|  |  |
| --- | --- |
|  | **The Profitability and Cost of Cryptomining as a Web Monetization Model**  Abdulrahman Alqahtani |

**The Profitability and Cost of Cryptomining as a Web Monetization Model**

**Abstract:**

A journal titled “Truth in Web Mining: Measuring the Profitability and Cost of Cryptominers as a Web Monetization Model,” explores the potential of cryptomining as an alternative web monetization model. The authors strive to determine whether cryptomining can replace advertising as the dominant model for monetizing the web. They conduct several experiments by comparing cryptomining and advertising to determine the most profitable option for web publishers. They also explore the impacts of each model on internet users.

Advertisements might irritate some internet users while cryptomining consumes a significant portion of computing resources. The rise in the number of cryptocurrencies, as well as the increasing mining speed, has promoted the use of web mining. The journal concluded that cryptomining has the potential to surpass advertising as the most profitable web monetization model in the long term. It also concluded that cryptojacking attacks are also on the rise as cyber criminals use sophisticated tools to monetize the computational capabilities of compromised computers.

***Keywords***: Cryptomining, advertising, cryptojacking, cryptocurrency, Drive-by Mining, web-mining.

**Introduction**

Over the past few years, cryptomining has attracted a lot of interest due to its potential to become a reliable web monetization model. This approach emerged as a possible solution to the dwindling revenues caused by the use of advertisement blocking tools. Cryptomining can be more profitable than the traditional advertising-based revenue generation model, if web users spend more time on a miner-supported website.

Although it is a relatively new technique, cryptomining is rapidly gaining adoption among web publishers. However, cyber attackers have also developed sophisticated tools for exploiting web users’ computing resources without the knowledge of the victims. Solutions to cyber-crime are vital to the success of this new revenue generation approach. Thus, over time, cryptomining could surpass advertising to become the most reliable method of generating revenues from web content.

**Background**

Cryptomining emerged after the development of the digital currency. The creation of alternative cryptocurrency coins, which were much simpler to mine compared to Bitcoin, the first cryptocurrency introduced, increased the popularity of web mining [1]. However, finding valid hashes is quite costly, as the process consumes a lot of computational resources.

The development of the JavaScript implementation of Monero in 2017, provided a new method of monetizing the web while minimizing the costs of cryptomining. Coinive’s JavaScript-based miner can be incorporated in any website, thereby enabling web publishers to compute hashes by utilizing the processor and memory of web users’ devices [1]. Thus, cryptomining is becoming a reliable alternative to the traditional advertising model of generating revenue from the internet.

Cryptomining is aided by mining service providers (MSPs). These third-party entities synchronize the computations, collect hashes, and share revenues with web publishers [1]. MSPs also provide mining libraries, which are sent to users’ devices upon visiting a miner-supported website.

According to security researcher Troy Mursch from Bad Packets Report about 50,000 sites are secretly infected with crypto-mining scripts [3]. Leading providers of mining libraries include Coinhive, JSE coin, Coinpot, CryptoLoot, Coin-have, Hashing, Webmine, PPOI, Coinimp, and Adless [1]. Coinhive is the most widely used tool. Figure 1 below shows the percentage of websites that use these mining libraries.

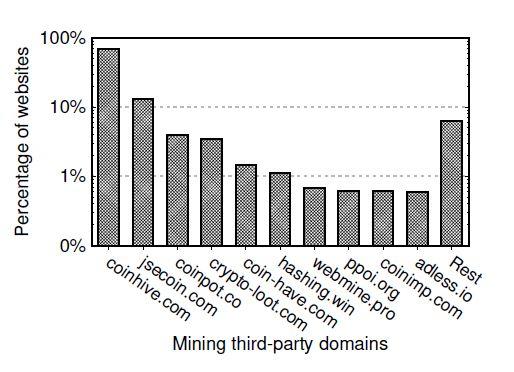


Figure 1: Usage of third-party mining libraries.

**Benefits of Cryptomining Over the Advertising Model**

Cryptomining has massive potential as a web monetization model. Web publishers neither track user activity nor collect personal information [1]. Hence, content providers do not incur the costs of collecting and analyzing user behavioral data. Internet users also receive a secure browsing experience. They do not realize the existence of cryptominers, unlike advertisements that are visible and can be easily blocked using ad-blockers [1]. Moreover, web publishers can earn a significant amount of money by using cryptominers.

