Blockchain, Crypto Mining, Cryptojacking - A Survey

Ashwin A[1]| Suriya K[2] | Nadesh S[3]

[1] - Rajalakshmi Institute of Technology - Kuthambakkam, Chennai, Tamil Nadu.
[2,3] -SRM Valliammai Engineering College - Kattankulathur, Kanchipuram, Tamil Nadu.

Abstract: ***Nowadays websites have traditionally used advertisements and pop ups to monetize services that are offered free of charge. When a user visits a website, the ad that displays on the website or the pop up that occurs while clicking anywhere in the website generates ad revenue for the website owners. This approach has been accompanied with a new monetization model named Cryptojacking where the website visitors' computational resources are used to mine cryptocurrencies for the handlers without the concern of the user. Cryptojacking is a type of cybercrime which involves use of people's devices (smartphone, laptop and desktop) to perform crypto mining on their device's background without giving the slightest hint. Crypto mining works on the concept called Blockchain where a complex mathematical equation is solved using computational power and the data is stored in a ledger. Like many other cyber attacks, the motive is profit but the main difference being that it is easy to set up the code in users' systems and hard to detect.***

Keywords: Cryptojacking, Crypto mining, Decentralization Blockchain, Ledger, SHA 256, Hashing.

1. Introduction:

It is no surprise that people prefer digital currency over paper currency. This momentum can be attributed to the convenience offered by digital transactions. There are various forms of digital currencies and one such form is the Cryptocurrency. Cryptocurrency is considered more as a digital asset that is spread across a number of computers. This decentralized structure allows them to bypass the third party entity which is often prevalent in other digital transactions. Cryptocurrencies hold the promise of making it easier to transfer funds directly between two parties, without the need for a trusted third party like a bank or credit card company. Bitcoin, Ethereum, Litecoin, Dogecoin, etc are some of the popular Cryptocurrencies with Bitcoin being the first ever Cryptocurrency, allowing digital transactions to be accurately calculated. Since the creation of Bitcoin in 2009, many other cryptocurrencies have hit the market: as of 2021, there are 6853 different types of cryptocurrency as per coinmarketcap. Along with the perks of investing in Cryptocurrencies also come new threats and risks. With Cryptocurrency gaining its momentum, cybercriminals have also shifted their focus from Ransomware attack to the latest cyberattack called Cryptojacking. Unlike Ransomware, where cybercriminals outright put-forth their demands, Cryptorjacking is carried out by unauthorized use of someone else's computer to mine cryptocurrency.

2. CryptoCurrency:

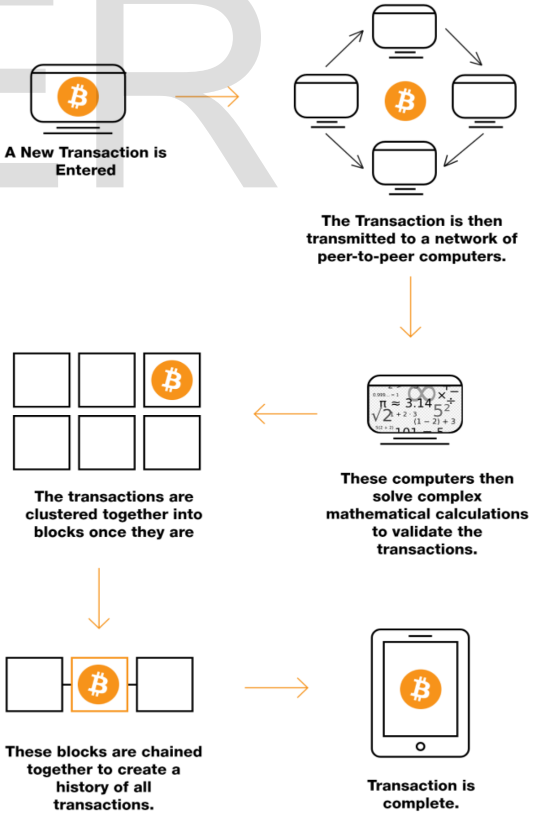
Cryptocurrency is a subtype of digital currency and the main difference being the concept of decentralization, making it easier to transfer funds directly between two parties, without the need for a trusted third party like a bank or credit card company. Cryptocurrency companies also use the concept of Blockchain to store the details of its customers. Bitcoin was the first cryptocurrency, allowing digital transactions to be accurately recorded. Since the creation of Bitcoin in 2009, many other cryptocurrencies have hit the market: as of 2021, there are 6853 different types of cryptocurrency as per coinmarketcap. Bitcoin, Etherium, LItecoin, Dogecoin are some of the familiar cryptocurrencies available in the market today.

