A study on the issue of blockchain's energy consumption

Eshani Ghosh[1] and Baisakhi Das[2]

Department of Information Technology, Institute of Engineering and Management,
Salt lake Eletronics Complex, Sector V, Kolkata, India,
ghosh.eshani34@gmail.com and baisakhi83@gmail.com

Abstract. Blockchain technology is one of the biggest innovative technology that has been developed and has potential usage in fields of education, business and industries. Since the creation of bitcoins, blockchain has emerged as a means for storing digital information without the intervention of any third parties. However, now it is used for various other applications than just being a simple distributed ledger. With time it has imposed a larger impact on different fields of economy and has gained popularity for its immutability. But, there are some issues faced by blockchain. One of such issues is the energy consumption. Blockchains are found to consume exorbitant amount of energy because of the algorithm followed for its creation. This paper explores the blockchain technology and the impacts of energy consumption due to the technology used.

Keywords: Blockchain, Proof of work, Energy Consumption

1 Introduction

Being an immutable distributed ledger, blockchains have gained popularity in the recent years. It was first introduced as a cryptocurrency (bitcoin) by Satoshi Nakamoto [1]. He found bitcoin to be a digital way of transacting currencies using the peer-to-peer network policy and presenting bitcoin as a highly secure system for strong transaction histories without the intervention of any third parties [3]. The technology behind the development of the bitcoin, known as blockchain, became popular and emerged as a powerful system for storing any kind of digital information [1].

The most attractive features of the blockchain is its irresistibility to any information leakage. This property is acquired from cryptographic algorithms which are used to join the blocks in the chain. Also, its peer-to-peer network communication and decentralised structure has strengthened the security. Blockchain architecture uses proof-of-work mechanism to mine a new block and stores the digital information permanently in the blockchain. The architecture of blockchain has paved the way for many applications [2]. Companies are nowadays trying to use blockchains for storing employee records, project records etc. It is also used in the medical field for storing various medical records. Its use is not only limited to this, in broader sense it can be used for implementing IoTs, storing legal information, supply chain management etc. in the near future [6]. Altogether it can be used for digitalizing the world in a protected manner.

Blockchain technology, being so advantageous, faces many challenges in its implementation. One of such challenges is the energy consumption issue. It has been found that blockchains, for enhancing its security is consuming enormous amount of energy and the root cause behind this is the proof-of-work mechanism. Proof-of-work, a mechanism to mine block, is found to consume maximum amount of energy out of the entire blockchain architecture. This is of great concern as the sources of energy are the non-renewable resources, so solving the energy consumption issue is the need of the hour for implementing blockchains. This paper discusses a survey on the blockchain architecture, the issues on energy consumption and methods to overcome the exorbitant energy consumption. Section 2 explains the blockchain architecture. The issues on energy consumption of blockchain is defined in Section 3. Section 4 explains the methods to reduce energy consumption and Section 5 concludes the paper.

2 Blockchain architecture

Blockchain architecture uses the mechanism of distributing the digital information rather than copying it. It is intended to timestamp digital documents so that it is not possible to tamper with them, whenever an information is recorded. Blockchains can be defined as a chain of blocks which can hold certain records and the blocks are linked to one another using the principles of cryptography. Each block consists of three main sections- data, hash and hash of previous block. The data that is stored depends on the type of blockchain used. For instance, if it is a cryptocurrency then it stores information about the transactions that have occurred. Hash in a block is the fingerprint and is unique to that particular block. If any changes are made to the block then the hash value also changes. So, hashes can be used to detect changes to a block. Hash of the previous block helps to create the chain and makes the system more secure as shown in Fig. 1. Block 2, contains its own hash function (2BIF) and hash of block 1 (AQCN) as the previous hash and so on and hence creates the chain of blocks. Whenever someone changes the hash value of the block then that hash value needs to be updated in the next block. The next block will have a changed hash value due to the insertion of a new previous hash value. This is how the entire chain has to be updated to change a particular block which is practically impossible and hence improves the security of the system. That is why, blockchains are more commonly known as immutable ledger because it is not possible to tamper with them.

Blockchains - An immutable ledger

As stated earlier, blockchains are distributed, decentralised and immutable ledger system. In blockchain, the blocks are connected to each other via links which are established by the hash of each block.

