Journal of Green Energy Research and Innovation

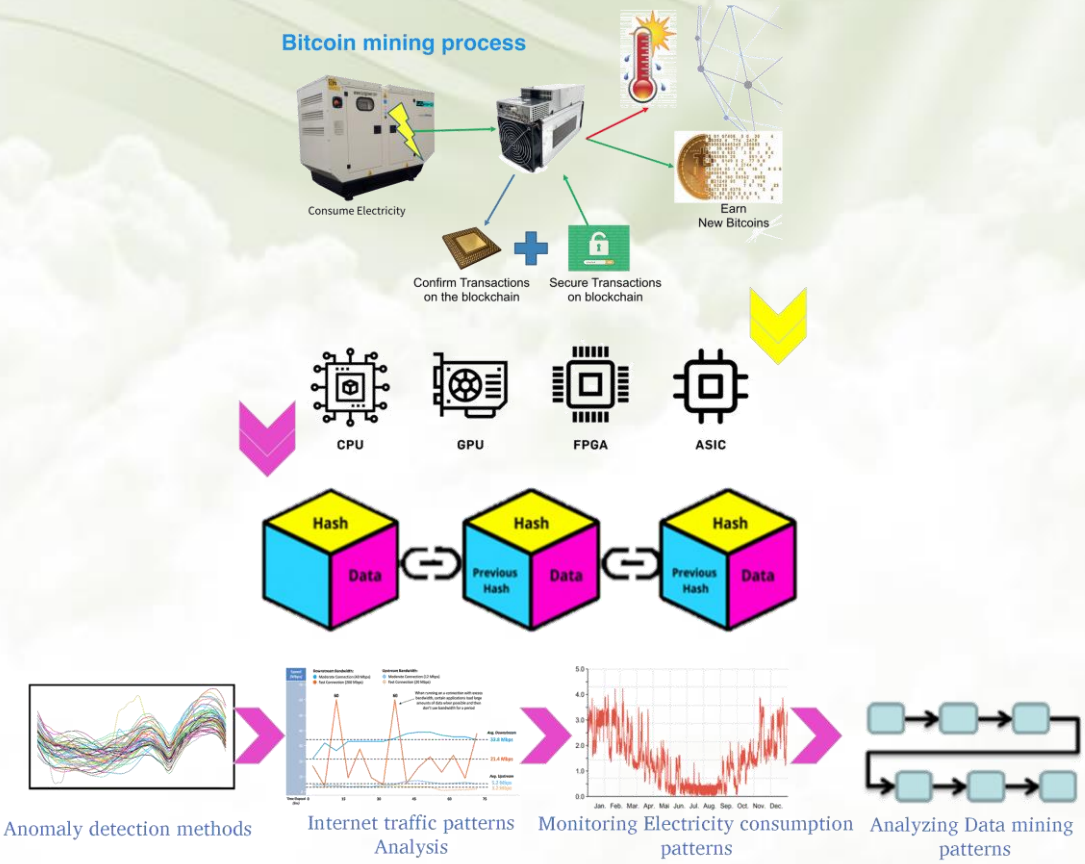
A Survey of Different Methods for Miner Detection and Challenges of Them in Power Industries

Mohammad Hossein Shakoor

Highlight

- **Some aspects of Mining, blockchain, Hash, Cryptocurrency, Encryption and Decryption**
- **A comprehensive study on different methods of miner detection**
- **Some suggestions to enhance the power electricity consumption**

Graphical Abstract



Use your device to scan and read the article online

Citation

M. H. Shakoor, " A Survey of Different Methods for Miner Detection and Challenges of Them in Power Industries," *Journal of Green Energy Research and Innovation*, vol. 1, no. 3, pp. 96-109, 2024.

https://doi.org/10.61186/jgeri.1.3.96

Online ISSN: 3041-9018

Journal of Green Energy Research and Innovation

Journal Homepage: www.jgeri.araku.ac.ir

A Survey of Different Methods for Miner Detection and Challenges of Them in Power Industries

Mohammad Hossein Shakoor *

Department of Computer Engineering, Faculty of Engineering, Arak University, Arak, 38156-8-8349, Iran.

* ***Corresponding Author:*** *mh-shakoor@araku.ac.ir*

ARTICLE INFO

Keywords:
Power consumption,
Cryptocurrency mining,
Miner detection.

