Crypto Jacking a Technique to Leverage Technology to Mine Crypto Currency

Haitham Hilal Al Hajri, Badar Mohammed Al Mughairi,
Mohammad Imtiaz Hossain, Asif Mahbub Karim

To Link this Article: http://dx.doi.org/10.6007/IJARBSS/v9-i3/5791 DOI: 10.6007/IJARBSS/v9-i3/5791

Received: *01 Feb 2019,* ***Revised:*** *17 Feb 2019,* ***Accepted:*** *29 Feb 2019*

Published Online: 04 March 2019

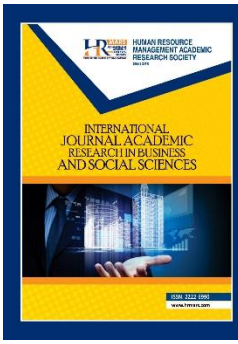
In-Text Citation:(Hajri, Mughairi, Hossain, & Karim, 2019)

To Cite this Article: Hajri, H. H. Al, Mughairi, B. M. Al, Hossain, M. I., & Karim, A. M. (2019). Crypto Jacking a Technique to Leverage Technology to Mine Crypto Currency. *International Journal Academic Research Business and Social Sciences*, *9*(3), 1220–1231.

Vol. 9, No. 3, 2019, Pg. 1220 - 1231

http://hrmars.com/index.php/pages/detail/IJARBSS **JOURNAL HOMEPAGE**

Full Terms & Conditions of access and use can be found
athttp://hrmars.com/index.php/pages/detail/publication-ethics


INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES
HRMARS MANAGEMENT ACADEMIC RESEARCH SOCIETY EXPLORING INTELLECTUAL CAPITAL
www.hrmars.com
ISSN: 2222-6990

Crypto Jacking a Technique to Leverage Technology to Mine Crypto Currency

Haitham Hilal Al Hajri[1], Badar Mohammed Al Mughairi[2], Mohammad Imtiaz Hossain[3], Asif Mahbub Karim[4]

[1,2]PhD Researcher, Binary University of Management & Entrepreneurship, Malaysia

[3]MSc in Business Economics, Faculty of Economics and Management. University Putra Malaysia, Malaysia

[4]Dean, Binary Graduate School, Binary University of Management & Entrepreneurship, Malaysia

Abstract

Society dependency on technology is becoming an obligation of modern life society, hence the advancement and innovation on Information and Communication Technologies Sector, especially when it comes to the development of infrastructure and various services provided by many vendors governmental or commercial. It is all, due to the constant revaluation of technology used by society today. Blockchain made its first debit as a proof of concept on money exchange platforms back in 2008, where the born of the first cryptocurrency. However the technology had more potential than just platform of exchanging valuable currency, it has spanned, out to open a whole work of possibility to enhance today modern day society further. However, as usually, cyber-criminals have found a way to leverage this technology to benefit them by exploiting the technology weaknesses to carry own their deeds. This paper will demonstrated the phenomenon of the crypto jacking and other related methods utilised by a hacker to leverage mining crypto. The objective of this paper is to investigate the state-of-the-art crypto mining attacks by overviewing different types of malware like crypto-jacking.

With the current revaluation of technology, cybercriminals are being creative on discovering and implementing methods to abuse the leverage technology to meet their deeds, and lately, the majority of cybercriminals are experimenting with cryptocurrency and methods or techniques to mine cryptocurrency effectively and anonymously, the attack is known by Cryptojacking. The results from static and dynamic analysis uncover the techniques employed by the malware to exploit potential victims.The study concludes that enterprises face the greatest risk of cryptojacking due to the broad attack surface and moderate consequence severity. This research recommends anticipating trends in cybercrime monetization to inform defense strategies and increased communication about cyberattack information to better understand and defend against the cryptojacking threat.

