ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 9, September 2018

# Cryptocurrency Mining using Amazon Web Services

Ashka Alkeshkumar Soni[1]

Undergraduate Student, Department of Computer Engineering, G H Patel College of Engineering & Technology, Vallabh Vidyanagar, Gujarat, India[1]

**ABSTRACT:** Currency nowadays is not just confined to paper notes. Several modes of payment have been introduced like Electronic Transaction, Digital transaction and so on. Digital Transaction Management (DTM) is a classification of cloud services that manages document-based transactions digitally. DTM makes quicker, simpler and compelling procedures for different transactions to take place. A cryptocurrency is an advanced digital resource designed to work as a medium of exchange. It uses cryptography for secure transactions and to control the creation of additional units of the currency. Cryptocurrencies are a subset of advanced and virtual monetary standards. This project mines the cryptocurrency in the minimal time to generate revenue. It throws light on the subtleties of digital money mining process, the customary machines utilized for mining, their constraints, about how cloud-based mining is the coherent subsequent stage and the favorable position that cloud stage offers over the conventional machines.

**KEYWORDS**: Cryptocurrency; Cloud platform; Ethereum; Blockchain Mining; Amazon Web Services; Hashrate.

## I. INTRODUCTION

A **cryptocurrency** (or **crypto currency**) is a digital asset designed to work as a medium of exchange using cryptography to secure the transactions and to control the creation of additional units of the currency [2][3]. Cryptocurrencies are classified as a subset of digital currencies and are also classified as a subset of alternative currencies and virtual currencies. In cryptocurrency, a transaction is a transfer of coins from one wallet to another. When a transaction is made, the details of the transaction will be broadcast to every node in the network. The transactions made over a set period of time are collected to form a 'Block'. To incorporate transparency in the system, it is designed in such a way that all the transactions made from the inception of the currency are recorded and maintained in a general ledger called the 'Blockchain' which, as the name suggests, is a list of blocks created from the beginning [4].

Miners play a predominant role in mining. Miners process transactions by verifying the ownership of the currency from source to destination. Every transaction contains the hash of the previous transaction made by the owner through which authenticity of a present transaction is tested, thereby validating it. Miners also inhibit double spending of the currency through this validation process [4].

The main purpose of mining is to generate and release coins into its coin economy. Whenever a transaction takes place and is validated, miners collect these transactions and include them into the block they are currently solving. Every block has to be solved before being broadcasted and put in the blockchain. Solving of a block involves mathematical puzzles which are difficult to unlock and crack provided there will be some constraints on the output generated. Only on solving the mathematical puzzle is one allowed to add the block to the ledger and a reward of coins is given in return. Thus, mining eventually boils down to a competition of mathematical puzzles to solve for the reward of coins. This mechanism prevents miners from easily procuring coins and thus maintains the fairness of the system [4].

The aim is to mine the decentralized digital currency i.e. Ethereum, to minimize the exchange rates and maximize the revenue in the transaction.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 9, September 2018

## II. RELATED WORK

During initial times, CPU was used to mine cryptocurrency with hash rates of about 10MH/sec. But due to increase in the mining mechanisms, the usage of CPU became tedious as machines with higher hashing power was needed.

In [1], the author talks about how cloud mining is an alternative over GPU and CPU mining.

Cloud computing goes beyond a single company or enterprise. The applications and data served by the cloud are available to a broad group of users, across enterprises and across platforms. The access is via internet. Any authorized user can access these docs and apps from any computer over any Internet connection.

Cloud computing should not be confused with network computing where all the information are hosted on the company‘s single network and it can be accessed by members on that network only. Cloud is much bigger than that and it encompasses multiple companies, servers and networks. In order to first think about implementing cloud technology with Bitcoin mining, it is essential to understand why a Cloud network based application is important. This can be explained by considering advantages of cloud computing, which are many but a few significant ones are listed as:

- Low cost computers
- Improvement in performance of computers
- Lower IT infrastructure cost
- Lower software cost
- Fewer maintenance issues

## III. PROPOSED ALGORITHM

### A. *Proof of Work:*

A block that is mined is considered valid on if it contains Proof of Work (PoW) of a given difficulty, The Proof of Work is basically data that is difficult to produce but is easy to verify.

