Club de Investigación Tecnológica
Desde 1988

Arquitectura y taxonomía de blockchain

Daniel Truque
Telegram @truque
www.linkedin.com/in/danieltruque

Perfil de Symbiont

Datos Claves

Fundada en 2013

100+ empleados

Nueva York & Amsterdam

Premios

Fintech 250

CB INSIGHTS 2020

The Innovators 2019 Global Finance

Risk.net

Compañía FinTech del Año 2017

Forbes FINTECH 50 2018

Selectee

Buy-Side Technology waterstechnology

Mejor Distributed Ledger Technology 2016 & 2017

Inversionistas

Nasdaq

HUNDSUN

citi

MEDICI VENTURES

Raptor

Danhua Capital

GALAXY DIGITAL

FENBUSHI CAPITAL

BTIG

SENAHILL

Equipo Symbiont

Mark Smith | CEO

- Co-Fundador NexTrade, MatchBook FX
- COO & Co-Fundador de LavaFX, adquirida por Citigroup for $350M

Adam Krellenstein | Chief Scientist

- Co-fundador y Arquitecto Principal de Counterparty
- Experto en sistemas descentralizados

Chuck Ocheret | CTO

- 30+ year veteran of software engineering
- Tech leadership positions at DB, JPM, BS, UBS, MS and Amaranth Capital

Duncan Niederauer

- Ex CEO, NYSE Euronext & Presidente Intercontinental Exchange (ICE)
- Director Gerente de 555 Capital

Daniel Gallagher

- Ex Comisionado del Securities and Exchange Commission (SEC)
- Director Legal, Mylan

Jack Markell

- Gobernador de Delaware (2009-2017)
- Ex VP Senior Desarrollo Empresarial, Nextel

Shiv Govindan - Chair

- Socio, The Helios Co's
- Miembro Gerente de Celeridad Capital

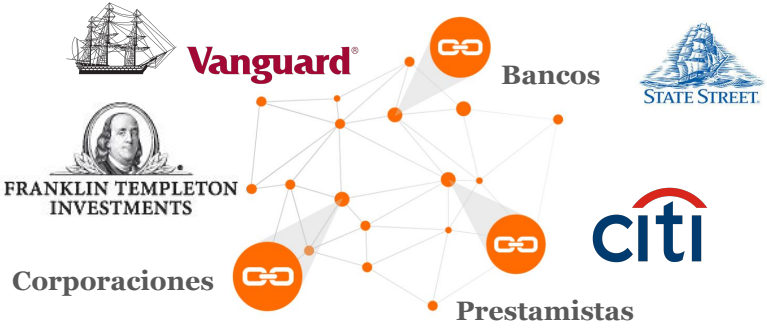
Todd Ruppert

- Ex CEO & Presidente, Global Investment Services T. Rowe Price
- VP, Greenspring Assoc.

Aplicaciones de Plataforma Assembly de Symbiont

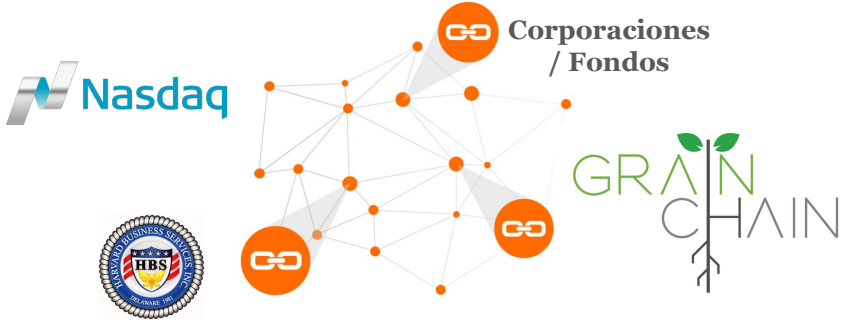
Hipotecas

Renta Fija y Monedas



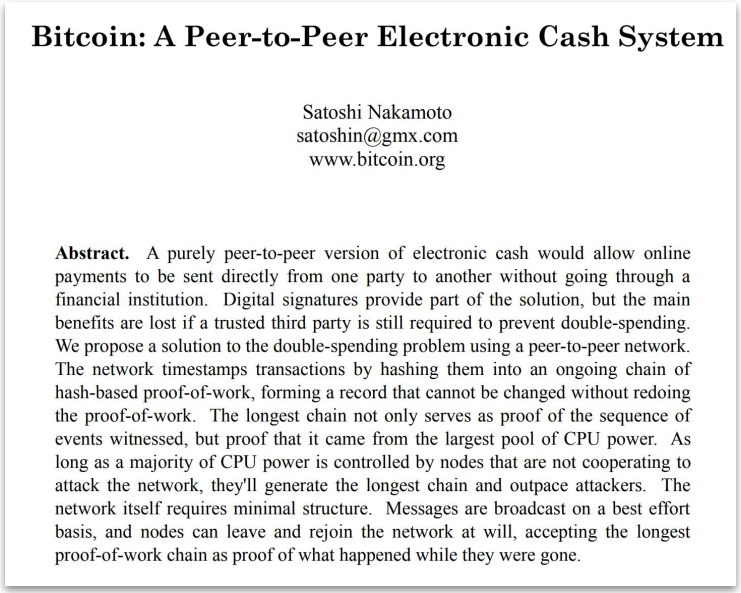
Índices Financieros

Activos Alternativos



Inicio de la Era de Blockchain

White Paper de Satoshi - Oct. 31, 2008



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

- Sistema de pagos de P2P (sin intermediarios)
- Elimina el problema de doble pago
- Hashes como Marca de Tiempo Digital
- Consenso de Prueba de Trabajo (PoW SHA256)
- Mensajes Publicados en Red
- ~~Blockchain~~

Inicio de la Era de Blockchain

Blockchain fue basado en varios conceptos anteriores

References

[1] W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998.

[2] H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirements," In *20th Symposium on Information Theory in the Benelux*, May 1999.

[3] S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In *Journal of Cryptology*, vol 3, no 2, pages 99-111, 1991.

