|| Volume 5 || Issue 4 || April 2020 || ISSN (Online) 2456-0774
INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH
AND ENGINEERING TRENDS

CRYPTOMINING/HASHING RIG

Swapnil Shukla[1], Pragati Pandey[2], Abhilasha Mishra[3]

Computer Engineering, Shree L. R. Tiwari College of Engineering, Maharashtra, India[1,2,3]
imwapnilshukla@gmail.com[1] , pandeypragati65@gmail.com[2], abhilashmishra238@gmail.com[3]

Abstract: A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network time stamps transactions by hashing them into an ongoing chain of hash-based proof-of work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and re-join the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Keywords: *Cryptocurrency, Block chain, MinningRig, Bitcoin, E-Cash, Digital Cash, Bitcoin mining, Payment Node.*

I INTRODUCTION

In 1983, the American cryptographer David Chaum conceived an anonymous cryptographic electronic money called ecash. Later, in 1995, he implemented it through Digicash, an early form of cryptographic electronic payments which required user software in order to withdraw notes from a bank and designate specific encrypted keys before it can be sent to a recipient. This allowed the digital currency to be untraceable by the issuing bank, the government, or any third party. During E-cash the cryptocurrency technology uses block-chain which secures the system or enhances the security of the system.

Unlike traditional payments, like cash and credit cards, cryptocurrencies are digital and encrypted; you cannot be ripped off in a transaction like you can be with legacy payment systems, and it is much harder to steal cryptocurrency compared to a wallet full cash. In a world where so many of our transactions are online, and our savings and credit rating are at stake at all times, anything that provides increased transactional security is a plus. And there is currently no transaction mechanism that is currently more safe and secure than those that use cryptocurrency.

Another great benefit of using cryptocurrency, especially when purchasing real property, is that digital currency can help eliminate expensive brokers, lawyers, and other typical "middlemen" who inevitably raise the costs of already expensive transactions. Cryptocurrency can essentially act like "a large property rights database", according to one financial expert, and can be used to execute and enforce two-party contracts on items like real estate and automobiles, thus eliminating expensive brokerage and legal fees.

As more people, including billions of people in the developing world, increasingly use mobile devices linked to the Internet to conduct financial transactions, cryptocurrency is truly going to come into its own. All Cryptocurrency is designed for low cost, no-fee transactions, so undoubtedly these digital currencies will become increasingly popular as more people have access to mobile devices to conduct financial transactions. In the late 1990s and early 2000s, mobile phone technology spread rapidly through the developing world, and saturated markets where standard landline telephones had never been established; cryptocurrency is poised to do the same exact thing.

If you do business globally, or travel frequently, you are often exposed to exchange rate risk; that is, the transaction can be affected by currency exchange rates. You may also be subject to fees associated with exchanging one currency for another, or find challenges in exchanging currency altogether. Fortunately, with cryptocurrencies like Bitcoin, that is

a non-issue, as the digital currency is universally recognized at a given value. This helps to save time in determining a price for a transaction, as well as any fees associated with exchanging money from one form to another. As cryptocurrency is increasingly adopted around the world, it is going to make financial transactions faster and simpler, which is a great thing for everyone involved.

One of the best things about cryptocurrency is that, unlike virtually any other type of money retaining system (save for a wall safe or your wallet) you totally own it. Think about it: most traditional liquid asset systems – banks, credit unions, brokerage houses, or even high-tech ones like PayPal – take control of your funds and leave you subject to their terms of service. If they decide that you have violated those terms, they can suspend your account. They can change their terms of service, and cause you to have to pay more or receive fewer funds for important transactions. With cryptocurrency, you retain all of the funds on hand, so to speak, digitally, with no third-party involvement; the only one who can change the terms of your crypto currency use is YOU.

