EUROPEAN ACADEMIC RESEARCH
Vol. V, Issue 8/ November 2017

Impact Factor: 3.4546 (UIF)
DRJI Value: 5.9 (B+)

ISSN 2286-4822
www.euacademic.org

Blockchain Expenses - Resources Need to Generate Cryptocurrency

IJAZUL HAQ[1]
MIR HASSAN
International School of Software
Wuhan University, Wuhan, Hubei, China

Abstract:

Cryptocurrencies have shown their considerable adoptability in recent years. Bitcoin emerged recently and became the most successful cryptocurrency, with the economic value of billions of dollars. Bitcoin network is one of the most powerful computer networks on the planet. It's a sum of remarkable hardware resources and consumes tremendous electric power. Although, these expenses help to extend the security of cryptocurrency network – Blockchain. But spending too many resources just for the creation of intangible digits on the internet is a side-effect of Bitcoin technology. The purpose of this paper is to analyze the resources and measure the expenses need to create cryptocurrency and run its underline network. The results we present in this paper are obtained through an experiment. We developed a mining simulator and run it on different computers to measure the Time, Electricity and Hardware resources required for bitcoin mining. The results we found are useful for further research in Blockchain as well as in the field of Green Computing. Besides that, this paper is helpful for a layman to know the effort involved in cryptocurrency creation.

Key words: Distributed Systems, Blockchain, Cryptocurrency, Bitcoin, Green Computing

[1] Corresponding author: ijaz@whu.edu.cn

I. INTRODUCTION

Information Technology has a great influence on every aspect of our lives and has made things very easy. To send an email, image, or document across the world is now only a matter of seconds. But when we need to transfer values (i.e. Money) then the things become complicated, that's a question mark for IT. From several decades experts have been trying to figure out solutions to this issue. The one common approach by many researchers was to implement a cryptocurrency system independent of a third party (i.e. Bank or Government). Cryptographers even proposed some systems to decuple currency from banks. But to put money on internet wasn't an easy task and various issues rose time to time. In 1908, someone with pseudonym Satoshi Nakamoto (whose real identity is still unknown) integrated all the previous ideas and presented a cryptocurrency system called Bitcoin, with the underlying protocol named Blockchain [1]. Followed by the implementation source code of Bitcoin software in 2009. Bitcoin is a system that completely decuple the currency from a third trusted party successfully for the first time in history.

Bitcoin network is one of the largest and powerful computer networks on the planet, and spend a huge amount of electric power. Apart from several other limitations of Bitcoin technology, one issue that's worth noticing is the amount of resources need to generate bitcoins, and run its underline network – blockchain. Although some proponents of Bitcoin technology consider it an advantage of the blockchain network, because the more resources need to generate bitcoins means the more secure is the Bitcoin network. But the reality is that it's a side effect of the Bitcoin technology, and it need to be measured how much is the side effect.

In bitcoin mining, miners compete to solve mathematical problem. To solve mathematical problem we need computing power, and for that we need energy and time. In this paper we

describe the energy and time a computer need to solve that mathematical problem. We also consider the energy consumption of hashing in the form of *kilowatt hours* that can be easily described in local currency. The results we found are helpful for future research in this field and also give a clear understanding to common person about the real value of cryptocurrency.

The remaining of papers is organized as follows: In section II, We have briefly explained Cryptocurrency, Bitcoin and Blockchain technology. Section III include a description of blockchain expenses, PoW (Proof-of-Work) is explained and describe Mning process. In Section IV we have explained the simulator, the experiment we conducted and analyzed the results we found. Section V is the last section that conclude the document.

Note: This paper is not about a specific cryptocurrency but we'll use Bitcoin as an example for demonstration purpose. When used in the sense of technology, Bitcoin is written capitalized i.e. "Bitcoin" but in the sense of unit its written "bitcoin" (e.g. "Bitcoin protocol" and "10 bitcoins"), sometimes "BTC" is used instead of bitcoin (not Bitcoin).