Article history:
Received: 20 January 2024;
Revised: 20 February 2024;
Accepted: 2 March 2024;

Article type:
Review Article

ABSTRACT

Cryptocurrency mining requires high consumption power. In recent years, because of the increase in the price of cryptocurrencies and due to the cheap price of electricity in Iran, mining Bitcoin and other cryptocurrencies has been very profitable. Some miners are legally engaged in cryptocurrency mining, but many miners do it illegally and without permission. Since cryptocurrency mining is an operation that consumes a lot of electricity, it is one of the reasons for the lack of electricity, especially in the summer season, and it has caused power outages and financial losses to various industries. In this paper, different methods of detection of illegal mining are reviewed. In this research, by collecting the small number of researches done in the world, a comprehensive study of this issue has been tried. The methods of identifying miners and related consumers are divided into several different categories. Some of them are based-on data mining and mostly to identify consumers who use the output of the converter for the miner device. The second category is related to people who illegally get their electricity from behind the meter or unmetered branches, which are much more difficult to identify than the first type. These methods will be mentioned more in this article. Finally, some suggestions are provided for better identification of these consumers. Furthermore, at the end of the paper, some renewable and new sources of electrical power are discussed for using as an electricity power for miners instead of traditional fossil fuel and gas planes.

1. Introduction

More than a decade has passed since the introduce of digital currencies or cryptocurrencies. Although this innovation has important advantages and capabilities, some of them have also led to some challenges, the most important of which is the increase in electricity consumption, especially in low-price countries, where compared to the rest of the world, the price of electricity for consumers is very low. Because of this reason, cryptocurrency mining is very cost-effective. It requires a lot of power energy and it increases electricity consumption in our country significantly. Therefore, it seems necessary to conduct research in order to detect illegal miners. The first article related to

Bitcoin was published in 2008 by the pseudonym Satoshi Nakamura [1]. In the past decade, although cryptocurrency mining machines have made many improvements in terms of power consumption, they still belong to the high-consumption systems. Cryptocurrency mining imposes a lot of consumption on the power network [2]. According to reports in 2013, every day one billion watt per hours of electricity is spent for Bitcoin mining [3]. That is about the electricity consumption of 30,000 American households. This year, the mining speed was around 60 tera hash per second. With the advancement of technology, not only the hash speed is increased, but also the power consumption of miners decreased drastically. However, by increasing the number of miners, the problem of high-power consumption still remains.

According to research, about 0.55% of the world's electricity is consumed in the digital currency industry [4]. According to statistics, about 5% of the total Bitcoin mining was done in Iran in April 2021. Which more percentage of it is illegal. Miner detection is done for two reasons. The first reason is to identify delinquent consumers in electricity consumption, and the other reason is to identify the location of hidden miners that are robbed. This article is more about the first goal. But the stated methods can also be used for the second purpose. Identification of illegal consumers of cryptocurrency mining is a type of anomaly detection in electricity consumption [5]. The conventional method of identifying consumption anomalies is to compare the consumption of each user with his consumption at similar times in the past [6]. Of course, this method cannot be used for consumers who use unauthorized branches. Some articles [7] have presented methods based on game theory, in which by placing a series of hardware in the distribution network, it is possible to monitor and examine the amount of consumption in different parts and identify significant changes in consumption.

Since this method requires special hardware, it cannot be used everywhere. Rahimi et al. [8] presented a method based on statistics and with artificial intelligence tools, which is based-on a smart network. In this method, sudden changes in consumption are detected first, then users are divided by clustering and high consumption consumers are identified. Some researchers identify mining farms by using the analysis of electricity current characteristics such as current harmonics or identifying specific noises created by cryptocurrency mining power supply devices [6]. This method is also not very effective because there are various devices whose current harmonics or their produced noises are similar to miners and actually make it very difficult to detect a miner. Some methods use clustering to predict the amount of consumption in the next hour and identify any excessive consumption [9]. It is presented in a method based on time series analysis [10], in which the amount of monitor consumption and abnormal consumption is detected using Internet of Things tools. It is presented in a method for detecting abnormality of consumption, which has divided the data into three categories of consumption on working days, holidays and abnormal consumption. After detection of unusual uses, they are again divided into three categories, one of which is miners [11].

Data analysis through different protocols such as NetFlow and IPFIX and data mining and statistical analysis is another way to identify miners [12,13]. An example of these

supervised learning processes in machine learning is the method presented by some papers [14]. In this method, the important discriminative features are extracted from the data flow and the data flow classification operation is performed. In some articles [15], they identify the communication flows between miners and mining pools by analyzing the packets of the Internet network and according to the IP address and MAC address. In this work, packets that have a series of special features and use protocols of miners are detected as suspicious data for extraction. Then, by using the active method and communication with the sender of these packets, it is possible to find out their connection with the miners. Some researches have comprehensively analyzed Bitcoin mining theoretically [3]. Some papers [16,17] have investigated various economic aspects of cryptocurrency mining and analyzed it based-on game analyzing. A lot of research has been done in connection with activities and unauthorized users of cryptocurrencies [18]. Some of these unauthorized activities are private-key theft, spam and malwares. Huang et al. [19] have presented a comprehensive study of cryptocurrency mining malware. Some researchers developed methods that associate the mining bot with its mining pool. In addition, some methods have been able to estimate the number of infected devices produced, identify the income and the duration of infection with mining malware [20].

