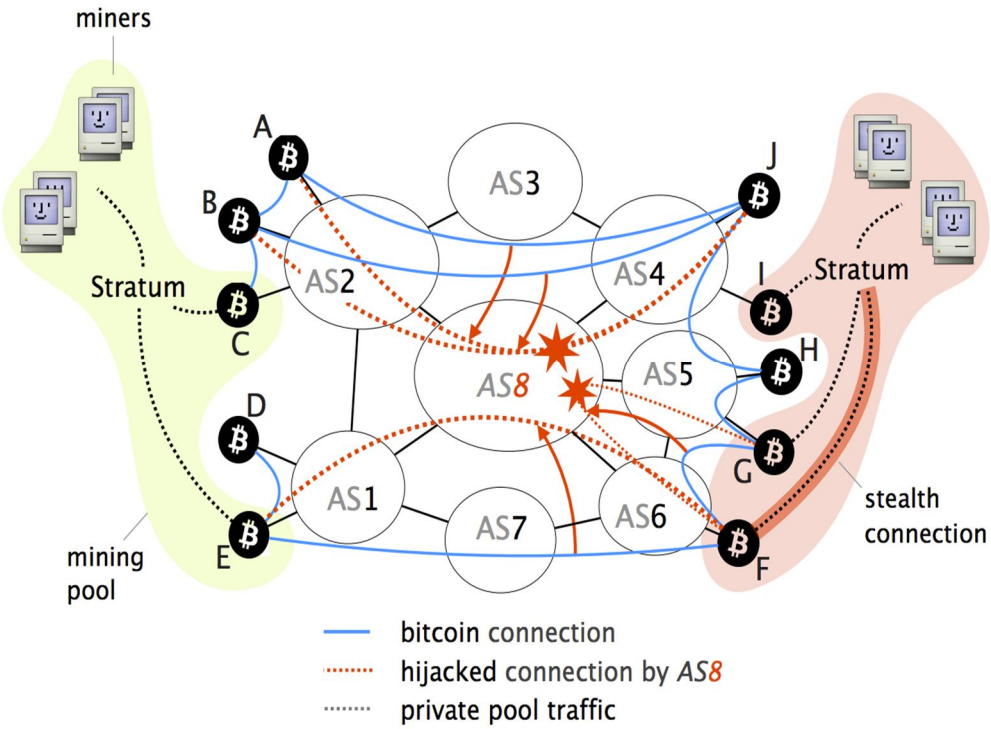


Fig. 6 Routing Attack

Hijacking Bitcoin: Routing Attacks on Cryptocurrencies

When a routing attack occurs, blockchain participants are typically ignorant of the vulnerability since data transfer and activities continue as usual. These attacks offer the danger of exposing private data or extracting cash without the user's knowledge.

To avoid routing attacks:

1) Secure routing techniques must be implemented (with certificates).
2) Encrypt your info.
3) Passwords should be changed on a regular basis, and they should be strong.
4) Educate yourself and your workers on the dangers of information security.

D. Sybil Attacks

In a Sybil attack, hackers create a large number of bogus network nodes. The hacker can gain majority consensus and interrupt the chain's transactions by using such nodes. As a result, a large-scale Sybil assault is essentially a 51% attack.The Sybil Assault is a form of attack found in peer-to-peer networks in which a node in the network deliberately operates numerous identities at the same time, undermining authority/power in reputation systems. The main goal of this assault is to win the majority of network influence in order to carry out unlawful (in terms of network rules and regulations) acts in the system. A single entity (a computer) may develop and maintain several identities (user accounts, IP address based accounts). These many phoney identities look to outside observers to be actual distinct individuals.

To avoid Sybil attacks:

1) Use suitable consensus algorithms.

2) Keep an eye on the activity of other nodes and look for nodes that are only forwarding blocks from one user.

While these algorithms may not totally block these assaults, they do make the hacker's execution difficult.