2.1 Advantages of cryptocurrency over digital wallets

- Since transactions take place over a decentralized network, third party impediments like technical issues at the bank can be bypassed.
- Sometimes, organizations like banks may be subject to Distributed Denial of Service attacks where the servers may go down or identities of customers may be stolen while breaching the bank's database.
- Data is stored in blocks using the concept of Blockchains.

3. Blockchains

Blockchain can be defined as a chain of blocks that are interconnected and contain information of each transaction which uses a distributed database where each transaction that occurs on the Blockchain network is recorded on the public ledger. It differs from a typical database in the way it stores information; blockchains store data in blocks that are then chained together. For instance, if a transaction is made from one point of the world to another point of the world through a Blockchain, a block is created. This block enters the Blockchain network where the miners of the public ledger verifies this and adds the block to the network if it is legitimate. These miners are rewarded with cryptocurrency for validating each block. To tamper a block of information during encryption, it requires the tampering of the previous block as well. As a result, a lot of computational power and resources and electricity is required for maintaining the stability of the network chain. The block in a Blockchain comprises four components : data, previous hash, nonce, and hash. Data consists of aggregated details such as sender and receiver details and the amount of transaction that takes place. A block can have multiple transactions of data. Previous hash connects the current block with the previous block i.e which has the hash value of the previous block. Nonce is a random value generated by the Proof of work algorithm used to vary the output of the hash value. Proof of work algorithm is used to verify each transaction in a Blockchain. Hash is defined as the digital fingerprint of each block. Hash takes data, nonce and previous hash value as input and provides a 256 bit hash value as output. As new data comes in it is entered into a fresh block. Once the block is filled with data it is chained onto the previous block, which makes the data chained together in chronological order. Decentralized blockchains are immutable, which means that the data entered is irreversible.


A New Transaction is Entered
The Transaction is then transmitted to a network of peer-to-peer computers.
These computers then solve complex mathematical calculations to validate the transactions.
The transactions are clustered together into blocks once they are
These blocks are chained together to create a history of all transactions.
Transaction is complete.

4. Crypto Mining:

Crypto mining refers to the process of gaining cryptocurrencies by solving cryptographic equations with the use of high-power computers. The solving process comprises verifying data blocks and adding transaction records to a public record (ledger) known as a blockchain.

4.1 Process:

Mining is a tricky task to perform. For instance, Bitcoin mining uses cryptography, with a hash function called double SHA-256. A cryptographic hash function is an algorithm that takes an arbitrary amount of data input—a credential—and produces a fixed-size output of enciphered text called a hash value, or just "hash." That enciphered text can then be stored instead of the password itself, and later used to verify the user. Simply, A hash takes a portion of data as input and shrinks it down into a smaller hash value.With a cryptographic hash, there's no way to get a hash value you want without trying a whole lot of inputs. But once you find an input that gives the value you want, it's easy for anyone to authenticate the hash.Thus, cryptographic hashing has become a reliable way to moderate Mining.

5. Cryptojacking:

Cryptojacking is a cyberattack where a person's computer is used to mine cryptocurrency. Normally, mining a cryptocurrency requires a lot of computational resources and electricity. So, In crypto jacking where a malicious link is sent via a mail, clicking the link runs a crypto mining code or setting an ad trap in a website where a JavaScript code runs automatically on the victim's browser. The crypto mining code works in the background and it's hard to suspect. Only indication is the performance of the computer becomes slow or lags oftenly when executing or opening an application.