Keywords: BlockChain Techology, Cryptocurrency, Cryptomining, Cryptojacking, Ransomware, Malware, Cyber Threat

Introduction

Cryptojacking is considered to be among the top consistent and renewable persistent threat in the digital era of technology today. Recently the trend within cyber-criminal world has shifted, as more malware code writers are improving on their malware to include crypto jacking and crypto-mining capability to their arsenal kit. The new generation of malware has implemented crypto jacking code to their exploit, to hunt for digital crypto wallet address and to mine crypto on victims or targeted machines or devices. Therefore this paper will showcase the blockchain technology and associated functions within about mining crypto, along with some highlight on the terminology used in crypto jacking and the technique used to conduct crypto jacking. Cryptojacking has become a profitable business indeed, according to the 2018 IBM X-Force Threat Intelligence Index the frequency and sophistication of malware based mining is increasing and that clearly shows that the interest of targeting cooperate, personal and financial data to have as a hostage for ransom has shifted into mining Cryptocurrency (Gu, 2018).The nature of mining Cryptocurrency was by utilising the power of Central Processing Units (CPU). However, with the increase of complexity in mining the next coin, the shift went to utilizing the power of Graphics Processing Unit (GPU) in mining cryptocurrency (GPU Crypto-Miner), which was proven useful in processing complex mathematical calculations, that was convenient to be used in password cracking or various high volume processing such as used in digital forensics machines. Though the bourn of the ASIC (Application-Specific Integrated circuit) is a microchip that is designed to handle specific or particular application, the ASIC can be integrated with other microprocessors and integrated chips so it can be further customised. So ASIC becomes somehow popular in mining cryptocurrency for the benefits it provides. However, the crypto world is increasing, and more coins with more advanced features such as speed of transaction and security in the privacy have emerged. Therefore, the developers and designers of the new cryptocurrency have identified the possibility of utilising such machines and technology to mine the crypto in future, and that would affect the reputation and the stability of market value. They have taken measures to ensure mining is running on a personal computer rather than detected machines. Like the ASIC miners in which it gained considerable popularity among miners of bitcoin. Therefore, the newer generation of cryptocurrency is ASIC- Resistances. Subsequently, miners of such crypto will have to do it on regular PC, which has unintentionally aided the spread of malicious mining malware, and now all standard pc around the globe has become a target for crypto jacking and malware mining.

Cryptocurrency

Cryptocurrency refers to a digital or a virtual currency, where the terminology is consist of a combination of two parts **A**: crypto which refers to the technique (technology) and the base used to establish the currency which is cryptography **B**: reference to usage part which is the currency. Cryptocurrency is an asset that can be used to purchase goods or services. Since it is a virtual asset, it does not belong to a central agency or regulator neither its backed by treasured and precious entity like gold. The value of crypto determined by other factors such as;

1. popularity and reputation that lead to mass adaption of the cryptocurrency among society,
2. operation stability of the network and speed which is an essential factor when dealing with cryptocurrency,
3. privacy and anonymity which is a primary concern when dealing with cryptocurrency, as it begins the preferred mean of payment for a lot of underground activity or services that of illegal nature .

Blockchain

When dealing with payments, organisations require a ledger, and the ledger needs to have a very meticulous input mainly when it associated with repetitive transactions, which are highly complicated and fluctuating constantly. Therefore the bourn of Blockchain technology came into light. The concept of blockchain has defined as "Blockchain is a Decentralized digital ledger, which is extended to the members of the same chain via peer to peer networking, who are together can manage the database of information (transactions) in sequential order, without the need of central authority. The transactions stored in blocks and connected logically using a mutual cryptic algorithm and transactions is shared publicly with members of the same chain". Blockchain technology is relatively new, and emerging technology. The world still finds new ways where blockchain can implement and further advanced to meet other requirements. Currently, there are three main types of blockchain and a few others which are a combination of two or more types *Hybrid*.