[4] D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," In *Sequences II: Methods in Communication, Security and Computer Science*, pages 329-334, 1993.

[5] S. Haber, W.S. Stornetta, "Secure names for bit-strings," In *Proceedings of the 4th ACM Conference on Computer and Communications Security*, pages 28-35, April 1997.

[6] A. Back, "Hashcash - a denial of service counter-measure," http://www.hashcash.org/papers/hashcash.pdf, 2002.

[7] R.C. Merkle, "Protocols for public key cryptosystems," In *Proc. 1980 Symposium on Security and Privacy*, IEEE Computer Society, pages 122-133, April 1980.

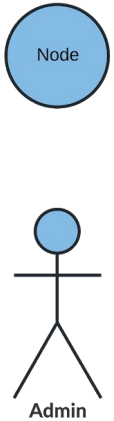
[8] W. Feller, "An introduction to probability theory and its applications," 1957.

Descentralización y Gobernanza

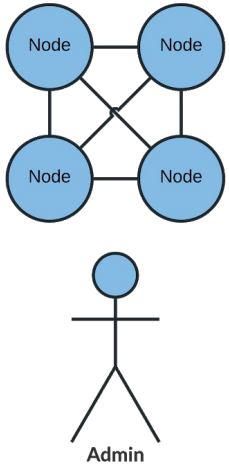
Consideraciones de Datos
- Solidez & Resistencia
- Integridad & Consistencia
- Disponibilidad & Accesibilidad

Consideraciones de Usuarios
- Gobernanza
- Confianza
- Privacidad

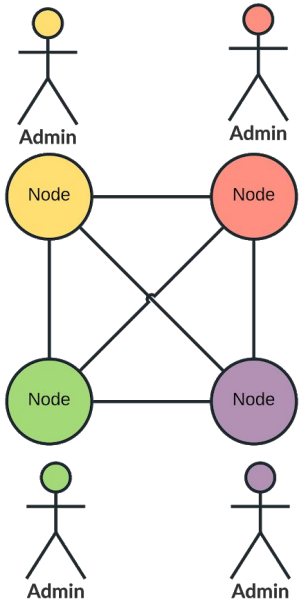
Centralizado
Nodo Único con Admin. Global



