

SERVERUS: LA IMPLEMENTACIÓN DEL BLOCKCHAIN EN LA VIDA COTIDIANA

SERVERUS: THE IMPLEMENTATION OF BLOCKCHAIN IN EVERYDAY LIFE

José Rubén Ruelas Amézquita

Tecnológico Nacional de México en Celaya
rubenamesz@gmail.com

Enrique Salazar Baez

Tecnológico Nacional de México en Celaya
enriquesalazarbaez@outlook.com

José Guillermo Martínez Manríquez

Tecnológico Nacional de México en Celaya
jos.guillermo@gmail.com

Mauro Santoyo Mora

Tecnológico Nacional de México en Celaya
mauro.santoyo@itcelaya.edu.mx

Salvador Manuel Malagón Soldara

Tecnológico Nacional de México en Celaya
salvador.malagon@itcelaya.edu.mx

Ángel Cárdenas León

Tecnológico Nacional de México en Celaya
cardenas.leon.angel@gmail.com

Gilberto González Gómez

Tecnológico Nacional de México en Celaya
gilberto.gonzalez@itcelaya.edu.mx

Resumen

Mucho se ha hablado en los últimos años sobre la industria 4.0, sin embargo, fue hasta hace poco que se implementó realmente tanto en la industria, como en la vida cotidiana. Este término se le ha acuñado al uso de tecnologías como sistemas ciberfísicos (Samaniego & Deters, 2016), a la cultura maker (cultura Hágalo usted mismo), a la manufactura automatizada, al servicio al cliente con el uso de Inteligencia artificial (bots), al internet de las cosas y al blockchain, donde

este último, ha demostrado un gran potencial con innumerables aplicaciones que todavía se siguen desarrollando. Su principal uso ha sido en el intercambio de criptomonedas tales como el Bitcoin, Ethereum, entre otras cerca de 1900 criptomonedas que diariamente mueven en el mercado cerca de 12 mil MDD. Por otro lado, el intercambio de dinero no es la única aplicación que tiene el blockchain, por mencionar algunas, se tienen: registro de propiedades, almacenamiento en la nube, redes privadas de intercambio de información, identidad digital para mejor control de información, gestión de autorías, y en general, cualquier contrato que pueda hacerse físicamente. Serverus es un servicio de transmisión de datos y encriptamiento con implementación de tecnología blockchain, que puede ser aplicado en el uso personal, la administración de recursos en MiPymes, además de poder programarse en redes más robustas de seguridad informática gubernamental. Este servicio se destaca por buscar el impulso de la tecnología de punta en México, generando una cultura diferente ante el inminente cambio en la gestión de data digitales en la industria, la oficina y la vida doméstica.

Palabras Clave: blockchain 3.0, Ethereum, industria 4.0, privacidad.

Abstract

In recent years it has been talked a lot about 4.0 industry, however, it was until recently that it was really implemented as in industry as in everyday life. This term has been coined to the use of technologies such as cyberphysical systems (Samaniego & Deters, 2016), maker culture (Do-it-yourself culture), automated manufacturing, customer service with the use of artificial intelligence (Bots), IoT and blockchain. The latter which has shown great potential with innumerable applications that are still being developed. It's main use has been in the exchange of cryptocurrency such as the famous Bitcoin, Ethereum, among around other 1900 cryptocurrencies that daily move in the market about 12 thousand MDD. On the other hand, money exchange is not the only application that Blockchain has; to name a few, there are: property registry, cloud storage, information interchange private networks, digital identity for better control of information, authorship

management and, in general, any contract that can be done physically. Serverus is a data encryption and transmission service with the implementation of blockchain technology, which can be applied to personal use, resource management in MiPymes, besides allowing it's programming in robuster networks. This service stands out for seeking the momentum of cutting-edge technology in Mexico, generating a different culture before the imminent change of digital data management in the industry, office and domestic life.