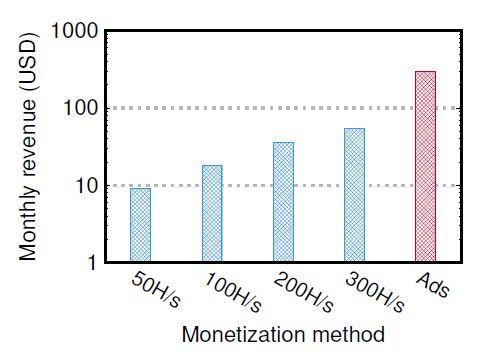
For instance, a publisher receives 0.0001468 Monero coins for every one million successfully generated hashes [1]. As shown in Figure 2 below, spending more time on a miner-supported website increases profits. Thus, web providers can earn more by providing content that keeps visitors on a site for a longer duration.

Figure 2: Web monetization method.

**Challenges of Cryptomining**

The growth of cryptomining has led to a rise in cyber-crime. Technologies that support cryptomining as a web monetization method have also been used by cyber-criminals to launch cryptojacking attacks [1]. As web content publishers deploy cryptomining to increase their revenues, cyber attackers also apply the same technology to monetize web users’ computational resources illegally.

While legitimate cryptominers use the web users’ computing resources only when the browser tab is open, cyber attackers can inject mining payload into several websites that the victim visits [2]. The rise in cryptojacking incidents has affected the use of cryptomining as a legitimate way of monetizing web usage. To counter this type of crime, major browser vendors have developed tools for detecting and blocking all cryptominers [1]. For example, Google removed browser extensions that perform web mining from Chrome. Similarly, many antivirus software applications consider web mining scripts as malware.

Cryptomining also burdens user computing resources. Miner-supported browsers consume up to fifty-nine times of processor memory than browsers that use advertisements [1]. Consequently, a computer may fail to support multiple parallel programs. Browsers that support cryptomining also require more memory than those that display ads. Figure 3 below shows memory usage by cryptominers and advertisements.

Moreover, users of miner-supported websites consume more than twice as much energy as visitors to sites that run advertisements [1]. The high energy consumption increases the temperature of a device by more than fifty percent [1]. Cryptomining also escalates costs for users who access the web over a cellular network [1]. Therefore, cryptomining may adversely affect user experience.

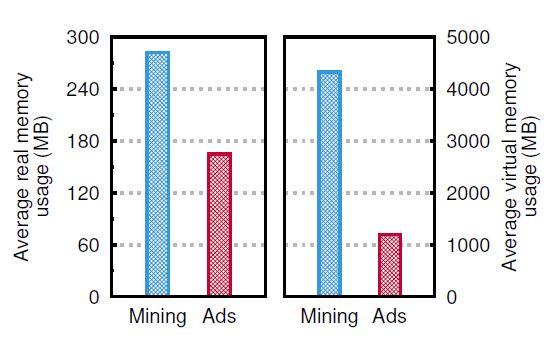


Figure 3: Memory Usage by Mining and Advertisements.

Cryptomining serves as the third party trustee to validate transactions and place blocks in their applicable chains. Once a miner has validated 1 MB (megabyte) worth of bitcoin transactions, known as a "block", that miner is rewarded with a quantity of bitcoin. This bitcoin can be exchanged for several different cryptocurrencies or cashed out for fiat money. Although this may seem as a promising method of generating high revenue, cryptominers still face some high energy costs, scalability and security concerns.

Some of these concerns are high energy costs, vulnerability to cryptojacking, double spending and greatly slower processing speed compared to Visa. Moreover, there are also some additional costs such as transaction fees, equipment costs, and cellular network fees.

**Suggested Solutions for Cryptomining:**

**High Energy Cost:**

CBS News reported that bitcoin mining uses more electricity than 159 countries [5]. In other words, bitcoin mining computers and networks that are responsible for the proof of work processes use over 29.05 TWH (Terawatt-hours) annually [5]. In order for miners to earn a living, they compete against one another hoping to be the first miner to discover the 64-digit hexadecimal number known as a hash.

A miner does not solve complex mathematical problems but relies on a computing power. It has been reported that the more machines a miner works with, the more profit that is generated. As a result of this, cryptominers pay significantly hefty fees on electricity used to mine cryptocurrencies.

This problem can be solved by using cryptomining facilities and data centers that are powered by renewable hydroelectricity and solar energy. In 2019, an article published on the famous TV channel National Geographic, reported that hydropower provides approximately 16% of the world's electricity [6].

It was reported that Norway produces about 99 % of its electricity with hydropower. Nevertheless, Figure 4 below shows China has been the leading producer of hydropower in the world. Some countries' geographic location might not be feasible for hydroelectricity due to their limited access to falling water. In this case, thermoelectric power can be used to generate electricity. For instance, in Saudi Arabia hydropower is not commonly used due to its nature but a tremendous amount of electricity is produced every year using solar energy.