Distribuido
Multiple Nodos on Admin. Global

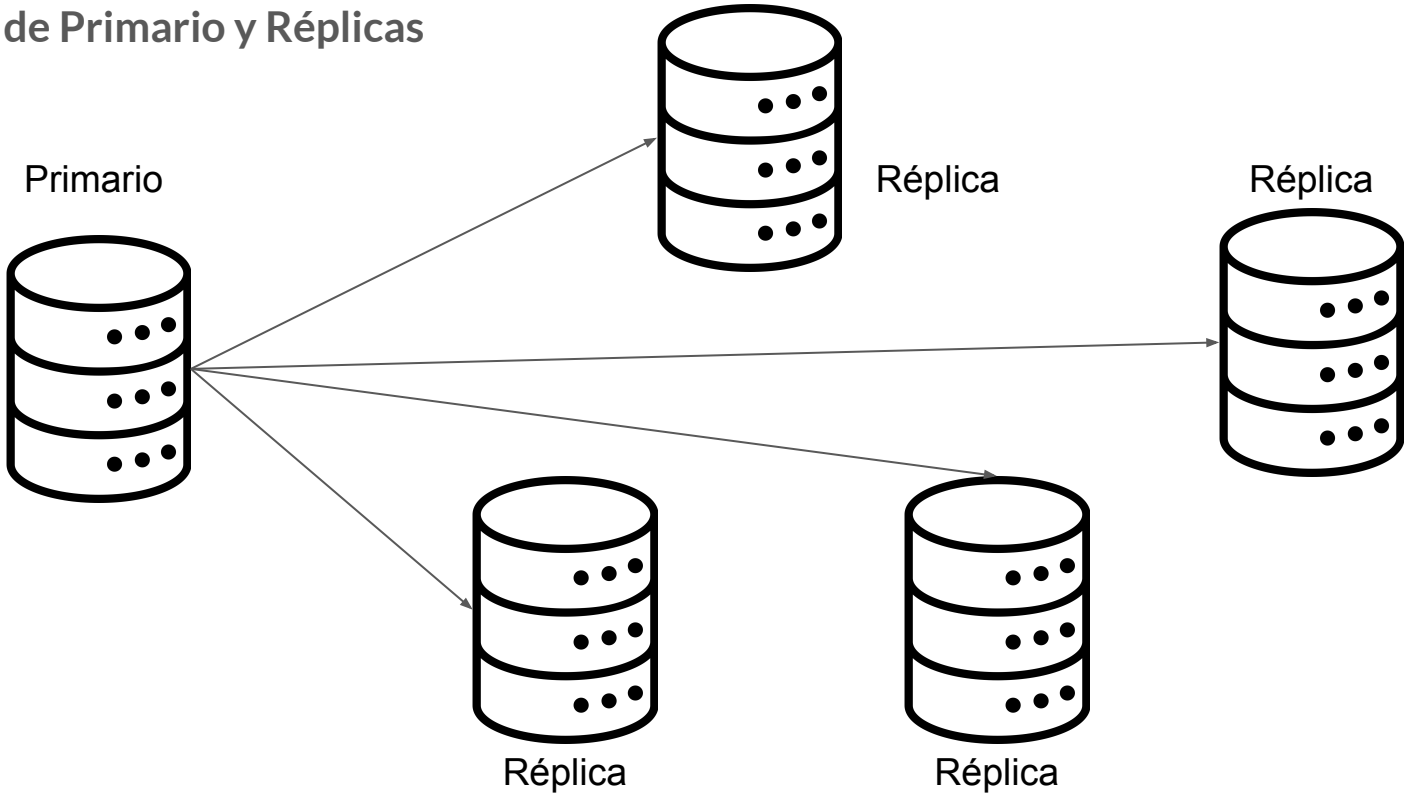


Descentralizado
Sin Administrador Global



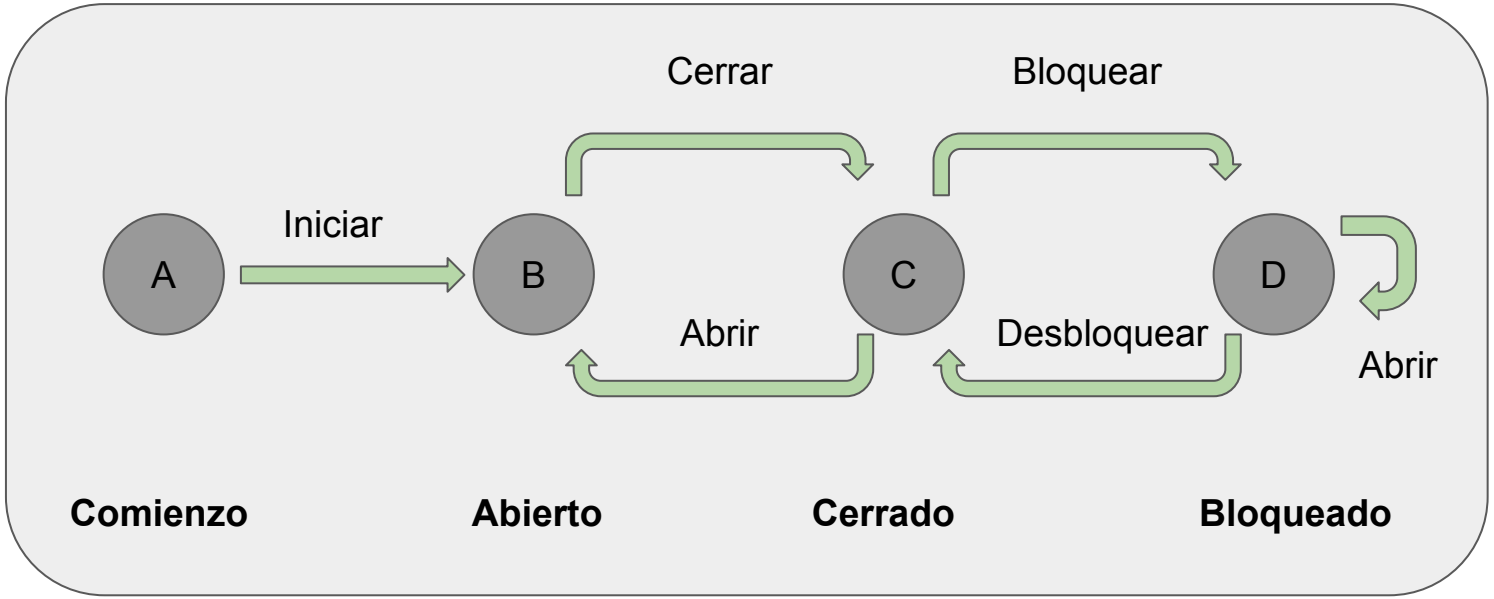
Definición de Blockchain

Esquema de Primario y Réplicas



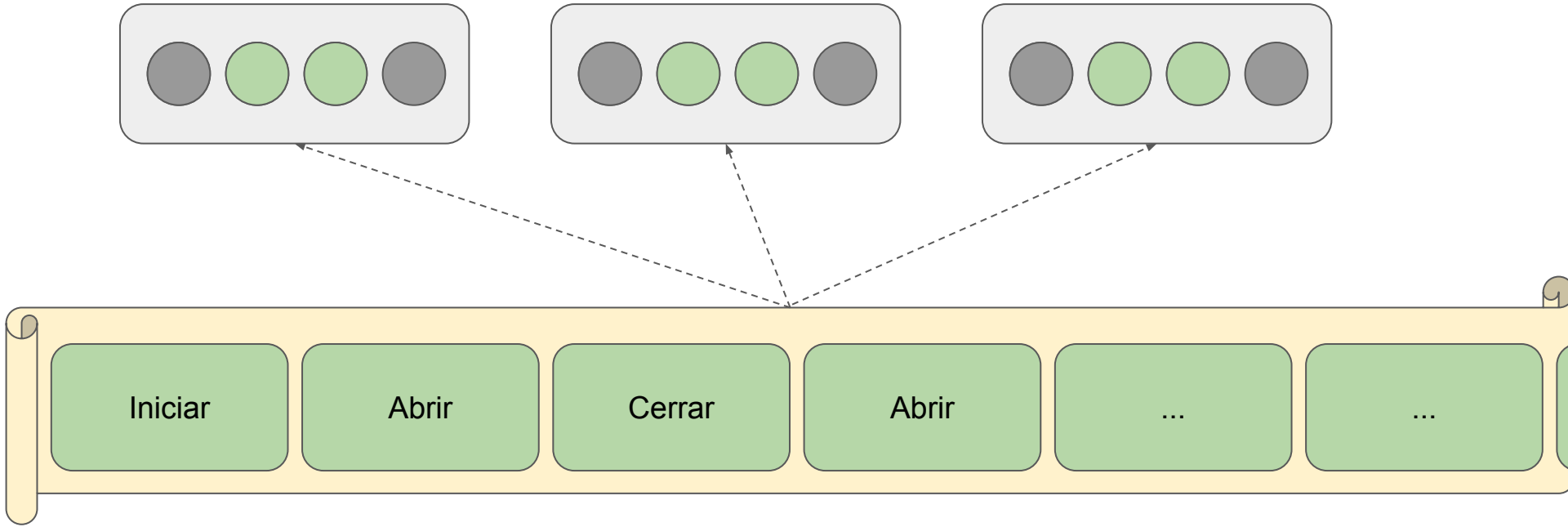
Definición de Blockchain

Esquema Máquina de Estados



Definición de Blockchain

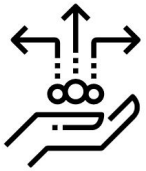
Esquema Replicación de Máquina de Estados