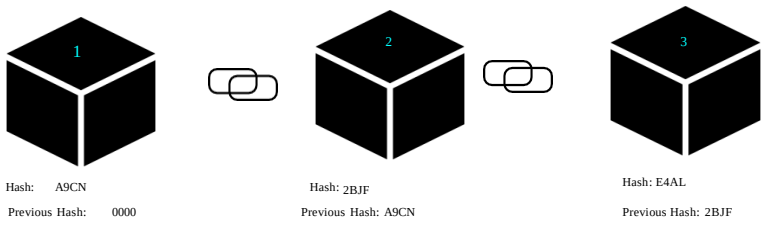

Fig. 1. Structure of Blockchain [3]

If any change is made to the block then the entire blockchain needs to be updated. So, blockchains are said to be immutable ledger. Fig. 2 explains how a digital data is certified using blockchain. The data is kept inside a blockchain and it generates a hash value for that newly added block. The data is signed by encrypting the hash value and then stamped as certified [3]. Then the verification process is done by decrypting the hash value and matching it with the one that is generated. If it matches, it means the data got verified and is authentic.

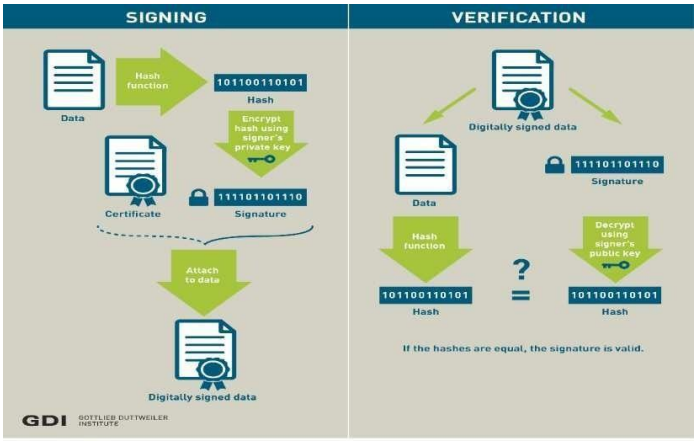

Fig. 2. Certification of digital data using blockchains [3]

Blockchain as a distributed peer-to-peer network

There can be a situation where someone tampers with a block and also updates the entire blockchain to make the changes acceptable for all the blocks. This can result in information hacking or changing or even deletion of a block. To prevent such tampering, blockchain architecture has a distributed peer to peer network system. The blockchain is not only available in one computer but it is distributed to all the computers in a network. So, any change made to the blockchain that information gets communicated to all the computers in a network. So, if a hacker changes the contents of a block and also modifies the immediately following blocks' previous hash value, then that modification is compared with blockchains in other computers in a network. If any change is detected in one blockchain then that is cancelled and the previous state of blockchain is preserved. This helps in making the system more secure. Fig. 3 shows how the peer-to-peer network is working when a transaction takes place and a new block gets added to the blockchain [4]. The block is then shared to all other computers in a network.

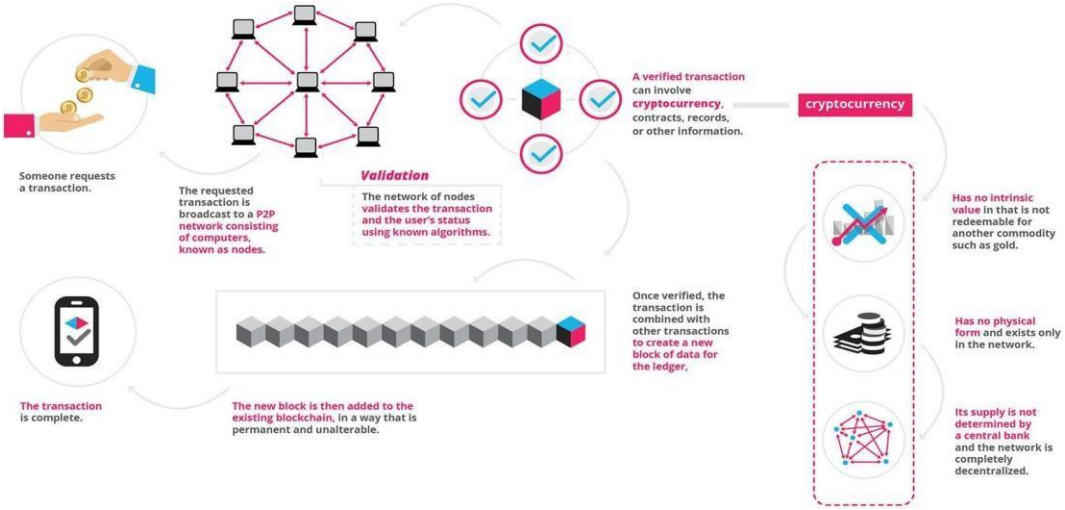

Fig. 3. A simple transaction using blockchain [4]

