Blockchain y *smart contract* para la trazabilidad de las donaciones

Rossy Espinoza / Carlos Ugaz

En la actualidad, una organización que administra donaciones tiene dificultades para controlar el flujo de ingreso y salida de donativos, dificultando la trazabilidad de estos. En esta investigación se propone un sistema basado en *blockchain* que garantice la trazabilidad de los donativos desde su origen hasta su destino, utilizando un protocolo de consenso *proof of work* y un contrato inteligente (*smart contract*) con funciones específicas.

Blockchain and Smart Contract for Traceability of Donations

At present, an organization that administers donations has difficulties in controlling the inflow and outflow of such donations, hindering their traceability. This research proposes a blockchain-based system that guarantees the traceability of donations from their origin to their destination, using a proof of work consensus protocol and an intelligent contract with specific functions.

BLOCKCHAIN Y *SMART CONTRACT* PARA LA TRAZABILIDAD DE LAS DONACIONES

Rossy Espinoza
20131797@aloe.ulima.edu.pe

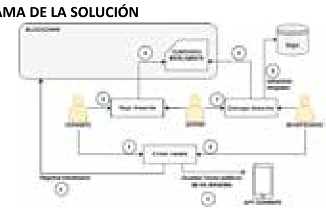
Carlos Ugaz
20131349@aloe.ulima.edu.pe

RESUMEN: En la actualidad, las organizaciones que administran donaciones tienen inconvenientes para controlar el flujo de ingreso y salida de donativos, dificultando la trazabilidad de estos. En esta investigación se propone un sistema basado en *blockchain* que garantice dicha trazabilidad, desde su origen hasta su destino, utilizando un protocolo de consenso *proof of work* y un contrato inteligente (*smart contract*) con funciones específicas.

INTRODUCCIÓN

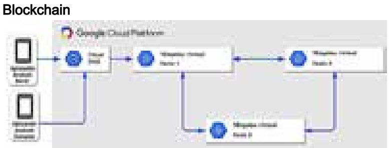
- Falta de control de donaciones, pues ninguna organización de gestión de donaciones cuenta con un sistema exclusivo para el donante que le permita realizar la trazabilidad a sus donativos.
- El grupo Servir, de la Universidad de Lima, carece de un sistema de control de flujos.
- Se plantea la creación de un sistema basado en *blockchain* con la integración de un contrato inteligente (*smart contract*) que permita la implementación de validaciones y restricciones en la gestión de los donativos, para permitir la trazabilidad de estos.

DIAGRAMA DE LA SOLUCIÓN



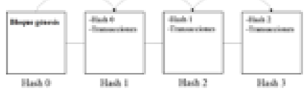
MÉTODOS

Blockchain



Arquitectura del blockchain

Protocolo de consenso



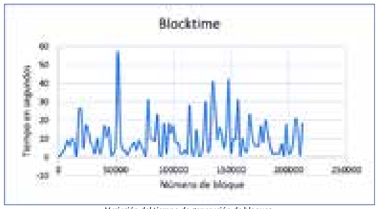
Proof of work

Funciones del contrato inteligente (*smart contract*)

- Crear usuario.
- Crear donación.
- Enviar donación.
- Obtener usuario.
- Obtener donación.

RESULTADOS

Blockchain



Variación del tiempo de generación de bloques

Trazabilidad

Al momento de registrar una donación se crea una transacción en la que se almacena la llave pública del donante y la del grupo Servir, y al enviar la donación, la transacción que se efectúa contiene esa llave pública tanto de Servir como del beneficiario.

#	Transacción	Origen	Destino	Hash
1	Crear donación	[illegible]	[illegible]	[illegible]
2	Enviar donación	[illegible]	[illegible]	[illegible]

Transacciones realizadas para verificar la trazabilidad

Aplicativo

Responsable	Escenario	Resultado
Donante	Crear cuenta	✓
Donante	Iniciar sesión	✓
Grupo Servir	Crear donación	✓
Grupo Servir	Crear beneficiario	✓
Grupo Servir	Enviar donación	✓
Donante y Grupo Servir	Visualizar estado del donativo	✓

Funcionalidades del aplicativo

CONCLUSIONES

- El sistema para la trazabilidad de donativos es aceptado por la encargada del grupo Servir.
- Se pudo demostrar que un sistema basado en *blockchain* con un contrato inteligente (*contract smart*) puede ser utilizado para la gestión de donativos, permitiendo validar la trazabilidad de estos.
- El contrato inteligente, según la evaluación por juicio de expertos, está a un nivel adecuado para la solución propuesta.
- Se demostró la compatibilidad del contrato inteligente (*contract smart*) con el sistema basado en otro *blockchain* existente.

REFERENCIAS

Abdellatif, T., y Brousmiche, K.-L. (2018). Formal verification of smart contracts based on users and blockchain behaviors models. *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, 1-5. doi:10.1109/NTMS.2018.8328737

Gervais, A., Karame, G. O., Wüst, K., Glykantzis, V., Ritzdorf, H., y Capkun, S. (2016). On the *Security and Performance of Proof of Work Blockchains. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS'16)*, Association for Computing Machinery, New York, 3-16. doi:10.1145/2976749.2978341

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Recuperado de https://bitcoin.org/bitcoin.pdf. doi:10.1.1.221.9986

AGRADECIMIENTOS

Agradecemos a nuestras familias, al magíster Daniel Cárdenas, al ingeniero Juan José Miranda, a la magíster Natalie Gil y a Andrea Cueva, y a todas las personas que intervinieron y nos apoyaron en esta investigación.