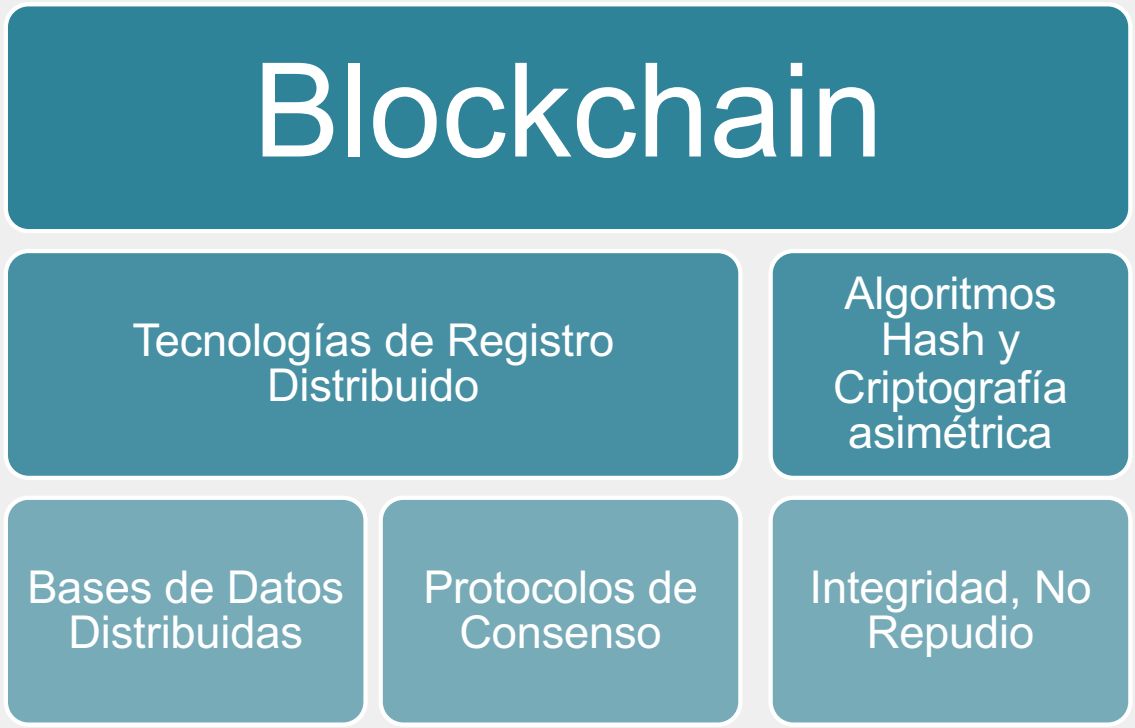
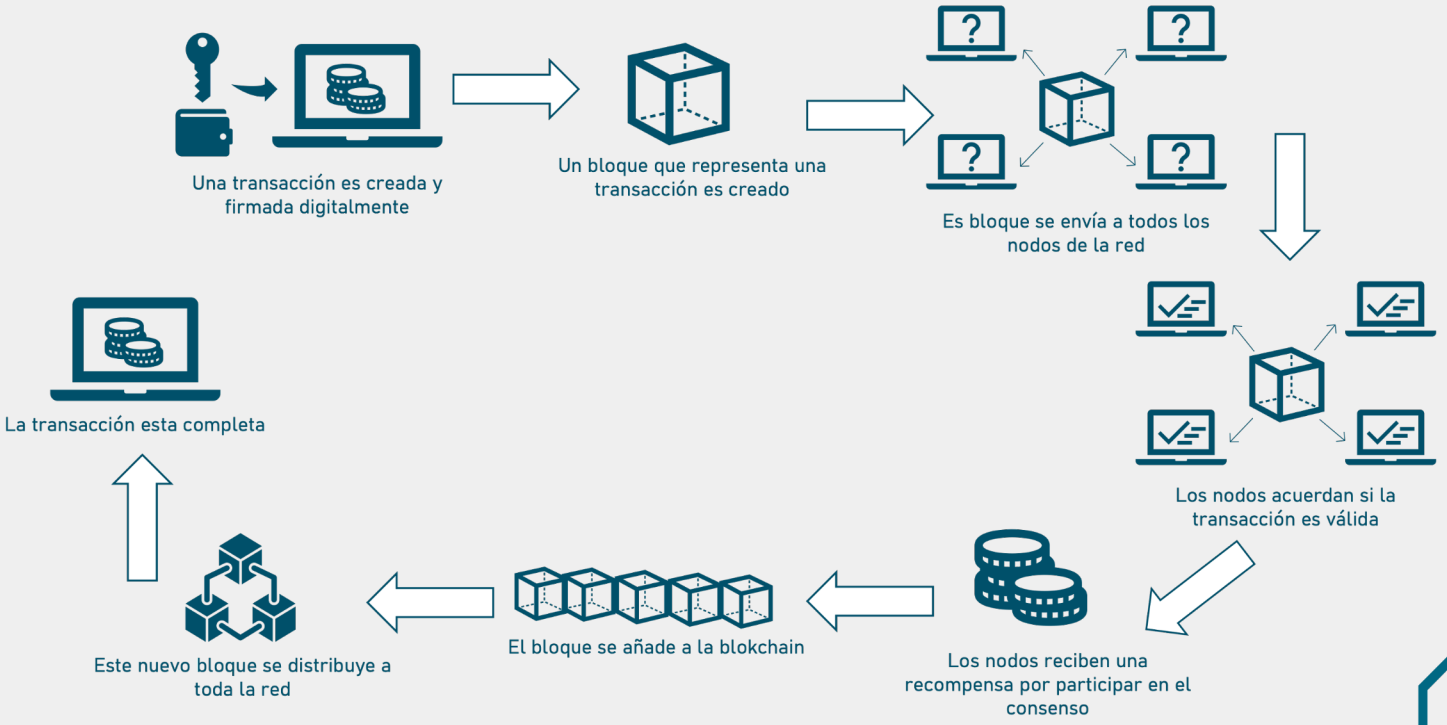
2. ¿Qué es Blockchain?