Proof-of-work

It is a protocol which works by asking all the nodes in the network to solve a cryptographic puzzle by using the brute force algorithm [2]. Whenever a block is to be added it should have a hash.

The hash is a 64-bit hexadecimal value which is generated using the sha256 algorithm. There is a field called nonce (number used only once) which is present in every block along with the hash, previous hash and the block number as shown in figure 4. There is a range generated within which the hash value of the block should lie. On changing the nonce value, the hash value that is generated is checked if it matches the required condition for block generation or not. This process of checking consumes energy along with that the values of hash that is generated requires long sequence of arithmetic operations that needs a lot of energy to be evaluated. Also, the values of hash abruptly change with the change in nonce and so a lot of evaluations are involved in this step. Whenever a miner solves the cryptographic puzzle (the entire process of hash generation) a new block is added to the blockchain and the block is transmitted and added to all the blockchains in the different nodes using peer-to-peer communication and this is how all blockchains get the new block added to them. But the generation of each block involves a lot of arithmetic computations which consumes a lot of energy. So, in blockchains the mining process is the root cause for the energy consumption issue behind it.

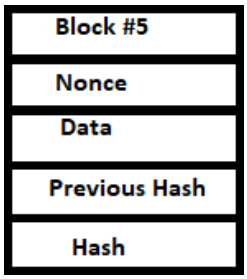

Fig. 4. Structure of a block

3 Issues on the energy consumption of blockchains

One of the major issues faced by blockchains is that it consumes exorbitant amount of energy mainly during the process of mining. The algorithm used for evaluating proof-of-work needs to be executed multiple times to match the target value and as the hash value change in a non-uniform way so it is completely based on trial and error method. For instance, in the case of bitcoin, miners take about ten minutes to mine a new block. This process has surely induced security but at the cost of enormous energy consumption.

In an article by Steven Huckle in 2016, named Socialism and Blockchain, we get an alarming information. In this article we get an estimate that bitcoin mining's annual energy consumption is 3.38 Terawatt Hours (TWH). This enormous amount of energy is equal to the total annual consumption of Jamaica in the year 2014 [21]. As stated by [17], the energy consumption of the entire bitcoin network is found to be higher than Ireland. Study says that bitcoin will use 0.5% of electricity of the world by the end of 2018, as we know that the electricity demand comes from complex computing and with days more complex puzzles need to be solved. So, this has become a threat to the environment for its enormous amount of energy consumption which in turn increase the carbon footprint [17].

The mining cost of metals like gold are very high because of its extraction and its demand in the markets. Similarly, energy cost associated with mining of blocks is high because of the Proof-Of-Work mechanism used. According to a study by Oak Ridge Institute in Cincinnati, it has been found that energy cost of mining of bitcoins is nearly 7 megajoules of energy which is equivalent to mining platinum [13]. Out of all the cryptocurrencies bitcoin consumes the maximum energy as compared with the energy equivalent to mining copper, platinum and gold and the energy cost for further mining increases over time [13]. Figure 7 shows that the cryptocurrencies mining needs more energy per dollar generated compared to mining of copper, platinum and gold.

However, the annual consumption of this currency is rising in an exponential manner, currently which has approached a colossal amount of 55 TWH. This is obviously a matter of concern. [21] discusses that between 3 m and 13 m metric tonnes of CO_2 was released in the environment due to bitcoin mining, that too only in the first half of 2018. If the utilization of bitcoin keeps on increasing, then severe consequences might be faced by the future generations. The effect of emission is such that it can contribute in an overall global temperature rise of 2 degree Celsius, as approximated by a team in Hawaii. Not only this, the global money supply in circulation is estimated as $ 11,000 billion. This will lead to corresponding energy consumption exceeding a huge amount 4000 GW [22]. This insane amount of energy is eight times the electricity consumption of France and twice the United States. The bitcoin can therefore be the burden for the climate.