Keywords: *blockchain 3.0, Ethereum, Industry 4.0, privacy.*

1. Introducción

Blockchain es un sistema descentralizado y distribuido (figura 1), capaz de realizar intercambio de datos (información, archivos, contratos, adjudicaciones o transacciones) a través de una red de dispositivos conectados entre sí (Gatteschi, Lamberti, Demartini, Pranteda, & Santamaría, 2018). En él, cada usuario de la red puede verificar los datos, utilizando algoritmos propios del mismo sistema, con lo cual, se puede garantizar la transparencia de cada movimiento. El intercambio de información dentro de una red de este tipo se lleva a cabo de manera segura y privada (Crosby, Nachiappan, Pattanayak, Verma, & Kalyanaraman, 2016), gracias a sus características, la cuales incluyen:

- Validación por consenso.
- Agrupación en cadena.
- Inmutabilidad.
- Información distribuida y replicada.
- No falsificable.
- Conservación del historial.
- Accesibilidad privada, pública o por consorcio.

Serverus (figura 2) es una red privada de intercambio de información basada en la blockchain de Ethereum, con lo cual adquiere la flexibilidad de ofrecer servicios tales como SmartContract, BackUp, comunicación segura entre dispositivos, transacciones monetarias y almacenamiento en la nube.

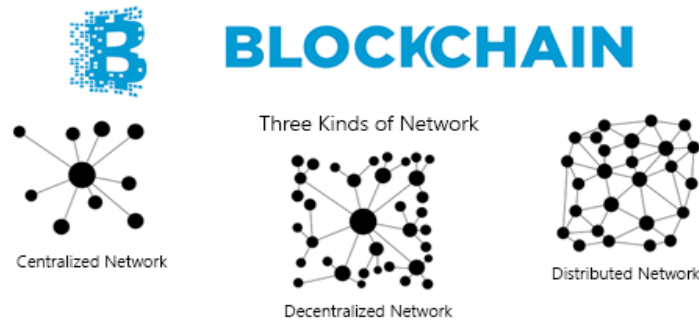


Figura 1 Tipos de distribución de redes.



Figura 2 Logotipo del proyecto SERVERUS.

La finalidad del proyecto es transformar algunos de los procesos que se realizan en la vida cotidiana, con vista hacia un mejor futuro donde se garantice que la seguridad de los datos personales esté al alcance de todos.

