AN EXPLORATIVE ANALYSIS ON BITCOIN USING BLOCKCHAIN TECHNOLOGY

R Saradha * and Vidhya Sathish **

Introduction

Bitcoin (in any other case known as BTC) is virtual cash made through Satoshi Nakamoto and added in 2009 [1]. Bitcoin is circulated, decentralized, shared digital virtual cash. Since Bitcoin is digital virtual cash, it does not have any form and length just like the economic paperwork we use these days, and is placed away in Bitcoin wallets which are made to shop digital economic paperwork. Bitcoins may be moved to each other making use of the Bitcoin address. Since its origin, it has evolved in reputation and its utilization. All things considered, the innovation stays like purchasing something with virtual cash, yet one advantage of Bitcoins is that the agreement stays unidentified. The personality of the sender and the recipient remains scrambled. Also, that is the reason it has turned into a confided-in type of sending cash on the web. By custom, the intricacy in making dispersed cash is the requirement for a proposition to forestall twofold spending. One individual may simultaneously communicate two exchanges, sending the comparative coins to two separate gatherings on the organization; however deficient with regards to a focal server to figure out the two exchanges and go to a lawful choice, difference emerges over the genuine history and responsibility for a given coin [2].

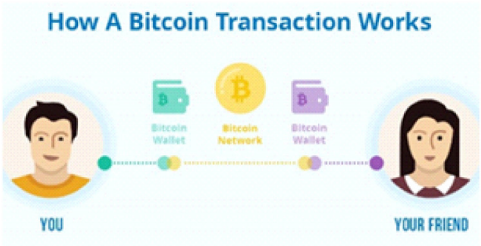

Fig 1. Bitcoin Example

II. OVERVIEW OF BITCOIN MINING

Bitcoins don't exist truly and are just a succession of virtual information. However, it tends to be traded for veritable cash and is generally allowable in many nations throughout the planet. There's no focal expert for Bitcoins, like a national bank that controls monetary

* Assistant Professor,Department of Computer Science,Applications,SDNB Vaishnav College for Women,
** Assistant Professor,Department of Computer ,SDNB Vaishnav College for Women

forms [3]. All things being equal, software engineers settle complex riddles to support Bitcoin exchanges and get Bitcoins as an award. This action is called Bitcoin mining, and with some information on encoding codes and touches of longing for capital, anyone can get breaking.

Mining Bitcoins

This is fairly intricate. Yet, assuming you need to take it head-on, here's how it works: Get a prevailing CPU with the best handling power. A blasting quick web interface. Following the stage, there are numerous web-based organizations that rundown out the most up-to-date Bitcoin exchanges occurring continuously. Sign on with a Bitcoin customer and endeavor to approve those exchanges by assessing squares of information, called hash [4]. The correspondence travel through a few frameworks called hubs, which are simply squares of information. Furthermore, since the data is encoded, a digger is needed to check if his answers are definite. When the hubs get affirmed, an exchange becomes effective and the excavator is remunerated with some Bitcoins. To put it plainly, you're going about as a bank representative, alongside numerous other bank agents meeting on the web. Whosoever confirms the arrangement gets rich. Excavators from everywhere on the planet attempt to be quick to coordinate with their hash with the arrangement, and it takes a normal of 10 minutes for the right answer to show up. The numerical brainteaser is planned to adjust the trouble level consequently. On the off chance that the normal opportunity to figure the right answer falls under 10 minutes, the riddle becomes more earnestly to break, as well as the other way around [5]. Additionally, after fixed spans, the motivations continue to get split until it arrives at nil. After that, the software engineers who break the right arrangements are compensated with simply an exchange charge for their endorsement.

Working Mechanism of Bitcoin Blockchain

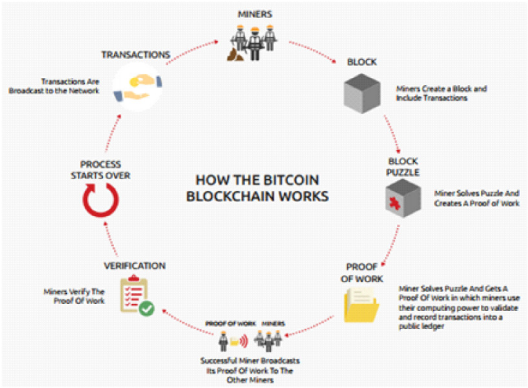

Fig. 2. Working of a Bitcoin Blockchain.