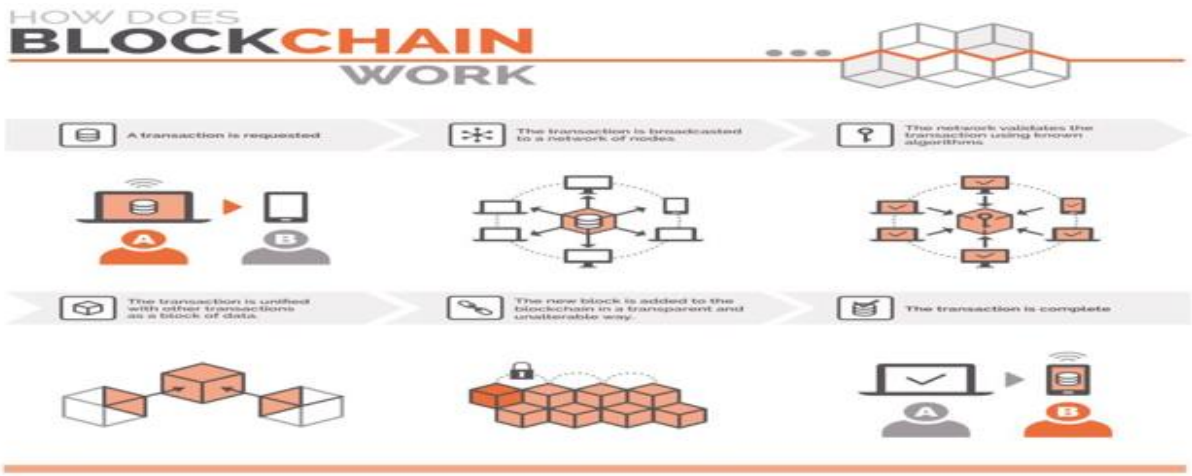


Figure 1:Blockchain Works (The Accounting Degree Review,n.d)

Methods to Establish Consensus on Blockchain

A consensus algorithm is a terminology that used to describe the process involved within the agreement of multiple distrusted systems "nods" on one unified result of data or value within a network of some sort (Blockchain). In an aim to attain reliability and sustainability of network outputs with the possibility of interference of unreliable sources of information (nods with malicious aim) within that defined network (Rouse ,2017) . Consensus algorithms are considered to be a very significant and critical part of the blockchain network, and without it, the blockchain

would not function accordingly. Therefore it is safe to assume that consensus algorithms are the backbone of the blockchain. There are many consensus algorithms available today which all contest to solve an existing issue within the blockchain domain and each algorithm can fit a specific needs of the blockchain technology and can serve as an alternate option for others. Subsequently, it is all down to the objective of that specific blockchain function what they are trying to achieve. The following are examples algorithms of the blockchain which considered one of the most famous and used consensuses.

Proof of Work (PoW)

Proof of Work system consensus in use in Bitcoin, Ethereum and another cryptocurrency. Bitcoin to be the first and oldest cryptocurrency and Ethereum as the second largest crypto after bitcoin at the times of writing this paper. Proof of work considered to be expansive as it requires a lot of detected equipment that consumes much power and generates much heat (Harper & Colin , 2018). Due to that, it needs a continues maintenance an upgrade to keep up with the speed of changing difficulties of bitcoin mining or cryptic puzzle solving. It works by allowing miners to compete and race to solve an encrypted puzzle that ensures the integrity of the coin. The first one is to solve the encrypted puzzle gets a block to reword and get recorded on the public leader after announcing the solution to all in the network.

Proof of Stake (PoS)

The second common alternative to proof of work is the proof of stake. It works by the amount of stake (COIN) an individual has and for how long have had it by selecting the validator based on the amount and time in order to be able to mine and validate the transaction. The miner invests on the cryptocurrency coin itself to be able to mine and collect fees. Also, it has shown that it is more economical, as it will not require an investment in high-end equipment's or spend much money on power and cooling. According to Investopedia, this prevents the chance of a 51% attack, which has coast a massive loss for altcoins such as the privacy and security-focused coin.(InvestoPedia,2018)

Proof-of-Authority (PoA)

Proof-of-Authority PoA consensus has been introduced first on March 2017, the term coined by Gavin Wood, co-founder of Ethereum and Parity Technologies, is based on the Ethereum protocol, and the network was called Kovan. The consensus based on optimised Proof of Stake model, which uses identity as a form of stake instead of staking tokens like "Prof of stake" method. The identity is supported by a group of validators known as (authorities) who maintain software that pre-approve and validate transactions and blocks within the respective network. There are certain conditions should be met first to be selected as a validator, and it has to do with the reputation of the validator as a prime condition. The group of validators is meant to remain in small numbers (25 or less) to ensure efficiency and manageability of security within the network (Curran, 2018)

Proof of activity (PoA)