In 2018 the Center for Climate and Energy Solutions reported that about 2% of the world’s electricity is produced with solar energy. In 2017, Apple initiated its $1 billion green bond to further its renewable initiatives; one year later Apple announced that its entire facilities are 100% powered by renewable energy [7].

Furthermore, there are other types of energy that can be used such as kinetic energy that mostly uses wind turbines. In the end, using dedicated facilities for cryptomining will reduce the electricity cost and would be more efficient.

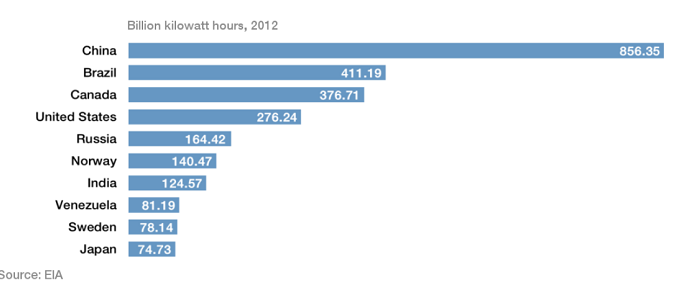


Figure 4: Countries producing the most hydropower.

**Scalability:**

The security of cryptocurrencies has always been the main focus of this industry which has led to relatively secured systems using various methods such as hashing algorithms, blockchain technology, and serious validation processes such as proof of work, proof of stake, and proof of authority.

Figure 5 below shows that each transaction processed on blockchain technology has to go through very complex processes which makes blockchain technology payments have lower capacity in transactions throughput compared to Visa and MasterCard. Visa can process up to 24,000 transactions per second, Bitcoin's maximum speed is 7 transactions per second [8]. Also, Visa cards are accepted in over 200 countries of the world, while Bitcoin is fighting back to gain consumers’ trust.

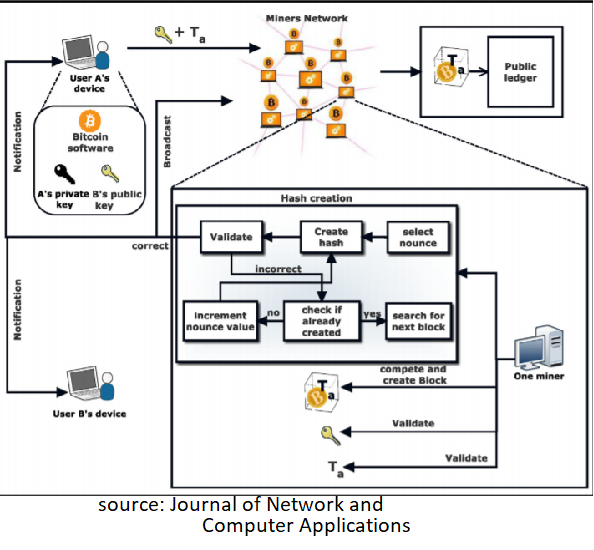
****

Figure 5: Lifecycle of transaction in Bitcoin network.

Many Bitcoin enthusiasts believe that in the near future Bitcoin scalability may beat that of Visa and MasterCard. However, enhancing Bitcoin’s performance will jeopardize its security. In order to process more payments, Bitcoin has to adopt new block size which is currently 1 MB [9]. Increasing the size of the block means having the capacity to hold larger data input.

For instance, if the block size was 4 MB you can possibly store 4 of the current blocks in a single block. Therefore, a miner can validate less blocks and more transactions can be processed. Additionally, relying on machine learning algorithms instead of miners will increase speed and performance. This can be achieved by having a dedicated block that serves as the parent block for other blocks.

In other words, you might think of this block as the genesis block that is the first block in any blockchain-based protocol. It is the basis on which additional blocks are added to form a chain of blocks. In this block, users will be required to record personalized phrases that will be stored in this block to be used for automatic speech recognition(ASR). The phrases will be personal and only recognized by the user and the machine. Each time a user processes a transaction the user has to say the specific phrases as another layer for security.

People are creatures of habit which makes it easier for machine learning. That being said, user’s habits will be stored in the first block and are used every time he/she processes a transaction. This technology is being used today by financial institutions to detect fraud and protect consumers.

In 2018 JPMorgan Chase & Co announced they are starting to use individuals’ unique voiceprints to identify customers who are calling to inquire about their credit card accounts. A miner will only be needed if the algorithm suspects fraud is committed by the user or any third party.