Mining requires an assignment that is extremely interesting to perform, yet simple to check. Bitcoin mining utilizes cryptography, with a hash work called twofold SHA-256. A hash accepts a piece of information as information and therapists it down into more modest hash esteem (for these situations 256 pieces). With a cryptographic hash, it's impossible to get the hash esteem you need without attempting a ton of sources of info [6]. However, when you discover information that gives the worth you need, it's simple for anybody to verify the hash. In this way, cryptographic hashing turns into a decent way of applying the Bitcoin "confirmation of work".

To be a Bitcoin excavator, joining the Bitcoin organization and interfacing with different hubs is required. There are principally six assignments that should have been performed by excavators.

1. Excavator needs to tune in for the exchanges that are communicated to the organization. They should check those exchanges by checking the marks' accuracy and whether the yields have been spent previously or not. This is done to moderate the twofold spend issue.

2. Before joining the organization, excavators should have every one of the past blocks that are a piece of the blockchain. They tune in for the new squares that are communicated to the organization. Then, at that point, they should approve each square that is gotten by approving every exchange in the square. They likewise need to check whether the clock has legitimate nonce or not.

3. When the excavators have the most recent duplicate of the blockchain, they can start constructing their squares. To do this, the excavator bunch exchanges that are heard into another square which expands the latest square.

4. Presently excavators need to discover a nonce that makes the square substantial. This is one of the essential strides during mining which requires a lot of work.

5. Expect that the square is acknowledged after discovering a nonce. There is no assurance that the square will be part of the agreement chain regardless of whether the square is acknowledged. On the off chance that different diggers acknowledge a similar square and start mining on top of it, then, at that point, the square will be a piece of the agreement chain [7].

6. If every one of the excavators acknowledged the square and added to the piece of the agreement chain, then, at that point, the digger who chipped away at discovering the nonce for that specific square will get compensated. The square compensation at this point is 12.5 Bitcoins. Also, if any of the exchanges in the square contained exchange charges, the excavator gathers those exchange charges as well. [8]

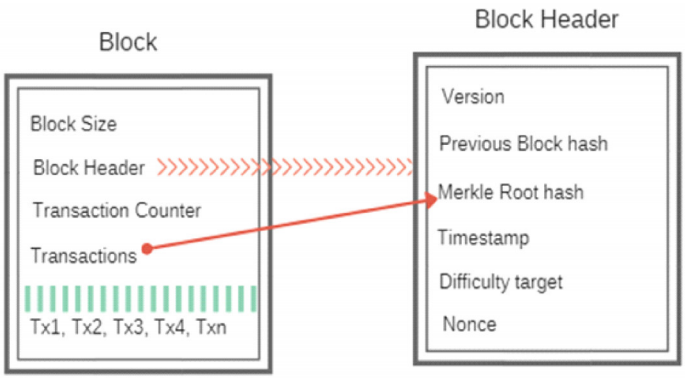

Fig.3. Structure of Bitcoin Block.

The block header contains a modest bunch of fields that represent the block. The main field in the block is the convention form. It is trailed by the hash of the first block in the blockchain, which guarantees every one of the blocks structures a persistent succession in the blockchain. The following field is the Merkle root, an exceptional hash of the multitude of exchanges in the block. This is additionally a vital piece of Bitcoin security since it guarantees that exchanges can't be modified once they are part of a block. Next is a timestamp of the block, trailed by the mining intricacy esteem bits. At long last, the nonce is an irregular worth that is augmented on each hash endeavor to give another hash esteem. The troublesome aspect of mining is discovering a nonce that works.

III. BITCOIN TRANSACTION

A Bitcoin exchange is a marked part of the information that is shipped off the organization and, if substantial, brings about the formation of a square in the blockchain [9]. A Bitcoin exchange includes moving responsibility for a specific measure of Bitcoin to a Bitcoin address. At the point when you send Bitcoin, your wallet customer makes a solitary information structure, known as a Bitcoin exchange, which is then transmitted to the organization. Bitcoin network hubs will impart and rebroadcast the exchange, and if it is substantial, hubs will remember it for the square they are mining. Regularly, the exchange will be incorporated, alongside different exchanges, in a square in the blockchain within 10-20 minutes. The receiver can see the exchange sum in their wallet from this position. Coming up next are the shading-coded fundamental parts of this standard exchange: Transaction identifiers Descriptors and meta-information Inputs and results [10].

