

ANÁLISIS DE CONSUMO ENERGÉTICO DE REDES BLOCKCHAIN EN DISPOSITIVOS EMBEBIDOS DE BAJO CONSUMO

Javier Antonio Guerra Coronado*, **Juan Ignacio Guerrero Alonso**, **Samuel Domínguez Cid**, **Daniel Fernández Valderrama**, **Diego Francisco Larios Marín** y **Carlos León de Mora**
Departamento de Tecnología Electrónica, Escuela Politécnica Superior, Universidad de Sevilla, Sevilla.

E-mail de correspondencia*: jgcoronado@us.es

RESUMEN

Se presenta un estudio para la integración de dispositivos embebidos IoT (Internet of Things), que son capaces de gestionar la información proveniente de sensores de forma eficiente con un mínimo coste computacional, con la tecnología Blockchain, que permite garantizar la veracidad de los datos, generalmente a cambio de un alto coste computacional. Se analiza una red Blockchain ejecutada sobre IoT, así como las variables que definen la capacidad que tiene dicha red para almacenar la información, y su consumo energético.

INTRODUCCIÓN

La cantidad de información que se obtiene hoy día por dispositivos interconectados es realmente grande y crece continuamente, hasta llegar a la estimación de 20 mil millones de dispositivos conectados para 2020 (Gartner, 2017), aunque esto no ha podido ser contrastado, en parte por la situación sanitaria mundial. Generalmente IoT hace referencia a dispositivos de bajo consumo, prestaciones y específicos, diseñados para comunicarse entre ellos y con los usuarios.

Así, uno de los retos de la industria está siendo la implantación de IoT, dando lugar a la denominada Industria 4.0, convirtiendo el término IoT en Industrial IoT o IIoT. Se estima que IIoT permitirá la comunicación entre distintas máquinas de una industria de forma precisa, constante y segura. Para ello, IIoT puede apoyarse en tecnologías como Blockchain (Sisinni *et al.*, 2018). Este trabajo aborda una comparativa del consumo energético y de la velocidad de ejecución de dispositivos IIoT ejecutando redes Blockchain.

BLOCKCHAIN

La funcionalidad Blockchain se puede simplificar como un libro de contabilidad digital, donde la información no puede ser eliminada o modificada, usando algoritmos criptográficos que permiten a los nodos Blockchain generar un bloque

mediante funciones de hash, que son complicadas de calcular, pero sencillas de comprobar (Bellare, Canetti, y Krawczyk, 1996). Como los hashes permiten mantener la integridad de la Blockchain, será la variable para evaluar: cuanto mayor sean los hashes por segundo, más rápidamente se generará un nuevo bloque.

PROBLEMÁTICA

Una red Blockchain es una red compleja, que consume muchos recursos, exigiendo además constante comunicación entre ellos. Por otra parte, IoT se diseña para consumir poca energía, se comunican de forma intermitente y tienen prestaciones pequeñas. Por tanto, ambas tecnologías parecen ser incompatibles.

SOLUCIÓN PROPUESTA

Instrumental

En este trabajo, se analizará el consumo energético de los dispositivos de la Figura 1 ejecutando Blockchain:

- Raspberry Pi 4 (RPi): conocida placa de desarrollo multipropósito. Tiene un pico máximo de potencia de 15 W.
- Nvidia Jetson TX2 (TX2): placa de desarrollo optimizada para operaciones de aprendizaje automático, con una unidad de procesamiento gráfico, con un consumo máximo de 90 W.



Figura 1. Raspberry Pi 4 y Jetson TX2.

Se ha utilizado en ambos dispositivos el programa Geth (Ethereum, 2020), un cliente de la red Ethereum escrito en Go. Como sistema operativo se ha utilizado Ubuntu Server para la RPi, y Ubuntu Desktop para la TX2. Para ambos dispositivos se ha medido el cálculo de Hashes por segundo y su consumo energético. Para el

cálculo de Hashes por segundo se ha utilizado la consola de Geth, mientras que para el consumo se ha utilizado un dispositivo externo que ejecutaba un algoritmo programado en Python para calcular el consumo.