Fig. 5 shows the relative energy consumption of bitcoins in different countries where the X-axis is representing the percentage that could be powered by Bitcoin and the Y-axis is showing the various countries. According to this, Czech Republic has the maximum percentage of energy consumption whereas USA has the least energy consumed by bitcoins. A statistic of 2018 [7],[3] in Table 1 shows the energy consumption of a bitcoin in terms of electricity consumed, carbon footprint and global power consumption:

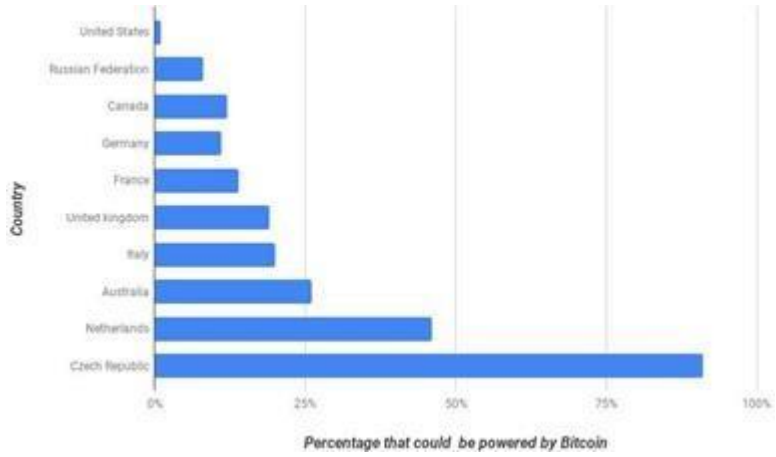

Fig. 5. Statistics of Energy Consumption of Bitcoin [3]

Table 1. Energy consumption of a Bitcoin

Description	Values
Current estimated annual electricity consumption(TWh)	73.12
Current minimum electricity consumption(TWh)	57.76
Annual carbon footprint(kt of co2)	35.830
Electricity consumed per transaction(kWh)	892
Carbon footprint per transaction(kg of co2)	437.26
Minimum global power consumption of software(TWh)	22
Peak power usage of bitcoin network(TWh)	67

The main reason for this high energy consumption is that in the process of evaluating the proof-of-work algorithm all other computers in the network are trying to find the solution. So, to solve the cryptographic puzzle all the computers are free to participate but only the one which finds the solution will be rewarded with some bitcoins. So, only one computer will come up with the actual solution and it then shares the result with all other computers in the network. This means, that energy is consumed not only by the winning computer but also by all other computers in the network who are trying to find the solution. This process of finding the solution actually uses a lot of energy to repeatedly change and find a nonce value that matches the target. From the environmental point of view a large source of electricity generation are the non-renewable sources of energy which are responsible for increasing the carbon footprint. It has also been found that blockchains use energy that is approximately equal to the energy consumption of a nation annually, because of this process of mining. According to [16], it has been found that a dishwasher energy consumption for a year is equivalent to the energy consumed by bitcoin network per transaction.

Table 2. Bitcoin Mining Hardware

Name	Power efficiency (W/Gh)
AntMinerS7	0.25
AntMiner S8	0.98
AntMiner S8	0.98
Avalon6	0.29
Antminer V2	1.0
BPMC Red Fury USB	0.96
Gekko Science	0.33

Bitcoins are mined using special mining hardware which were designed and improved over time to reduce their energy consumption. Earlier CPUs were used to mine blocks which were slow and used more power. So, GPUs are used now, which calculates nearly 100 times faster than possible with a CPU and also uses less energy comparatively. This was further improved by the arrival of Application Specific Integrated Circuit (ASIC) which is faster and consumes less power than FPGA, CPU or GPU [19]. Table 6 shows the different bitcoin mining hardware and the corresponding power efficiency. Figure 6 gives a comparison among the different mining hardware on the basis of power efficiency.