II. PRELIMINARIES

A. CRYPTOCURRENCY

Cryptocurrency can be defined as "A virtual coinage system that functions much like a standard currency, enabling users to provide virtual payments for goods and services free of a central trusted authority" [1]. In case of Traditional currency there is a central trusted authority responsible for all the monetary operations, and transactions take place on a central server that maintains a ledger. In case of cryptocurrency there is no central authority, but all the transactions take place on a network of computers. The word "Cryptocurrency" doesn't means "Digital Currency" but they are two different things, and cryptocurrency is a type of digital currency. The common digital currency is

controlled by a government, where there is a bank to make account and deposit money in it. Then we use internet to access our account. And when we make transactions, the bank update the ledger. In cryptocurrency there is no bank where we should deposit or withdraw money, but the money is only existed on internet and has no physical form. Cryptocurrency means that the currency has been encrypted using cryptography that prevent it from been copied. The basic mechanism of cryptocurrencies is the transmission of digital information decupled from central authority or government – while using cryptographic algorithms to ensure that the transactions are legitimate and unique.

The history of cryptocurrency starts back from Chaum's proposal for "Blind Signature" and "Untraceable Payments" in 1983 [2]. After Chaum's idea of preventing the bank from linking users to coins, many prototypes and extensions of the scheme were proposed and significant contributions were made. Several startup companies (i.e. DigiCash [3] and Peppercoin [4] etc.) tried to bring digital cash into practice but none of these schemes achieved significant success. In 1989 *Merkle Tree* was introduced, mainly used to make sure that the data blocks received from other nodes in a P2P network are received unaltered and undamaged. Merkle Tree was a breakthrough in hash-based cryptography [5]. In early 1990s the basic building block of modern cryptocurrencies known as *PoW* (proof-of-work[2]) was proposed [6], followed by some other useful techniques in cryptography, including preventing different types of *denial-of-service* attacks [7]. In late 1990s public ledger was proposed for detecting *double-spending,* where the bank maintains a database to make sure the validity of coins and avoid spending money more than once [8]. Wei Dai moved a step further towards the realization of cryptocurrency and published a description of *b-money* in 1998 – a distributed

[2] Proof-of-work was originally proposed for combating junk emails but not widely used for that purpose.

electronic cash system [9]. The same year Szabo created *Bit Gold,* a PoW based electronic currency system [10]. Hal followed Dai and Szabo's work and created a currency system based on a *reusable proof-of-work* in 2004 [11]. Finally someone with pseudonym Satoshi Nakamoto integrated all the existing ideas and presented a decentralized public ledger named *Blockchain* in 2008 [12]. Blockchain has the solution to all the issues related to cryptocurrency. Based on Blockchain, Satoshi proposed a new type of currency called *Bitcoin* that's considered the most successful cryptocurrency of the day. After the popularity of bitcoins, many *altcoins*[3] introduced in market. At the time of writing, there are 1277 types of cryptocurrencies introduced and some of them have gained significant popularity e.g. Ethereum, Ripple and Litecoin etc. The market cap of all the cryptocurrencies together is 207 billion USD as of September 2017 [13].

B. BITCOIN

The world's first completely decentralized cryptocurrency, created by an unidentified programmer named Satoshi Nakamoto in 2008 [12] [14]. Bitcoin has been emerged as the most successful cryptocurrency in history [15], with a market cap of $121 billion as of November 2017 [16] [17]. Bitcoin works almost like a traditional currency system. A user can exchange bitcoins over the internet to do almost anything that one can do with the conventional currency, including shopping, trading, storing values and above all is the remittances across borders etc. A lot of platforms have already been developed where bitcoin can be exchanged for other currencies, purchased and sold. Because of its ultimate security, fast payment and borderless nature, bitcoins is the perfect form of currency over the internet. There is no central authority in Bitcoin network, it means there is no one to increase or decrease the value of bitcoin by manipulating its supply. Not having a central entity

[3] A term used for all the other cryptocurrencies except Bitcoin

means no one can inflate bitcoin's price or devalue it by manipulating its supply, and no risk of printing more bills by government to devalue your savings. New bitcoins come to circulation by a stable rate, decided by bitcoin software, and no one can change that rate without the consensus of all miners. In Bitcoin network, participants use bitcoin software to solve math problem and if there answer (also called Proof-of-Work) is correct, they can attach there block of transactions to the blockchain. If a participant's block is valid, he is issued certain amount of bitcoins as reward, that's how new bitcoins come into use. The block reward was initially set to 50 bitcoins, and after every 210,000th block (that takes about 4 years), the size of reward is halved. The total number of bitcoins that will be generated is 21M, and all of them will be mined by the year 2140. Bitcoin encourage everyone to join the network and participate in mining, there is no proposal or criteria to go through.