Introducing Proof of Activity concept in 2014 by four authors one of them is the creator of lite-coin cryptocurrency project, as they attempted to solve the issue of "hyperinflation" means too much of

currency, due to the reality of bitcoin reaching the caped 21M bitcoin. The Authors have come up with a "Mix Approach Protocol" that combines the best fetchers of two protocols(Bentov et al, 2014). The Mix Approach Protocol achieved by incorporating a set of extended instructions designed to perform a frequently used operation within the bitcoin mining routine called "follow-the-satoshi". Picking a pseudo-random index among zero and the entire number of satoshis in presence till the last block, checking the block in which this Satoshi was minted and following each transaction that transferred this Satoshi to next random address until reaching the address that currently controls this Satoshi. This method can be regarded as selection a pseudorandom stakeholder in a uniform fashion. The used approach allows the miners to start the process of the classical way as a Proof of work "Pow", where miners compete to solve the cryptic puzzle and get to generate the block. However, the block yet not reworded as phase two will begin by the switch to Proof of stake protocol "PoS". Where they use the headers information on the "Shall Block" (created but not yet validated Block) to locate a pool of "Pseudorandom Stakeholder" (people who have a large share of the coin than select and determine who is in the network that meets the two control conditions. (1)- The oldest (Time) and (2)- has most shares of the coin. Based on that the system, will be randomly selected who get to sign and validate the black to get reworded. The extension of the protocol makes it more complicated to mine. It did slow down the mining and rewarding process, but it has criticised that it still requires a consume significant recourses to mine. On the flip side, it did aid on mitigating against 51% attack. Decerd is the only coin right now using a variation of proof of activity (Walters, 2018)

Proof of Burn (PoB)

Proof of Burn consensus, as the name, indicates it has something to do with burning a crypto coin for reasons of controlling the coin demand, creating new coin or ensure rewording system is stable. However, more uses can be applied to the "PoB" protocol (Khatwani, 2018). The Coin burn done by sending the coin to a specific wallet that is irretrievable, and since every transaction recorded on the public ledger, it is possible to track the coin amount and ensure that coins remain on the burn wallet.

Proof of Capacity (PoC)

Proof of capacity, proof of storage and proof of space are all versions of the same concept which has to do with investing on digital storage space and plotting that drive space for services in exchange the user get to mine coin, so the larger the drive the more chances you have to validate the next black and get rewarded. It works by producing detected plots on the drive which will result in "nonce" which repeated hashing that associated with account ID (Andrew,2018). Therefore, more space will be available for more plotting increasing the chances of the miner to mine.

Proof of Elapsed Time (PoT)

This method presented in 2015 by famous Microchip and processor companies in an aim to build a trusted execution environment (TEE) within the Intel's 6th generation Core Processors and SGX functions. It is a set of commands for a CPU which utilised by the running applications to isolate specific trusted areas of code and data. However, the idea behind it is to enhance proof of work

concept, so it will consume fewer resources and electricity, by utilising Intel's invention SGX to produce random signed timer object (blocks), to participants within the block chain to avoid any possibility of, malicious party manipulating the system to over-mine blacks. Even thou this concept may sound appealing, but it will depend on trusting a third party such intel propriety software to distribute the blocks, and again this goes against the idea of freeing the currency from any governing party (Curran, 2018)

Byzantine Fault Tolerance (BFT)

Blockchain technology has been designed to be decentralised. Therefore the Byzantine fault tolerance developed to enhances the availability and reliability of the replicated crypto mining between connected nodes in an aim to avoid fault arbitrarily nodes too ensure minimum required connected nodes of any deterministic service(Cowling et al,2006). The BFT ensure all communication and transaction between the replicas agreed on order to execute the mining operations. Consequently, It works as a fault tolerance approach for blockchains technology.

Cryptojacking

Ben William, a director of the operation at Adblock Plus, describe the Cryptojacking as " the act of secretly using another's computing device to mine digital currencies" (Williams , 2018).To Mine and create new digital coins, miners must solve complex computational problems, requiring large volumes of computing power and energy that cost a considerable amount of money. However, By hacking into another's computer systems, attackers can bypass these barriers and limitations, and start to mine and create new currencies with very minimal costs. We can define Cryptojacking "*is the unconsented use of digital resources in order to mine cryptocurrency*", and that can be achieved by the utilisation of various methods adopted by malicious entity (hacker/cyber-criminal) where malicious user deploys "Phishing Technique" to spread infected URL injected with mining script so, the host will work as a mining host for the miner. The attacker can mine via leveraging the web browser of the victim while visiting the infected website.