5.1 Working: There are two primary ways used by the hackers to breach into a victim's device to secretly mine cryptocurrencies:

- Malicious links - usually sent via email and once the victim opens the link, a crypto mining code is loaded in the computer.
- Malicious websites or online ads - once the site is loaded, a JavaScript code is auto-executed within milliseconds.

Both methods are preferred by hackers to maximize their return. The script runs complex mathematical problems as a script on the victim's device and sends the results to a server which is controlled by the hacker. Certain mining scripts affect other devices and servers that are connected to the same network because of the worming capabilities which makes them harder to find and remove. Once the script is loaded in a device it checks whether the device is already infected by any mining malware and if so, the script is disabled.

5.2 Effects :

Unlike other types of cyber attacks, there isn't any damage that is caused by cryptojacking scripts. Yes, they steal computer computational resources but for an individual user slower execution might be the only indication. It becomes a major issue if systems in organization are cryptojackted because it can incur real cost.

For instance:

- The use of help desk and IT time and resources spent tracking down performance issues and replacing systems or components in the hope of solving the problem.
- Increased electricity costs.

6. Recent Attacks:

- Eight different apps were removed from the Microsoft Store in 2019 for secretly mining cryptocurrencies with the resources of those who purchased them. The apps were allegedly created by three independent developers, but it was suspected that they were all created by the same person or organisation. The potential cryptojacking apps might be found through keyword searches in the Microsoft Store, as well as on lists of the best free apps. When a user downloaded and launched one of the apps, they would inadvertently download cryptojacking JavaScript code. The miner would turn on and begin seeking for Monero, consuming a large portion of the device's resources and slowing it down.

- Cryptojacking code was discovered hidden within the Homicide Report page of the Los Angeles Times in 2018. When people visited the Homicide Report page, their computers were used to mine Monero, a prominent cryptocurrency. Because the script consumed very little computer power, the threat went undetected for a long time, and many users were unaware that their machines had been compromised.

- A cryptojacking attack compromised over 200,000 MikroTik routers in Brazil in July and August 2018, injecting CoinHive code into a significant amount of web traffic.

- It was discovered in early 2018 that the CoinHive miner was running on YouTube Ads through Google's DoubleClick platform.

- The Prometei botnet, which dates back to 2016, is a modular and multi-stage botnet that is meant to mine the Monero cryptocurrency. It infects devices and spreads through networks using a variety of methods. However, Cybereason learned in early 2021 that Prometei was deploying malware and harvesting credentials by leveraging Microsoft Exchange vulnerabilities used in the Hafnium attacks. The botnet would then mine Monero on the infected devices.

7. Measures:

Browser Extensions:

Most of the scripts are distributed on the browser, therefore using some popular browser extensions such as minerBlocker, No Miner and Anti Miner can help you prevent it.

Ad Blocker:

Online ads are set as traps to install the mining code in the user computer, installing an ad blocker can be effective.

Disable JavaScript:

Disable javascript while browsing which can help to prevent cryptojacking code from infecting. The downside of disabling JavaScript is that it deters other basic functionalities possessed by most of the websites.

Spot Phishing Emails:

Sending malicious links via emails is considered to be the most effective way to trick the users. Educating the users to identify potentially harmful links is essential.

Check CPU Usage:

CPU usage can be monitored in the Task Manager. Websites that contain minimal media content do not use much CPU memory. When memory usage increases when using such websites, these are signs that cryptomining code may be running in the background.

8. References:

[1] M. King, J. Atkins, and M. Schwarz. Internet advertising and the generalized second-price auction: Selling billions of dollars worth of keywords. The American economic review, 97(1):242–259, 2007.

[2]G. Rydstedt, E. Bursztein, D. Boneh, and C. Jackson. Busting frame busting: a study of clickjacking vulnerabilities at popular sites. In IEEE SSP, volume 2, 2010.

[3]M. Rosenfeld. Analysis of bitcoin pooled mining reward systems. arXiv preprint arXiv:1112.4980, 2011.

[4] D. Y. Huang, H. Dharmdasani, S. Meiklejohn, V. Dave, C. Grier, D. McCoy, S. Savage, N. Weaver, A. C. Snoeren, and K. Levchenko. Botcoin: Monetizing stolen cycles. In NDSS, 2014.