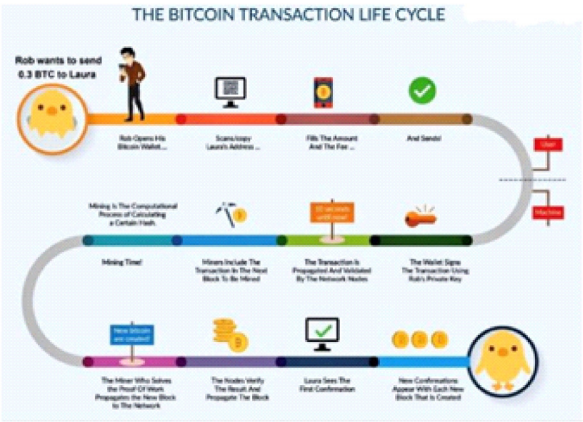

Fig 4: Life cycle of Bitcoin transaction.

Four clear facts about exchanges:

" Bitcoin sum that we send is constantly shipped off a location.

" Bitcoin sum we get is locked to the getting address which is associated with our wallet.

" Each time we spend Bitcoin, the sum we spend will consistently come from reserves before got and right now present in our wallet.

" Addresses get Bitcoin, yet they don't send Bitcoin is sent from a wallet [11].

IV. BITCOIN WALLETS

Bitcoin wallets accumulate the private keys you want to access a bitcoin address and pay your funds. They come in different forms, intended for special types of devices. You can even use paper storage to avoid having them on a computer. It is very essential to protect and backup your bitcoin wallet. Bitcoins are a new cash correspondent and every day another merchant starts accepting them as payment. We know how a bitcoin transaction mechanism is generated and how it works, but how are they stored? We store cash in a physical wallet and bitcoin works similarly, except that it is generally digital. Well, to be completely accurate, it technically doesn't store bitcoin anywhere. What it stores are secure digital keys that are used to access your public bitcoin addresses and sign transactions. A Bitcoin wallet is a computerized wallet like the financial balance which is utilized to store Bitcoin [12]. A product called Bitcoin wallet ought to be downloaded to get a Bitcoin address. The product permits safely sending, getting, and putting away Bitcoin in the Bitcoin organization [13]. There are fundamentally two unique sorts of Bitcoin wallets which are software wallets and hardware wallets.

" **Desktop wallets**

On the off chance that you have effectively introduced the first bitcoin customer (Bitcoin Core), then, at that point, you are running a wallet, yet may not know it. As well as handing-off exchanges on the organization, this product additionally empowers you to make a bitcoin address for moving and getting the virtual money and to collect the private key for it [14]. MultiBit runs on Windows, Mac OSX, and Linux. Hive is an OS X-based wallet for certain particular elements, including an application store that interfaces directly to bitcoin administrations. Some work area wallets are modified for improved security: Armory falls into this gathering. DarkWallet utilizes a lightweight program module to offer administrations incorporating coin blending in which client's coins are traded for other people, to forestall locals following them.

" **Mobile wallets**

An application on your cell phone, the wallet can amass the private keys for your bitcoin addresses, and permit you to pay for things straightforwardly with your telephone. Sometimes, a bitcoin wallet will even take advantage of a cell phone close field correspondence (NFC) angle, empowering you to tap the wireless against a user and pay with bitcoins without entering any data whatsoever [15] [16]. One general component of versatile wallets is that they are not finished by bitcoin customers. A full bitcoin customer needs to download the whole bitcoin blockchain, which is continually developing and is numerous gigabytes in size. a ton of telephones wouldn't have the option to hold the blockchain in their memory, regardless. as another option, these portable customers are more than once planned with a worked-on installment check (SPV) at the top of the priority list. They download a tiny subset of the blockchain, and depending on others, confided in hubs in the bitcoin framework to ensure that they have the specific data. Instances of versatile wallets contain the Android-based Bitcoin wallet, Mycelium.