Nevertheless, the attackers may adopt the "Malvertising Technique" where the malicious entity embeds a malware into a legitimated advertisement or websites. Therefore, the visitors will be a victim of mining malware, and that brings an infamous attack known as "watering hole attack" where attackers target a popular website to attract a large volume of visitors in a regular base. This attack strategy infects the visitors via web browser mining or by spreading malware infused with Cryptomining software. Consequently, many users will be infected and will start to mine crypto-Currency for the attacker. As noticed drive-by downloads are becoming a widespread preference for cybercriminals to utilise in illegal crypto mining, and they find their grounds on extremely accessed websites such as YouTube, video sharing websites, torrents indexing websites or video editing web pages.

Cryptojacking First Appearances

Cryptojacking technique first debuted on September 2017, when a website known as Coinhaive released a code that facilitates crypto-miners to mine a specific cryptocurrency known as "Monero". This allowing the crypto-miners to mine online utilising the CPU resources thru a web

browser as indicated in the Threat Bulletin issued on May 2018 titled as "Cryptojacking" by the Allot, who is considered to be among the top companies which are specialised on intelligence and security solutions titled as "Cryptojacking" (Allot, 2018) Monero is an alternative cryptocurrency known by the ticker XMR, it has few renowned characteristics, as it is developed to be private, secure and untraceable cryptocurrency (Monero, 2017).That is an indication that Cryptojacking is still relatively new grounds, and yet to be further exploited by cybercriminals.

Cryptojacking Technique (the Infection & Spread)

Figure 2: Cryptojacking infection methods

From the way we understand crypto jacking it is the utilisation of victim's electronic resources without the consent of the user and leverage the processing power and graphical power (CPU&GPU) to mine cryptocurrency, there are two known methods adopted by cybercriminals in Cryptojacking. The following figure illustrates the process of Cryptojacking methods.

- **Drive-By download**

This technique executed via browser adds that infected with a malware code allowing the attacker to mine the victim's machine via the browser to mine crypto. The cybercriminals target websites that have vulnerabilities to run the mining scrip on the website and any visitor machine will be used to generate hash rates. Also known as the hash power, which considered as proof of work for the amount of power consumed to mine /generate a black within the subscribed mining pool, proof of work is the result of mathematical problems which is than reworded by a portion of cryptocurrency (Khatwani , 2018)

- **Drive by Mining**

Drive by mining referred to the concept of implementing or embedding a mining script on popular websites that have a high traffic footprint, in order to leverage all visitors machine to mine crypto. However, within this concept, it can be split intotwo subdomains, when the script itself is deployed by the website owner deliberately, or for two it can be done maliciously, without the consent or the

knowledge of the website owner, and in this case nor the visitor of the website.Few examples can be illustrated such as, pirate-bay a popular tormenting website site which have jumped on the idea of mining crypto from the visitors in order to generate some passive income to replace the dependency on advertisement to pay their bills. According to an article published by TorrentFreak, who is a publication dedicated to bringing the latest news about copyright, privacy, and everything related to file-sharing, have estimated the possibility of generating up to 12000$ Per Month (Ernesto, 2017)

Cryptojacking Threat Landscape Expansion

- **Computer Browser**

As it has indicated, crypto-mining started with scripts that can be deployed on websites and then through the browser the scripts start to leverage the device power to mine crypto, via utilising various vulnerabilities related to flash, java scripts and browser extensions (browser plugins that extend and enhance some functionality within the browser).

- **Mobile Cryptojacking**

Cybercriminals are making their mark on the mobile computing domain, as smart mobile phones make a great host to mining scripts due to the fact it always connected to the internet, constant power refill and above all mass adaptation from the general public makes it is a lucrative device to be exploited by hackers and cybercriminals. Subsequently, as Cybersecurity protection companies, such as Symantec and ESET, have released two reports in March 2018 indicating a significant increase in mobile crypto jacking, via infected websites and adds that utilise the device processor when a user opens the infected website on the mobile browser (Hio , 2018). Furthermore, an uprising malware based crypto started to surface, as researchers from Trend Micro have found out that former malware been undertaking few upgrades and capabilities including, the ability to redirect victims to referral websites that have injected with miner scripts, along with the ability to steal account credentials (Khandelwal, 2018)