C. BLOCKCHAIN

Bitcoin system is based on blockchain technology, a novel P2P approach to link together a sequence of events or transactions in a way that is immutable. Blockchain maintains a public ledger of all the transactions ever been occurred since the *Genesis-Block*. Each transaction occurred is broadcast to all the peers in the network who maintain the ledger, called Miners. Every miner check these transactions, combine the valid transactions into a block. When the block size reached to about 1MB (in case of Bitcoin blockchain), they assemble it, then push it to the network. All the other nodes update their local blockchain. Every block must contain a hash-digest of the previous block. This technique is used to link every block in blockchain to the previous block all the way to genesis-block.

Blockchain is not Bitcoin, "Blockchain is a distributed timestamp server technology introduced for the realization of bitcoin" [12]. Beyond cryptocurrency, blockchain applications

are countless, a detail is given in [18]. Blockchain implements a public ledger shared across the network. It validates existence of digital assets and monitor where the control of these assets exists on the network – without the control of a central authority [19]. Each transaction in the public ledger is verified by consensus of a majority of the nodes connected to the network [20]. Each node has a blockchain stored locally on his computer. And once entered, information can never be erased. Blockchain contains a certain and verifiable record of every single transaction ever made.

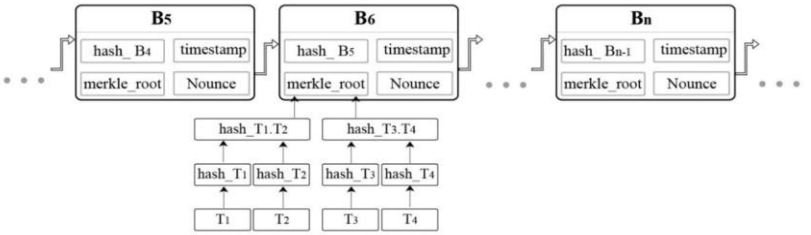

Figure 1: The structure of a Blockchain

The most series problem ever in creation of cryptocurrency was double-spending problem. Because digital tokens can be easily replicated and used more than once. Blockchain is the first successful implementation ever to solve double-spending problem. It stores the record of transactions in the form of blocks. All the blocks are linked by chaining the hash of previous block in the header of subsequent one. To make sure that the user spending the bitcoins really owns them, blockchain maintains a timestamp ledger and distribute that ledger among all the participating nodes. Every node update his ledger to the longest and latest chain. This mechanism prevents the system from attack, as if a slight change occurs to the previous block, it will propagated to all the subsequent blocks. The attacker will then need to re-mine all the affected blocks again to commit the change. And even if attacker succeeds to re-mine the blocks on one computer, the other nodes will not

accept that change. The only way to change a single transaction is to control 51% of all the computing power in the network. It's known as the 51% attack that require a significant computing power.

III.BLOCKCHAIN EXPENSES

A. POW (PROOF-OF-WORK)

In fiat money we have notes/bills – in cryptocurrency we have proof-of-work (PoW). Cash is difficult to generate and we can use it only once that's why it has value, and PoW does have the same properties it's difficult to generate and it can be used only once. In cryptocurrency, transaction is not considered genuine until certain amount of energy has been expend. "A proof-of-work (PoW) is a piece of data which is difficult (costly, time-consuming) to produce but easy for others to verify and which satisfies certain requirements" [22]. "PoW adds an economic cost to perform a given function" [1]. Producing PoW is a random process with low probability and need a lot of trial and error before a valid PoW is generated. Bitcoin use *Hashcash* PoW algorithm, proposed by Adam Back in 1997 (Adam, Hashcash 2004).