" **Online Wallets**

Electronic wallets store your private keys on the web, on a PC confined by another person, and coupled to the Internet. various such internet-based administrations are accessible, and some of them attach to versatile and work area wallets, reproducing your addresses among various gadgets that you own [17]. One addition of electronic wallets is that you can get in touch with them from any place, notwithstanding which gadget you are utilizing. however, they additionally have one significant disadvantage: except if carried out fittingly, they can put the association running the site responsible for your private keys fundamentally removing your bitcoins from your power. That is a prohibiting thought, especially assuming you initiate to add bunches of bitcoins. Coin base, an incorporated wallet/bitcoin

trade works its internet-based wallet all around the world. Clients in the US and Europe can purchase bitcoin through its trade administrations. Circle offers clients worldwide the capacity to store, send, get and purchase bitcoins. Blockchain additionally has an acknowledged electronic wallet, and Strong coin offers a combination wallet, which allows you to scramble your private location keys preceding sending them to its server's encryption is dropped in the program.

" **Hardware Wallets**

Equipment wallets are presently exceptionally incomplete in number [18]. These are sharp gadgets that can get a handle on private keys electronically and make simple installments. The Trezor equipment wallet is focused on bit coiners who wish to safeguard a considerable reserve of coins, however don't have any desire to depend on middle person bitcoin capacity administrations or not down to earth types of cold stockpiling. The conservative Ledger USB Bitcoin Wallet utilizes smartcard assurance and is accessible at a reasonable cost. Keep Key dispatched an equipment wallet in September 2015, which is evaluated at $239 a unit. The Keep Key wallet programming was initially a part of Trezor's code.

" **Paper Wallets**

One of the most parts appreciated and least expensive choices for keeping your bitcoins free from any harm is to some degree called a paper wallet. There are various destinations offering paper bitcoin wallet administrations. They will deliver a bitcoin address for yourself and produce a picture containing two QR codes: one is the public location that you can use to get bitcoins [19]; the other is the private key, which you can use to pay out bitcoins put away at that location. The benefit of a paper wallet that is made appropriately is that the private keys are not put away carefully wherever, and are along these lines not exposed to run-of-the-mill digital assaults or equipment disappointments.

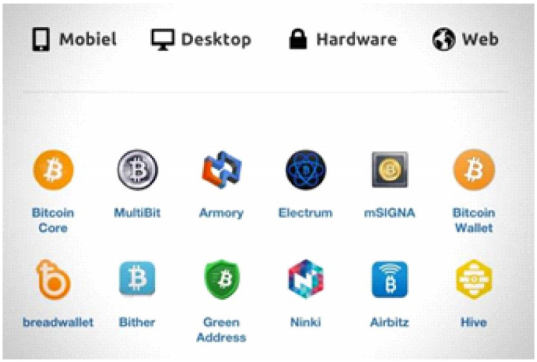

Fig 5: Types of Bitcoin Wallets.

V. FEATURES OF CRYPTO-CURRENCY

Bitcoin crypto money is widely used and accepted globally due to a few highlights that make it different from others [20] [21].

- Decentralized and no central authority: In Bitcoin cryptocurrency, exchanges are managed and validated by a widespread network. There is no central authority governing this open organization unlike traditional currency owned by state administrations and banks. The PC network is spread all over the world known as nodes.
- Anonymous / Pseudo-Anonymous: The customer's personality remains mysterious or obscure to the different clients in the system while trading with the Bitcoin cryptocurrency, as a focal expert is not required to execute the transaction. The new exchange will be registered on the blockchain every time the exchange is sent and after being verified on the decentralized organization. Authentication is guaranteed through the use of public and private keys in Bitcoin. Clients can use computerized personalities and wallets for their exchanges through the decentralized organization while keeping the exchange secure and authenticated.
- Irreversible and immutable (cannot be dispersed): the transaction once recorded on the blockchain cannot be canceled or changed by anyone. Secure cryptography makes swapping exceptionally difficult. Change on the exchange required to change hubs on the blockchain, which is beyond the realm of possibility. All exchanges are registered on the blockchain and made visible to the public.
- Limited Supply and Shortage: Most computerized bastards have a limit on the supply of their tokens. Bitcoin cryptocurrency will also reach its most extreme value by 2040, which is limited by the timetable written in its code.
- what's more, banks, the Bitcoin cryptographic money has just its maximum worth of 21 million. Conventional money has its disadvantages of being deteriorated throughout the period as a result of its inflationary nature. The traditional currency additionally has a vulnerability in its activity. Moreover, conventional money can be given by the government or managed by an account with no upper cap. Bitcoin cryptographic money on the other hand, when arrives at its most extreme worth of 21 million can't be additionally mined. This makes Bitcoin a more attractive and significant asset.
- Divisibility: Bitcoin can be additionally partitioned into smaller units known as Satoshi. Satoshi is the littlest unit of Bitcoin. 100,000,000 Satoshi is comparable to one Bitcoin.
- Fast and Global: The exchanges are autonomous of their actual areas and are proliferated and verified almost in a split second over the disseminated network.

