Performance of Raspberry Pi during Blockchain Execution using Proof of Authority Consensus

J. A. Guerra[1][a], J. I. Guerrero[1,2][b], A. Gallardo[1][c], D. F. Larios[1,2][d] and C. León[1][e]

[1]Department of Electronic Technology, EPS, Universidad de Sevilla, 41011 Sevilla, Spain
[2]Department of Electronic Technology, ETSII, Universidad de Sevilla, 41012 Sevilla, Spain

Keywords: Blockchain, Internet of Things, Benchmark, Raspberry Pi, Proof of Authority.

Abstract: Raspberry Pi is one of the most popular devices for research in many different fields. It is proposed to analyse its performance as a lightweight blockchain node. This could enable the Raspberry Pi to execute other tasks and the same time, like data acquisition or working as an Internet of Things node, without losing performance. To achieve this, a specific consensus protocol is used to light the processing load. This testbed is evaluated in several benchmarks, whose results clarify the limits of this device as a lightweight blockchain node.

1 INTRODUCTION

Blockchain technology has become one of the most promising technologies in the last decade (Zheng, Xie, Dai, Chen, & Wang, 2018). In fact, every month appears news about emerging blockchain networks or their associated cryptocurrencies and related business (Kimani, et al., 2020). Furthermore, the use of blockchain as a digital ledger has created a set of technological solutions for issues such as traceability, confidence, or data integrity (Maesa & Mori, 2020).

In this sense, from the original Bitcoin blockchain to today, the deployment of the blockchain network has been heterogeneous. It is possible to develop nodes for different blockchains on many different devices, depending on how the blockchain client is deployed. From the computer to specific devices such as an application-specific integrated circuit (ASIC), mobile phones, or even Raspberry Pi, blockchain exists in many different devices with different performance (Ding, Wang, Wan, & Zhou, 2020).

One of the most popular devices worldwide, Raspberry Pi, is commonly used with lightweight blockchain clients as a blockchain node, in networks that do not require heavy network traffic. For applications like those, this device has enough performance to work properly.

Unfortunately, most scenarios are related to work under ideal conditions. It is possible that with all nodes in the blockchain network running, the number of transactions (Tx) and the execution of Smart Contracts (SCs) cause the device to saturate and not function properly. Due to the properties of the blockchains related before, this would not cause a data loss, but it would affect the performance of the entire network (Buccafurri, Lax, Nicolazzo, & Nocera, 2017).

In this contribution, the performance of a Raspberry Pi is studied on a specific blockchain, trying to maximize its performance, and guessing how many transactions this device can process before a failure. Because of this, the blockchain network has been carefully chosen, with a custom genesis block and an alternative consensus protocol. Performance has been measured by benchmarking the execution of an SC over the blockchain network.

[a] https://orcid.org/0000-0002-7845-4446
[b] https://orcid.org/0000-0003-3986-9267
[c] https://orcid.org/0000-0003-1720-0298
[d] https://orcid.org/0000-0002-4309-6028
[e] https://orcid.org/0000-0002-0043-8104

Guerra, J., Guerrero, J., Gallardo, A., Larios, D. and León, C.
Performance of Raspberry Pi during Blockchain Execution using Proof of Authority Consensus.
DOI: 10.5220/0011119300003179
In *Proceedings of the 24th International Conference on Enterprise Information Systems (ICEIS 2022) - Volume 1*, pages 287-292
ISBN: 978-989-758-569-2; ISSN: 2184-4992

2 BACKGROUND

The uses of a Raspberry Pi for blockchain are strongly related to the Internet of Things (IoT). In (Xhafa, Kilic, & Krause, 2020) the performance of this device is used to create an infrastructure for data streaming using edge computing. Another use of Raspberry Pi is as a high-capacity sensor to implement some applications on it (Gasull, Larios, Barbancho, León, & Obaidat, 2012).

The authors in (Zhang, Srinivasan, & Ganesan, 2021) propose the use of a Raspberry Pi as a hub to measure ten air quality metrics from different sensors. Other uses of the device as a data processor refer to health, as the electroencephalogram shows in (Dhillon, et al., 2021), where Raspberry Pi is used to data acquisition, signal processing, and feature extraction, to obtain key metrics in the field of Traumatic Brain Injury. But Raspberry Pi and blockchain are specifically related to the integration of the Raspberry Pi as an IoT device and a blockchain node (Tsang, Wu, Ip, & Shiau, 2021).