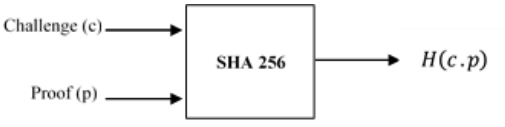

Figure 2: Hashcash PoW system

Figure 2 shows a basic hashcash system where c and p are the challenge and proof respectively:

$$H(c.p) \leq T \qquad (1)$$

Where T is the target hash digest with a specified number of zeros in the beginning, "." is the concatenation operator and H means Hash function. The original hashcash PoW algorithm was based on SHA-1 cryptographic hash function, but

blockchain use the extended version based on SHA-256. A cryptographic hash algorithm is a one way collision resistant[4] function that is easy to compute but hard to invert. In other words, a functions that create a fixed length output value of n bits for an arbitrary message (input value) of length m, such that: $H(m) = n$

But there is no function H' to compute m from n:

$$H'(n) \neq m$$

To find the value of m it's nearly impossible that need tremendous computational power and time. The only way to calculate back the value of m is brute-forcing and need a lot of trial-and-error. In Bitcoin system, this type of random search in order to find the required hash digest is called *Mining*.

B. MINING

The blockchain infrastructure is provided by miners. Mining is one of the key concepts, where every miner want to add a new block to the blockchain. To add block, miner has to provide the answer/proof to a specific challenge called PoW, and it needs a large amount of computational power. In Bitcoin blockchain, a block must contain five parameters to be attached to blockchain successfully. Every minor first prepare four of them, *Merkel Root* of all transactions, *Timestamp*, *Version Number* of bitcoin software and the *hash-digest* of previous block. Then a race among the miners started to find the fifth parameter. Every miner want to find a number called *Nonce* that when concatenated with the other four parameters and hashed, it create a hash value that satisfy certain conditions. Nonce can be found only by brute-forcing that need a lot of trial and error. The one who has the more computational power has the more probability of finding the *Golden-Nonce*[5]. The miner who find the golden-nonce and publish the completed block to the

[4] Where two or more different input values cannot produce one hash digest.
[5] The nonce that when concentrated with the other four parameters, produce the required minimum hash-digest.

network is rewarded a set amount of bitcoins, and this is the only way to bring new bitcoins in circulation. Figure 3 show the procedure of bitcoin mining.

In Bitcoin blockchain, the criteria for a hash digest to be valid is given in Equation 1. It's shown that the PoW can be achieved by randomly choosing the nonce p until $H(c.p)$ become less then T. When p is found the block can be send to the Bitcoin network. The other nodes update their ledger, and the miner who found the block is rewarded with bitcoins. As we know that the length of SHA-256 hash-digest is 64 characters alpha-numeric value. If we want to search for an exact hash value, it'll take very long time (maybe months or up to years). Therefor it's a hint for miners to just find the value that produce a hash-digest lower than a certain threshold value. In other words, the hash-digest should contain certain number of zeros in the beginning. The number of zeros in the beginning of required hash-digest has a direct relationship with the expenses and resources need to find the required nonce, we'll discuss it in detail in next section.

Before 2014 Bitcoin miners relied on CPU and GPU technology that were efficient for running SHA-256 hashes and need less power. Later on miners started to operate computer chips known as Application Specific Integrated Circuits (ASICs), especially designed for running SHA-256 that increased the power consumption to an extreme level. The current computational power of Bitcoin network as of November 2017 is 11,000,000 TH/S [21]. And as of 2014 analysis the total power consumption of Bitcoin mining was equivalent to Ireland's average electricity consumption [24].

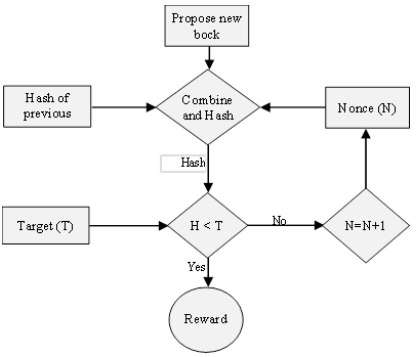

Figure 3: The procedure of bitcoin Mining

IV. SIMULATION AND RESULTS

In this paper we discuss three types of expenses, Time, Electricity and Hardware. The most important of them is time, because if we find the time then we can easily find the power consumption also. Let say T_n is the time to find the nonce and T_p is the time to propagate the block to the network. In Bitcoin blockchain, only T_n and T_p are significant. In this paper we'll ignore T_p, because the value of T_p is very small and negligible compared with T_n, it will not affect our results.