The adoption of blockchain technology is taking place at a fast pace. Security features inherent in blockchain make it resistant to attack, but they do not make it immune, and blockchain security risks do exist.

V. CONCLUSION

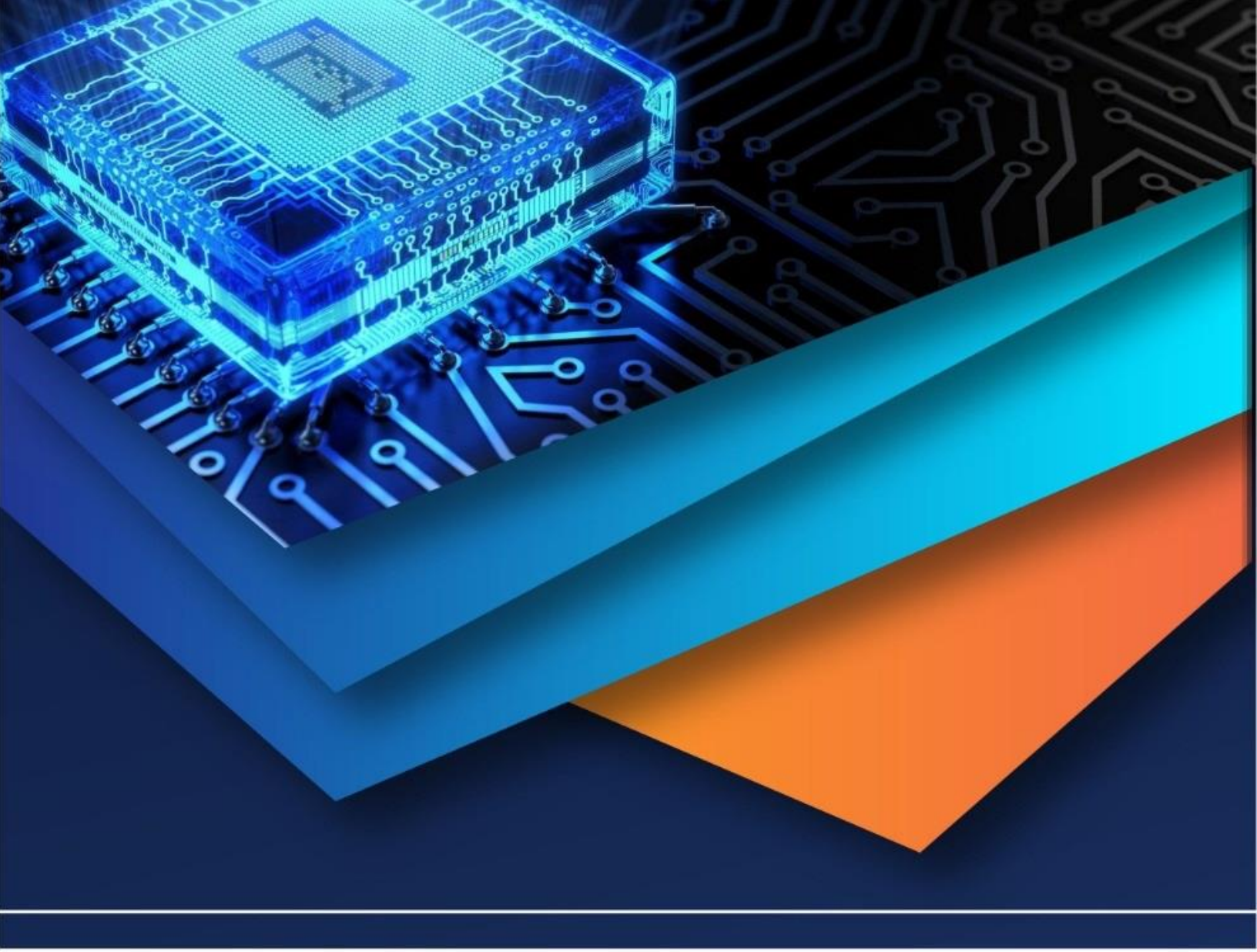
Blockchain is a new and extremely disruptive technology that is still in its early stages. Blockchain technology is one of the most significant recent inventions. However, before mainstream enterprises begin constructing actual infrastructure on blockchains, the technology must improve in terms of safety, accountability, and usability. This mature block will be provided by Concordium.The business model can also be a combination of different ideas, and it completely depends on what the business wants to do. There is no hard and fast rule on how a business model should function. The companies or organizations are free to experiment the way they want.With its essential properties of decentralisation, consistency, anonymity, and auditability, blockchain has demonstrated its potential to revolutionise traditional industries.In this paper, we present that how these businesses or project make profits and generate revenue. We identified key hurdles and concerns that might hamper blockchain development and reviewed some available solutions. Some potential future directions are also suggested.