### B. *Blockchain:*

A **blockchain**,[2][3][4] originally **block chain**,[5][6] is a continuously growing list of records, called *blocks*, which are linked and secured using cryptography.[2][7] Each block typically contains a cryptographic hash of the previous block,[7] a timestamp and transaction data.[8] By design, a blockchain is inherently resistant to modification of the data. It is "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way".[9] For use as a distributed ledger, a blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for inter-node communication and validating new blocks. Once recorded, the data in any given block cannot be altered retroactively without the alteration of all subsequent blocks, which requires collusion of the network majority.

Blockchains are secure by design and exemplify a distributed computing system with high Byzantine fault tolerance. Decentralized consensus has therefore been achieved with a blockchain.[10] This makes blockchains potentially suitable for the recording of events, medical records,[11][12] and other records management activities, such as identity management,[13][14][15] transaction processing, documenting provenance, food traceability[16] or voting.[17]

### C. *Mining Ethereum:*

**Ethereum** is an open-source, public, blockchain-based distributed computing platform and operating system featuring smart contract (scripting) functionality [18]. It supports a modified version of Nakamoto consensus via transaction based state transitions.

**Ether** is a cryptocurrency whose blockchain is generated by the Ethereum platform. *Ether* can be transferred between accounts and used to compensate participant mining nodes for computations performed [19]. Ethereum provides a decentralized Turing-complete virtual machine, the Ethereum Virtual Machine (EVM), which can execute

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 9, September 2018

scripts using an international network of public nodes. "Gas", an internal transaction pricing mechanism, is used to mitigate spam and allocate resources on the network [18][20].

D. *Cloud Mining:*

**Cloud Mining** is the process of bitcoin mining utilizing a remote data center with shared processing power [21][22]. This type of cloud mining enables users to mine bitcoins or alternative cryptocurrencies without managing the hardware [21]. The mining rigs are housed and maintained in a facility owned by mining company and the customer simply needs to register and purchase mining contracts or shares [23]. Since Cloud Mining is provided as a service there is generally some cost and this can result in lower returns for the miner.

We are using Amazon Web Services in the form of Software as a Service (SaaS) to mine Ethereum. **Amazon Web Services** (**AWS**) is a subsidiary of Amazon.com that provides on- demand cloud computing platforms to individuals, companies and governments, on a paid subscription basis. The technology allows subscribers to have at their disposal a full- fledged virtual cluster of computers, available all the time, through the Internet. AWS's version of virtual computers have most of the attributes of a real computer including hardware (CPU(s) & GPU(s) for processing, local/RAM memory, hard-disk/SSD storage); a choice of operating systems; networking; and pre-loaded application software such as web servers, databases, CRM, etc. Each AWS system also virtualizes its console I/O (keyboard, display, and mouse), allowing AWS subscribers to connect to their AWS system using a modern browser. The browser acts as a window into the virtual computer, letting subscribers log-in, configure and use their virtual systems just as they would a real physical computer. They can choose to deploy their AWS systems to provide internet-based services for their own and their customers' benefit.

We are using Amazon g2.2xlarge instance for mining. The g2.2xlarge version comes with 15 GB memory, 60 GB of local storage, 26 EC2 Compute Units (that's an Intel Sandy Bridge processor running at 2.6 GHz) and a single NVIDIA Kepler GK104 graphics card (with 1536 CUDA cores).

E. *Ethash Algorithm:*

Ethash is the planned Proof-of-Work algorithm for Ethereum 1.0. It is the latest version of Dagger-Hashimoto, although it can no longer appropriately be called that since many of the original features of both algorithms have been drastically changed in the last month of research and development. It identifies the nonce input to the result in such a way that it is lower than the threshold determined by the difficulty. A new block can be found by simply manipulating the difficulty. Estimatedly, on an average each block is produced after 12 seconds.