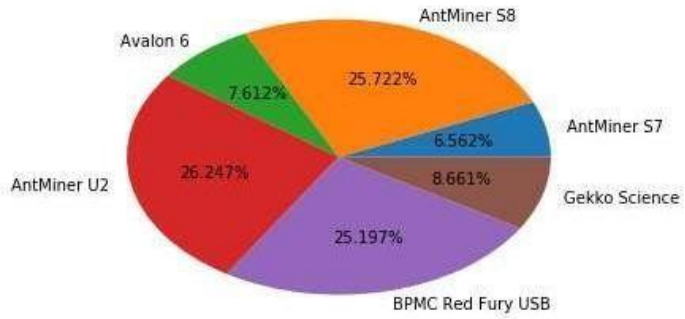

Fig. 6. Comparison of power efficiency of mining hardware

Fig. 8 diplays one of the world's largest bitcoin mines which is located in the industrial park of SanShangLiang, the outskirts of Ordos city, Mongolia. It is around 400 miles from Beijing, capital of China. As bitcoin mining consumes huge enormous amounts of electricity, so miners found locations that offer cheap energy. Founded in 2014, Ordos mine is China's oldest large-scale bitcoin mining facility. It was acquired by Bitmain in 2015. It is powered by electricity mostly from coal-fired power plants. Its daily electricity bill amounts to 39,000 USD [20].

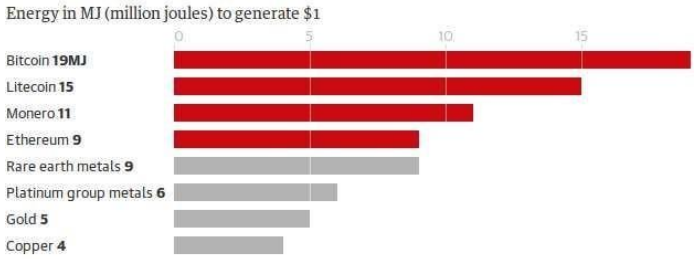

Fig. 7. Comparison chart of different energy consumption [13]

Fig. 8. Bitcoin mining machine [20]

4 Methods to reduce energy consumption in blockchain

One way of reducing the energy consumption is by lightning network, where the transactions occurs off-chain by positioning channels between the users and permitting the transactions to be recorded on closing of the channels [8]. It is used for fast transactions among the parties by directly setting up channels across them. In this network, channels will be setup between users and thus the transaction will only be recorded on the blockchain when the channel is closed. But this would not lead to efficient solution for reducing energy consumption as very small amount of energy is used by the nodes to record transactions. The scheme was proposed by Thaddeus Dryja and Joseph Poon in 2015 [12]. Here, a user-initiated channel is designed which permits dealing with transactions without the engagement of any third parties. Information is stored only when the channels are closed. It is not stored on open state. Two parties are provided with a wallet differently (displaying the amount of bitcoin) on start of the transaction. First the address of the wallet is saved and then the virtual channel of the two parties are stored in blockchain. Every transaction is updated only when the whole transaction is done or completed [12]. This has minimized the energy consumption per transaction and hence consumes much less energy. Though a bit of energy has been reduced by faster transactions using lightning network method but the huge energy consumption for mining could not be minimized by this method. So, instead of using proof-of-work mechanism another algorithm called proof-of-stake can be used. PoS uses economic game theory in order to maintain network consensus. In this system, the network validators must deposit and lock-up or stake the coins to the network. In case of any fake transaction or any unfair means, the staked coins will be lost entirely. In PoS ,the amount of coins staked ,along with the amount of time, the coins that have been staked in the network will work as the parameters for choosing which validator will likely to be given chance to validate the next block of transactions. The validator will earn additional coins as a reward for its validation work. Thus PoS becomes an energy-saving alternative of PoW and this is the reason why bitcoin Oils Pos- based technology will be much more beneficial as compared with bitcoins current PoW model.

Proof-of-stake

This protocol uses less computations and can be used for Ethereum and certain altcoins [2]. It was first implemented in a cryptocurrency named Peercoin [5]. According to this protocol, the creator of the next block is chosen randomly on the basis of wealth or age [6]. This means that miners with large amount of digital currencies can add a new block to the blockchain. In this case, not all computers are allowed to participate in the mining process instead only one computer is participating in the mining process. This saves

the power that all the computers in a network waste searching for the solution in proof-of-work algorithm and cuts down the cost of mining by 99% [9]. So, proof-of-stake proves to be more energy efficient and cost effective than proof-of-work algorithm and this reduces the need to release too many coins for keeping the miners motivated [5].