II LITERATURE REVIEW

Sr No.	TITLE	FINDINGS	PROPOSED SOLUTION
1	[1] M. Bedford Taylor, "The Evolution of Bitcoin Hardware", Computer, vol. 50, no. 9, pp. 58-66, 2017. Available: 10.1109/mc.2017.3571056 [Accessed 11 June 2019].	The author traces the evolution of the hardware underlying the system, from early GPU-Based homebrew machines to today's data centres powered by application specific integrated circuits. These ASIC Clouds Provide a glimpse into planet scale computing's future.	Use of Algorithm of Etherhash, Neoscript, CryptoNight for secure block Generation
2	[2] F. Calvão, "Crypto-miners: Digital labor and the power of blockchain technology", Economic Anthropology, vol. 6, no. 1, pp. 123-134, 2018. Available: 10.1002/sea2.12136 [Accessed 11 June 2019].	Require more and more miners to engage and contribute to mine	Use of Pool mining for more use of labours and generate efficient outcome
3	[3] K. Brown, "Bitcoin and Ethereum: Empirical Evidence on Node Distribution", CU Scholar, 2020. [Online]. Available: https://scholar.colorado.edu/concern/undergraduate_honors_theses/2n49t217r. [Accessed: 04- Jan- 2020].	Use of Cross-sectional node and panel data to reduce 51% attack on blocks	Trying to increase more labours/miners by using pools such as nanopool,Slush,F2pool,DPool
4	[4] M. Andoni et al., "Blockchain technology in the energy sector: A systematic review of challenges and opportunities", Semanticscholar.org, 2020. [Online]. Available: https://www.semanticscholar.org/paper/Blockchain-technology-in-the-energy-sector%3A-A-of-Andoni-Robu/60be2610dba19761d6458bbac27527b744b0109e. [Accessed: 14- Jan- 2020].	Block-chains promise transparent, tamper-proof and secure systems that can enable smart contracts	Use of more numbers of systems for more electricity generation and for fast solution of block

III PROPOSED SYSTEM

Figure below depicts the basic idea of proposed system of the project, it represents how by analysing the market an algorithm which generates maximum profit is chosen by the software tool that we have selected after doing research of various software tools.

Transactions are sent to the block chain in form of

Blocks and then sent to miners/nodes for verification as shown in figure. Verification process involves solving graphical problems by each miner and the first one to solve it earns rewards in form of crypto currency.

Ultimately all the Alt coins are converted into BTC for further payout.