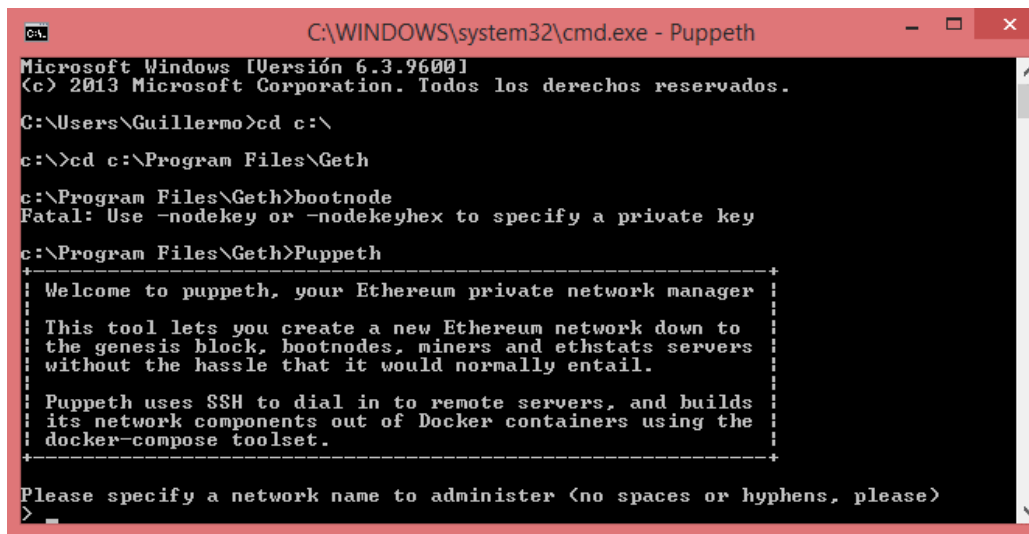
2. Métodos

Dentro de la institución a la cual pertenece el grupo de trabajo, se tiene un gran número de computadoras y dispositivos, las cuales, durante todo el día se mantienen intercambiando datos personales. Todos estos datos tienen información valiosa que debería tener un método de seguridad, además tener la capacidad de conectar todos estos ordenadores a una sola red, ya que actualmente, se tienen muchas subredes que dividen a toda la comunidad. Teniendo todo esto en cuenta, este grupo de trabajo buscó la manera de crear una red basada en blockchain, que fuera versátil y flexible para satisfacer las necesidades de la institución, y dando un plus aprovechando los demás servicios que ofrece la red. Por dicha razón, se prosiguió a elegir la cadena de bloques de

Ethereum. Para realizar dicha red, se recurrió a la interfaz de línea de comandos Geth, ejecutando un nodo Ethereum implementado en Go.

Para comenzar una red en blockchain, primero fue necesario crear el nodo “Genesis” (primer bloque de la cadena, sin predecesor) e inicializar nuestra cadena de bloques, para posteriormente arrancar la cadena privada y conectar la consola de administración en la cual se parametrizó (figura 3). Dicha configuración incluye:

- *config*: La configuración del *blockchain*
- *chainId*: Protección contra ataque por repetición (un usuario no autorizado que actúa como el remitente original). Por ejemplo, si una acción se valida al hacer coincidir cierto valor que depende de la identificación de la cadena, los atacantes no pueden obtener fácilmente el mismo valor con una ID diferente.



```
C:\WINDOWS\system32\cmd.exe - Puppeth
Microsoft Windows [Versión 6.3.9600]
(c) 2013 Microsoft Corporation. Todos los derechos reservados.

C:\Users\Guillermo>cd c:\
c:\>cd c:\Program Files\Geth
c:\Program Files\Geth>bootnode
Fatal: Use -nodekey or -nodekeyhex to specify a private key
c:\Program Files\Geth>Puppeth
-----
| Welcome to puppeth, your Ethereum private network manager |
| This tool lets you create a new Ethereum network down to |
| the genesis block, bootnodes, miners and ethstats servers |
| without the hassle that it would normally entail.         |
| Puppeth uses SSH to dial in to remote servers, and builds |
| its network components out of Docker containers using the |
| docker-compose toolset.                                   |
-----
Please specify a network name to administer (no spaces or hyphens, please)
>
```

Figura 3 Caracterización de algunos parámetros de la red.

- *homesteadBlock*: Homestead es el segundo lanzamiento importante de *Ethereum* (el primer lanzamiento es *Frontier*).
- *epi155Block*: “epi” significa Propuesta de Mejora Ethereum (traduciendo sus siglas al español), donde los desarrolladores proponen ideas sobre cómo mejorar *Ethereum* y contribuir a este proyecto.

- *difficulty*: Dificultad de minería. Establecer este valor bajo para que no tenga que esperar demasiado tiempo para los bloques de minería.
- *gasLimit*: El límite del costo del gas por bloque. Establece este valor alto para evitar ser limitado cuando se prueba.
- *alloc*: Dirección prefinanciada, el primer parámetro de cada uno es la dirección. Necesita ser una cadena hexadecimal de 40 dígitos (160 bit, un dígito hexadecimal es 4 bit).

El proceso completo descrito por las instrucciones anteriores se muestra en el diagrama de flujo de la figura 4.