In this paper, firstly, some important concepts of cryptocurrencies and their extraction are explained. Then the common illegal methods of extracting cryptocurrencies are reviewed. The methods of bypassing the identification of miners are also described briefly, and in the main part, various methods for the detection of miners will be discussed. At the end of the paper, some renewable energy sources are illustrated that are explored for electricity production as a sustainable and eco-friendly alternative to traditional fossil fuels [21].

2. Related Concepts

In this section, some contents related to cryptocurrencies and their mining are explained.

2.1. Encryption and Hash

The main basis of cryptocurrencies is digital encryption. In general, cryptography is divided into several different categories. Key-based encryption includes symmetric and asymmetric encryption [22]. The difference between these two methods is in their key. In symmetric methods, encryption and decryption operations use the same key. The important feature of these methods is their very high speed, and these methods are used for high volume data. An example of this method is MD5. The major disadvantage of these methods is that if the key is leaked during transmission, the entire encrypted data will be revealed. On the other hand, asymmetric methods include methods where the encryption key is different from the decryption key. That is, we encrypt with one key (public key), but the decryption is done with another key (private key). Naturally, in this type of method, revealing the public key does not cause much problem, and the important thing is the private key. Since in these methods, key transfer is not done like in symmetrical methods,

the risk of key leakage is also eliminated. The most famous of these methods can be called RSA and El-Jamal [22]. These methods are mostly used to transfer very important and short data (such as data containing a symmetric encryption key)

There is another type of encryption that is not based on a key. Hashing is one of these methods. In hash operation, the input data of any size (naturally, there are limits to the data length) is entered into the algorithm and the encrypted data is output as a block with a specific length [22]. This operation is not reversible. The output block is the same input data that has been changed with operations such as shift, addition, division and logic. These methods have high speed, but their most important disadvantage is collision. Collision means that the algorithm takes two different data inputs, but a same output block is produced for them. In fact, when the collision occurs, the algorithm will lose its credibility. A famous example of these methods is SHA, which started with SHA-1 and now SHA-256 is used as an encryption method in Bitcoin and many cryptocurrencies. In fact, Bitcoin mining machines are always running SHA-256.

2.2. SHA-256

In encryption, data is converted into a secure format that cannot be read unless you have the key. In encryption, data may be unbounded, but in hashing, data of arbitrary size is converted to fixed-size data. In SHA-256 hash, a 512-bit data string is converted into a 256-bit string. In hash encryption, the hash data is encrypted in such a way that it is not reversible. For this reason, it is almost impossible to convert the mentioned 256-bit hash to its original 512-bit form. The Bitcoin encryption algorithm is SHA-256, which is an extended version of SHA-1,2. What each miner executes billions of times per second is the hashing algorithms and the speed of each miner is determined by the number of hashes per second. SHA-2 is shown in the Figure 1. This algorithm is a combination of logical relations of shift, inflectional combination (and), exclusive arc, exponentiation and contradiction.

2.3. Transaction and Blockchain

A digital coin is a chain of digital signatures of previous owners. Anyone who sells it, with a digital signature on the hash of previous transactions and the public key of the next owner, it transfers it and adds this signature to the end of the chain of previous signatures. In the Figure 2, person #1 hashes the public key of person 2 with the chain of previous transactions and then digitally signs it and transfers it to person 2.

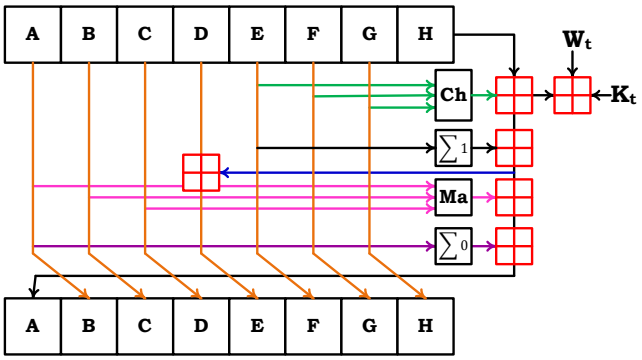


Figure1. Hashing diagram of SHA-2.