- **Industrial Control Cryptojacking**

Cybercriminals have stumbled upon a gold mine when it comes to mining crypto. In order to mine faster, The miner will require a more powerful processor to be utilised to generate more power hash as proof of work. For that, the logical move for cybercriminals is to hunt for the organisation in which they host supercomputers to conduct their daily routine. Organisations which host industrial control systems considered as part of the critical national infrastructure, due to the criticality of its operation. Therefore cyber criminals shifted focuses to exploit such systems, and so they did when Radiflow, a provider of cyber security solutions for critical infrastructure, announced on the 8th Feb 2018 that the company had encountered the first crypto currency malware attack on industrial control system SCADA (Radiflow, 2018).It discovered as a part of the routine monitoring of operation technology network of water consumption. An analysis shows that such malware that runs a mining script, will result in increase on CPU and bandwidth consummation, that will result on slow responses to its original task and may cause critical delays in controls related to pumps, fans,

and other machinery that consciously will affect the reading's and outputs produced by Human Machine Interface (HMI). Many risks, is raised when successful malware can be deployed and ran on such a criticalsystem aslegit users will not be able to view or obtain accurate data transitorily. Also, updates related to operating system and protection might be compromised and therefore may cause fatal problems.

Legitimate Vs Malicious Mining

- **Legitimate mining**

Mining can be done legitimately via different sources, the whole idea of being able to mine legitimately is by utilising once own resources such as computers, mining grids or renting an online mining power rigs. Many individuals have been creative in ways to utilise old machines to mine cryptocurrency.

- **Malicious Mining**Since legitimate mining bound by the limited CPU power that the individual can utilise. Malicious hackers started to look for ways to leverage vulnerable devices to mining Cryptocurrency, and they have been very creative in resurrecting old malware or developing new once with crypto-Mining functionality added to it. This idea has created a shift in the malware industry as many malware developers started to develop their malware to mine crypto as it is considered far more beneficial than ransomware which is expected to fullback in the near future after a major spike during 2015-2018.

Conclusion

Although cryptojacking has been possible since Bitcoin's inception, it was not considered very profitable and was not very commonly observed with the exception a few large botnets. As a result, cryptojacking was not a subject of significant research or interest. There are several examples of cryptojacking affecting individuals, enterprises, and critical infrastructure. The method of infection, whether browser-based or compromise-based, determines the severity of consequences and potential harmful effects. We provide the systematic exposition Bitcoin and the many related cryptocurrencies . Drawing from a scattered body of knowledge, we identify key components of Bitcoin's design that can be decoupled. This enables a more insightful analysis of Bitcoin's properties and future stability.Moreover,this research reviewed the relevant literature related to cryptocurrency and cryptojacking to identify technical specifications.Cryptocurrency as a proof of concept has proved itself since the born of the bitcoin idea by Satoshi Nakamoto Paper titled Bitcoin: "*A Peer-to-Peer Electronic Cash System"* in 2008. Since then, the first cryptocurrency knew by bitcoin came to life, and slowly it gained momentum as more and more people started accepting the crypto-coin as a method of exchanging goods and services without relying on FIAT Money (legal tender defined by the government which issued it).However, only within the year 2017 bitcoin started peaking casing headlines widely around the globeand just like the gold rush bitcoin has become the most expansive crypto among others, which made cybercriminals interested in finding ways to generate, steal or mine cryptocurrency. Researchers expect that this review paper will

provide a holistic view to the body of knowledge and create awareness to protect individuals and organizations as well from this monetary loss.

Corresponding author:
Name:Mohammad Imtiaz Hossain
Address: Faculty of Economics and Management,UPM.43400, Serdang, Selangor, Malaysia.
Email:gs53627@student.upm.edu.my

References

Andrew, P. (2018, January 31). What is Proof of Capacity? An Eco-Friendly Mining Solution. *Coin Central.* Retrieved from: https://coincentral.com/what-is-proof-of-capacity/.

Allot, (2018).Threat Bulletin: Cryptojacking. *Allot.* Retrieved from: allot.com/wp-content/uploads/TB_Cryptojacking.pdf, US.