**Cryptojacking:**

Cryptojacking also known as malicious cryptomining is the unauthorized use of a computer, tablet, mobile phone, or connected home device by cybercriminals to mine for cryptocurrency. Malicious cryptomining can be done in several ways including phishing tactics and web browser miners.

Malicious phishing is one of the most popular cryptojacking methods simply because of its efficacy. Phishing can be done through emails, text messages, phone calls or social engineering. Phishing emails is one of the greatest tactics where a user receives an email seemingly from a legitimate and trusted party. Cybercriminals will always use a very similar URL link barely distinguishable to the naked eye.

An example of this is adding an extra letter in the website name such as [WWW.chasse.com](http://www.chasse.com) for chase.com, or Paybal.com for Paypal.com. Also scammers sometimes use different extensions such as chase.net, or chase.me. Upon clicking on the link or downloading the attachment, it runs a code that downloads the cryptomining script on the computer. The script then works in the background without the victim’s knowledge as it mines user’s data.

Web browser miner is another deceptive method for cryptomining. Cybercriminals will inject a cryptomining script on a website or in an ad that is placed on multiple websites. Oftentimes, websites use ads cookies to generate income, some of these ads are harmless. These cookies will store your browsing data and based on your search it will generate future ads.

For instance, if you are on google looking to buy a car, a day later when you visit CNN or any website that has no association with cars, a pop-up car ad appears usually in the upper right corner with car pictures. In the case of malicious ads when the victim visits the infected website, or if the malicious ad pops up in the victim’s browser, the script automatically executes. In this method, no code is stored on the victim’s computer. This method is responsible for most advanced persistent threats (APTs)[[1]](#footnote-1) and ransomware.

Detecting Cryptojackingis not easy. Cryptojackers use deceptive tactics such as pop-under, reducing the usage of the victim’s processing resources, and communicating with mining service providers through cloud-based proxy servers [1]. These techniques allow cryptojackers to operate stealthily in the background. Moreover, some cryptominers do not notify users about the presence of mining scripts on their websites.

Cryptojacking is very advanced and is financially rewarding for cybercriminals. Education and transparency are two great key successes that cryptominers should provide to their clients. Some cryptocurrencies investors manage their accounts using public Wi-Fi, and are unaware that they are vulnerable to cyberattacks.

In 2017, an incident occurred in Buenos Aires where public Wi-Fi was injected with malware that caused a 10-second delay when logging in to the cafe’s Wi-Fi network [10]. The 10 seconds delay was used to plant a mining script on the user’s account leading to the mining of the user’s digital assets.

Educating cryptocurrencies’ users on the safe approach to manage their accounts and the importance of being on a private network or using VPN will lead to safer browsing. This can be approached by setting requirements from miners to submit at least one new security threat and the solution for it at the beginning of every two weeks. These educational resources will be communicated to every investor on the platform.

**Hardware Cost:**

Initially when cryptomining began, miners relied on their personal computers (CPU) computing power. However, as many miners joined this industry it created an overwhelmingly greater competition. The faster a miner processes the complex calculation known as hashes, the greater chance of earning money. Consequently, more miners started using specialized hardware called Application Specific Integrated Circuits (ASIC). ASICs are each designed to solely perform one specific type of function. Each ASIC miner is constructed to mine a specific digital currency. So, if a miner is trying to mine Bitcoin, then a miner will have dedicated ASICs specialized only in mining Bitcoin. ASICs are designed to perform one specific task, which makes it easier and faster than microprocessors that rely on MIPS pipelining, and task parallelism.

Bitmain.com is one of the most popular sites that sells ASICs miners, and it currently lists Antminer S19 Pro for approximately $ 2,400. In order for a miner to earn significant profit several ASICs are needed. Therefore, for an individual to start mining, an investment of several thousand dollars is a must, and this has created a monopoly in the market. Creating a data center powered by renewable energy will not only save the environment but it will also be equipped with cutting edge technology.

In a data center, mining pools will be the most efficient approach where miners will invest their efforts together leading to more profits and less time invested. Many miners that share geographical connections have established mining centers such as Giga Watt in Washington state, Bitmain Ordos in Mongolia and Bcause LLC in Virginia Beach. It was reported that the massive Bitmain Ordos in Mongolia consists of 25,000 machines that process $250K worth of BTC daily [11]. Sadly, most of these mining centers do not use renewable energy due to the installment costs.