To find the value of T_n, we write a program in Java to calculate hashes and record the execution time. We run the program on three different computers having different processing power, we named them *Low*, *Med* and *High*. The hardware properties and approximate market price of each computer (at the time of writing) is known, as shown in table 1.

Name	CPU	CPU Freq.	CPU Cashe	Power	RAM	Approx. Price (USD)
Low	AMD-APU	1.35 GHz	NA	10 W	2 GB	$ 240
Med	Core i3	2.40 GHz	3 MB	35 W	4 GB	$ 500
High	Core i7	4.00 GHz	8 MB	88 W	24 GB	$ 1500

Table 1: Properties of the three computers used in our experiment

The source code of simulator is written as follows:

First we generate three random variables named $timeStamp$, $prevHash$ and $merkelRoot$. Then we used a While Loop (starting from 0 and incremented by 1), to find the fourth variable $nonce$. We used the counter of while loop as nonce. Inside thee while loop we concatenated all the four variables and passed it to a function named sha256. sha256 return 64 characters alphanumeric hash-digest of any input string that we pass it as type String argument.

$$hashDigest = sha256(timeStamp + prevHash + merkelRoot + nonce);$$

The minimum threshold value is determined by the number of zeros in the beginning of hash-digest, defined with a variable named *startWith*. Every time when sha256 function return the *hashDigest*, we count the number of zeros in its start. Using Java "if else" statement, we check if the number of zeros is greater than or equal to *startWith*, we found the golden-nonce. We assign the loop counter to a variable named *golderNonce* that we have initialized previously to *NULL*, and terminate the while loop. The time elapsed to run the While loop is recorded in the form of milliseconds.

To get more accurate results, we repeat the experiment fifty times and then calculate the average values. We repeat the experiment for four different number of 0s. The results we found are given in Table 2, and a graph of results is shown in Figure 4.

Number of zeros: n	**Time to find golden-nonce: Tn**			**Nonce**
	Low	**Med**	**High**	
4	1.90	0.42	0.13	77199
5	39.09	7.49	1.43	1396073
6	351.09	68.25	18.28	12729183
7	13094.34	673.19	285.19	152455185

Table 2: Results of three different computers for different number of starting 0s in hash-digest

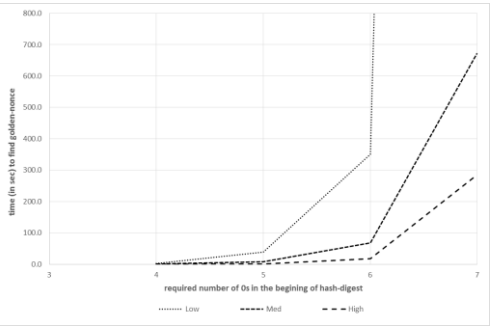

Figure 4: Time required to find the hash-digest for different number of starting 0s

In table 2, n is the number of 0s in the beginning of required hash value, T_n is the average time to find the golden-nonce. From the results shown, we can find that if we increase n by 1, the value of T_g will be increased 15.87 times, it can be written as follows:

$$T_{gn+1} = 15.87 \times T_{gn} \quad (2)$$

In Bitcoin blockchain, the value of n is 18, as of November 6th, 2017. We used equation 2 and calculate the value of T_n for all of the three computers. Following table show the value of T_n (in Hours) when the value of n become 18.

Number of zeros: n	**Time to find golden-nonce: Tn (in Hours)**		
	Low	**Med**	**High**
18	58496130833931	3007322479989	1274025107233

Table 3: The value of T_n for n = 18

The data in table 3 shows that, if the value of n is 18, our High computer will take 12.7×10^{11} hours to find the golden-nonce and mine one block.

The High computer we used in our experiment is 88 W, as shown in table 1. So, its power consumption in the form of kWh is as follows:

$$P = 1.27 \times 10^{12} \times 88 = 1.12 \times 10^{19}\, Wh$$

$$P = \frac{1.12 \times 10^{19}}{1000} = 1.12 \times 10^{16}\, kWh$$

And the reward for mining one block at the time of writing is 12.5 BTC, therefore:

$$\text{Power consumption for one bitcoin } = \frac{1.12\times10^{16}}{12.5} = 8.96 \times 10^{14}\, kWh \qquad (3)$$

As we can see in equation 3, if we use a standard PC worth $1500 approximately, it will use a tremendous amount of electricity to find the nonce. These figures seem very strange, but these are the results for a standard general purpose PC. To lower the amount of expenses, miners use special type of chips called ASICs, designed for calculating hashes. The initial purchasing price of these chips are relatively high, but they reduce the mining time and electricity consumption effectively.