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**.

¿Cómo funciona Blockchain?



Algorand
Centre of Excellence

Elementos

- Red punto a punto
  - Nodos participantes
    - Con par de llaves asimétricas (wallet)
    - Distribución de paquetes
  - Nodos validadores
    - Protocolo de consenso
- Base de datos distribuida
  - Función hash
  - Árbol de Merkle

Tipos

Públicos

En un **blockchain público** cualquiera puede unirse a la red y participar dentro de ella.

Es descentralizada y no es controlada por una sola entidad.

Los datos son seguros, ya que no es posible modificar o alterar los datos una vez que han sido validados.

Privados

En un **blockchain privado** se restringe que entidades que pueden participar en la red.

Hay una o más entidades que controlan la red, i.e. se depende de terceras partes de confianza.

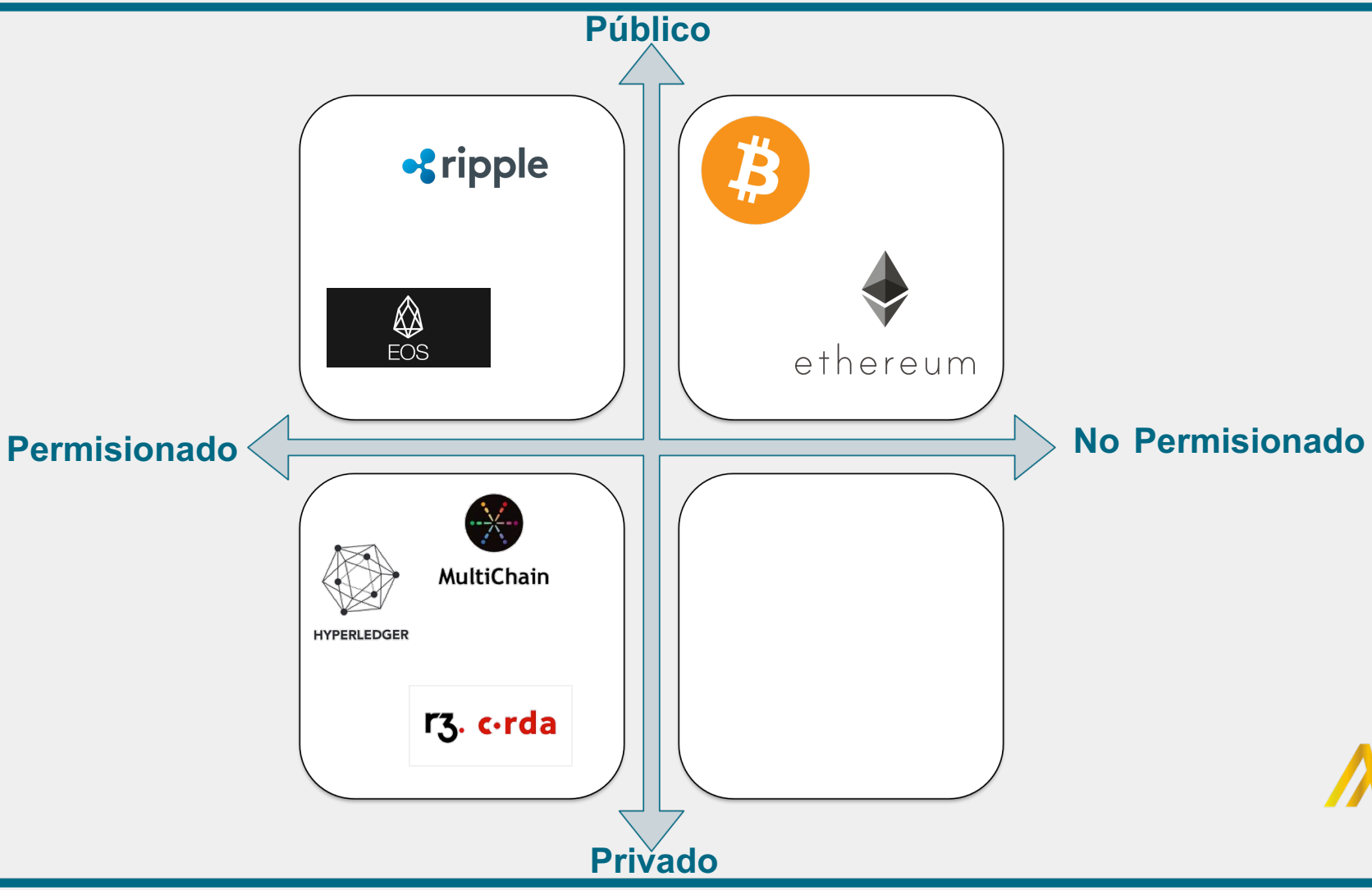
Sólo las entidades que participan tienen conocimiento de las transacciones.