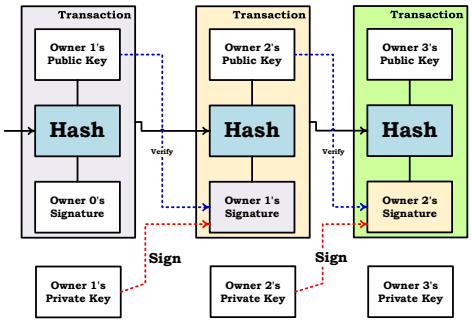


Figure2. Chain of blocks in a blockchain.

For person 2, during the digital signature, the previous chain must be confirmed, while with the private key, he can access his coin and sell it. The problem is that the buyer cannot understand whether the seller is selling for the first time or not. One solution is to have a verification center that works with centralized reason and has all the problems of centralized systems. In fact, by surveying the majority of nodes (miners), the buyer can be informed that the seller will not sell the coin a second time. The solution is to use the time constant as a distributed time server, whose job is to perform the time constant of each block and hashing with the previous blocks. To implement a distributed time server, you must use the work confirmation method. The hash starts with zero bits, the more the number of zeros, the average processing tasks increases exponentially. The difficulty of the work is determined based on the average output of the hash, when the speed increases, the difficulty of the work increases.

2.4. Miners

The operation of confirming the transaction by the miners, which leads to a reward for them, is called the mining operation. As mentioned before, miners perform hash operations many times every second. Four generations of Bitcoin miners have been made, and recently the fifth generation of them, which have more speed and less power consumption, has been presented. Bitcoin mining has been done in five generations by different hardware [3]. In the first generation of this hardware, the main processor i.e., CPU was used. The second generation of miners used graphics processors or GPUs. The third generation of miners used FPGA for mining. ASIC circuits are used in the fourth and fifth generation of cryptocurrency miners. The circuit of this type of miner is designed in such a way that they only implement the hash algorithm and cannot be used in other processing applications. Table 1 compares these different generations.

Table 1. Comparison of different generations of miners in terms of speed and power consumption.

Miner Generation	Hardware	Speed (Hash)	Power Consumption per GH/Sec
1	CPU	1 to 5 MH/Sec	4000 W
2	GPU	0.33 GH/Sec	210 W
3	FPGA	100 to 500 MH/Sec	50 W
4	ASIC	10 to 30 TH/Sec	0.35 W
5	ASIC	70 to 112 TH/Sec	0.0295 W

3. Detection Methods of Mining

The most common illegal methods for mining can be divided into several types. Which are mentioned below.

- Unauthorized branching of the meter
- Using a power distribution system without meter
- Abuse of manufactories with agricultural and industrial electricity
- Using power to extract currency instead of using it for licensed applications
- Branching from remote lines
- Crypto jacking: Using the processor of users when they work with popular sites and software

The main discussion of this paper is to review the methods of miner detection. Here, various methods of miner detection are discussed.

- Statistical processing of meter consumption
- Data mining and processing of meter parameters
- Consumption processing with anomaly detection methods
- Tracking the electricity leakage in a group of consumers
- Analysis of parameters of power distribution lines
- Tracking through the Internet addresses and profiles (Mac, IP, wallet)
- Analysis and tracking of data flows on the Internet
- Sound and heat tracking
- Antiviruses

In the following section, each of these methods is explained.

3.1. Statistical processing of meter consumption

Most of the ordinary consumers and people use the miner for the first time. They use home branches and only one miner device. It is not difficult to identify these consumers according to the changes in their consumption compared to the same period of the previous year, and it is easy to identify the consumers who use meter branches to extract cryptocurrency. The main problem of this method is that many illegal electricity consumers use the branches that bypass the meter. Therefore, it is difficult to identify them by statistical processing of meter [6]. Also, some other illegal consumers use electricity to extract cryptocurrency instead of their authorized applications, such as in industry or agriculture. Therefore, there is no significant statistical change in their consumption. For example, they remove some parts of their production lines that are less economical than mining and use miners on holidays.

3.2. Data mining and processing of meter parameters

In some paper [6] by using data mining and analysis of the parameters measured by the meter, it is possible to trace electricity consumers with miners. This method, like the previous method, is used to identify people who use meter branches to consume the electricity of their miners. One of the limitations of this method is that the meter must be intelligent in order to measure some different parameters of the distribution network. In some of the few researches, the analysis and data mining of parameters of meter is employed for miner detection [5]. For this purpose first, a repeating patterns are

identified, then learning operations are performed with the decision tree to distinguish between miners and non-miners. In this method, firstly, according to the noticeable changes in consumption compared to similar times, the relevant consumer is selected. Then, by processing the parameters measured by the meter, the validity of the miner is confirmed or rejected. Various parameters and characteristics are checked to detect whether the consumer is a miner. For example in the article [5], parameters such as date and time, Power, Cos(Fi), Cos(Fi) L1, L2, L3, Voltage L1, L2, L3 and Reactive Power is used for detection. The main challenge of this method is related to the high false positive error rate. It is because of the similarity of network parameters of miners and some other devices such as water pumps or even electric heaters. Most of these devices are detected instead of miners and the positive detection error increases.