Cuándo Implementar Blockchain

Silos de Datos

Múltiples Contribuyentes



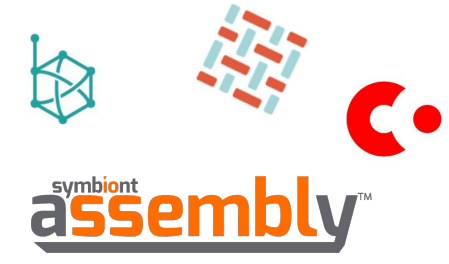
Intercambio de Datos y Lógica

Flujos de Trabajo y Dependencias

Terceros Involucrados

Confianza Incierta

Trilema de Blockchain



Escalabilidad

- Capacidad de Carga
- Rendimiento
- Latencia

Seguridad

- Integridad
- Consistencia
- Confidencialidad

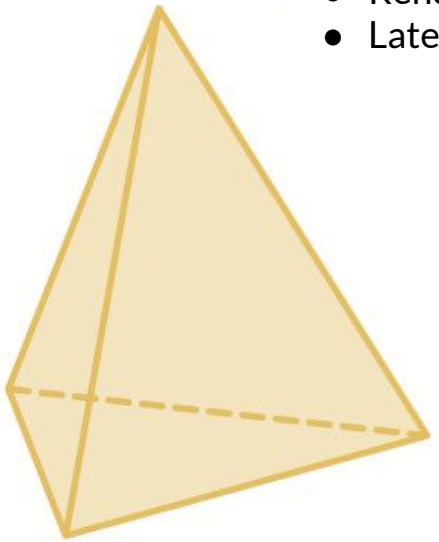
Descentralización

- Accesibilidad
- Disponibilidad
- Transparencia

Cuadlema de Blockchain

Escalabilidad

- Capacidad de Carga
- Rendimiento
- Latencia



Seguridad

- Integridad
- Consistencia

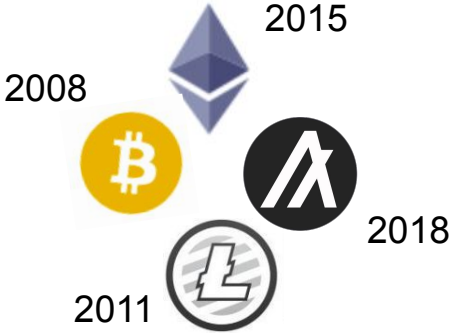
Descentralización

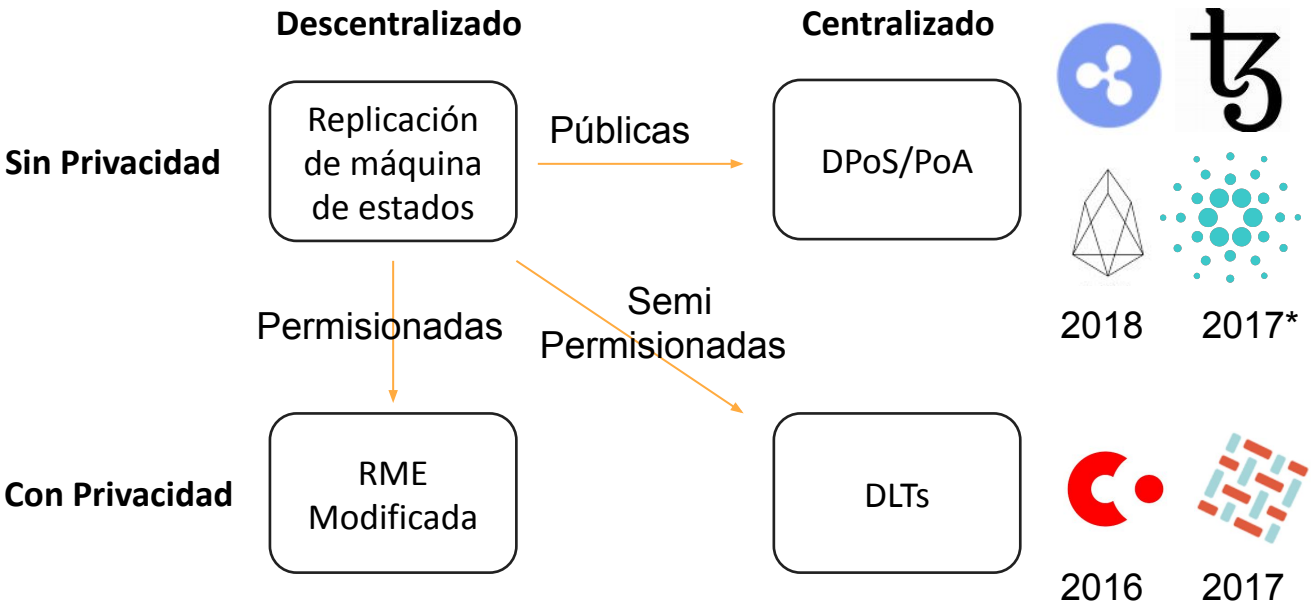
- Accesibilidad
- Disponibilidad
- Transparencia

Privacidad

- Anonimidad
- Confidencialidad

Blockchains & DLT: Historia y Taxonomía





* Cardano lanzó en 2017 con PoW y cambió a PoS en 2017

Categorización por Acceso y Procesamiento

	Membresía Pública	**Membresía Privada**
Infraestructura Permisionada	Servicios Públicos	DLTs permisionados
Infraestructura Abierta	Blockchains Públicos Tradicionales	?!

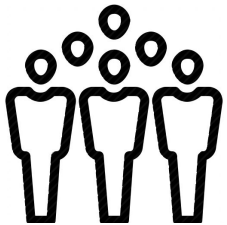
Categorización por Acceso y Procesamiento

	Membresía Pública	Membresía Privada
Infraestructura Permisionada	Cadenas Públicas	Cadenas Permisionadas
Infraestructura Abierta		X

Cadenas Públicas y Permisionadas (no “Privadas”!)

