Mining Monero on Raspberry Pi

Ayyaz Akhtar
Department of Cybersecurity
New York University
New York, USA
aia7143@nyu.edu

***Abstract*—The research aims to prove that a cheap hardware can provide competitive computation hash rates by using Raspberry Pis to mine Monero on a mining pool. These Raspberry Pis will need to take advantage of fast CPU instructions to perform computation. Having cheap hardware allows anyone to join and can help mitigate a 51% attack.**

Keywords—Cryptocurrency, Mining, Monero, Operating System, Distributed computing.

I. Introduction

The problem domain will focus on privacy blockchain protocols. Blockchain has many use cases, but some popular coins such as Bitcoin will display every transaction on the public ledger, which can be analyzed to find patterns and eventually unmask an individual.

Some coins such as Monero (XMR) has a unique protocol with privacy in mind. This shift can allow shady actors a safe place for nefarious purposes, but it will also provide a new system unlike it before for users that want their digital transactions complete hidden from any entity. These entities can be the one of the many three letter agencies, but also data brokers from identifying patterns in the public ledger.

Another unique feature of XMR is that evens out the playing field for participating in the decentralized system protocol. This is achieved by not gatekeeping the hardware requirements, essentially anyone can mine or help validate transitions without buying expensive hardware. In addition, mining pools can be used to aggregate the entire pool resources and share the rewards amount the group.

A distributed network can still allow bad actors by performing a 51% attack. Which is when a user or group becomes the majority in a blockchain protocol. This can lead to operations be skipped or altered and destroying the confidentiality, integrity, and availability of the system.

In section 2, some information on related research will overlap with the research in this study. Section 3 will provide details on how this study will be conducted on a pi cluster. In section 4, the hypothesis about the experiment is explained with metrics. In section 5, the paper will provide conclusions and next steps.

II. Related Research

A. *Monero mining: CryptoNight Analysis*

The study by Konstantinidis [1] goes over many blockchain and Monero concepts. A focus highlights the crypto night protocol. This protocol purpose is to allow any CPU available to mine cryptocurrency mining, this is intended to be ASIC Poof of work resistant. The prevents a high a single owner of expensive ASIC mining hardware control the network. Using this context here was helpful in using raspberry pi, which are inexpensive computers the size of a credit card.

B. *Enterprise security assessment framework for cryptocurrency mining based on monero*

The article by Bissaliyev et al. [2] focus on mitigating unauthorized usage of computation for mining cryptocurrency in enterprise environments. The analysis highlighted power consumption, web resources, and network logs. The research here differs in that it focusses more on monitoring and detection tools of mining in a network.

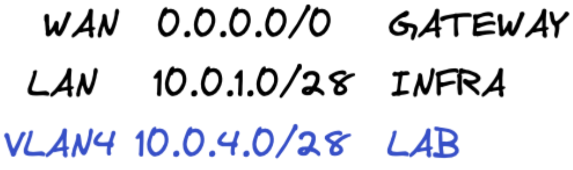
C. *Monero usage and mining from usable security point of view*

The research conducted by Lipovčan [3] focuses on user experience of a miner and crypto holder. Surveys were conducted to identify best practices for key management, backups, miner operations, deployment, and secure usage. These techniques that were surveyed from users and miners provided a trove of information to use this coin in the most native and smart way.

III. Motivating Example

For this research, there will be 5 Raspberry Pis setup as a cluster to join a mining pool. The software to compute hashes and communicate with the network will be installed through kubernetes. This flexible installation will provide even more isolation of the protocol usage and configurations to tweak performance.

The segmented network topology is configured to allow network isolation and privacy to interact with the network mining pool protocol. The purpose here is to mine a privacy cryptocurrency by remaining private using cyrpto technologies.



WAN	0.0.0.0/0	GATEWAY
LAN	10.0.1.0/28	INFRA
VLAN4	10.0.4.0/28	LAB

Fig. 1. Segmented Networks for security and isolation.