3.3. Anomaly detection methods

Some methods used the abnormalities in consumption for miner detection. Cryptocurrency miners are abnormal and they are distanced among other electricity consumers. These consumers are tracked by data mining and anomaly detection approaches [11]. In this state, consumers are divided into three categories of consumption on working days, holidays and unusual consumption based on consumption time. Then the unusual consumers are again divided into three other categories, one of them is miners. Some other methods [23] have been presented anomaly detection of consumption based-on cloud processing, but they use only for detection of high-consumption customers and not only cryptocurrency miners

3.4. Miner detection based-on reference points

One of the methods of detecting unusual consumers among a set of electricity consumers is based-on batch monitoring [7]. In these methods, consumers are divided into several groups, usually based on geographic location. Then, the main electricity distribution line of that area is monitored with a reference meter, and the total consumption of that area is stored in memory by the meter at certain time. The same work is done by the smart meters of each consumer, at the certain time. For example, every hour, the consumption value of the meter is stored. Then this information is read and analyzed from the consumers' meters and the reference meter. Naturally, the consumption value measured by the reference meter has a difference to summation of the all consumption in the network. It is because of the loss energy in the network. If this difference is greater than a certain limit, it means that there is an unauthorized branching in that area without a meter. The most important challenge for this method is related to all consumers. All of them must have a smart meter. In addition, the hours of the meters must be accurate.

3.5. Analyzing the parameters of power

Some techniques, proposed methods for analyzing the parameters of power lines. These methods are based-on the measurement of power harmonics in the power distribution network [6]. These approaches often have a false positive error. It is because

some high consumption devices have behavior similar to miners in the distribution network. They increase the false positive error of miner detection. In addition, in a distribution power network, most of these parameters are merged together and they do not provide discriminative features. One of the important challenges of this method is the need to have hardware measuring for all consumers to measure these parameters.

3.6. Detection based-on Internet addresses and profiles (Mac, IP, and wallet)

Most of the miners have to use a wallet or mining pool to store or sell their cryptocurrencies. One of the traditional methods for miner detection is based-on the tracking the address of wallets or mining pools in the Internet. Today this method usually is not used. It is because miners use anti-tracking techniques. Some methods use traffic control for detection. They monitor and control the packets that have the same keys. That means, for example, the source and destination IP address, port, and protocol are the same [24]. By monitoring the network, it is possible to identify active miners connected to the pool by analyzing the address. In the flowing discussion of this part, each type of this method is explained. (i.e., identification based on MAC address, IP address and wallet address).

3.6.1. Miner Detection based-on MAC address

Mines, like any other device that connects to the Internet, have two identification addresses, IP address and MAC address. Normally, MAC addresses are fixed and stored in the ROM. Therefore, changing their address is difficult. One of the methods of miner detection is based-on the MAC address. Recently, most ASIC devices have been used for Bitcoin mining. However, GPU rigs are often used for Ethereum. Miners have a specific MAC address range. It is easier to detect some second-hand miners than new ones. Because they have been used before and many of their traces, including their MAC address, have been recorded in some places such as mining pools. This is a traditional method to track mostly mobile phones and their network standards. Because mobile phone can connect to the network without router. It is hard to use this technique for miner devices, because most miner devices are connected to the network with an intermediary, such as a router, and it makes hard to track it by its address [15]. All in all, the use of routers by users makes it difficult to identify a miner by MAC address. Most of the new routers have a section called Mac clone, which it can be covered any desired MAC address for the router, and this MAC address is visible in the WAN network and can filter. Besides, there are other ways to bypass miner identification using a MAC address. One of these methods is to use a VPN with a fixed server address.

3.6.2. Miner Detection based-on IP address

Each device used a temporary address to connect to the Internet. This address is called IP for identification in the network. This address can be changed every time the device is connected to the Internet. Since miner devices are permanently connected to the Internet, this address usually remains constant, unlike most common devices, the IP address of the device is fixed for a long time. Because the IP changes in a mining pool can disrupt the

mining process [15]. There are different ways to prevent the miner detection by IP address. To prevent the miner from being identified by the IP address, users usually use VPNs with a fixed address or VPS. Miner usually cannot register VPN settings on itself. To solve this problem, the purchased VPN must be set on a modem or router. Since the stability of the Internet connection is very important in mining, it is more appropriate to use a router because it allows the user to define two separate Internet connections for it. If one of its accesses is interrupted or disturbed, the network automatically uses an alternative Internet connection. If a large number of miners are used, a switch must be used to connect all of them to the router.