- Secure: Only the proprietor of the Bitcoin cryptocurrency has admittance to the private key so no other person can access and use it. Solid cryptographic calculations (SHA 256) were issued to scramble the exchanges and blockchain. The exchanges are recorded on the disseminated record known as a blockchain and consequently, there is no chance of any coming up short or likelihood of weakness. This makes transactions less inclined to bugs, hacking, and framework disappointment as information is decentralized on an appropriated network which in turn makes Bitcoin cryptographic money more secure.
- No Permission Required: Clients are not needed to take assent from anyone in a request to utilize Bitcoin cryptocurrency. The clients without a doubt need to download programming for free. Thereafter, they can trade Bitcoin digital currency with others.
- No Debt however Bearer: The conventional cash is generated by obligation and the numbers on the record addressing the debt. The Bitcoin cryptographic money doesn't indicate debts. They are cash like some other actual assets.
- Efficient: Since the Bitcoin cryptographic money utilizes peer to peer information base and there is no focal authority for controlling and approving the flow of computerized currency, the exchanges are verified and approved on the blockchain. Additionally, any client having a web connection can trade Bitcoin money across the world. Therefore, the expense of working the computerized currency, in specific Bitcoin cryptography is a lot lower than any other conventional cash traded through bank transfer.
- Trustless: Bitcoin cryptographic money depends on no trust among the member clients as a result of the underlying decentralized network implies nobody needs to trust anyone else in the organization. The exchanges are communicated over the disseminated network and computerized marks are validated before being recorded on the blockchain. It is disposed of if the approval bombs in any case included the blockchain. Being virtual, Bitcoin is so enabled these days that it is a significant contender for supplanting the at money.

V. MINING PROCESS OF BITCOINS

Bitcoin mining is the process of generating Bitcoins through the use of hardware to solve a complex mathematical puzzle [22]. Individuals known as miners protect the Bitcoin network. Mining Bitcoins necessitates the use of hardware. Miners have used various types of hardware to mine Bitcoin blocks over time. Initially, Bitcoin Mining was originally done with a CPU, but over time, hardware evolved to include GPUs, FPGAs, and ASICs.

F **Mining with CPUs:**

During the early stages of Bitcoin mining, Central Processing Units (CPUs) were used as mining hardware. It is thought to be the first generation of Bitcoin mining. It was as simple as running the code below to mine CPUs. The code linearly searches nonces before computing SHA-256 in software and determining whether the result is a valid block [23]. As previously stated, the SHA-256 algorithm is used twice in the code.

```
target = (65535 << 208) / difficulty;
Coinbase nonce = 0;
while (1)
 {
header = blockHeader (transactions, coinbase_nonce);
for (header_nonce = 0; header_nonce< (1 << 32); header_nonce++ ) {
if (SHA256 (SHA256 (blockHeader (header, header_nonce))) < target)
Break; // block is found
 }
Coinbase nonce++;
}
```

The computation takes about 20 million hashes per second (MH/s) on a high-end desktop PC. At that rate, finding a valid block would take several years on average.

F **Mining with GPUs**

GPU mining is thought to be the second generation of Bitcoin mining. GPU mining began as a result of the low computational power of CPU mining. GPU mining outperformed CPU mining, but it was unable to keep up with the increasing difficulty rate over time. Overheating and a high level of hardware utilization during the mining process are two disadvantages of GPU mining.