Con respecto a la obtención de los datos se han tomado muestras cada décima de segundo, durante un minuto. Posteriormente, se ha dejado pasar unos minutos y se ha vuelto a muestrear durante más de un minuto. Tras realizar este proceso de forma iterativa durante un período superior a una hora, se ha comprobado que el cálculo de hashes por segundo es prácticamente constante una vez la red Blockchain está en producción.

Resultados

Se observa que la potencia consumida durante la ejecución de la Blockchain para el cálculo de hashes es prácticamente constante, y además con un valor bastante más bajo del máximo teórico. De forma aproximada, la RPi consume un 40% de los 15 W su potencia máxima, valor que se reduce hasta menos del 10% en la TX2.

Sin embargo, el cálculo de hashes de la TX2, entorno a los 85 kH/s, que casi duplica al de la RPi (unos 50 kH/s). Esta diferencia de rendimiento se agudiza más cuando se utilizan clientes optimizados para la TX2, como Ethminer (Lanfranchi, 2020), con rendimientos superiores a los 300 kH/s consumiendo en torno a 7.5 W.

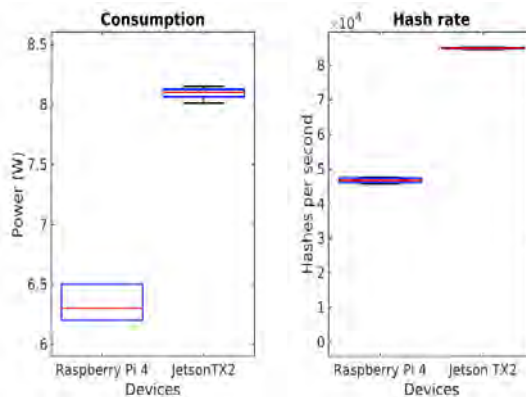


Gráfico 1. Resultados experimentales.

CONCLUSIONES

Aunque los resultados de esta comparativa muestran una clara ventaja de la TX2 sobre la RPi, este último dispositivo cuenta con dos puntos importantes a su favor: las funciones hash son paralelizables, por lo que se podrían colocar varios dispositivos y

distribuir el coste computacional de la función hash entre ellos. Segundo, la RPi tiene un coste del orden de 10 veces más económico que la TX2.

Si la red Blockchain va a tener pocos dispositivos IoT conectados, seguramente sea más interesante utilizar la TX2. Sin embargo, si el número de dispositivos aumenta, será necesario un análisis más minucioso, para decidir cuál es la arquitectura óptima.

Estos resultados permiten plantear la realización de una arquitectura multicapa, donde parte del cálculo se realice en servidores, y otra parte en una capa más próxima a los sensores IoT, acercando la computación al origen del dato, con objetivo de minimizar la manipulación de los datos antes de ser almacenados. Este modelo, llamado estructuras Multi-access Edge Computing o MEC (Shahzadi *et al.*, 2017), también disminuye la cantidad de información que se transmite a través de este, por lo cual se considera una arquitectura a investigar en profundidad en estudios posteriores.

REFERENCIAS BIBLIOGRÁFICAS

- Bellare, M., Canetti, R., y Krawczyk, H.** (1996). Keying Hash Functions for Message Authentication. *Advances in Cryptology — CRYPTO '96* (pp. 1–15). Springer Berlin Heidelberg. https://doi.org/10.1007/3-540-68697-5_1
- Ethereum.** (2020, 22 de noviembre). *Go Ethereum*. <https://geth.ethereum.org/>
- Gartner.** (2017). *Leading the IoT*. https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf
- Lanfranchi, A.** (2020, 23 de noviembre). *Ethminer*. <https://github.com/ethereum-mining/ethminer>
- Shahzadi, S., Iqbal, M., Dagiuklas, T., y Qayyum, Z. U.** (2017). Multi-access edge computing: open issues, challenges and future perspectives. *Journal of Cloud Computing*, 6(1). <https://doi.org/10.1186/s13677-017-0097-9>
- Sisinni, E., Saifullah, A., Han, S., Jennehag, U., y Gidlund, M.** (2018). Industrial Internet of Things: Challenges, Opportunities, and Directions. *IEEE Transactions on Industrial Informatics*, 14(11), 4724–4734. <https://doi.org/10.1109/tii.2018.2852491>