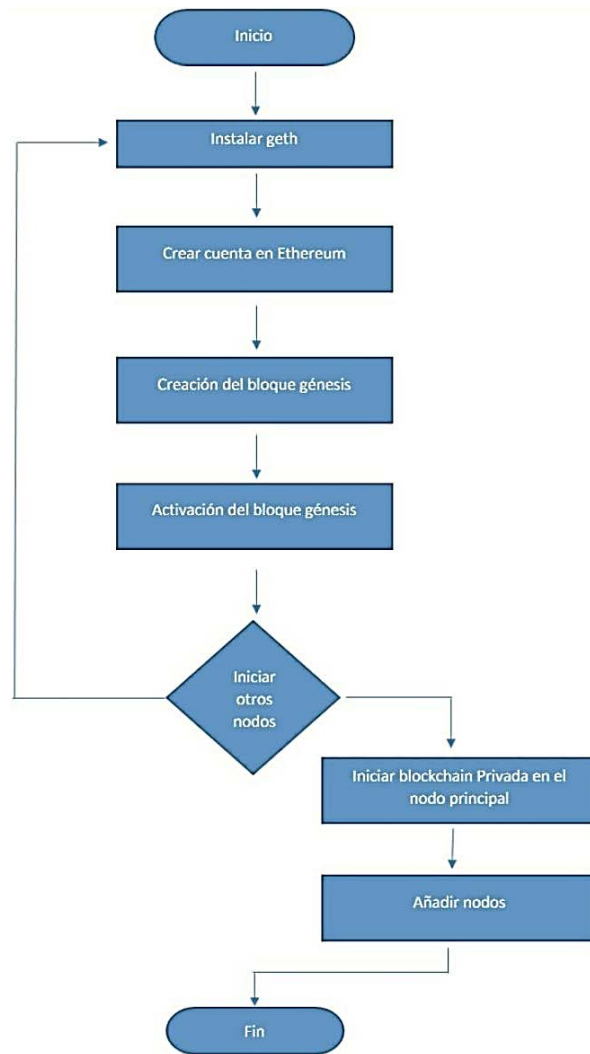


Figura 4 Diagrama de flujo de la elaboración de Serverus.

3. Resultados

Después de identificar las necesidades de los usuarios de la red, investigar las distintas opciones, elegir minuciosamente la mejor opción, y finalmente implementarla, se logró llegar al objetivo principal; el óptimo desarrollo de una red privada basada en la cadena de bloques de Ethereum, como se muestra en la figura 5.

```

C:\> Símbolo del sistema - geth
[INFO [09-13:14:56:07.384] Allocated cache and file handles database="C:\Users\Red Mustang\AppData\Roaming\Ethereum\geth\chaindata" cache=768 handles=1024
[INFO [09-13:14:56:09.211] Initialised chain configuration config="{ChainID: 1 Homestead: 115000 DAO: 192000 DAOsupport: true EIP150: 246300 EIP155: 267500 EIP158: 267500 Byzantium: 437000 Constantinople: <nil> Engine: ethash}"
[INFO [09-13:14:56:09.222] Disk storage enabled for ethash caches dir="C:\Users\Red Mustang\AppData\Roaming\Ethereum\geth\ethash" count=3
[INFO [09-13:14:56:09.237] Disk storage enabled for ethash DAGs dir="C:\Users\Red Mustang\AppData\Ethash" count=2
[INFO [09-13:14:56:09.244] Initialising Ethereum protocol versions="[63, 62]" network=1
[INFO [09-13:14:56:09.258] Loaded most recent local header number=8064 hash=0eb9b4.e63109 td=1287906912014888
[INFO [09-13:14:56:09.264] Loaded most recent local full block number=0 hash=d4e567.cb8fa3 td=17179869184
[INFO [09-13:14:56:09.270] Loaded most recent local fast block number=7886 hash=d02fd1.24c916 td=1211083532471761
[INFO [09-13:14:56:09.320] Loaded local transaction journal transactions=0 dropped=0
[INFO [09-13:14:56:09.326] Regenerated local transaction journal transactions=0 accounts=0
[INFO [09-13:14:56:09.370] Starting P2P networking
[INFO [09-13:14:56:11.674] UDP listener up self=enode://e612cd62ac9032533be3c3da0ebf83005f8d5f07c6fcf8832cd6718a8baa90b898c384a177985306ce77f6370953a82305b723d907c5a3fca1ddd4a327f1990[::1:30303]
[INFO [09-13:14:56:11.686] RLPx listener up self=enode://e612cd62ac9032533be3c3da0ebf83005f8d5f07c6fcf8832cd6718a8baa90b898c384a177985306ce77f6370953a82305b723d907c5a3fca1ddd4a327f1990[::1:30303]
[INFO [09-13:14:56:11.756] IPC endpoint opened url=\\.\pipe\geth.ipc
[INFO [09-13:14:57:01.706] Block synchronisation started
[INFO [09-13:14:57:32.663] Imported new block headers count=14 elapsed=4.208s number=8078 hash=92c6ee.ae14a3 ignored=178
[INFO [09-13:14:57:35.186] Imported new block receipts count=9 elapsed=983.9µs number=7895 hash=38d907.4d322b size=1.11kB ignored=0
[INFO [09-13:14:57:35.228] Imported new block receipts count=9 elapsed=0s number=7904 hash=567978.061c2f size=36.00B ignored=0
[INFO [09-13:14:57:38.282] Imported new block receipts count=67 elapsed=1.000ms number=7971 hash=14b23f.28f051 size=2.43kB ignored=0
[INFO [09-13:14:57:38.315] Imported new block receipts count=1 elapsed=0s number=7972 hash=7caca9.9204a2 size=4.00B ignored=0
[INFO [09-13:14:57:39.792] Imported new block receipts count=64 elapsed=1.000ms number=8036 hash=2c0c31.f504ch size=3.49kB ignored=0
[INFO [09-13:14:57:41.645] Imported new block receipts count=7 elapsed=0s number=8043 hash=e32c18.03497a size=28.00B ignored=0
[WARN [09-13:14:57:52.303] Node data write error de f88745.e628f2 failed with all peers (0 tries, 0 peers)" err="state no
[WARN [09-13:14:57:52.304] Rolled back headers count=14 header=8078->8064 fast=8043->8043 block=0->0
[INFO [09-13:14:57:52.304] Imported new block receipts count=35 elapsed=1.000ms number=8078 hash=92c6ee.ae14a3 size=2.84kB ignored=0
[INFO [09-13:14:57:52.310] Imported new state entries count=199 elapsed=1.001ms processed=13213 pending=846 retry=0 duplicate=0 unexpected=0
[WARN [09-13:14:57:52.327] Synchronisation failed, retrying err="receipt download canceled (requested)"
    
```