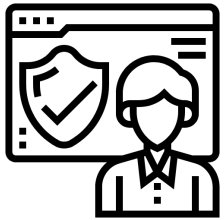
Públicas

- Membresía abierta
  → Participantes anónimos
- Consenso más lento - PoW, PoS
  → Requiere criptomoneda
  → Finalidad probabilística (rollbacks)
- Contratos inteligentes sin privacidad
- Gobernanza abierta
- Almacenamiento de datos limitado



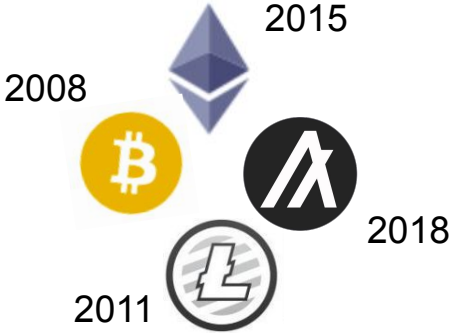
Permisionadas

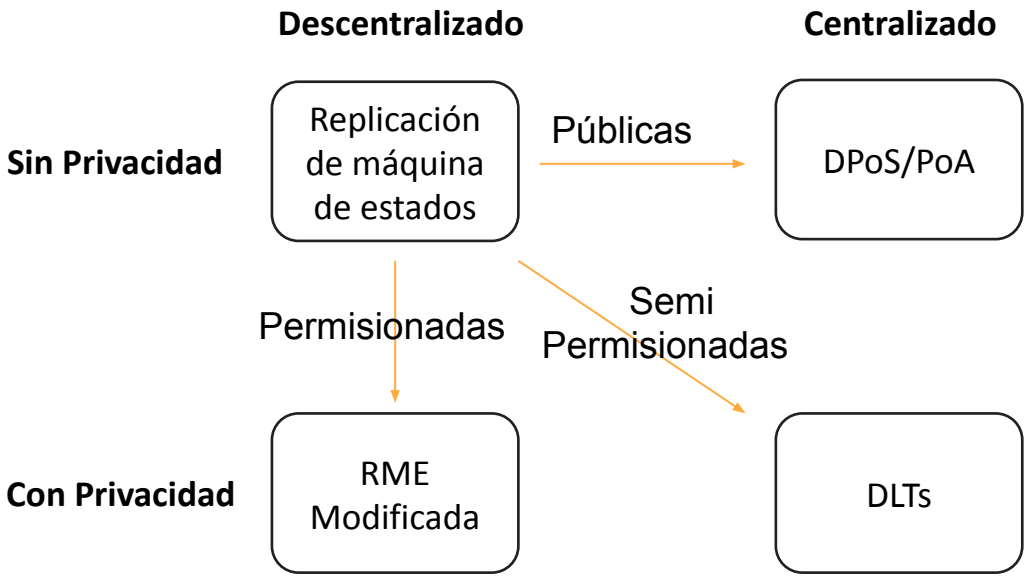
- Membresía por permiso
  → Participantes conocidos
- Consenso más rápido - CFT, BFT
  → No requiere criptomoneda
  → Finalidad absoluta
- Gobernanza controlada

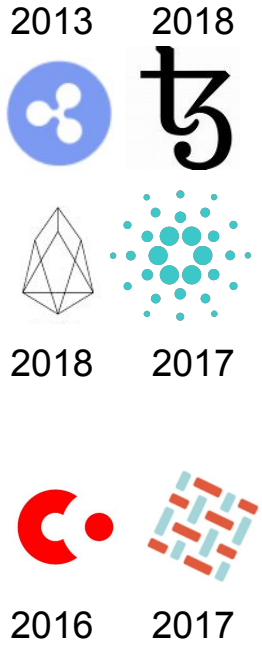


Escalabilidad depende del caso de uso!