Bentov, I., Lee, C., Mizrahi, A., & Rosenfeld, M. (2014). Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake. *IACR Cryptology ePrint Archive*, *2014*, 452.

Curran, B. (2018, September 11). What is Proof of Elapsed Time Consensus? (PoET) Complete Beginner's Guide. *Blockonomi*. Retrieved from: https://blockonomi.com/proof-of-elapsed-time-consensus/.

Cowling, J., Myers, D., Liskov, B., Rodrigues, R., & Shrira, L. (2006, November). HQ replication: A hybrid quorum protocol for Byzantine fault tolerance. In *Proceedings of the 7th symposium on Operating systems design and implementation* (pp. 177-190). USENIX Association.

Curran, B. (2018, July 5). What is Proof of Authority Consensus? Staking Your Identity on The Blockchain. *Blockonomi*. Retrieved from : https://blockonomi.com/proof-of-authority/.

Ernesto (2017). How Much Money Can Pirate Bay Make From a Cryptocoin Miner?.*TF*. Retrieved from: https://torrentfreak.com/how-much-money-can-pirate-bay-make-from-a-cryptocoin-miner-170924/.

Gu, A. C. (2018, July 17). Move Over, Ransomware: Why Cybercriminals Are Shifting Their Focus to Cryptojacking. *Security Intelligence*. Retrieved from https://securityintelligence.com/move-over-ransomware-why-cybercriminals-are-shifting-their-focus-to-cryptojacking/.

Harper, C.(2018, January 24) "Making Sense of Proof of Work vs. Proof of Stake." *CoinCentral*. Retrieved from https://coincentral.com/making-sense-of-proof-of-work-vs-proof-of-stake/

Hio, L. (2018). Cybercriminals now cryptojacking mobile phones. *The Straits Times* Retrieved from.: https://www.reuters.com/article/us-cryptocurrency-cybercrime/cybercriminals-target-booming-cryptocurrencies-report-idUSKBN1FL5Q7.

InvestoPedia (2018).Proof of Stake (PoS). *InvestoPedia*. Retrieved from: https:// www.investopedia.com/terms/p/proof-stake-pos.asp.

Khatwani, S. (2018, October 10). What Is Coin Burn In Cryptocurrency: A Guide For Investors. *Coin Sutra*. Retrieved from: https://coinsutra.com/proof-of-burn/.

Khandelwal, S. (2018, May 01). A New Cryptocurrency Mining Virus is Spreading Through Facebook. *The Hacker News*. Retrieved from: https://thehackernews.com/2018/05/facebook-

cryptocurrency-hacking.html.

Lee, B. (2017, November 7). Unit 42 Report - Ransomware: Unlocking the Lucrative Criminal Business Model. *Palo Alto Networks*. CA, USA.Retrieved from
https://www.paloaltonetworks.com/resources/research/ransomware-report

Monero (n.d). Retrieved from: https://monero.org/.

Radiflow (2018, Februray 8). Radiflow Reveals First Documented Cryptocurrency Malware Attack on a SCADA Network. Retrieved from:
https://radiflow.com/radiflow-reveals-first-documented-cryptocurrency-malware-attack-on-a-scada-network/.

Rouse, M. (2017). *Techtarget.*Retrieved from : https://whatis.techtarget.com/definition/consensus-algorithm

Khatwani, S. (2018). Explaining Hash Rate Or Hash Power In Cryptocurrencies*. Coinsutra*. Retrieved from: https://coinsutra.com/hash-rate-or-hash-power/.

The Accounting Degree Review.(n.d). *blockchain_info2.* Retrieved from : https://cdn.accounting-degree.org/wp-content/uploads/2018/01/blockchain_info2.jpg.

Walters, S. (2018,April 6) . Proof of Activity Explained: A Hybrid Consensus Algorithm*. Coinbureau.* Retrieved from: https://www.coinbureau.com/blockchain/proof-of-activity-explained-hybrid-consensus-algorithm/.

Williams, B. (2018, April 24). What Exactly Is 'Cryptojacking', And How Can Businesses Respond To The Spiralling Cyber Threat?. *Isbuzznews* Retrieved from.:
https://www.informationsecuritybuzz.com/articles/what-exactly-is-cryptojacking/.