[5] Z. Durumeric, D. Adrian, A. Mirian, M. Bailey, and J. A. Halderman. A search engine backed by Internet-wide scanning. In ACM CCS, Oct. 2015.

[6] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder. Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton University Press, 2016.

[7] CheckPointResearchTeam. October's most wanted malware: Cryptocurrency mining presents threat.https://blog.checkpoint.com/2017/11/13/octobers-wanted-malwarecryptocurrency-mining-presents-new-threat/, 2017.

[8] Coinhive. Coinhive monetize your business with your users cpu power. https://coinhive.com/, 2017. Accessed: 2017-11-20.

[9] Cryptonote. Cryptonote technology. https://cryptonote.org/inside.php#equal-proof-of-work, 2017. Accessed: 2017-11-20.

[10] DeepDotWeb. Coinhive hacked and launches newopt-inservice.https://www.deepdotweb.com/2017/11/11/coinhive-hackedlaunches-new-opt-service/, 2017. 24. https://twitter.com/badpackets/status/928044219222048769

[11] M. E. Acer, E. Stark, A. P. Felt, S. Fahl, R. Bhargava, B. Dev, M. Braithwaite, R. Sleevi, and P. Tabriz. Where the wild warnings are: Root causes of chrome https certificate errors. In CCS, CCS '17, pages 1407–1420, New York, NY, USA, 2017. ACM.

[12]European-Commission.Cookies. http://ec.europa.eu/ipg/basics/legal/ cookies/index en.htm, 2011. Accessed: 2017-12-08.

[13] ExtremeTech. Browser-based mining malware found on pirate bay, others. https://www.extremetech.com/internet/255971-browserbased-cryptocurrency-malware-appears-online-pirate-bay, 2017. Accessed: 2017-11-20.

[14] Fortune. Popular google chrome extension caught mining cryptocurrency on thousands of computers. http://fortune.com/2018/01/02/google-chrome-extension-cryptocurrency-mining-monero/, 2017. Accessed: 2018-01-20.

[15] BBC. Websites hacked to mint crypto-cash. http://www.bbc.com/ news/technology-41518351, 2017.

[16] BleepingComputer. The internet is ride with in-browser miners and it is getting worse each day. https://www.bleepingcomputer.com/news/security/the-internet-is-rife-with-in-browser-miners-and-itsgetting-worse-each-day/, 2012. Accessed: 2017-12-08.

[17] A. Kumar, C. Fischer, S. Tople, and P. Saxena. A traceability analysis of moneros blockchain. In European Symposium on Research in Computer Security, pages 153–173. Springer, 2017.

[18] LiveHelpNow. Security incident nov 23rd, 2017.https://blog.livehelpnow.net/security-incident-nov-23rd-2017/, 2017. Accessed: 2017-12-14.

[19].Monero. MONERO private digital currency. https://getmonero.org/, 2014. Accessed: 2017-11-20.

[20] A. Miller, M. Moeser, K. Lee, and A. Narayanan. An Empirical Analysis of Linkability in the Monero Blockchain. Technical report, arXiv, 2017.

[21] TheGuardian. Ads dont work so websites are using your electricity to pay the bills.https://www.theguardian.com/technology/2017/sep/27/pirate-bay-showtime-ads-websites-electricity-pay-billscryptocurrency-bitcoin, 2017. Accessed: 2017-11-20.

[22]TheVerge. Hotel caught injecting advertising into webpages on complimentary wi-fi network. https://www.theverge.com/2012/4/ 7/2931600/hotel-caught-injecting-advertising-into-web-pages-oncomplimentary-wi, 2012. Accessed: 2017-12-08.

[23] R. Tahir, M. Huzaifa, A. Das, M. Ahmad, C. Gunter, F. Zaffar, M. Caesar, and N. Borisov. Mining on someone else's dime: Mitigating covert mining operations in clouds and enterprises. In RAID, 2017.