There are examples where the authors used blockchain as an access control to the IoT platform, such as (Zhang, Kasahara, Shen, Jiang, & Wan, 2019). In other cases, it is used as a marketplace for energy trading (Guerra, et al., 2022). A close reference to this contribution was made by (Suzen, Duman, & Sen, 2020), where the authors analyse Raspberry Pi and other devices by testing under a convolutional neural network.

(Qahtan, et al., 2022) proposes a benchmark to evaluate blockchain networks in healthcare industry systems, to guarantee security and privacy, based on weighting different criteria. Unfortunately, it is not related to an existing device, but to the blockchain itself.

Proof of Authority has become a revolution for blockchain in devices with lower performance in network data sharing (Javed, et al., 2020), or secure sharing of health data using SCs (Gürsoy, Brannon, & Gerstein, 2020) or even managing the own blockchain using machine learning (Sajid, et al., 2022). Therefore, the limits of this consensus protocol with such popular hardware as Raspberry Pi are essential.

3 BLOCKCHAIN

Blockchain is a technology that could be explained from a technological point of view, oversimplifying, as a distributed and decentralized ledger. These are two of the main properties any blockchain has (Wust & Gervais, 2018). Also, in any blockchain, the data recorded on the blockchain network preserve its integrity. It is almost impossible to modify a blockchain register and also to tamper with it and introduce rogue data. The blockchain is modelled as a chain of blocks. A block is a set of transactions between nodes, the participants in the network. When transactions reach a certain amount, it is recorded in a block by a node, with some metadata and security information. Then, some nodes in the network verify, using hash functions, that the information inside the block is correct. If it is, the node is propagated to the network and linked to the last block in the chain before this.

This method needs some security protocol to ensure that a node is not writing wrong data in a block. Apart from verifying it afterwards, all nodes have a kind of competition to write a block. This is managed by different algorithms, called consensus algorithms. Each consensus algorithm has its own way to make all nodes compete to finish a block, so that the node that is the chosen one has something to offer in return. This could be executing difficult cryptographic algorithms, showing the node publicly to the network, reserving a large amount of disk space, staying connected with no fails waiting its turn, and so on.

As can be guessed from above, the complete identity of the nodes is private to the rest of the network. That is, all node has a pair of public and private keys to identify each one. The public key is known for all the network, it is public, and it is possible to search for all data transferred from or to a particular node. But it is difficult to identify a node only from its public key, and even more difficult to forge it. This is the sense of the private key that allows to sign and approve Tx from or to the node.

But the blockchain would not be as useful without Smart Contracts. SCs are pieces of executable code inside the blockchain. This allows us to run code using data inside the blockchain and save it on the same network. These SCs are deterministic, since several steps must be done until the end of execution. It implies that two executions of the same Smart Contract with the same input data result in the same output data. Thus, this contribution research not only sends or receives Tx, but executing them inside an SC.

The use of SCs opens the blockchain technology to external data from many different sources (Zheng Z. , et al., 2020). Before, the use of SCs is restricted to the data inside the network. Now, with the help of external applications, such as oracles, it is possible to use application programming interfaces (APIs) to obtain data outside the blockchain and manage inside it (Lin, Zhang, Li, Ji, & Sun, 2022).

3.1 Integration of IoT and Blockchain

IoT and blockchain seem to be two technologies with great differences. IoT is intended to send only a few messages in concrete time windows when the sensors send data. On the other hand, blockchain is a technology that requires continuous synchronization between all nodes if they want to participate in the process of creating blocks. Despite this, the combination of the two technologies results in important benefits:

- Data immutability. As in IoT data is acquired and is needed to guarantee its quality, blockchain allows data to be saved with security on the blockchain. In fact, it is possible to record with security the data close to the point where the data were generated if there was a device that works both as an IoT node and as a blockchain node.
- Data replication. All nodes in the blockchain contain, partially or totally, the whole chain of transactions. Thus, this guarantees that data uploaded to the blockchain network cannot be lost or deleted accidentally.
- Data security. In the blockchain, all recorded transactions are hashed data, not the data itself. Therefore, the hashed data are public for all nodes in the blockchain network, and it is almost impossible to obtain the original data from the hashed one.
- Data availability. Due to data replication, recorded data uploaded to the blockchain network are available at any time. Only if all nodes that contain the whole chain fail at the same time the availability of the data could be compromised.