F **FPGA mining**

FPGA mining is considered the third generation of Bitcoin mining. After the first implementation of Bitcoin mining came out in Verilog, several miners switched from GPU mining to FPGA mining. The computation power of FPGA mining was much better than GPA mining during that time. Later on, the number of miners increased which increased the difficulty of the network. Due to the increase in the difficulty of mining the blocks, FPGA mining could not satisfy the expectations.

Fig 6: Bitcoin Mining using several FPGAs

F ASIC Mining

The fourth generation of Bitcoin mining is ASIC mining. Bitcoin ASICs currently dominate mining. These ASIC chips are designed, built, and optimized solely for Bitcoin mining. Some large vendors manufacture and sell ASIC mining hardware to customers. Today's ASIC mining hardware includes the Antminer S9, Terminator T3, Dragonmint T1, and others.

Fig 7: Antminer S9 for Bitcoin Mining.

Every miner has to deal with high electricity costs and excess heat produced by the hardware during the mining process. Cloud mining is an alternative to these issues because the miner does not have to worry about high electricity costs or excess heat [24]. However, it has a few other limitations, such as the risk of fraud, lower profit, and a lack of control and flexibility, making it ineffective in comparison to other mining techniques. As mining technology advances, an increasing number of companies begin producing dedicated Bitcoin mining hardware.

The most popular Bitcoin miners are EBIT E11++, Terminator T3, Antminer S15, DragonMint T1, Antminer S9, AvalonMiner 841, and so on.

Application-specific integrated circuits (ASICs) dominate the Bitcoin ecosystem. Graphics processing units (GPUs) and field-programmable gate arrays (FPGAs) are the dominant form factors for the majority of other cryptocurrencies. Several coins use the same hashing algorithm as Bitcoin (SHA256) and are compatible with Bitcoin mining ASICs. The table below gives the comparison of bitcoin mining algorithms.

Chip	**Definition**	**Mining Algorithms**	**Example Hardware**	**Comments.**	**Used by Author & Year**
ASIC	Chipsets that are optimized to perform one specific function (ex. SHA256)	SHA256	Antminer S17, AvalonMine r, WhatsMiner , M20S	ASICs can be made for any mining algorithm although SHA256 is the most common.	J Prat, B Walter, 2021
FGPA	Chips that are designed to be reprogrammable by the user.	can be programme d to work for any mining algo.	Xilinx VU9P, Bittware, CVP-13, Blackminer	It is very difficult to program FGPA s and difficult to set up.	Hoai Luan Pham, Thi Hong Tran, Tri Dung Phan, 2020
GPU	Chips designed to do repetitive calculations (typically for video graphics)	Ethash, Equihash, Cuckaroo2 9, etc.	NVIDIA 2080Ti, AMD Radeon, VII	GPUs are good for the long tail of tokens outside of Bitcoin	SG Iyer AD Pawar, 2018
CPU	Chips are designed to perform general-purpose computing tasks.	Crypto Night	AMD Ryzen 1950X	While it was possible to mine with CPUs initially, it's typically not profitable today.	SG Iyer AD Pawar, 2018

Table1: Comparison list of popular bitcoin mining hardware algorithms.

The examination of Bitcoin mining in this section shows various variables remembered for Bitcoin mining. Some of the significant variables that ought to be thought about are:

F Type of equipment picked for mining Bitcoin

F Bitcoin reward per block

F Cost of power

F The spending plan for the equipment costs

F Type of mining: solo or pool mining

F If joining on pool mining, we should investigate network share, the hash pace of a mining pool, mining compensation from the mining pool, etc.

VI. AVAILABLE IMPLEMENTATIONS.

A variety of available technologies were investigated for implementing the private and permissioned blockchain. The sections that follow discuss the relevant implementations and our rationale for not selecting them.

VII. CONCLUSION AND FUTURE WORK.

Bitcoin is being utilized as an option in contrast to government-issued types of money. Different nations like Japan, the USA, Australia, China, and so on have begun utilizing Bitcoin as the installment strategy [25]. There are loads of eateries, shops, and stores that are tolerating Bitcoin as an option in contrast to different monetary forms. Since Bitcoin is decentralized and chips away at the idea of the blockchain, every one of the exchanges is straightforward and reasonable. Mining Bitcoin is becoming more earnestly step by step with an increment in trouble rate and the opposition between the excavators with the best equipment accessible in the market. A couple of years back mining a Bitcoin was a lot simpler contrasted with these days. Mining a Bitcoin requires a great deal of calculation and great equipment that can convey a great hash rate with low energy.