Blockchains & DLT: Historia y Taxonomía







Arquitectura de Blockchain - Lenguajes de Programación

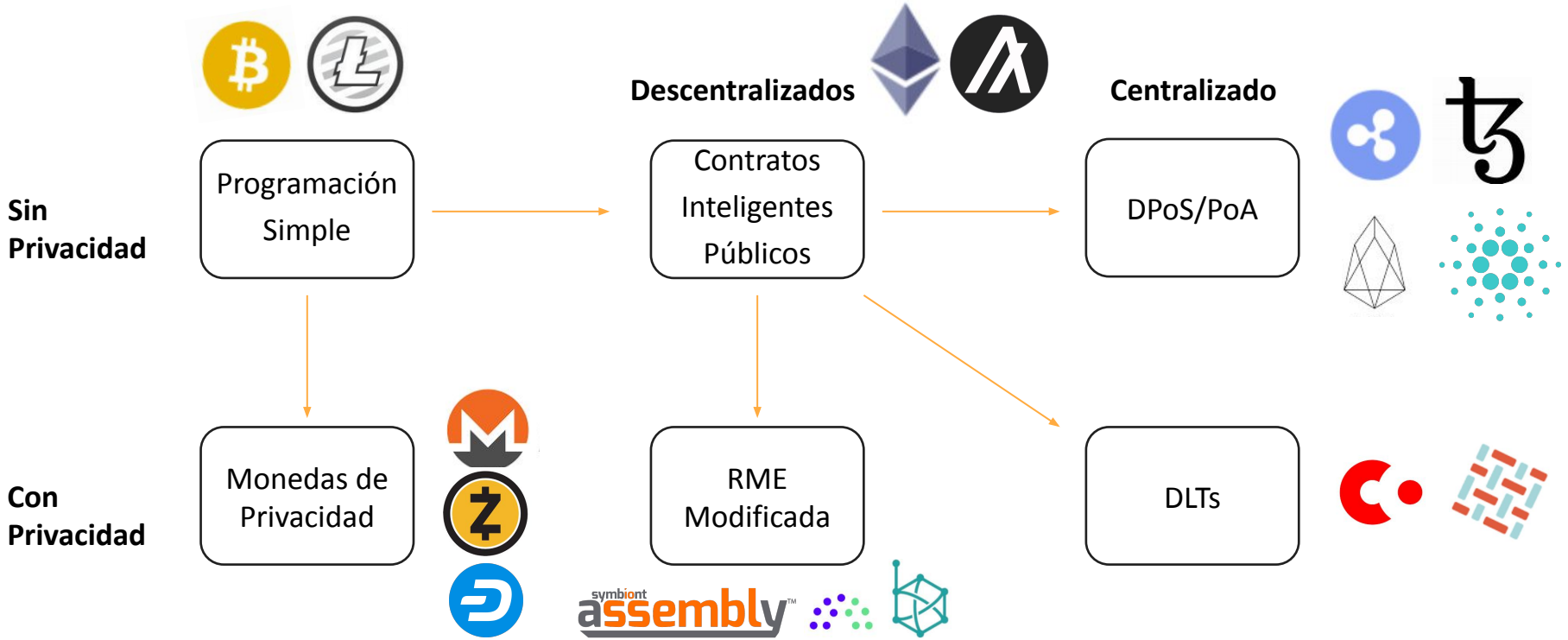
Consideraciones

- Ejecución determinística
- Monitoreo de Recursos
- Mecanismos de Privacidad & Concurrencia para compartir datos de manera segura
- Mecanismos para evitar pulgas
- Versiones y Actualizaciones
- Funcionalidad & Modularización

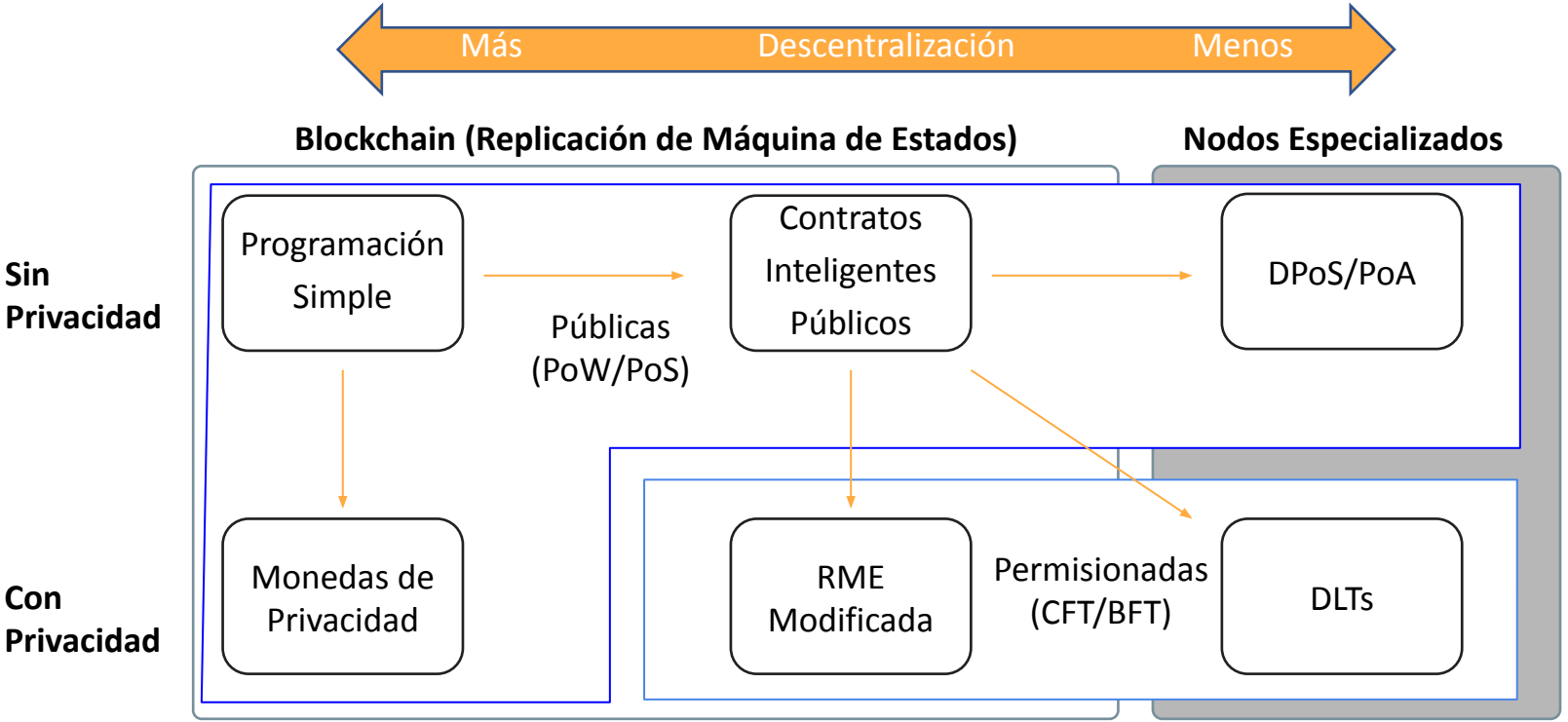
	Lenguajes de Dominio Específico	Lenguajes Generales
Sin Privacidad	Ethereum (Solidity) Cardano (Plutus)	EOS (C++)
Con Privacidad	Symbiont (SymPL) Digital Assets (DAML)	Corda (Java, Kotlin) HL Fabric (Go, NodeJS, Java)

El lenguaje interno de plataforma no es lo mismo que el lenguaje externo de contratos

Blockchains & DLT: Historia y Taxonomía



Blockchains & DLT: Historia y Taxonomía



Arquitectura de Blockchain - Algoritmos de Consenso

Consensos de Qué y entre Quiénes

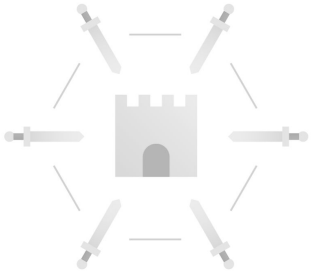
- Dato único o estado de la red en un sistema distribuido
- Por participantes en el sistema

Prueba de Trabajo (PoW)

Prueba de Participación (PoS)

Tolerancia de Fallas Benignas (CFT)

Tolerancia de Fallas Bizantinas (BFT)