Permisionados

En un **blockchain permisionado** se requiere de autenticación.

Esto hace que sea posible conocer la identidad de los participantes.

No estan totalmente descentralizados, solo algunos mantienen el blokchain.


Público
Permisionado
No Permisionado
Privado
ripple
EOS
ethereum
MultiChain
HYPERLEDGER
r3. c·rda

Propiedades

Confianza

Verificación Pública

Transparencia

Integridad

Redundancia

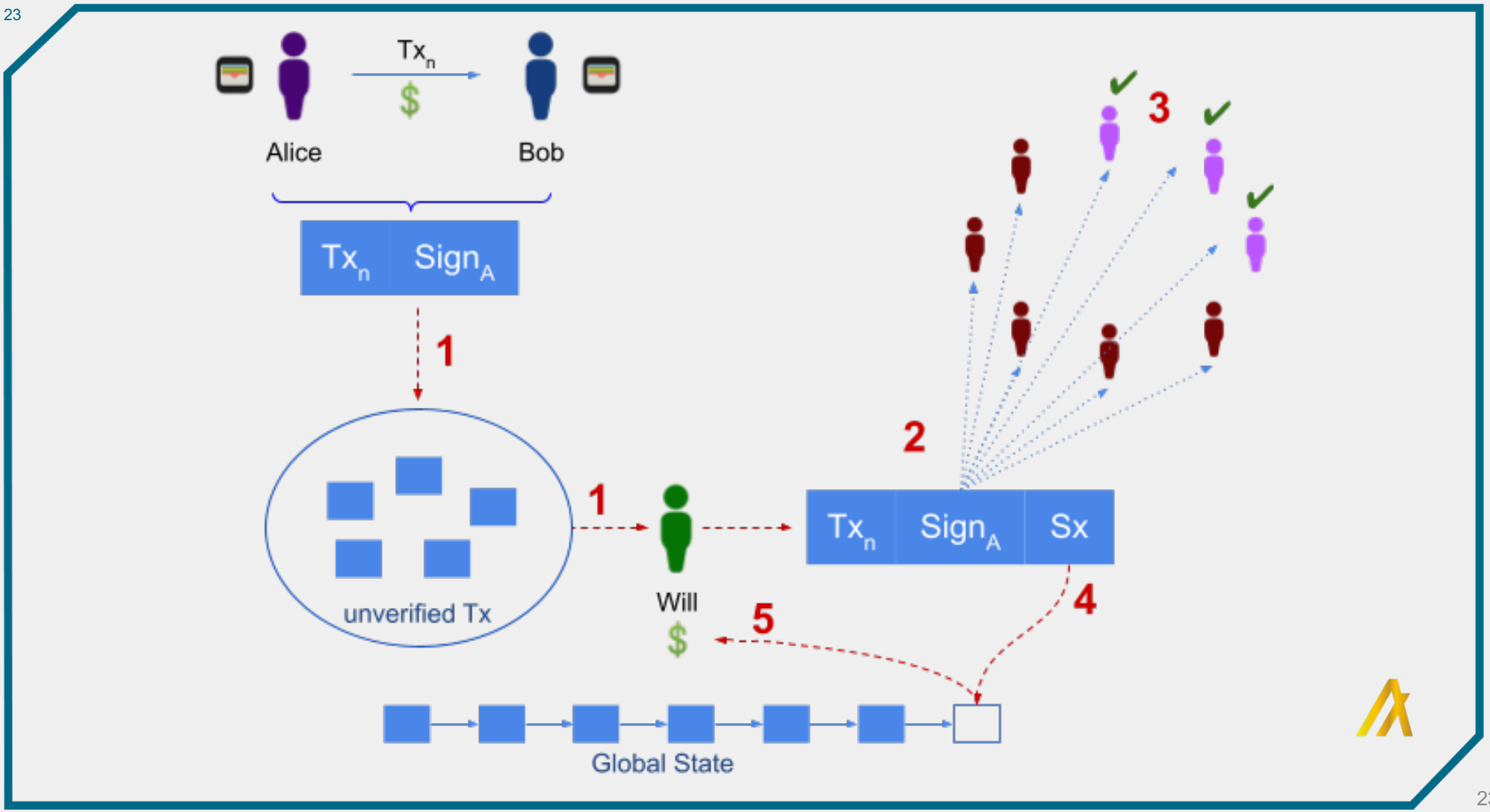
Anonimato

Ventajas

- No hay punto central de fallo
- Confianza basada en evidencia digital y no en terceras partes de confianza
- Es posible tener anonimato
- Desarrollar aplicaciones a través de contratos inteligentes

Desventajas

- Consumo energético
- Velocidad
- Escalabilidad
- Costo
- No hay autenticación
- No hay confidencialidad
- Integridad fuera del sistema no se garantiza


Tx_n
$
Alice
Bob
Tx_n Sign_A
1
unverified Tx
1
Will
$
2
3
Tx_n Sign_A Sx
4
5
Global State

Referencias

- Sherman, A. T., Javani, F., Zhang, H., & Golaszewski, E. (2019). On the Origins and Variations of Blockchain Technologies. IEEE Security and Privacy, 17(1), 72–77. https://doi.org/10.1109/MSEC.2019.2893730
- Maull, R., Godsiff, P., Mulligan, C., Brown, A., & Kewell, B. (2017). Distributed ledger technology: Applications and implications. Strategic Change, 26(5), 481–489. https://doi.org/10.1002/jsc.2148
- Lin, I. C., & Liao, T. C. (2017). A survey of blockchain security issues and challenges. International Journal of Network Security, 19(5), 653–659. https://doi.org/10.6633/IJNS.201709.19(5).01
- Nakamoto, S. (n.d.). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from www.bitcoin.org
- Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). Handbook of Applied Cryptography. CRC Press.
- Partala, J., Nguyen, T. H., & Pirttikangas, S. (2020). Non-interactive Zero-knowledge for Blockchain: A Survey. *IEEE Access*. https://doi.org/10.1109/ACCESS.2020.3046025
- Rene Davila, Rocio Aldeco-Perez and Everardo Barcenas, “Formal Verification of Blockchain Based Tender Systems”, Programming and Computer Software, Springer ISSSN 0361-7688, Special Issue 2022.
- Rebollar, F., Aldeco-Perez, R., & Ramos, M. A. (2022). Modeling a multi-layered blockchain framework for digital services that governments can implement. *Journal of Intelligent & Fuzzy Systems*, *42*(5), 4551–4562. https://doi.org/10.3233/JIFS-219244
- José Antonio Jiménez Miramontes and Rocío Aldeco-Pérez, “Trazabilidad de imágenes digitales usando Blockchain”, Congreso Internacional CORE CIC-IPN, 2022 (en prensa).
- Xiao, Y., Zhang, N., Lou, W., & Hou, Y. T. (2019). A Survey of Distributed Consensus Protocols for Blockchain Networks. *IEEE Communications Surveys and Tutorials*, *22*(2), 1432–1465. https://doi.org/10.1109/COMST.2020.2969706