**Conclusion**

In conclusion, cryptomining has the potential to become more profitable than digital advertising in the long term. Digital advertisements are easily seen eventually blocked using ad-blockers such as AdLock, AdBlock Plus, and many more. Although some mining blockers exist, they are proven to be less effective due to the sophisticated nature of mining digital advertising. Some of these mining blockers include Coin-Blocker, No Mining, MinerBlock, noMiner and CoinBlock. Furthermore, many cryptominers use mining libraries provided by third parties, which are referred to as Mining Service Providers (MSP). Therefore, cryptominers do not have to spend time developing a mining script and instead invest the time adding these mining ads on as many websites as possible.

Cryptomining is less intrusive since web content providers do not collect personal or browsing data about site visitors. Besides enhancing the privacy of web users, cryptomining eliminates the costs that web publishers would have to incur analyzing advertisement impressions. These benefits have increased the demand for cryptomining technologies.

Despite these advantages of cryptomining, there are also several drawbacks to this technology. Cyber attackers pose the biggest threat. Cybercriminals use advanced tools to generate cryptocurrency by utilizing the processor and memory of compromised devices. Heavy usage of computing resources can lower the performance of a device. However, some solutions have been developed to address these issues.

Cryptomining can become more profitable than the traditional advertising model especially if a miner is cryptomining on hundreds of computers simultaneously. According to an article published by Symantec Blogs some miners can possibly earn up to $750K over the course of 30 days [4].

Overall, the growth of cryptomining has led to a rise in cyber-crime. Cybercriminals disguise themselves to look more like legitimate ads and upon clicking on the ads, a script will be downloaded to mine your information. As a matter of fact, some fake ads download scripts that store all your data including your usernames, passwords and later send all that to the cybercriminals, this practice is known as malvertising. Technologies that support cryptomining as a web monetization method have also been used by cyber-criminals to launch cryptojacking attacks. These same cyberattack techniques have always been used with digital ads.

**References**

1. P. Papadopoulos, P. Ilia, & E. P. Markatos. (2018). Truth in web mining: Measuring the profitability and cost of cryptominers as a web monetization model. *arXiv preprint arXiv:1806.01994*.

2. R. K. Konoth, E. Vineti, V. Moonsamy, M. Lindorfer, C. Kruegel, H. Bos, & G. Vigna. (2018). Minesweeper: An in-depth look into drive-by cryptocurrency mining and its defense. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1714-1730).

3. Mursch, Troy. “How to Find Cryptojacking Malware.” *Bad Packets, 4 Apr. 2019, badpackets.net/how-to-find-cryptojacking-malware/.*

*4.* Gorman, Brigid O. “Cryptojacking: A Modern Cash Cow.” *Symantec Blogs, BROADCOM, 5 June 2020, symantec-enterprise blogs.security.com/blogs/threat-intelligence/cryptojacking-modern-cashcow?utm\_content=79386076&utm\_medium=social&utm\_source=facebook.*

*5.* Martinez, P. (2017, November 28). Bitcoin mining consumes more energy than 159 countries. Retrieved June 23, 2020, from <https://www.cbsnews.com/news/bitcoin-mining-energy-consumption/>

*6*. Nunez, C. (2019, May 13). Hydropower, explained. Retrieved June 23, 2020, from <https://www.nationalgeographic.com/environment/global-warming/hydropower/>

*7.* Potuck, M. (2017, June 14). Apple moves closer to 100% renewable energy as it issues $1 billion green bond. Retrieved June 23, 2020, from <https://9to5mac.com/2017/06/13/renewable-energy-1-billion-green-bond/>

*8*. , B. (2018, March 07). Blockchain speeds & the scalability debate. Retrieved June 23, 2020, from <https://blocksplain.com/2018/02/28/transaction-speeds/>

*9.* Magazine, B. (2020, May 19). What Is the Bitcoin Block Size Limit? Retrieved June 23, 2020, from <https://bitcoinmagazine.com/guides/what-is-the-bitcoin-block-size-limit>

*10.* Davis, G. (2017, December 14). Starbucks Bitcoin Mining Incident Reminds Us of the Risks of Public Wi-Fi. Retrieved June 24, 2020, from <https://www.mcafee.com/blogs/consumer/consumer-threat-notices/starbucks-bitcoin-mining/?_ga=2.127620237.1633897581.1592935871-1263072666.15929358>

*11.* HAMILTON, D. (2018, May 10). The Top 5 Largest Mining Operations in the World. Retrieved June 25, 2020, from https://coincentral.com/the-top-5-largest-mining-operations-in-the-world/

1. APTs is a stealthy cyber-attack on a computer network where the attacker gains and maintains unauthorized access to the targeted network and remains undetected for a significant period. [↑](#footnote-ref-1)