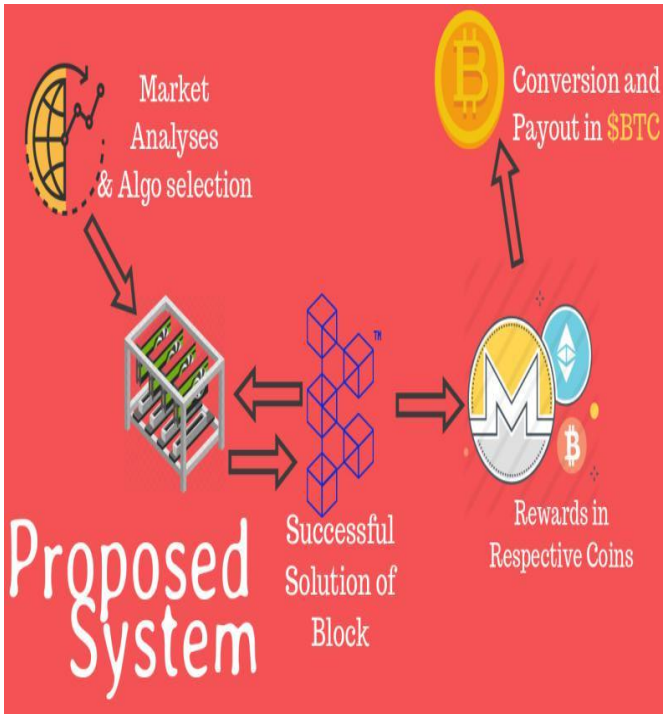
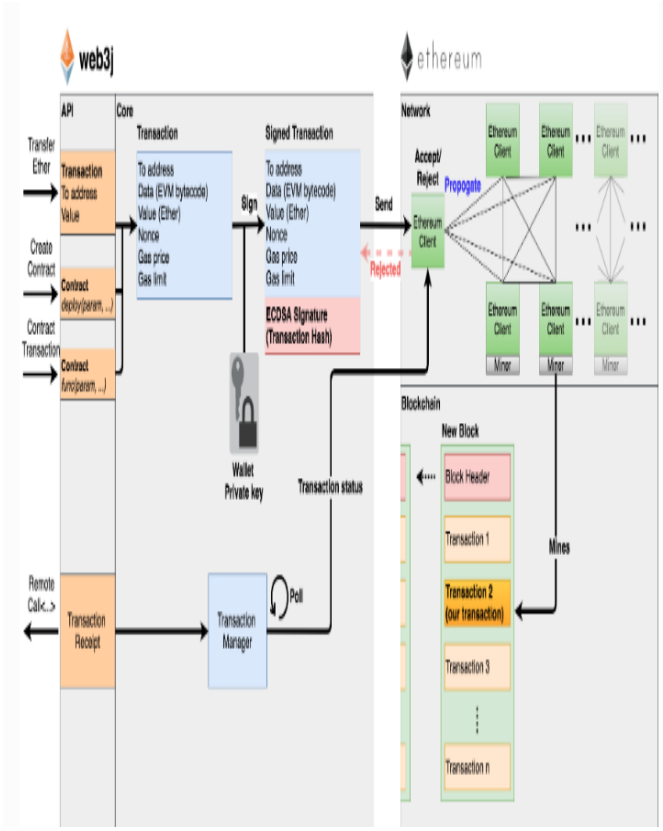


Figure given below represents the detailed process involved in transactions, verification and reward generation of the proposed system.

Web3j: It is an API which contains all the details of each and every transaction carried out such as the address value, transaction receipt, contract etc.

Core of Web3j: It receives the transaction and all its details from API, using the wallet private key ,each and every transaction is encrypted and signed and then it is sent to ethereum client where it is either accepted/Rejected

Network of Ethereum: In the ethereum network all the ether clients are present, interconnected to each other, we can see each and every block's block diagram, which consists of a block header and n transactions. Each and every ethereum client acts as a miner who verifies the transactions.



3.1 Algorithm used for feature detection

1. Scrypt

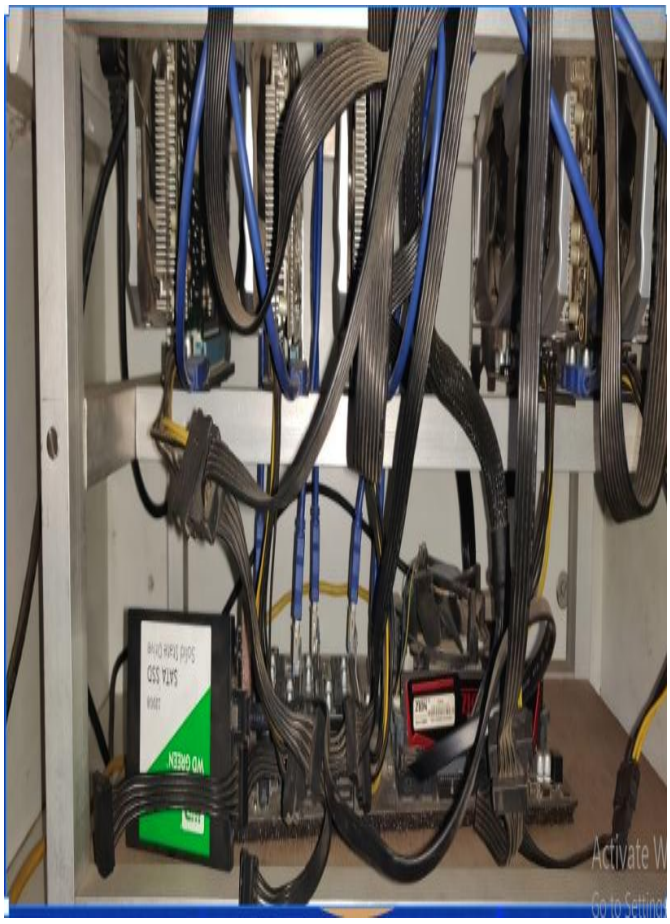
- HASHRATE:7.5151TH/s
- ACTIVE MINERS:15514
- ACTIVE ORDERS:36
- PAYING:0.2043 BTC/TH/day