Arquitectura de Blockchain - Nodos Especializados

En algunas arquitecturas, no todos los nodos validan y ejecutan transacciones

Nodos Idénticos

Todos los nodos validan y ejecutan transacciones

- Públicos:
  - Bitcoin, Ethereum
- Permisionadas:
  - Symbiont, Quorum*, Besu

Nodos Especializados

Solo ciertos nodos ejecutan transacciones

- Público:
  - Ripple (validator nodes)
  - EOS (dPOS, block producers)
  - Tezos (bakers)
- Permisionada:
  - HL Fabric (orderers, endorsers)
  - R3 Corda (notaries)

* En versiones iniciales,un “regulador” era necesario para implementar privacidad

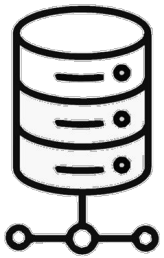
Arquitectura de Blockchain - Roles Permisionados

Plataforma	Autoridad Central Habilidad de ver información privada
corda	“Notary”
HYPERLEDGER Fabric	“Endorsers” and “Orderers”
Quorum™	“Regulator”
Digital Asset	“Operator”
symbiont assembly™	*n/a*

Arquitectura de Blockchain - Almacenamiento de Datos

En Red (on-chain)

- Limitado por la arquitectura
  - Cadenas públicas: costo y tamaño de bloque
  - Permisionadas: recursos
- Mejor disponibilidad de datos
- Requiere privacidad robusta



Fuera de red (off-chain)

- Graba un hash en la red
- Ligada a recurso fuera de la red
- Fuera de red:
  - Centralizada (i.e., datacenter)
  - Distribuida (i.e., nube)
  - Descentralizada (e.g., IPFS)

Código Abierto vs. Código con Licencia

Código Abierto

- Cualquiera puede bajar el software
- Mucha gente puede detectar errores pero también se podrían aprovechar vulnerabilidades
- Soporte y mapa de desarrollo limitado
- Requiere equipo técnico en casa
- Patrocinadores del proyecto cuotas de desarrollo, soporte y consultoría

Licencia

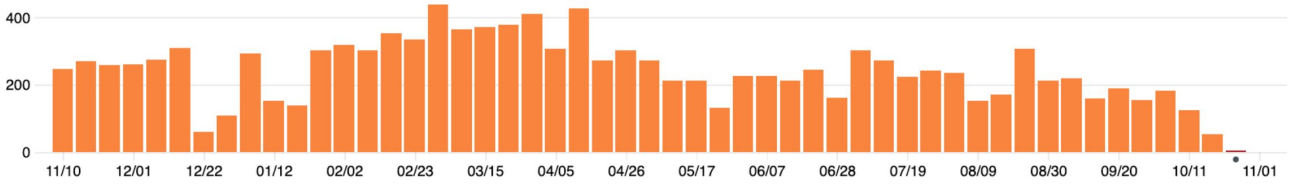
- Pago de licencia para uso del software
- Equipo de desarrollo dedicado
- Soporte técnico preferencial e influencia sobre el mapa de desarrollo
- No requiere mantenimiento en casa
- Puede tener un SDK para desarrollo externo y ofrecer soluciones a la medida

Código Abierto vs. Licencia - Commits

Github Commits por Semana

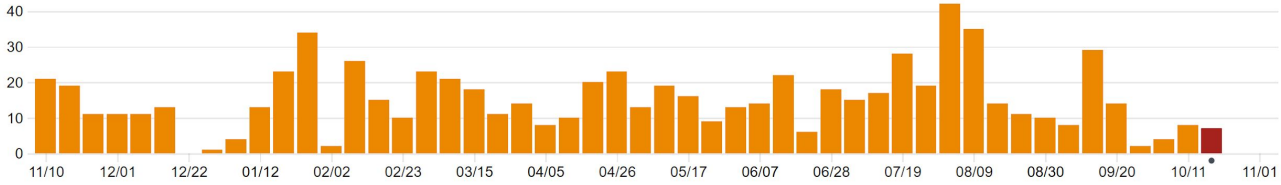
0 - 400

symbiont assembly™



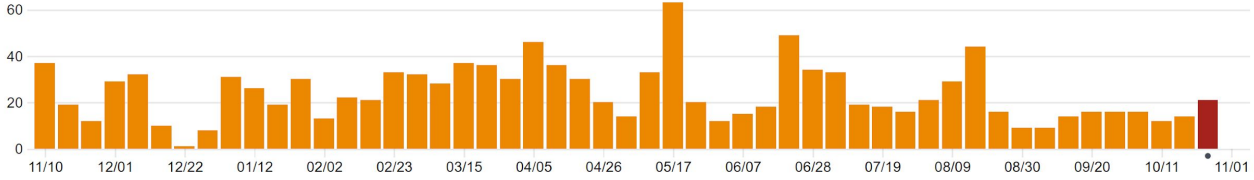
0 - 40

corda



0 - 60

HYPERLEDGER



Código Abierto vs. Licencia - Contribuciones

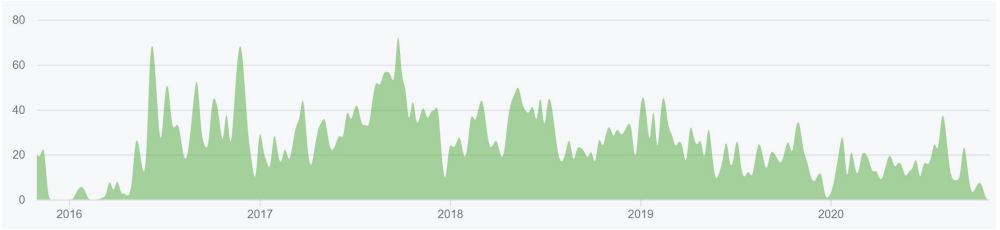
Contributions to master, excluding merge commits