3.6.3. Miner detection based-on wallet address

In the process of mining, the wallet address must be connected to the mining pool to deposit currency to the wallet. The request the cash from the miming pools is done in three ways: automatically based on a time period, reaches the value to a certain level, and by a manual request of user. Therefore, connecting to the mining pool to pay or receive is necessary and must be done through the connection. Internal users usually use an IP address that does not belong to their countries and they usually use the Internet connected to their mining rig by using a VPN with a fixed server address. If this is not possible, they use VPN individually and then enter their panel in the mining pool. Therefore, IP identification with this method, i.e., wallet, is very difficult. Another method of detection that is related to wallet address is used in local digital exchanges. It is intercepted and determined whether the input of digital currency is through mining. This method can be bypassed. Users almost use an interface to transfer their currency of wallet to local exchanges. Usually, users use an intermediary address such as the address of their Trust wallet and first transfer the currency to this address and then deposit it to the local exchange. Therefore, it makes more difficult to detect miner by wallet address [3].

3.7. Analyzing and tracking the data flows on the Internet

One method to miner detection is related to data processing and data streams in the Internet. Different clustering and classification methods are usually used for this purpose. Among the few comprehensive researches, it can be mentioned in the research article [15] in which a very large amount of data streams are used in the Internet. An example of this research was conducted in the Czech Republic. It is the most complete article ever published in this field. In this article, among the 3.6 billion internet data streams, which includes 27.8 billion packets and a volume of nearly 100 terabytes of data, a small number of data have been selected. This selected data includes 16 million streams containing 117 million packets in 54 GB format. Therefore, in most cases, it is impossible to prepare and process such a heavy volume of data. For this reason, we have to go to the information that has been filtered and reduced.

3.8. Sound and heat detection

One of the basic methods of miner detection is the methods based-on sound and heat. Cryptocurrency mining systems generate a lot of heat due to high power consumption and

heavy processing. This heat can be detected with heat detection devices. Furthermore, to cool the miners, ventilation and powerful cooling systems must be used, which produces sound. They can be detected by sound detection. Nowadays most of the modern cryptocurrency mining systems can mine by low noise of sound and with proper ventilation systems. Therefore, this method often fails due to the presence of new mining systems [3].

3.9. Antiviruses to detect malware

In some cases, illegal malwares attempt to extract currency by installing them on computer systems without the permission of the user [25]. It is names as cryptojacking. This challenge is different from the previous challenges and the problem of detection of electricity consumers is not raised in it, but this method is in the form of malware detection. It is the software added to the browser as an extension or intentionally placed inside the website by the designer of that website and uses the processing power of users illegally. This method is known as cryptographic attack or cryptojacking. The corresponding malware code connects the mining bot to the mining pool. Comprehensive research has been done on the malware associated with this type of illegal activity and the number of infected devices has been estimated. The methods for estimating the income and duration of infection with mining malware have also been stated [20].

These unauthorized activities can only be done for some sites that have many users that they are active on the site for a long time. These malwares can be detected by installing updated antiviruses. As it is mentioned before, some of them are not malware, but the site designer put them on the site page to use the user's processor. An example of this code is the CoinHiv Java library in web pages, which is used to mine Monero currency by the processors of site users. Table 2 shows the summarization of all of miner detection methods and their challenges that explained in this section.

Table 2. List of different methods for miner detection and their challenges.

Row	Reference	Miner Detection Method	Challenges
1	[6]	Statistical processing of meter consumption	Require a smart meter, cannot used for illegal branches
2	[5,6]	Data mining and processing of meter parameters	Require smart meter, cannot used for illegal branches
3	[11,21]	Anomaly detection methods	Can be misleading by users
4	[7]	detection based-on reference points	Require smart meter for all users
5	[6]	Analyzing the parameters of power	Require measurement instrument, have false positive problem
6	[15]	Detection based-on MAC address	Can be misleading by users
7	[15]	Detection based-on IP address	Can be misleading by users
8	[3]	detection based-on wallet address	Require processing and analyzing huge data
9	[15]	Analyzing and tracking the data flows on the Internet	Require processing and analyzing huge data
10	[3]	Sound and heat detection	Can be bypassed easily by users
11	[20]	Antiviruses to detect malwares	It is used rarely

4. Proposed and research results to reduce illegal miners

Here some proposed ways are introduced to decrease the unauthorized mining.