The general route that the algorithm takes is as follows:

1. There exists a **seed** which can be computed for each block by scanning through the block headers up until that point.
2. From the seed, one can compute a **16 MB pseudorandom cache**. Light clients store the cache.
3. From the cache, we can generate a **1 GB dataset**, with the property that each item in the dataset depends on only a small number of items from the cache. Full clients and miners store the dataset. The dataset grows linearly with time.
4. Mining involves grabbing random slices of the dataset and hashing them together. Verification can be done with low memory by using the cache to regenerate the specific pieces of the dataset that you need, so you only need to store the cache.

The large dataset is updated once every 30000 blocks, so the vast majority of a miner's effort will be reading the dataset, not making changes to it.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 9, September 2018

F. *Mining Algorithm:*

The mining algorithm is defined as follows:

```
def mine(full_size, dataset, header, difficulty):
target = zpad(encode_int(2**256 // difficulty), 64)[::-1]
from random import randint
nonce = randint(0, 2**64)
while hashimoto_full(full_size, dataset, header, nonce) > target
nonce = (nonce + 1) % 2**64 return nonce
```

G. *Working:*

The difficulty time after it is adjusted produces a block after 12 seconds on an average, dynamically. Any node that participates in the network generates its revenue, which is directly proportional to the mining power or hashrate.

Hashrate = No. of nonces tried per second normalised by the total hashrate of the network.

When the node starts, mining starts once the DAG is built from current epoch (100-hour window). The GPU Speed needs to be high.

## IV. IMPLEMENTATION RESULTS

The following test was implemented.