2.SHA-256

- HASHRATE:296.5860 PH/s
- ACTIVE MINERS:25388
- ACTIVE ORDERS:40
- PAYING:0.0199 BTC/PH/day

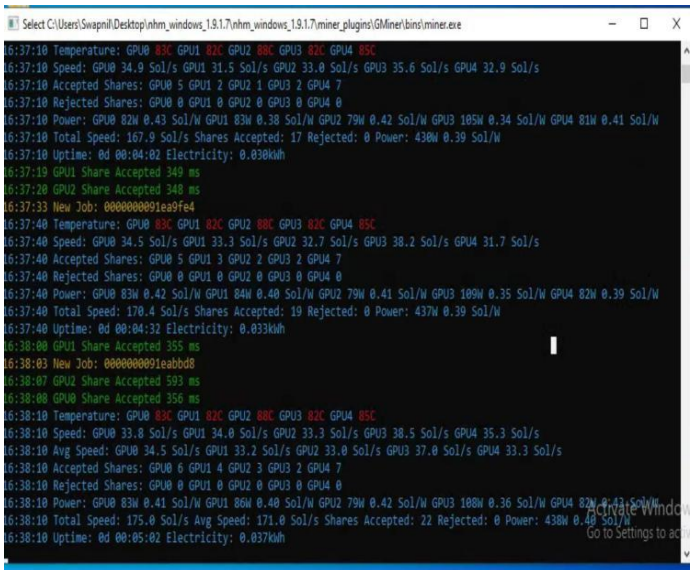
IV IMPLEMENTATION

4.1.1 Physical Representation of GPU with Hardware:



The above image represents the physical connection/configuration of GPU with hardware, how the slots of motherboard are configured with GPU due to proper connection

4.1.2 Configuration of GPU with the hardware:

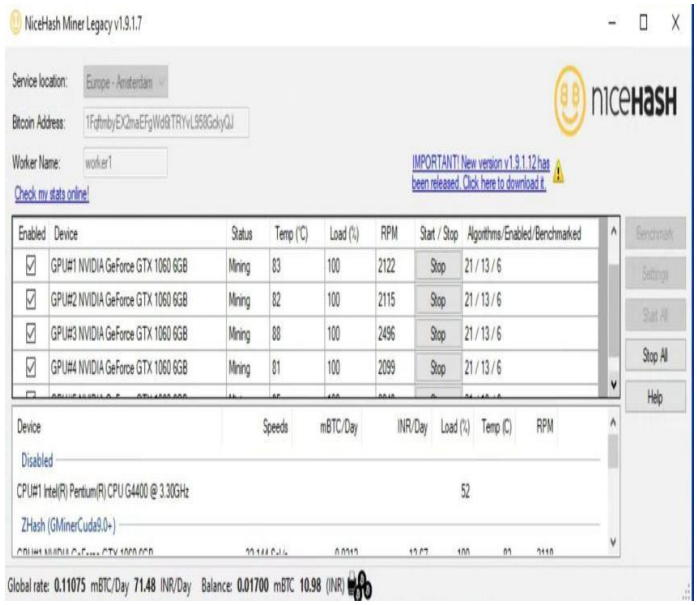


The Above image shows the

- Jobs Allocated to Each GPU
- GPU's which accept the share
- Temperature on which each GPU works
- Speed of GPU
- Power Consumed by Each GPU

In short, the overall status of GPU.