- Only low consumption miners and rigs should have a legal license
- Using a meter for all electricity consumers
- Using intelligent meters and reference points to calculate and detect electricity leakage in each area
- Inform people in order to use low power miners
- Processing meter data in order to detect illegal miners
- Monitoring the digital currency exchanges and transfers of cryptocurrency to these exchanges
- Cooperation with the telecommunications system in order to track the illegal miners through the Internet
- Using up-to-date antiviruses to detect mining malware
- Using the new energies for mining
- Amending electricity price and imposing heavy penalties on violators
- Public information in order to detect offenders and use a public information system
- Smart and continuous monitoring of industrial and agricultural electricity consumers
- Setting up smart laboratories to identify miners
- Recognition of mining and servicing and support of authorized cryptocurrency miners
- Establishing specific rules related to the mining, buying and selling of cryptocurrency
- Block some sites that teach illegal mining

5. Conclusion and Suggestions

In this paper, an overview of different methods of detecting unauthorized cryptocurrency mining was done. Also, some methods to bypass the detection and tracking of miners were mentioned. Although most of these tracking methods can be bypassed with different techniques, they work well in many cases and can detect miner devices accurately. Most of the challenges of this part can be solved by coordinating the government departments of countries. For example, with the cooperation of the telecommunication company and the electricity distribution company, it is possible to track unauthorized miners through the Internet. Some other proposed method for this challenge is related to use smart meter especially for agricultural and industrial electricity consumers. Also, all branches in each country must use the meter. Using private source of power may help some of these challenges. In general, using the private company for electricity production and new energies decreases most of the problems of this area. Naturally, if the production and consumption of electricity are done by the non-governmental sector at their expense, the field of better management will be provided, and perhaps it will be profitable for the electricity producers to carry out the extraction as well.

The last suggestion for mining is related to using renewable and new source of electricity power for mining of cryptocurrency. Using renewable sources of electricity power to mine crypto such as Bitcoin and cryptocurrency has been investigated in several studies. It has been found that using sustainable energy, such as hydropower or solar photovoltaic systems, can be financially and economically superior to using conventional fossil fuel systems [26]. Some studies have analyzed the feasibility of using renewable energy sources to power individual miners, shipping containers holding multiple miners, and commercial mining farm containers [27]. The profitability and return on investment of using renewable energy for mining vary depending on factors such as geographic location, solar flux, utility rates, and energy laws. While it may be negative in some locations with low-cost electricity, it can be substantial in other locations, ranging from 34% to 104% in U.S. cities. Overall, some studies suggest that using renewable energy sources for cryptocurrency mining can be financially viable and environmentally friendly [28].

References

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.

[2] K. O'Dwyer, and D. Malone, "Bitcoin Mining and its Energy Footprint," *25th IET Irish Signals & Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communications Technologies*, pp. 280-285, 2014.

[3] N. T. Courtois, M. Grajek, and R. Naik, "The Unreasonable Fundamental in Certitudes Behind Bitcoin Mining," *Arxiv Preprint Arxiv*, 1310,7935, 2013.

[4] K. J. O'Dwyer, and D. Malone, ''Bitcoin Mining and Its Energy Footprint,'' 2*5th IET Irish Signals & Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communications Technologies (ISSC 2014/CIICT 2014)*, p. 280 – 285, 2014.

[5] M. Amiri, and H. Askari, "Illegal Miner Detection Based on Pattern Mining: a Practical Approach," *Journal of Computing and Security*, vol. 9, no. 2, pp. 1-10, 2022.

[6] B. Dindar, and O. G¨ul, "The Detection of Illicit Cryptocurrency Mining Farms with Innovative Approaches for the Prevention of Electricity Theft," *Energy & Environment*, vol. 33, no. 8, pp. 1663-1678, 2022.

[7] R. Jiang, R. Lu, et al., "Energy-Theft Detection Issues for Advanced Metering Infrastructure in Smart Grid," *Tsinghua Science and Technology*, vol. 19, no. 2, pp. 105-120, 2014.

[8] A. Rahimi, A. Shahrestani, et al., "Filter Based Time-Series Anomaly Detection in AMI using AI Approaches," *2021 5th International Conference on Internet of Things and Applications (Iot)*, pp. 1-6, 2021.

[9] C. Chahla, H. Snoussi, L. Merghem, and M. Esseghir, "A Deep Learning Approach for Anomaly Detection and Prediction in Power Consumption Data," *Energy Efficiency*, vol. 13, no. 8, pp. 1633-1651, 2020.

[10] Z. Ouyang, X. Sun, J. Chen, D. Yue, and T. Zhang, "Multi-View Stacking Ensemble for Power Consumption Anomaly Detection in the Context of Industrial Internet of Things," *IEEE Access*, vol. 6, pp. 9623-9631, 2018.

[11] M. Li, K. Zhang, J. Liu, H. Gong, and Z. Zhang, "Blockchain-Based Anomaly Detection of Electricity Consumption in Smart Grids," *Pattern Recognition Letters*, vol. 138, pp. 476-482, 2020.