V. CONCLUSION

In this paper we describe the resources need for the creation of cryptocurrency. Our results show that using PC, it's nearly impossible to mine bitcoins, and extremely expensive. The use of ASICs can reduce mining expenses effectively, but it will increase the initial cost of equipment. The power consumption of an ASIC is very high compared with CPU as mentioned in section III, but its hash rate is extremely faster than CPU and GPU. The actual reason behind the value of bitcoin is these expenses, but spending too much resources for cryptocurrency creation is a side effect of blockchain. It's a question mark for IT in general and for green computing especially. The results we mentioned here are limited to standard general purpose PCs. To find the total power consumption of the blockchain network, it's beyond the scope of this paper, and we'll cover it in our future research.

REFERENCES

[1] F. Ryan, "An Analysis of the Cryptocurrency Industry," *Warton Research Scholars,* 2015.

[2] D. Chaum, "Blind Signatures for Untracable Payments," *CRYPTO,* 1982.

[3] B. Schoenmakers, "Security Aspects of the Ecash™ Payment System," in *State of the Art in Applied Cryptography*, 1997, pp. 338-352.

[4] R. L. Rivest, "Peppercoin Micropayments," in *Financial Cryptography*, 2004.

[5] C. M. Ralph, "Security, Authentication and Public Key Systems," Stanford University, Stanford, 1989.

[6] D. Cynthia and N. Moni, "Pricing via processing or combatting junk mail," *CRYPTO,* 1992.

[7] B. Adam, "Hashcash - A Denial of Service Counter-Measure," 2002.

[8] S. Tomas and T. Amnon, "Auditable, Anonymous Electronic Cash," in *CRYPTO*, Berlin Heidelberg, 1999.

[9] D. Wei, "b-money," 1998. [Online]. Available: http://www.weidai.com/bmoney.txt. [Accessed 12 10 2017].

[10] S. Nick, "Bit-Gold," 1998. [Online]. Available: https://unenumerated.blogspot.com/2005/12/bit-gold.html. [Accessed 12 10 2017].

[11] P. Hal, "Reusable Proof of Work," 2004. [Online]. Available: http://nakamotoinstitute.org/finney/rpow/. [Accessed 12 10 2017].

[12] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2009.

[13] "Cryptocurrency Market Capitalizations," coinmarketcap, [Online]. Available: https://coinmarketcap.com/. [Accessed 12 10 2017].

[14] A. C. Jerry Brito, "Bitcoin: A Premier for Policymakers," *Mercatus Center, George Mason University,* 2013.

[15] B. Joseph, M. Andrew, C. Jeremy, N. Arvind, A. K. Joshua and W. F. Edward, "SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies".

[16] "Market Capatalization," Blockchain Info, [Online]. Available: https://blockchain.info/charts/market-cap. [Accessed 10 10 2017].

[17] "Coindesk," Coindesk, [Online]. Available: https://www.coindesk.com/price/. [Accessed 10 10 2017].

[18] "Distributed Ledger Technology: Beyond Block Chain," UK Government Chief Scientifc Adviser, 2015.

[19] S. Kenji and Y. Hiroyuki, "What's so Different about Blockchain? - Blockchain is a Probabilistic State Machine - ," *IEEE Computer Society,* 2016.

[20] P. Dhiren, B. Jay and P. Vasudev, "Blockchain Exhumed," in *Asia Security and Privacy (ISEASP), ISEA*, Surat, India, 2017 .

[21] "Blockchain Info," Blockchain.com, [Online]. Available: https://blockchain.info/. [Accessed 10 11 2017].

[22] D. Cynthia and N. Moni, "Pricing via Processing or Combatting Junk Mail".

[23] B. Adam, "Hashcash," 2004. [Online]. Available: http://www.cypherspace.org/hashcash/. [Accessed 6 10 2017].

[24] J. Karl, O'Dwyer and M. David, "Bitcoin Mining and it's Energy Footprint," in *ISSC*, Limerick, 2014.