VI. ACKNOWLEDGE

It would not have been possible to complete this work without the cooperation and assistance of many persons who contributed to it.However, we would want to express our appreciation and debt of gratitude to our guide for their persistent support, kindness, and guidance.comprehension during the course of the article This paper has taken a significant amount of time and effort to complete. However, I would not have succeeded without the assistance and guidance of many others.I was able to complete my assignment. We want to thank each and every one of them from the bottom of our hearts.

REFERENCES

[1] T. Sun, W. Yu A formal verification framework for security issues of blockchain smart contracts Electronics, 9 (2) (2020), Article 225
[2] IBM, IBM Blockchain Suppy Chain Solutiuons https://www.ibm.com/uk-en/blockchain/industries/supply-chain
[3] Adams, R., Parry, G., Godsiff, P., & Ward, P. (2017). The future of money and further applications of the blockchain. [Article]. Strategic Change, 26(5), 417–422.
[4] Carlozo, L. (2017). Understanding blockchain. Journal of Accountancy, 224(2), 1–1.
[5] Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. IEEE Access, 4, 2292–2303.
[6] Eljazzar, M., Amr, M., Kassem, S., & Ezzat, M. (2018). Merging supply chain and blockchain technologies. arXiv preprint arXiv:.04149.
[7] Iansiti, M., & Lakhani, K. R. (2017). The truth about blockchain. Harvard Business Review, January-February 4-11.
[8] W. Zou, D. Lo, P.S. Kochhar, et al.Smart Contract Development: Challenges and Opportunities IEEE Trans. Software Eng.,, 47 (10) (2019), pp. 2084-2106
[9] B. Jiang, Y. Liu, W. Chan ContractFuzzer: fuzzing smart contracts for vulnerability detection Proceedings of the 33rd ACM/IEEE International Conference on Automated Software Engineering; 3–7 Sep 2018; Montpellier, France, IEEE, Piscataway, NJ, USA (2018), pp. 259-269
[10] H. Kalodner, S. Goldfeder, X. Chen, et al.Arbitrum: scalable, private smart contracts 27th USENIX Security Symposium; 15–17 Aug 2018; Baltimore, MD, USA, USENIX Association,Berkeley, CA, USA (2018), pp. 1353-1370
[11] Aune RT, Krellenstein A, O'Hara M, Slama O (2017) Footprints on a Blockchain: trading and information leakage in distributed ledgers. J Trading 12(3):5–13
[12] Dutra A, Tumasjan A, Welpe IM (2018) Blockchain is changing how media and entertainment companies compete. MIT Sloan Manag Rev 60(1):39
[13] Fanning K, Centers DP (2016) Blockchain and its coming impact on financial services. J Corp Account Finance 27(5):53–57
[14] O'Dair M, Owen R (2019) Financing new creative enterprise through blockchain technology: opportunities and policy implications. Strateg Change Brief Entrep Finance 28(1):9–17
[15] Treiblmaier H (2018) The impact of the blockchain on the supply chain: a theory-based research framework and a call for action. Supply Chain Manage Int J 23(6):545–559



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY