XXXI SEMANA NACIONAL DE INVESTIGACIÓN Y DOCENCIA EN MATEMÁTICAS

BLOCKCERTS - Credenciales en blockchain

Adrian Emilio Vazquez Icedo, Profesor asesor:Juan Pablo Soto Barrera
Ciencias de la computación

Introducción

Las criptomonedas han sido toda una revolución en el mundo tecnológico y económico, pero lo que ha permitido su desarrollo fue la utilización de un concepto llamado *blockchain*, el cual es una estructura de datos que, junto a técnicas criptográficas, apoyan la creación de bases de datos distribuidas que permiten dar soporte y garantizar la seguridad [1].

Con base a esto, se han desarrollado ideas como *Blockcerts*, el cual es un estándar abierto que permite crear aplicaciones que emiten y verifican documentos oficiales con base a *blockchain* [2], tales como credenciales académicas, licencias profesionales, registros civiles –entre otras.

Utilidad

Instituciones: Emitir credenciales digitales y verificables (por ejemplo, una universidad emite certificaciones para sus estudiantes) [3].

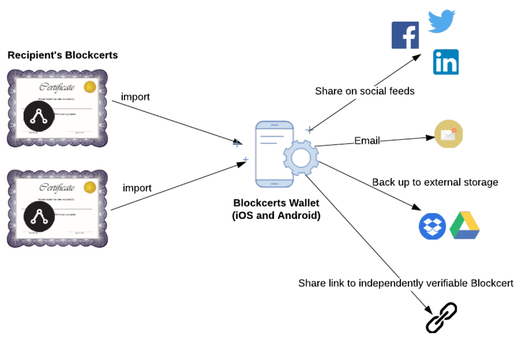
Usuario: Ser dueño de tus credenciales independientemente de las instituciones emisoras; perduran a pesar de que las instituciones dejaran de funcionar.

Empleador: Acelerar los procesos de verificación de documentos implementando sus propios servicios de verificación para agilizar los procesos de contratación.

Ventajas

- Seguridad: Al emitir un certificado los datos se comprimen en un hash y se registran en el *blockchain*, este registro es inmutable y distribuido por lo que los certificados no pueden ser manipulados.

- Recibir y compartir: Cada *Blockcert* contiene el certificado emitido y la evidencia requerida para verificar, por lo que el destinatario tiene el registro completo que puede compartir y respaldar.



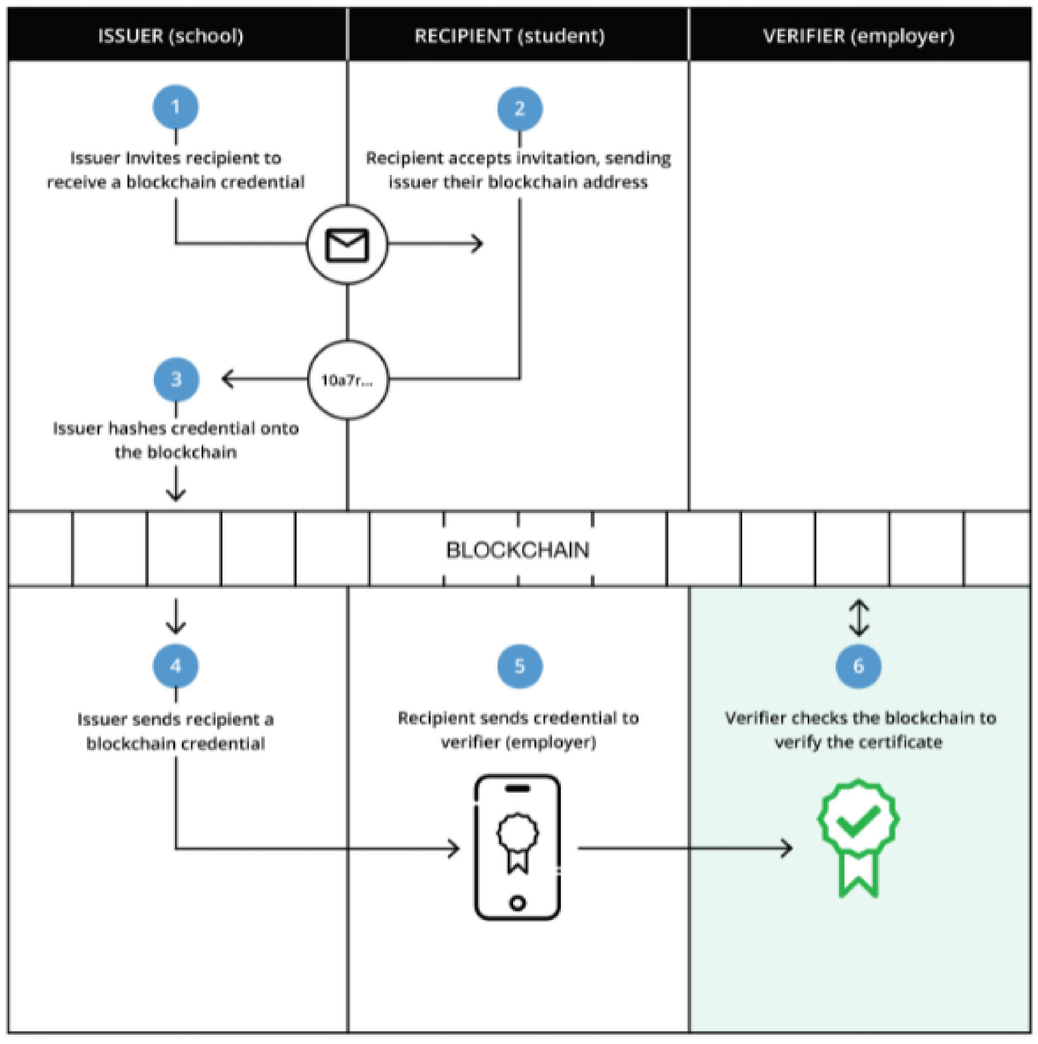
- Flexibilidad: Se puede utilizar con cualquier blockchain (Bitcoin, Ethereum). Lo cual permite adaptarse a los requisitos del desarrollador y las instituciones.

Proceso

1. El emisor invita al destinatario a recibir una credencial de *blockchain*.

2. El destinatario acepta la invitación y envía al emisor su dirección de *blockchain*.

3. El emisor coloca la credencial en la cadena de bloques.



4. El emisor envía al destinatario una credencial de *blockchain*.

5. El destinatario envía la credencial al verificador (empleador).

6. El verificador comprueba la cadena de bloques para verificar el certificado.

Conclusiones

El desarrollo e implementación de esta tecnología permite globalizar las instituciones gubernamentales y educativas permitiendo validar documentación de manera más eficiente y sin la necesidad de comunicación directa entre instituciones.

Por otro lado, trabajar sobre un mismo estándar se fortalece la seguridad permitiendo plena confianza entre las instituciones que pudieran colaborar.

Referencias

1. Bitcoin: A Peer-to-Peer Electonic Cash System, Satoshi Nakamoto (2009) https://bitcoin.org/bitcoin.pdf
2. Web BLOCKCERTS, The Open Standard For Blochain Credentials. https://www.blockcerts.org .
3. Blockcerts-An open infrastructure for academic credentials on the blockchain(2016), MIT Media Lab Learning Initiative. https://medium.com/mit-media-lab/blockcerts-an-open-infrastructure-for-academic-credentials-on-the-blockchain-899a6b880b2f