These are some of the properties that provide the integration of IoT and blockchain, and why it has been the basis of important research recently. If a device would act at the same time as an IoT node and a blockchain node, it would be possible to guarantee all these properties. This device should be placed to close as data generation, where it might not be possible to place an industrial computer or a specialized blockchain device.

To overcome this challenge, one solution is to use a device with lower performance acting as an IoT hub, acquiring data from different sensors and, at the same time, a node of a lightweight blockchain. Therefore, devices such as the Raspberry Pi, with good performance in relation to its size and consumption, are suitable for these tasks.

4 TESTBED

The device used as a testbed for this contribution is a Raspberry Pi 4 (RP4). Raspberry Pi is a set of different low-cost general-purpose devices. In this case, Raspberry Pi 4, the most powerful single board of all of them, is used. It is developed using an ARM-based central processing unit (CPU) with 4 GB of random access memory (RAM). This tiny device is powered by less than 10W, with 7.5W as its power peak. One of the main advantages of using this device is that it has a worldwide community and is relatively inexpensive, so multiple applications are developed for this popular device.

For the testbed, another RP4 with the same specs is used, as two nodes of a blockchain network.

Due to the ARM architecture the RP4 has, the selection of the optimal blockchain network has been restricted. Most of the blockchain clients that support this specific architecture are based on Ethereum or Hyperledger. For maturity, support, and customization possibilities, an Ethereum client programming in Go, called Geth, has been used. It is installed on an Ubuntu server operating system (OS), to use the Geth native install for this OS. Regarding hardware, the RP4 has a thermal pad and a fan over the GPU, to delay or even avoid any possibility of throttling.

Geth has two possible consensus protocols: ethash, based on Proof of Work (PoW), or clique, based on Proof of Authority (PoA). PoW is the original and most extended (Gervais, et al., 2016) blockchain consensus algorithm, which allows all nodes in the network to reach consensus and guarantee the truth of the information in each block. This algorithm is based on solving a cryptographical problem that uses as many computational capabilities as a device has to solve it. On the other hand, PoA is based on the reputation each node has on the network. This reputation allows nodes to vote for another node as the node that will complete a block, in exchange for showing it to the network to watch it. To make RP4 as lightweight as possible and to be able to use it as an IoT node or other purpose at the same time if necessary, clique has been chosen as the consensus protocol.

Apart from that, some changes have been made to the genesis block. The genesis block is the first block of any blockchain and the only one that has no link to the previous block. So, there is a different way to create it. It is also responsible for other parameters of the network that cannot be changed once it is generated. To obtain the best performance of the RP4, the genesis block has been generated with the minimum parameters required. In addition, these parameters have been optimized to create a blockchain as lightweight as possible.

5 RESULTS

It is created a network of two RP4 with a geth node in each one, connected over a local network. This network is private, provided by a router and isolated from any Internet connection. This is made to simulate an industrial behavior, where sensitive data is aisled from the main network. Both nodes have been created using the same genesis block and have the same inner parameters. To allow nodes to verify blocks, both nodes have been created as signer nodes in the clique protocol.

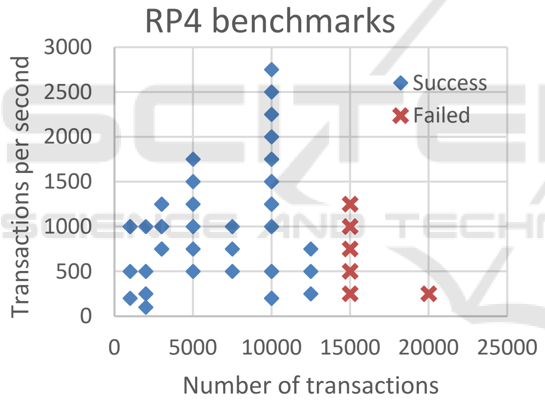

Figure 1: Benchmark execution results.

To measure RP4 performance over a massive execution of SCs it is used Hyperledger Caliper. It is an open-source tool to create benchmarks that are compatible with Ethereum-based blockchains. As both nodes are identical, the benchmarks have been executed on one of them. The benchmarks have been executed using an example of a complete SC. It has declarations, structures, mapped variables, events, and functions inside it, in over 70 lines of code using Solidity language. The SC have been deployed using Truffle, a blockchain deployment tool, and injected into one of the nodes while the blockchain is running.