[12] B. Claise, B. Trammell, and P. Aitken, Specification of the IP Flow Information Export (IPFIX) Protocol, RFC 7011. IETF. 2013.

[13] A. Almalaq, S. Albadran, and M. A. Mohamed, "An Adoptive Miner-Misuse Based Online Anomaly Detection Approach in the Power System: An Optimum Reinforcement Learning Method," *Mathematics*, vol.11, no.4, pp. 884-884, 2023.

[14] C. Livadas, R. Walsh, D. Lapsley, and W. T. Strayer, "Usilng Machine Learning Technliques to Identify Botnet Traffic," *2006 31st IEEE Conference on Local Computer Networks, Tampa*, pp. 967-974, 2006.

[15] V. Vesely, and M. Zadnik, "How to Detect Crypto Currency Miners? by Traffic Forensics," *Digital Investigation*, vol. 31, 100884, 2019.

[16] J. A. Kroll, I. C. Davey, and E. W. Felten "The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries," *The 12th Workshop on the Economics of Information Security, Washington DC*, 11-12 June 2013.

[17] Y. Lewenberg, Y. Bachrach, Y. Sompolinsky, A. Zohar, and J. S. Rosenschein, "Bitcoin Mining Pools: A Cooperative Game Theoretic Analysis," *AAMAS 15 Proceedings of the 2015 International Conference on Autonomous Agents and Multiagent Systems*, pp. 919–927, 2015.

[18] A. Juels, A. Kosba, and E. Shi, "The Ring of Gyges: Investigating the Future of Criminal Smart Contracts," *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pp. 283-295, 2016.

[19] D. Y. Huang, and H. Dharmdasani, et al., "Botcoin: Monetizing Stolen Cycles," *Proceedings of the 2014 Network and Distributed System Security Symposium. NDSS*, 2014.

[20] S. T. Ali, D. Clarke, and P. McCorry, "Bitcoin:Perils of an Unregulated Global P2P Currency," *Cambridge International Workshop on Security Protocols*, pp. 294-306, 2015.

[21] S. Solaymani, "A Review on Energy and Renewable Energy Policies in Iran," Sustainability, vol. 13, no. 13, p.7328, 2021.

[22] A. Zakir al-Hosseini, "Data Security," *Nas Publications*, *fifth Edition*, 2012.

[23] L. Feng, S. Xu, et al., "Anomaly Detection for Electricity Consumption in Cloud Computing: Framework, Methods, Applications, and Challenges," *EURASIP Journal on Wireless Communications and Networking*, vol. 2020, no. 1, p.194, 2020.

[24] R. Hofstede, P. Celeda, et al., "Flow Monitoring Explained: from Packet Capture to Data Analysis with Netflow and Ipfix," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, pp. 2037-2064, 2014.

[25] S. T. Ali, P. McCorry, P. H. J. Lee, and F. Hao, "Zombiecoin: Powering Next Generation Botnets with Bitcoin," *Financial Cryptography and Data Security Springer*, pp. 34-48, 2015.

[26] Y. Liang, C. B. Saner, et al., "Sustainable Energy-Based Cryptocurrency Mining," *2022 IEEE PES Innovative Smart Grid Technologies - Asia (ISGT Asia),* pp, 789-793, 2022.

[27] M. T. McDoald, K. S. Hayibo, F. Hafting, and J. M. Pearce, "Economics of Open-Source Solar Photovoltaic Powered Cryptocurrency Mining,", *Available at SSRN 4205879*, 2023.

[28] P. Rorich, K. Moloi, T. F. Mazibuko, and I. E. Davidson, "Cryptocurrency Mining Powered by Renewable Energy Using A DC-DC Connection,"*31st Southern African Universities Power Engineering Conference (SAUPEC),* pp. 1-7, 2023.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper. The ethical issues, including plagiarism, informed consent, misconduct, data fabrication and/or falsification, double publication and/or submission, redundancy, have been completely observed by the authors.

Credit Authorship Contribution Statement

Mohammad Hossein Shakoor: Conceptualization, Formal analysis, Project administration, Supervision, Validation, Investigation, Methodology, Roles/Writing - original draft.

Bibliography

Mohammad Hossein Shakoor received the B.Sc. degree in Computer Engineering from Shiraz University, Shiraz, Iran, in 1998 and M.S. degree in computer architecture from Isfahan university, Isfahan, Iran, in 2003. He received Ph.D. in Artificial Intelligent of Computer engineering from Shiraz University, Shiraz, Iran in 2016. His research interests include Texture Classification, Pattern Recognition and Computer Vision.