Miners should be cautious about picking equipment before beginning to mine Bitcoin since the expense of equipment is extremely high and the other added cost during mining is power cost and fixed cost. Even though CPU, GPU, also, FPGA mining equipment were utilized to mine Bitcoins previously, yet at this point contributing to them as mining equipment is an ill-conceived notion since they can't create the processing power needed to mine Bitcoin today. A single ASIC mining equipment also can't mine Bitcoin successfully since many mining pools are contending to mine the Bitcoin. A solitary client can't contend with a mining pool that has bunches of equipment assets. A few mining pools are closing down in China because of a misfortune in their business of mining. Picking the right area is one more basic advance for excavators or mining pools since the cost of power to run the

equipment is likewise a deciding element. Mining a Bitcoin burns through a great deal of power. Nations like Venezuela, Myanmar. Kuwait, Ukraine, Uzbekistan, India, and so forth would be an awesome answer for miners and the mining pool. Due to the limitation of hardware resources, we could not mine the Bitcoin on our own. The future work would be either buying some good hardware by securing funding or collaborating with mining pools to use their hardware for research purposes.

References :

1. Tseng, "Bitcoin's Consistency Property," in 2017 IEEE 22nd Pacific Rim International Symposium on Dependable Computing (PRDC), Christchurch, New Zealand, 2017 pp. 219-220. https://doi.ieeecomputersociety.org/10.1109/PRDC.2017.39
2. Eyal, Ittay. (2017). Blockchain Technology: Transforming Libertarian Cryptocurrency Dreams to Finance and Banking Realities. Computer. 50. 38-49. DOI:10.1109/MC.2017.3571042
3. Aljabr, Ahmad & Sharma, Avinash & Kumar, Kailash. (2019). Mining Process in Cryptocurrency Using Blockchain Technology: Bitcoin as a Case Study. Journal of Computational and Theoretical Nanoscience. https://doi.org/10.1166/jctn.2019.8515.
4. Guo, X.; Zhang, G.; Zhang, Y. A Comprehensive Review of Blockchain Technology-Enabled Smart Manufacturing: A Framework, Challenges and Future Research Directions. Sensors 2023, 23, 155. https://doi.org/10.3390/s23010155.
5. Le Vu Trung, Duong & Nguyen Thi Thanh, Thuy & Lam, Duckhai. (2020). A fast approach for bitcoin blockchain cryptocurrency mining system. Integration. 74. DOI:10.1016/j.vlsi.2020.05.003
6. Habib, G., Sharma, S., Ibrahim, S., Ahmad, I., Qureshi, S., Ishfaq, M. (2022). Blockchain Technology: Benefits, Challenges, Applications, and Integration of Blockchain Technology with Cloud Computing. Future Internet. 14(11). 341. https://doi.org/10.3390/fi14110341.
7. Cooper, Z. G. T. (2021). THE DEEP TIME OF BITCOIN: EXCAVATING THE "WORK" IN PROOF-OF-WORK CRYPTOCURRENCY SYSTEMS. AoIR Selected Papers of Internet Research, 2021. https://doi.org/10.5210/spir.v2021i0.11887
8. Xiaojing Yang, Jinshan Liu, Xiaohe Li. (2019). Research and Analysis of Blockchain Data. IOP Conf. Series: Journal of Physics: Conf. Series 1237 (2019) 022084. https://doi.org/10.1088/1742-6596/1237/2/022084.
9. Chao Yu, Wenke Yang, FeiyuXie, Jianmin He. (2022). Technology and Security

Analysis of Cryptocurrency Based on Blockchain. Complexity. 2022. 5835457.1-15. https://doi.org/10.1155/2022/5835457.