Before the execution of the benchmarks, the blockchain has no other Tx on it. Thus, the only Tx to be executed over the network will be due to the benchmark. Tens of benchmarks have been triggers, with variability in the total number of Tx to execute and in the number of Tx per second to send to the node. In case a transaction fails, defined as at least one transaction has not been recorded in the blockchain network, both nodes have been reset. This avoids carrying errors from previous benchmarks. Figure 1 shows the results of all these benchmarks.

It is possible to evaluate more benchmarks with a higher TPS / Tx ratio, but it does not make sense to send more TPS than the total Tx. On the other hand, as PoA is used to avoid high processing on the device, higher TPS than the studied are avoided.

From the results obtained, the main limitation is the amount of Tx. This is closely related to the number of Tx that RP4 can store as pending to run. Therefore, a higher TPS rate is not studied, as it implies higher Tx. At the time that there is too many Tx pending, the RP4 is unable to process that and starts to fail Tx. Table 1 shows the main statistics from the benchmark with ten thousand Tx and more than 1500 TPS.

Table 1: Main indicators of the highest benchmarks for ten thousand Tx.

TPS	Average Latency (s)	Throughput (TPS)	CPU average (%)
1500	54.96	56.5	71.01
1750	58.97	52.6	68.02
2000	68.98	43.5	65.06
2250	81.05	38.5	60.48
2500	104.89	31.9	58.43
2750	105.47	31	59.26

As is shown, latency is directly related to the number of TPS, although throughput decreases as the TPS increases. This explains why the RP4 is not able to process a larger number of Tx on the same benchmark. In detail, the decreases CPU load average slightly when TPS increases, due to the queue of Tx pending to be processed by the RP4.

5 CONCLUSSIONS AND FUTURE RESEARCH

RP4 is a very versatile device that can be used as a lightweight blockchain node. It is possible to use it in applications that do not require a high and constant Tx rate. It is shown that the RP4 can afford almost three thousand TPS for some seconds. So, in applications with only a few executions of Smart Contracts each minute, the device is optimal for it, like logistics or data integrity.

This research is only a first step to use all the performance of the RP4. It is certain that these results would be enhanced with a specifically programming consensus protocol instead of the one implemented in Geth. Another option would be to use racks of RP4 as a single node and try to parallelize the execution of SCs, trying to maximize throughput and minimize CPU load. This would be able to address the data processing to the device with less CPU usage.

However, probably the main advantage of knowing the limits of RP4 in blockchain is using it at the same time as an IoT node. It is, as IoT implies acquiring and /or recording data at a certain time windows, it is possible to restrict certain time windows for IoT processing, and other time windows for the execution of SCs in the blockchain, without losing performance of the RP4.

ACKNOWLEDGEMENTS

This research was supported by the Block of Things for Factory (BoT4F) project funded by the Fondo Europeo de Desarrollo Regional FEDER a través del Programa Interreg V-A España-Portugal (POCTEP) 2014–2020.

REFERENCES

Breland, D. S., Skriubakken, S. B., Dayal, A., Jha, A., Yalavarthy, P. K., & Cenkeramaddi, L. R. (May de 2021). Deep Learning-Based Sign Language Digits Recognition From Thermal Images With Edge Computing System. IEEE Sensors Journal, 21, 10445–10453. doi:10.1109/jsen.2021.3061608

Buccafurri, F., Lax, G., Nicolazzo, S., & Nocera, A. (2017, August). Overcoming Limits of Blockchain for IoT Applications. Proceedings of the 12th International Conference on Availability, Reliability and Security. ACM. doi:10.1145/3098954.3098983

Dhillon, N., Sutandi, A., Vishwanath, M., Lim, M., Cao, H., & Si, D. (April de 2021). A Raspberry Pi-Based Traumatic Brain Injury Detection System for Single-Channel Electroencephalogram. Sensors, 21, 2779. doi:10.3390/s21082779

Ding, L., Wang, S., Wan, R., & Zhou, G. (2020, November). Securing core information sharing and exchange by blockchain for cooperative system. 2020 IEEE 9th Data Driven Control and Learning Systems Conference (DDCLS). IEEE. doi:10.1109/ddcls49620.2020.9275195

Gasull, V. G., Larios, D. F., Barbancho, J., León, C., & Obaidat, M. S. (2012). A Wildfire Prediction Based on Fuzzy Inference System for Wireless Sensor Networks. En E-Business and Telecommunications (págs. 43–59). Springer Berlin Heidelberg. doi:10.1007/978-3-642-35755-8_4

Gervais, A., Karame, G. O., Wüst, K., Glykantzis, V., Ritzdorf, H., & Capkun, S. (October de 2016). On the Security and Performance of Proof of Work Blockchains. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. ACM. doi:10.1145/2976749.2978341