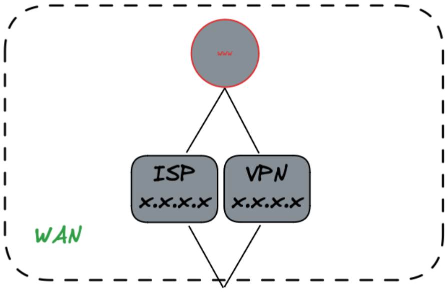


Fig. 2. Private Internet Access to mining pool

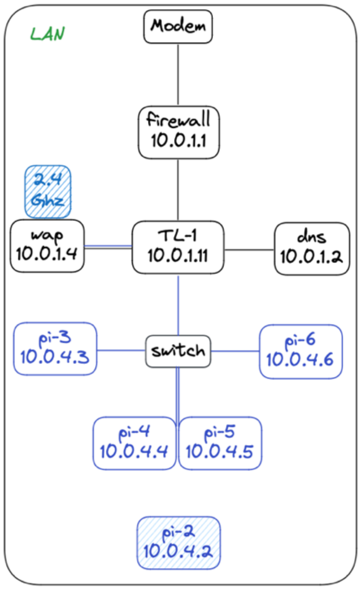


Fig. 3. LAN Physical and Logical diagram of Cluster of Pi

IV. Hypothesis and Empirical Evidence

This study plans to show a Raspberry Pi cluster with optimized software will output a higher Monero (XMR) hash rate in a mining pool compared to a mis configuration of software settings. The findings will show that cheap hardware can mitigate a 51% attack by outputting competitive hash rates.

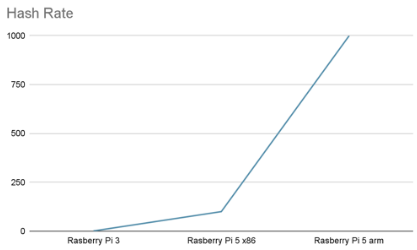


Fig. 4. Hash rate of three different configurations of raspberry pi

The hash rate fluctuated, but the average was identified as the following. Raspberry Pi 3 is very old hardware and not competitive due to resources constraints. However, the newer hard Raspberry Pi 5 is a massive upgrade is resources, jumping from 1 GB to 8 GB RAM. Packaging the software to be compact and native to ARM architecture vastly improved its hash rate by over 1,000%. At its peak it doubled its average to 2,000% percent.

Node	Hash Rates	x Increase
Min	1 H/s	x 1,000
16 cores = $280	1 KH/s	X 1
Median	4 KH/s	x 4
Mean	100 KH/s	x 100
Max	50 MH/s	x 50,000
Pool	300 MH/s	x 300,000
Network	2.5 GH/s	x 2,500,000

Table. 1. Summary of hash rates

V. Conclustions and Future Work

The conclusion of the results shows that the raspberry pi has drastically improved its hash rate by upgrading its hardware and using native software architecture.

The following steps would be to research what is the cost of electricity to mine on the hardware. Another area is of research is how compare earnings as a solo miner.

References

[1] O. Konstantinidis, “Monero mining: CryptoNight Analysis,” M.S. thesis, Dept. Informatics and Telecommunications, National and Kapodistrian Univ. of Athens, Athens, Greece, 2022.

[2] M. S. Bissaliyev, A. T. Nyussupov, and S. Zh. Mussiraliyeva, “Enterprise security assessment framework for cryptocurrency mining based on monero,” Journal of Mathematics, Mechanics and Computer Science, vol. 98, no. 2, pp. 67-76, 2018.

[3] B. R. Lipovčan, “Monero usage and mining from usable security point of view,” unpublished.

[4] S. A. Thyagarajan, G. Malavolta, F. Schmid, and D. Schröder, “Verifiable Timed Linkable Ring Signatures for Scalable Payments for Monero,” in *Computer Security – ESORICS 2022*, V. Atluri, R. Di Pietro, C. D. Jensen, and W. Meng, Eds. Cham, Switzerland: Springer, 2022, vol. 13555, Lecture Notes in Computer Science, pp. 469-487. doi: 10.1007/978-3-031-17146-8_23.

[5] O. Konstantinidis, “Monero mining: CryptoNight Analysis,” M.S. thesis, Dept. Informatics and Telecommunications, National and Kapodistrian Univ. of Athens, Athens, Greece, 2022.

https://stream.nyu.edu/media/Mining%20Monero%20on%20Raspberry%20Pi/1_fcb6q12m