Figura 5 Arranque exitoso de la red privada (minado de información).

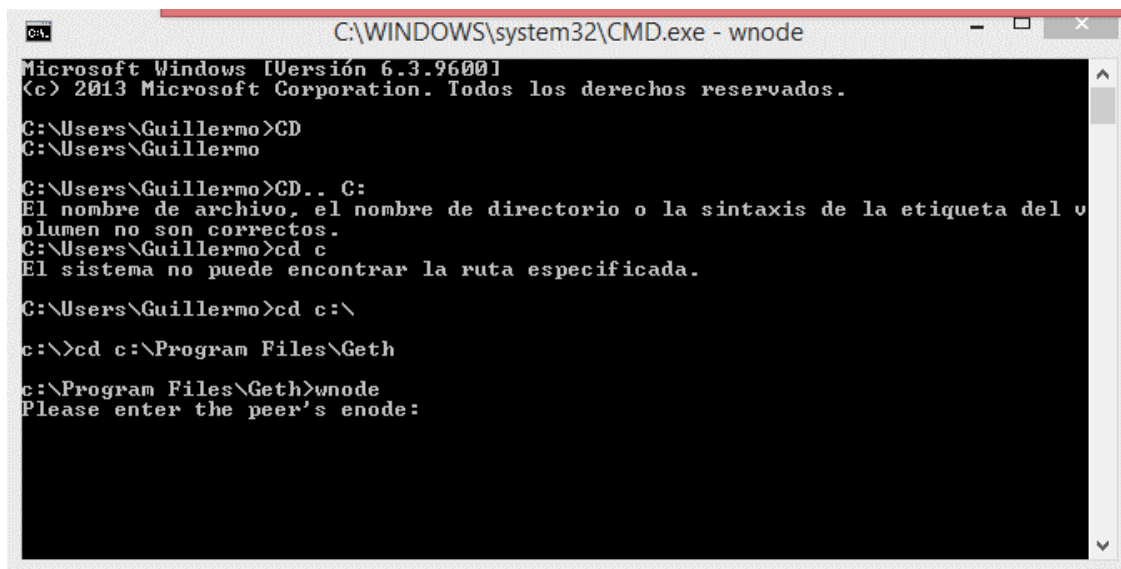
El alma del proyecto radica en el uso de los distintos dispositivos conectados a través de la red, los cuales reciben el nombre de “nodos”. Estos se dividen principalmente en 4 vertientes principales:

- Nodo “Genesis”.
- Nodos públicos.

