Fundamentos de Blockchain en Algorand

Dra. Rocío A. Aldeco P.

Semestre 2023-1

Algorand
Centre of Excellence

Introducción

¿Como se genera la confianza?

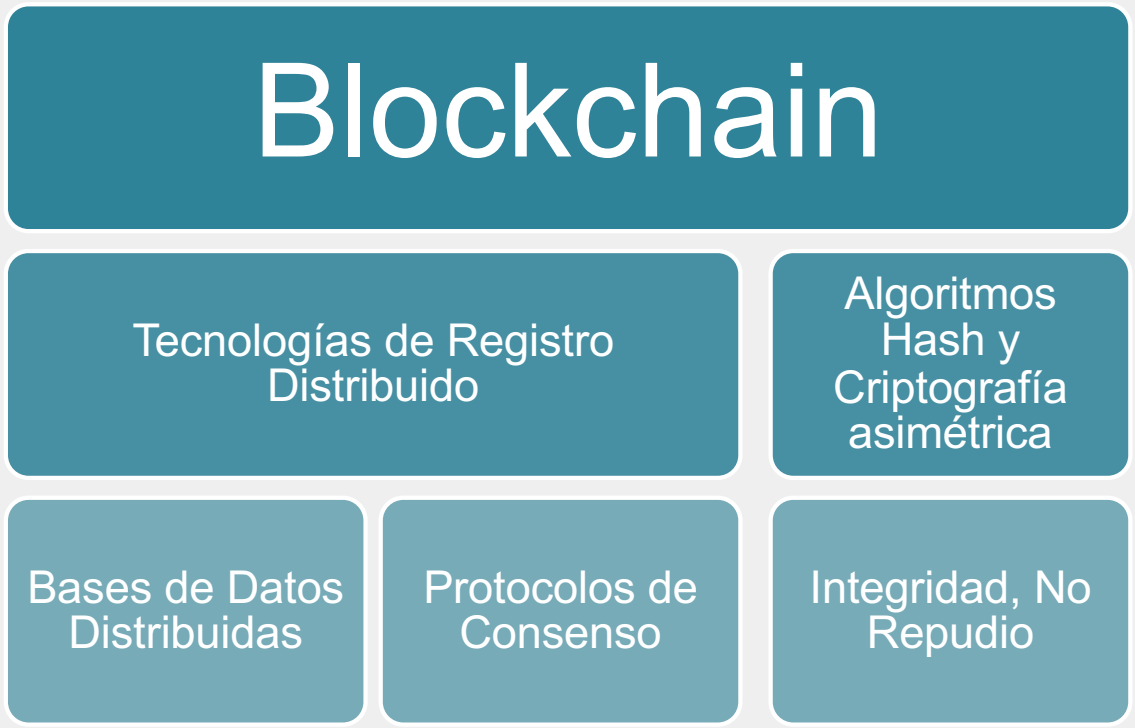
Confianza

Autenticación

No centralizado

- FOF [1]
- Recomendaciones [2]
  - Información falsa

1. Yu L. (2014) FOAF: Friend of a Friend. In: A Developer's Guide to the Semantic Web. Springer, Berlin, Heidelberg. http://www.foaf-project.org/
2. Golovin N., Rahm E. (2005) Automatic Optimization of Web Recommendations Using Feedback and Ontology Graphs. In: Lowe D., Gaedke M. (eds) Web Engineering. ICWE 2005. Lecture Notes in Computer Science, vol 3579. Springer.



Blockchain es una cadena de registros **distribuidos** y **descentralizados** unidos unos con otros que incluyen la firma digital de su creador. Una vez que estos registros son guardados no pueden ser alterados, ni en contenido ni en orden.
Esto hace a blockchain un registro **inmutable** y de sólo **agregación**.

Blockchain surge como respuesta a

Confianza

- Sistemas tradicionales tienen una **tercera parte** de confianza que se convierte en un punto central de fallo
- Estos sistemas trabajan bajo el supuesto de que esta tercera parte **existe** y siempre puede **confiarse** en ella

Anonimato

- Los sistemas tradicionales requieren de **autenticación** o incluso **identificación** de las partes involucradas

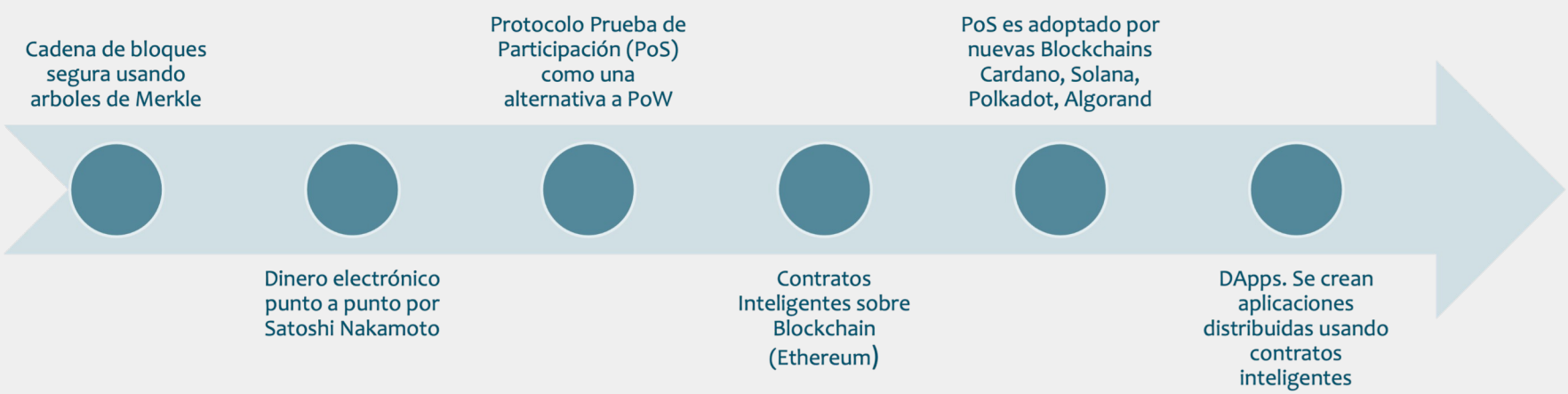
Integridad

- Si la tercera parte de confianza es **corrompida** la integridad del sistemas ya no puede ser garantizada

Propiedades

Confianza	Descentralización	Transparencia
Integridad	Redundancia	Anonimato

Historia de Blockchain



Historia de Blockchain

1 Bitcoin

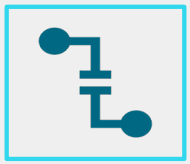
2 Blockchain

3 “Smart Contracts”

4 “Proof of Stake”

5 “Blockchain Scaling”

¿Qué obtenemos?



Confianza

Los sistemas tradicionales usan una tercera entidad de confianza que se vuelve un **punto central de fallo**.

Todos los sistemas tradicionales operan bajo el supuesto de que esta tercera entidad de confianza **existe**.

Anonimato

Los sistemas tradicionales requieren de **autenticación**, incluso de identificación por parte de los usuarios para poder ser parte del sistema.

Integridad

Si la tercera entidad de confianza es **corrompida** la integridad del sistema no puede ser garantizada.

Que NO es

NO ES SEGURIDAD

NO ES CRIPTOMONEDA

NO ES SOLUCIÓN MÁGICA

NO REEMPLAZA SISTEMAS CENTRALIZADOS

NO REPARA SISTEMAS ROTOS

¿Cuándo debería usar Blockchain?

Centralizado

vs

Descentralizado

Tercera parte de confianza

vs

Confianza basada en evidencia digital

Autenticación

vs

Anonimato

Transparencia

vs

Confidencialidad

Ejemplos

- Criptomonedas (FinTech)
- Contratos Inteligentes
- Reclamos de seguros
- Compra venta de propiedades
- Transparencia en uso de recursos públicos
- Salud
- Administración de identidades