Guerra, J. A., Guerrero, J. I., García, S., Domínguez-Cid, S., Larios, D. F., & León, C. (February de 2022). Design and Evaluation of a Heterogeneous Lightweight Blockchain-Based Marketplace. Sensors, 22, 1131. doi:10.3390/s22031131

Gürsoy, G., Brannon, C. M., & Gerstein, M. (2020, June). Using Ethereum blockchain to store and query pharmacogenomics data via smart contracts. BMC Medical Genomics, 13. doi:10.1186/s12920-020-00732-x

Javed, M. U., Rehman, M., Javaid, N., Aldegheishem, A., Alrajeh, N., & Tahir, M. (March de 2020). Blockchain-Based Secure Data Storage for Distributed Vehicular Networks. Applied Sciences, 10, 2011. doi:10.3390/app10062011

Kimani, D., Adams, K., Attah-Boakye, R., Ullah, S., Frecknall-Hughes, J., & Kim, J. (2020, December). Blockchain, business and the fourth industrial revolution: Whence, whither, wherefore and how? Technological Forecasting and Social Change, 161, 120254. doi:10.1016/j.techfore.2020.120254

Lin, S.-Y., Zhang, L., Li, J., Ji, L.-l., & Sun, Y. (2022, January). A survey of application research based on blockchain smart contract. Wireless Networks. doi:10.1007/s11276-021-02874-x

Maesa, D. D., & Mori, P. (April de 2020). Blockchain 3.0 applications survey. Journal of Parallel and Distributed Computing, 138, 99–114. doi:10.1016/j.jpdc.2019.12.019

Qahtan, S., Yatim, K., Zaidan, A. A., Alsattar, H. A., Albahri, O. S., Zaidan, B. B., Mohammed, R. T. (2022). Novel Multi Security and Privacy Benchmarking Framework for Blockchain-Based IoT Healthcare Industry 4.0 Systems. IEEE Transactions on Industrial Informatics, 1–1. doi:10.1109/tii.2022.3143619

Sajid, M. B., Ullah, S., Javaid, N., Ullah, I., Qamar, A. M., & Zaman, F. (2022, January). Exploiting Machine Learning to Detect Malicious Nodes in Intelligent Sensor-Based Systems Using Blockchain. (A. Basit, Ed.) Wireless Communications and Mobile Computing, 2022, 1–16. doi:10.1155/2022/7386049

Suzen, A. A., Duman, B., & Sen, B. (June de 2020). Benchmark Analysis of Jetson TX2, Jetson Nano and Raspberry PI using Deep-CNN. 2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA). IEEE. doi:10.1109/hora49412.2020.9152915

Tsang, Y. P., Wu, C. H., Ip, W. H., & Shiau, W.-L. (March de 2021). Exploring the intellectual cores of the blockchain–Internet of Things (BIoT). Journal of Enterprise Information Management, 34, 1287–1317. doi:10.1108/jeim-10-2020-0395

Wust, K., & Gervais, A. (2018, June). Do you Need a Blockchain? 2018 Crypto Valley Conference on Blockchain Technology (CVCBT). IEEE. doi:10.1109/cvcbt.2018.00011

Xhafa, F., Kilic, B., & Krause, P. (April de 2020). Evaluation of IoT stream processing at edge computing layer for semantic data enrichment. Future Generation Computer Systems, 105, 730–736. doi:10.1016/j.future.2019.12.031

Zhang, H., Srinivasan, R., & Ganesan, V. (January de 2021). Low Cost, Multi-Pollutant Sensing System Using Raspberry Pi for Indoor Air Quality Monitoring. Sustainability, 13, 370. doi:10.3390/su13010370

Zhang, Y., Kasahara, S., Shen, Y., Jiang, X., & Wan, J. (April de 2019). Smart Contract-Based Access Control for the Internet of Things. IEEE Internet of Things Journal, 6, 1594–1605. doi:10.1109/jiot.2018.2847705

Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: a survey. International Journal of Web and Grid Services, 14, 352. doi:10.1504/ijwgs.2018.095647

Zheng, Z., Xie, S., Dai, H.-N., Chen, W., Chen, X., Weng, J., & Imran, M. (April de 2020). An overview on smart contracts: Challenges, advances and platforms. Future Generation Computer Systems, 105, 475–491. doi:10.1016/j.future.2019.12.019