10. Easley, David & O'Hara, Maureen & Basu, Soumya, 2019. "From mining to markets: The evolution of bitcoin transaction fees," Journal of Financial Economics, Elsevier, vol. 134(1), pages 91-109. DOI: 10.1016/j.jfineco.2019.03.004.
11. Ahmed G. Gad, Diana T. Mosa, Laith Abualigah, Amr A. Abohany, Emerging Trends in Blockchain Technology and Applications: A Review and Outlook, Journal of King Saud University - Computer and Information Sciences, Volume 34, Issue 9,2022, Pages 6719-6742, ISSN 1319-1578, https://doi.org/10.1016/j.jksuci.2022.03.007.
12. F. Zhu et al., "Trust your wallet: A new online wallet architecture for Bitcoin," 2017 International Conference on Progress in Informatics and Computing (PIC), Nanjing, China, 2017, pp. 307-311, DOI: 10.1109/PIC.2017.8359562.
13. Tao Zhang, Zhigang Huang, Blockchain and central bank digital currency, ICT Express, Volume 8, Issue 2,2022,Pages 264-270, https://doi.org/10.1016/j.icte.2021.09.014.
14. Palos-Sanchez, P., Saura, J. R., Ayestaran, R. (2021). An Exploratory Approach to the Adoption Process of Bitcoin by Business Executives. Mathematics. 9(4). 355. https://doi.org/10.3390/math9040355.
15. Poonam Painuly., & Shalu Rathi (2016). Mobile Wallet: An Upcoming Mode of Business Transactions. International Journal in Management and Social Science, 4, 56-363.
16. Pousttchi, Key. (2008). A modeling approach and reference models for the analysis of mobile payment use cases. Electronic Commerce Research and Applications. 7. 182-201. 10.1016/j.elerap.2007.07.001.
17. Iddo Bentov, Charles Lee, Alex Mizrahi, and Meni Rosenfeld. 2014. Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake [Extended Abstract]y. SIGMETRICS Perform. Eval. Rev. 42, 3 (December 2014), 34-37. https://doi.org/10.1145/2695533.2695545
18. Barker, T. and Sekerkaya, A. (1992), "Globalization of Credit Card Usage: The Case of a Developing Economy", International Journal of Bank Marketing, Vol. 10 No. 6, pp. 27-31. https://doi.org/10.1108/02652329210017299.
19. Huh, Seyoung& Cho, Sangrae& Kim, Soohyung. (2017). Managing IoT devices using blockchain platform. 464-467. 10.23919/ICACT.2017.7890132.
20. Yuneline, M.H. (2019), "Analysis of cryptocurrency's characteristics in four perspectives", Journal of Asian Business and Economic Studies, Vol. 26 No. 2, pp.

206-219. https://doi.org/10.1108/JABES-12-2018-0107.

21. Fang, F., Ventre, C., Basios, M. et al. Cryptocurrency trading: a comprehensive survey. Financ Innov 8, 13 (2022). https://doi.org/10.1186/s40854-021-00321-6.
22. Ahmed G. Gad, Diana T. Mosa, Laith Abualigah, Amr A. Abohany, Emerging Trends in Blockchain Technology and Applications: A Review and Outlook, Journal of King Saud University - Computer and Information Sciences, Volume 34, Issue 9,2022, Pages 6719-6742, https://doi.org/10.1016/j.jksuci.2022.03.007.
23. Ankalkoti, Prashant & Santhosh, (2017). A Relative Study on Bitcoin Mining. "Imperial Journal of Interdisciplinary Research (IJIR). 3.
24. Hashimoto, Yoshinori and Noda, Shunya, Pricing of Mining ASIC and Its Implication to the High Volatility of Cryptocurrency Prices (April 8, 2019). Available at SSRN: https://ssrn.com/abstract=3368286 or http://dx.doi.org/10.2139/ssrn.3368286
25. Katarya, Rahul and Mustafa, Aamir, Blockchain and Consensus Algorithms (March 28, 2020). Proceedings of the International Conference on Innovative Computing & Communications (ICICC) 2020, Available at SSRN: https://ssrn.com/abstract=3562974 or http://dx.doi.org/10.2139/ssrn.3562974

References

1. Tseng, L., 2017. Bitcoin's Consistency Property. Proceedings of the IEEE 22nd Paci?c Rim International Symposium on Dependable Computing (PRDC), pp.219-220.
2. Viswam, A. and Darsan, G., 2017. An Ef?cient Bitcoin Fraud