4.1.3 Configuration of GPU with the Software (Nicehash)



The image above shows the integration of mining rig with the software which shows all the GPU's which help in mining and at any point of mining we can stop any of the GPU's we desire by looking the profit it is providing in mining.

4.2 DIFFICULTIES FACED

We made a Machine Which Earns by Solving Blocks, but the Problem was Profitability and how to increase it.

Do You know what was the main Costing For us to Run this Machine???

Power (Electricity) , How much ?

Lets do Maths :-

500W per Hr*24*30=360000

1unit = 1000W so 360000/1000 = 360Units

360*9.25=**3330 Inr**

So this is our Energy Costing

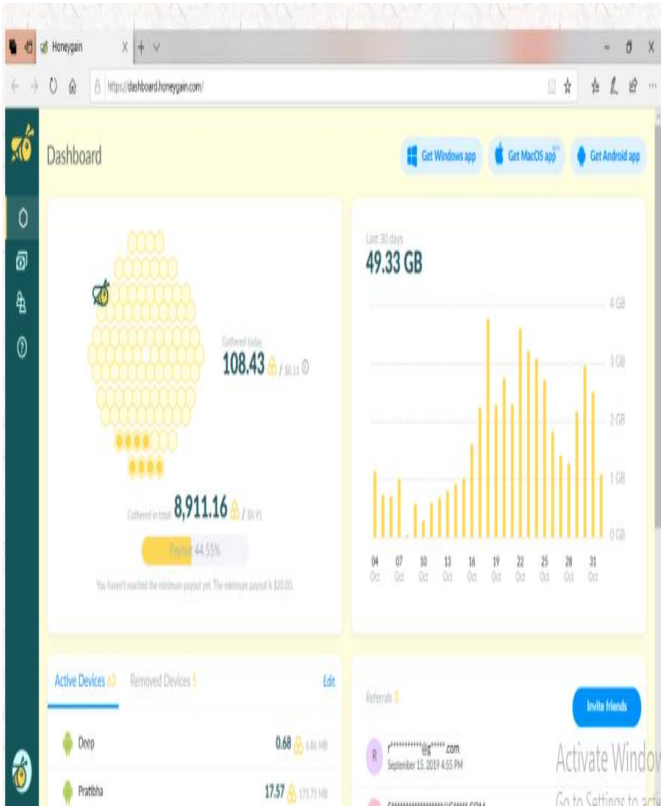
4.3 SOLUTION

- The per Day Costing is 111 Inr Max
- So we have tested a data reselling System which will give us 0.1$ per GB of Data
- We Resell ,which is 7.4 Inr. We upload approx 5GB data/day which turns out to be 40rs
- Also we are providing content delivering service for scientific research which pays based on time, Hence we are making 10rs/hr that turns out to be 240 rs per day

How it can Solve our Problem?

Approx 40rs/day from data reselling system and 240rs/day from content delivering service, i.e 280rs/day whereas our per day costing is 111 inr. Hence Profit=169 (as of now) per day which may vary time to time.

4.3.1 DATA OF DATA RESELLING SYSTEM OF 10/04/2020

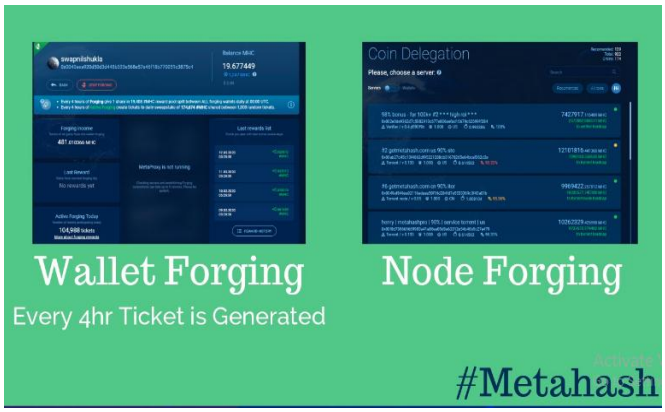


4.3.2 DATA OF CONTENT DELIVERY SYSTEM

We are doing two types of mining in proof of stake mining:

-Node forging

-System forging



V RESULT

time	algo	unpaid_total_amour	unpaid_algo_amour	profitability
2019-11-01 11:05:00	36	0.00001486	0.00000807	0.0000576
2019-11-01 11:05:00	38	0.00001486	0.00000053	0.0000576
2019-11-01 11:05:00	43	0.00001486	0.00000626	0.0000576
2019-11-01 11:00:00	36	0.00001458	0.00000785	0.0001008
2019-11-01 11:00:00	38	0.00001458	0.00000047	0.0001008
2019-11-01 11:00:00	43	0.00001458	0.00000626	0.0001008
2019-11-01 10:55:00	36	0.0000143	0.00000757	0
2019-11-01 10:55:00	38	0.0000143	0.00000047	0
2019-11-01 10:55:00	43	0.0000143	0.00000626	0
2019-11-01 10:50:00	36	0.00001417	0.00000744	0.0001008
2019-11-01 10:50:00	38	0.00001417	0.00000047	0.0001008
2019-11-01 10:50:00	43	0.00001417	0.00000626	0.0001008
2019-11-01 10:45:00	36	0.0000137	0.00000744	0.0000432
2019-11-01 10:45:00	38	0.0000137	0	0.0000432
2019-11-01 10:45:00	43	0.0000137	0.00000626	0.0000432
2019-11-01 10:40:00	36	0.00001346	0.0000072	0.0000864
2019-11-01 10:40:00	43	0.00001346	0.00000626	0.0000864
2019-11-01 10:35:00	36	0.00001304	0.00000678	0.0001296
2019-11-01 10:35:00	43	0.00001304	0.00000626	0.0001296
2019-11-01 10:30:00	36	0.00001265	0.00000639	0.0001296
2019-11-01 10:30:00	43	0.00001265	0.00000626	0.0001296
2019-11-01 10:25:00	36	0.00001223	0.00000597	0.0001152
2019-11-01 10:25:00	43	0.00001223	0.00000626	0.0001152

The image above shows the Mining of a very recent day where the date and time of each and every update is mentioned, the number of algorithms between which the nice hash miner has switched has been mentioned, the unpaid total amount and unpaid algorithm amount has been mentioned and the profitability of the mining has been mentioned.

VI CONCLUSION

Thus we have built a system which plays a small part of miner in transfer of value system and generates rewards for doing the same in terms of crypto currencies.

REFERENCES

[1] M. Bedford Taylor, "The Evolution of Bitcoin Hardware", Computer, vol. 50, no. 9, pp. 58-66, 2017. Available: 10.1109/mc.2017.3571056 [Accessed 11 June 2019].

[2] F. Calvão, "Crypto-miners: Digital labor and the power of blockchain technology", Economic Anthropology, vol. 6, no. 1, pp. 123-134, 2018. Available: 10.1002/sea2.12136 [Accessed 11 June 2019].

[3] K. Brown, "Bitcoin and Ethereum: Empirical Evidence on Node Distribution" CU Scholar,2020. [Online].Available:https://scholar.colorado.edu/concern/undergraduate_honors_theses/2n49t217r. [Accessed: 04- Jan-2020].

[5] Morgan E. Peck - The Bitcoin Arms Race is on! Spectrum, IEEE, vol.50 (2013), Issue: 6, pp. 11-13.

[6] Taylor, M. B - ―Bitcoin and the age of Bespoke Silicon‖. Compilers, Architecture and Synthesis for Embedded Systems (CASES), 2013 International Conference, 2013, pp. 1

[7]Hurlburt, G. F; Bojanova I. Bitcoin: Benefit or Curse‖. IT Professional, vol. 16(2014), Issue: 3, pp. 10-15