0 - 400

symbiont assembly™

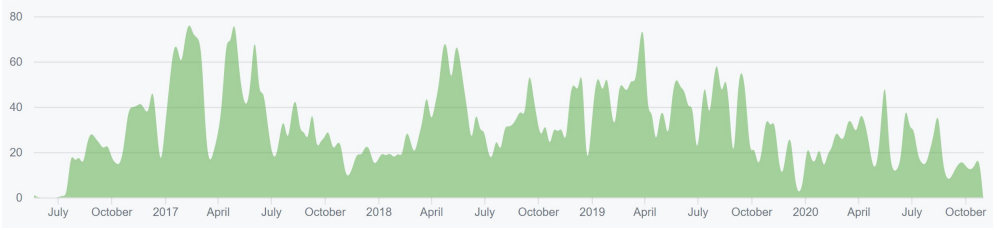
0 - 80

corda

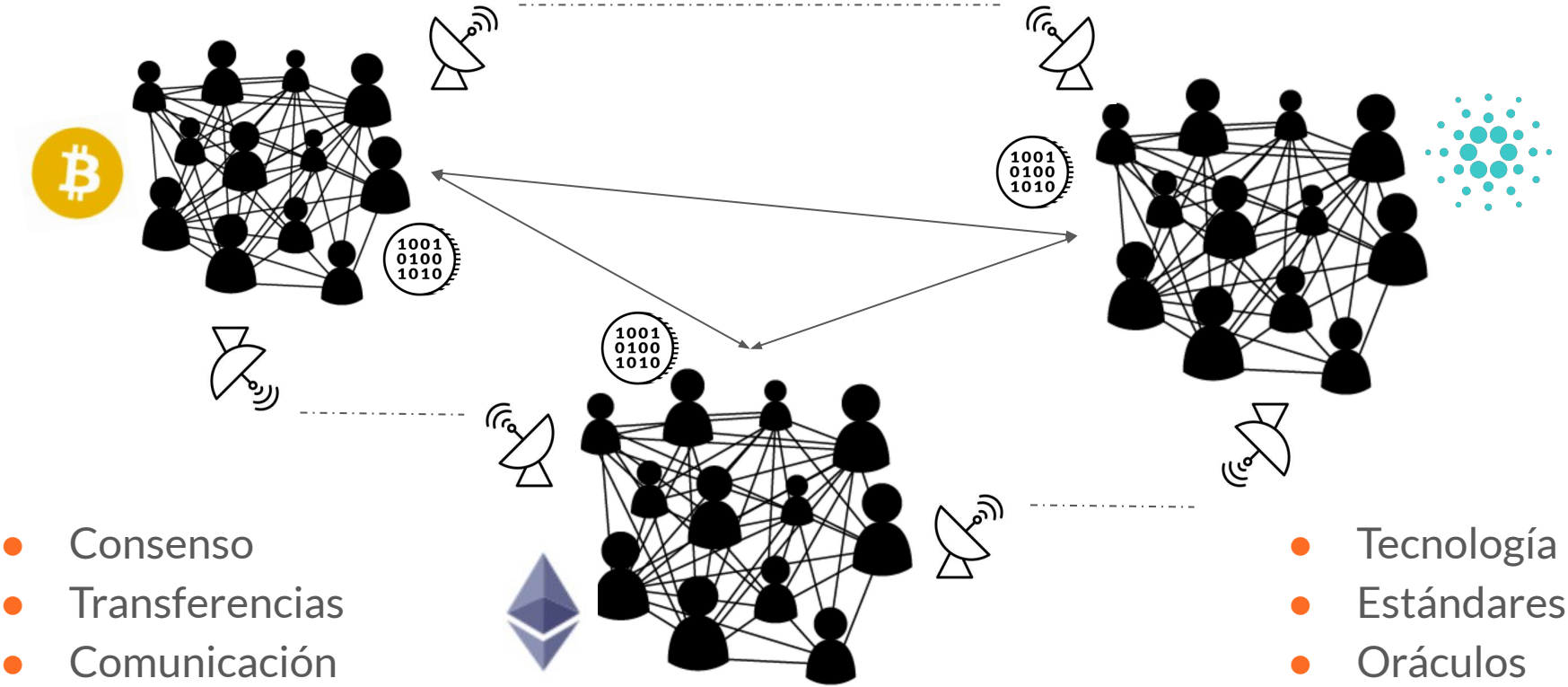


0 - 80

HYPERLEDGER



Interoperabilidad



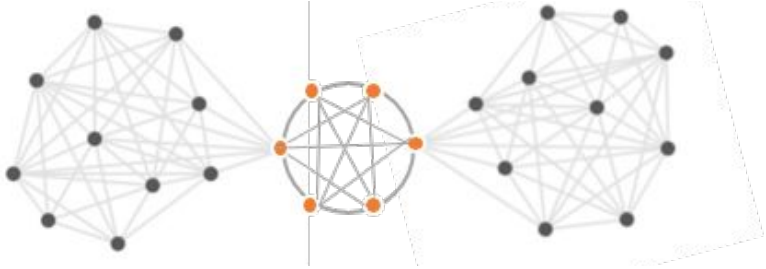
- Consenso
- Transferencias
- Comunicación

- Tecnología
- Estándares
- Oráculos

Arquitecturas Generales de Interoperablidad

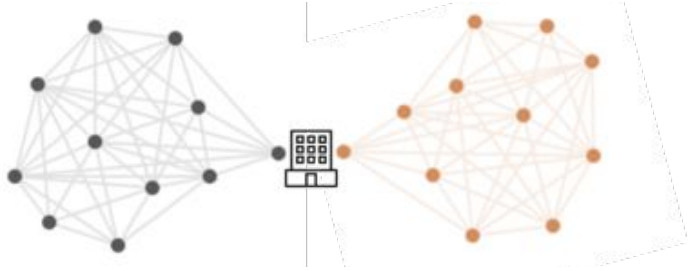
Ecosistema de Consenso

- Mueve un activo de una red a otra con el mismo protocolo de consenso
- Misma versión es necesaria
- Requiere un círculo de agentes que conectan los nodos, e.g., mainnet



Puentes Digitales (Hubs)

- Una entidad corre nodos en dos o múltiples blockchains
- Congela activo en una red mientras crea copia en otra
- Requiere confianza de custodia



Preguntas?

Arquitectura y taxonomía de blockchain

Daniel Truque
Blockchain: daniel.truque@symbiont.io
Criptomonedas: dt@satoshi.capital
Telegram/Twitter/Clubhouse @truque
Whatsapp +17869992735
www.linkedin.com/in/danieltruque