A modification of this protocol is the Delegated Proof-of-Stake protocol commonly known as DPos. Unlike the Proof-of-Stake protocol where a user put his coins on stake for acquiring the right to validate a transaction, DPos protocol allows users to vote a witness and the witness who gets maximum vote will get the right to validate a transaction. This protocol is also found to consume less energy as compared to Proof-of-Work and is also better than Proof-of-Stake [18].

Protocol	Characteristics
Proof-of-Work(PoW)	1.All users participate 2.More energy consumption 3.Slower than PoS
Proof-of-Stake(PoS)	1.User having more wealth participate 2.Less Energy consumption 3.Faster than PoW
Delegated Proof-of-Stake(DPoS)	1.Few users participate 2.Less energy consumption than PoW 3.Faster than Pos and Pow

Table 3: Comparison of mining protocols

Proof-of-Authority

In Proof-of-Authority protocol, there is a small group of people who validate the transactions and put their reputations at stake for validating a transaction. This protocol is found to be fast for doing computations with very less consumption of energy compared to Proof-of-Work [24].

Comparatively, it can be seen that Proof-of-Work uses the maximum energy. So, switching to other protocols like Proof-of-Stake or DPos or Proof-of-Authority can help in reducing the energy consumption for validating blocks or transactions.

Renewable sources of power generation

In reality, the best solution for getting rid of such energy consumption problem is using renewable energy for mining of crypto currencies. Inner Mongolia, which is one of the main places associated with bitcoin mining, uses coal power for the mining procedure and currently more than 70% of bitcoin mining is done there only [23]. This inevitably leads to global warming along with pollution of nature. Countries like Iceland and Norway produce more than 90% of their energy from renewable resources. If mining is located in such countries, then making use of renewable resources will be much easier because they have plenty of these resources [23].

As blockchains uses enormous amount of energy so, instead of using the non- renewable sources of energy, the renewable sources of energy can be preferred for production of power. Renewable sources of energy are found to cause less pollution and will not increase the carbon footprint. Renewable sources of energy include solar, wind, water etc. Companies like IBM and Intel are preferring green blockchains for the transaction process [10]. Also, blockchains can themselves provide the solution for power generation. Decentralisation of power is the first step towards it. Power will be generated by small communities using wind or solar energy [10]. That means, the world of passive energy consumers is getting replaced by new consumers who are not only buying power but also selling it. Then comes, the use of blockchains. Blockchains will create peer-to-peer communications among the different consumers of power. This entire setup is known as microgrid [11]. Here the consumers will pay using blockchains and they have to pay each other for generating power. Using blockchains, power will flow from those producing in surplus quantities to those who are in need of power without any human intervention. This is how green blockchains can be used with decentralisation of power that is renewable [11]. One of such microgrids is set up in Switzerland that is named as MyBit. It is a decentralised energy grid. It uses Iot, artificial intelligence and solar energy and have combined the three to become a source of energy [14]. In UK, a startup named as Electron has been set up that uses blockchain technology for energy trading [14]. The main idea behind switching to green blockchains is promoting sustainable development which means that apart from meeting the needs of the present generation we need to think about the future generation.

Reducing the energy consumption of the blockchains is the need of the hour. If these challenges can be overcome then blockchains will become the best option for the future world. ” If blockchain could provide an accounting system, it could turn the national grid from being the enemy of microgrids to being their friend”-Philip Sandwell, Imperial College London [15].

5 Conclusion

Blockchains are designed to provide security to all types of data so that no one can tamper with them. But also, at the same time they are found to be consuming enormous amount of energy. So, various organisations and companies are trying to find the solution for solving the energy issues of blockchains and at the same time they are trying to switch to renewable sources of energy for sustainable development and for reducing any environmental hazard that is associated with the use of blockchains. Blockchains are very useful if implemented, but to use it in every fields of the economy the workers and the employees need to be given proper knowledge of these blockchains. So, education is the main factor for the implementation of the blockchains.

References

1. Bitcoin: A peer-to-peer electronic cash system by Satoshi Nakamoto. Available online: https://bitcoin.org/bitcoin.pdf
2. Blockchain and its applications: A detailed survey by Supriya Thakur Aras and Vrushali Kulkarni, International Journal of Computer Applications (0975-8887); Dec 2017.
3. Alex de Vries; Bitcoin Energy consumption Index. Digiconomist. 2014. Available Online: https://digiconomist.net/bitcoin-energy-consumption.