- Nodos administrativos.
- Nodos de servicio.

Estos “nodos” son los encargados de mantener en operación la cadena de bloques, sin embargo, ninguno es indispensable para su correcto funcionamiento gracias a su arquitectura distribuida y descentralizada.

Al final, se lograron conseguir los resultados esperados e inclusive detectamos la posibilidad de escalar la red desarrollada agregando tantos nodos como sea necesario (figura 6), y aún más importante, es posible implementar la tecnología en tantas aplicaciones como se ha manifestado anteriormente, ya sea en la industria, oficinas o en un ambiente doméstico.



```
C:\WINDOWS\system32\CMD.exe - wnode
Microsoft Windows [Versión 6.3.9600]
(c) 2013 Microsoft Corporation. Todos los derechos reservados.

C:\Users\Guillermo>CD
C:\Users\Guillermo

C:\Users\Guillermo>CD.. C:
El nombre de archivo, el nombre de directorio o la sintaxis de la etiqueta del v
olumen no son correctos.
C:\Users\Guillermo>cd c
El sistema no puede encontrar la ruta especificada.

C:\Users\Guillermo>cd c:\
c:\>cd c:\Program Files\Geth
c:\Program Files\Geth>wnode
Please enter the peer's enode:
```

Figura 6 Asociación de nodos a la nueva red.

4. Discusión

Si bien en las últimas décadas la tecnología cada vez está más cerca de nosotros, la realidad que se vive actualmente en nuestra sociedad es un tanto contrastante, ya que desafortunadamente en nuestro país los avances tecnológicos suelen demorar unos años en llegar. Lo que se busca con Serverus es acercar la tecnología Blockchain al sector privado, gubernamental y

principalmente a la sociedad; aprovechando las aplicaciones que tiene, tales como:

- Transacciones de cryptodivisas.
- Intercambio de información de manera segura.
- Smart contracts.
 - ✓ Contratos empresariales.
 - ✓ Licitaciones.
- Registro de datos.
 - ✓ Contabilidad.
 - ✓ Derechos de autor.
 - ✓ Patentes.
 - ✓ Historial médico.
- Almacenamiento en la nube.
- Respaldo de información.

Empresas como IBM, Nasdaq (mercado bursátil), Master Card, BBVA, Banco Santander y Microsoft utilizan este tipo de tecnologías, sin embargo, en México son pocas las empresas y organizaciones que la utilizan por la escasa cantidad de proyectos. Aunado a esto, como ya se mencionaba, los pocos proyectos como Blockchain HackMx se enfocan principalmente al sector gubernamental, limitando el acceso a las empresas, MiPymes y a la sociedad, contribuyendo al crecimiento de la brecha tecnológica que se vive.

5. Bibliografía y Referencias

- [1] Crosby, M., Nachiappan, Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). BlockChain Technology: Beyond Bitcoin. *Applied Innovation Review (AIR)* (2), 6-19.
- [2] Ethereum Foundation. (2018). Build unstoppable applications. Obtenido de Ethereum Blockchain App Platform: <https://www.ethereum.org/>.
- [3] Miller, D. (2018). Blockchain and the Internet of Things in the Industrial Sector. (IEEE, Ed.) *IT Professional*, 20(3), 15-18.

- [4] Gatteschi, V., Lamberti, F., Demartini, C., Pranteda, C., & Santamaría, V. (2018). To Blockchain or Not to Blockchain: That Is the Question. (IEEE, Ed.) *IT Professional*, 20 (2), 62-74.
- [5] Samaniego, M., & Deters, R. (2016). Blockchain as a Service for IoT. 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). Chengdu, China: IEEE.