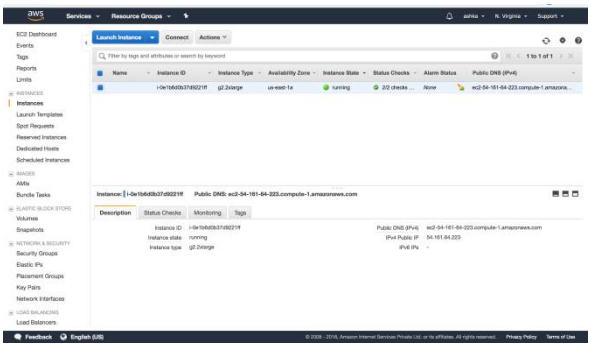

Fig.1. Amazon Instance Details

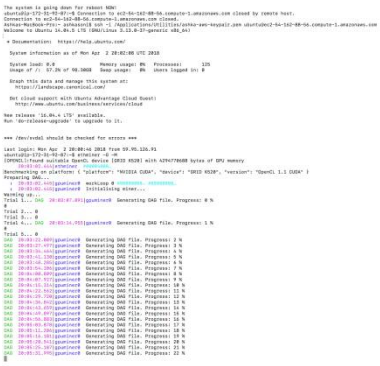

Fig.2. DAG Generation Process

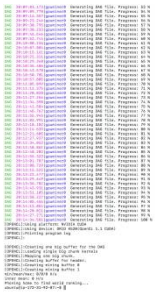

Fig.3. DAG Generation Process Continued

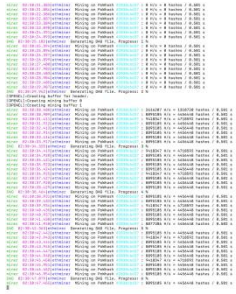

Fig.4. Miner Initialisation

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 9, September 2018

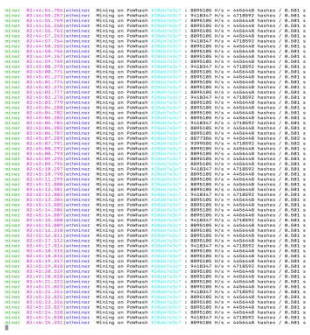

Fig.5. Mining in progress

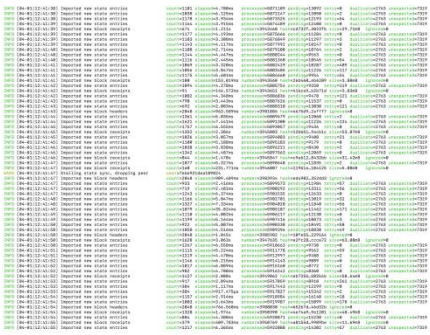

Fig. 6. Blockchain Mining

## V. CONCLUSION AND FUTURE WORK

Since the start of the virtual currency revolution, the speed of evolution of the mining techniques to maximize hashing rates to maximize profits has been staggering. However, the stability is a question with mining machines and technologies becoming redundant.

The project gives a summary of types of cryptocurrencies currently in operation, the types of mining algorithms, which led us to the next logical step of cloud-based mining. But of course, this is definitely not the final solution. As the complexity increases, the redesign of machines is indubitable. However, currently cloud mining presents the most pragmatic route towards maximizing profits.

## REFERENCES

1. Hari Krishna and Sai Saketh Y.,'Cryptocurrency Mining - Transition to Cloud', International Journal of Advanced Computer Science and Applications, Vol.6, Issue 9, 2015.
2. The Economist ,'Blockchains: The great chain of being sure about things', 31 October 2015.
3. Morris, David Z.,'Leaderless, Blockchain-Based Venture Capital Fund Raises $100 Million, And Counting', 15 May, 2016.
4. Popper, Nathan ,'A Venture Fund With Plenty of Virtual Capital, but No Capitalist', *New York Times*, 21 May 2016.
5. Brito, Jerry and Castillo Andrea ,' Bitcoin: A Primer for Policy Makers', George Mason University, 2013.
6. Trottier Leo,'Original Bitcoin', Github.
7. Narayan Arvind and Miller Andrew ,'Bitcoin and cryptocurrency technologies: a comprehensive introduction', Princeton University Press ISBN 978-0-691-17169-2.
8. Blockchain Investopedia, Archived from the original on 23 March 2016.
9. Iansiti Marco, Lakhani Karim R. , "The truth about blockchain" , Harvard Business Review, 18 January 2017.
10. Siraj Raval, " What is a decentralised application?", Decentralised Applications : Harnessing Bitcoin's Blockchain Technology, O'Reily Media,Inc, ISBN 978-1-4919-2452-5, 2016
11. Yuan Ben and Wendy Lin, " Blockchains and electronic health records", mcdonnell.mit.edu.
12. Ekblaw Ariel and Azaria Asaf, "MedRec: Medical Data Management on Blockchain", 19 September 2016.
13. Bryan Yurcan, 'How blockchain fits into the future of Digital Identity', American Banker, 8 April 2016.
14. Prisco Giulio, 'Microsoft Building Open blockchain-based identity system with blockstack,consenSys', BTC Media LLC, 3 June 2016.
15. Pricso Giulio, ' Department of Homeland Security Awards Blockchain Tech Development Grants for Identity Management and Privacy Protection', Bitcoin Magazine.
16. Ryan Browne, 'IBM partners with Nestle, Unilever and other food giants to trace food contamination with blockchain', CNBC, 22 August 2017.
17. What is Blockchain Technology?, Follow my vote, 15 January 2018.
18. 'Understanding Ethereum (Report), CoinDesk, 24 June 2016.
19. Cryptocurrencies: A Brief Thematic Review, Wayback Machine, Social Science Research Network, 28 August 2017.
20. 'Ethereum, Gas, Fuel & Fees', ConsenSys Media, 15 January 2017.
21. 'CLoud Mining - How to mine bitcoin without a miner', CoinDesk.
22. David Lee Kuo Chuen, 'Handbook of Digital Currency: BItcoin, Innovation, Financial Instruments and Big Data', Academic Press, 2015.
23. 'Bitcoin Cloud Mining Contract Reviews, Bitcoin Mining, 28 June 2017.
24. About Bitcoin Cloud Mining, Cloud Mining Report.