[24] TheVerge. Showtime websites secretly mined user cpu for cryptocurrency. https://www.theverge.com/2017/9/26/16367620/showtimecpu-cryptocurrency-monero-coinhive, 2017. Accessed: 2017-11-20.

[25] T. Mursch. Cryptojacking malware coinhive found on 30,000+ websites. https://badpackets.net/cryptojacking-malware-coinhive-foundon-30000-websites/, 2017. Accessed: 2018-01-20.

[26] N. J. D. of Consumer Affairs. New jersey division of consumer affairs obtains settlement with developer of bitcoin-mining software found to have accessed new jersey computers without usersknowledgeorconsent.http://nj.gov/oag/newsreleases15/pr20150526b.html, 2015. Accessed: 2018-01-20.

[27] Opera. New year, new browser. opera 50 introduces antibitcoin mining tool. http://blogs.opera.com/desktop/2018/01/opera50-introduces-anti-bitcoin-mining-tool/, 2018. Accessed: 2018-01- 20.

[28] S. Ruwhof. Massive child porn site is hiding in plain sight, and the owners behind it. https://sijmen.ruwhof.net/weblog/1782-massivechild-porn-site-is-hiding-in-plain-sight-and-the-owners-behind-it, 2017. Accessed: 2018-01-20.

[29] T. Micro. Malvertising campaign abuses google's doubleclick to deliver cryptocurrency miners. https://blog.trendmicro.com/trendlabssecurity-intelligence/malvertising-campaign-abuses-googlesdoubleclick-to-deliver-cryptocurrency-miners/, 2018. Accessed: 2018-01-31

[30] TheRegister. Cbs's showtime caught mining crypto-coins in viewers' web browsers. https://www.theregister.co.uk/2017/09/25/showtime hit with coinmining script/, 2017. Accessed: 2018-01-20.

[31] TheRegister. Crypto-jackers enlist google tag manager to smuggle altcoin miners. https://www.theregister.co.uk/2017/11/22/cryptojackers google tag manager coin hive/, 2017. Accessed: 2018-01-20.

[32] TheRegister. Uk ico, uscourts.gov... thousands of websites hijacked by hidden crypto-mining code after popular plugin pwned. https://www.theregister.co.uk/2018/02/11/browsealoud compromised coinhive/, 2018. Accessed: 2018-02-28.

[33] NakedSecurity. Unsecured aws led to cryptojacking attack on la times. https://nakedsecurity.sophos.com/2018/02/27/unsecured-awsled-to-cryptojacking-attack-on-la-times/, 2018. Accessed: 2018-02- 28.

[34] WallStreetJournal. Your computer may be making bitcoin for hackers. https://www.wsj.com/articles/hackers-latest-move-using-yourcomputer-to-mine-bitcoin-1509102002, 2017. Accessed: 2018-01- 20.

[35] Washingtonpost. Hackers have turned politifact's website into a trap for your pc. https://www.washingtonpost.com/news/theswitch/wp/2017/10/13/hackers-have-turned-politifacts-website-intoa-trap-for-your-pc, 2017. Accessed: 2018-01-20.

[36] S. Varlioglu, B. Gonen, M. Ozer, and M. F. Bastug, "Is cryptojacking dead after coinhive shutdown?" arXiv:2001.02975, 2020.

[37] AV-Comparatives, "Malware protection test march 2019," https: //www.av-comparatives.org/tests/malware-protection-test-march2019/, accessed: 2020-11-05.

[38] C. Davenport, "Opera mini and mobile now block cryptocurrencymining scripts," https://www.androidpolice.com/2018/01/22/opera-mini-mobile- now- block-cryptocurrency-mining-scripts/, accessed: 2020-10-16.

[39] T. Spring, "Cryptominer, winstarnssmminer, has made a fortune by brutally hijacking computers," https://blog.360totalsecurity.com/en/cryptominer-winstarnssmminer-made-fortune-brutally-hija cking-computer/, accessed: 2021-2-23.

[40] Palo-Alto-Networks, "Hildegard: New teamtnt cryptojacking malware targeting kubernetes," https://unit42.paloaltonetworks.com/ hildegard-malware-teamtnt/, accessed: 2021-02-26.