4. Ian Khan; What is Blockchain technology? A step-by-step guide for beginners. Blockgeeks; 2016. Available Online: https://blockgeeks.com/guides/what-is-blockchain-technology
5. Lisk Academy; Proof of Stake. Lisk; 2018. Available online: https://lisk.io/academy/blockchain-basics/how-does-blockchain-work/proof-of-stake
6. Blockchain challenges and opportunities: A survey by Zibin Zheng, Shaoan Xie, Hong-Ning Dai, Xiangping Chen and Huaimin Wang. 2018
7. Alex de Vries, Bitcoin Energy Consumption Index. Digiconomist. 2014. Available online: https://digiconomist.net/bitcoin-energy-consumption
8. Tom Copeland; How will Bitcoin solve its energy consumption problem? Newsbtc; 21 May 2018. Available online : https://www.newsbtc.com/2018/05/21/will-bitcoin- solve-energy-consumption-problem
9. Proof-of-Stake. Wikipedia; Available online: https://en.wikipedia.org/wiki/Proof-of-stake
10. Helen Zhao; Bitcoin and Blockchain consume an exorbitant amount of energy, Feb 2018. Available online: https://www.cnbc.com/2018/02/23/bitcoin- blockchain-consumes-a-lot-of-energy-engineers-changing-that.html
11. Maher Chebbo; Powering a sustainable future: How blockchain can solve bitcoins energy consumption crisis. Itproportal; 01 June 2018. Available On- line : https://www.itproportal.com/features/powering-a-sustainable-future-how-blockchain-can-solve-bitcoins-energy-consumption-crisis
12. Neolle Acheson; What is Bitcoins lightning network; Coindes; 21 March 2018. Available Online: https://www.coindesk.com/information/what-is-the-lightning-network.
13. Alex Hern;Energy cost of mining more than twice that of copper or gold.TheGuardian;5Nov2018.Availableonline: https://www.theguardian.com/technology/2018/nov/05/energy-cost-of-mining-bitcoin-more-than-twice-that-of-copper-or-gold.
14. Shermin Voshmgir; Blockchain and Sustainability. Medium; 11 Aug 2018.
15. Chris Baraniuk; Microgrids and the Blockchain are powering our energy future. Wired; 12 Oct 2017. Available online: https://www.wired.co.uk/article/microgrids-wired-energy.
16. Demiro Massessi; Public Vs Private Blockchain in a nutshell. Medium. 12 Dec 2018. Available online : https://medium.com/coinmonks/public-vs-private-blockchain-in- a-nutshell-c9fe284fa39f.
17. AlexHern; Bitcoin mining consumes more electricity a year than Ireland. 27 Nov 2017. Available online: https://www.theguardian.com/technology/2017/nov/27/bitcoin-mining-consumes- electricity-ireland
18. Shaan Ray; What is Delegated Proof-of-Stake, 15 April 2018 . Available Online: https://hackernoon.com/what-is-delegated-proof-of-stake-897a2f0558f9
19. Bitcoinmining. 2010. Available online: https://www.bitcoinmining.com
20. Joon Ian Wong and Johnny Simon, Photos: Inside one of the world's largest bitcoin mines. 18 Aug 2017. Available online: https://qz.com/1055126/photos- china-has-one-of-worlds-largest-bitcoin-mines
21. Steven Huckle; Bitcoins energy consumption is a concern but it may be a price worth paying; 7 Nov 2018. Available Online: http://theconversation.com/bitcoins-high-energy-consumption-is-a-concern-but-it-may-be-a-price-worth-paying-106282
22. Fabrico Flipo; The bitcoin and blockchain: energy hogs. 17 May 2017. Available online: https://theconversation.com/the-bitcoin-and-blockchain-energy-hogs-77761
23. Quora; Is Bitcoins energy consumption a problem for the world?2018.Available Online: https://www.quora.com
24. Kayla Matthews; 4 ways to counter blockchain's energy consumption pitfall; 18 April 2019. Available online: https://www.greenbiz.com/article/4-ways-counter-blockchains-energy-consumption-pitfall.