Blockchain e Industria 4.0

CETIC, VITORIA-GASTEIZ, 08 DE MAYO 2018

VICTOR MARTINEZ BAHILLO (@VTHOT4)

Sobre mi.

Arquitecto de sistemas en Versia Innovación.

- Cursando Grado de Ingeniería Informática.
- Cursando Grado de Ciencias ambientales.

- Miembro Meetup Blockchain Bilbao.

versia

bitcoin
blockchain
bilbao

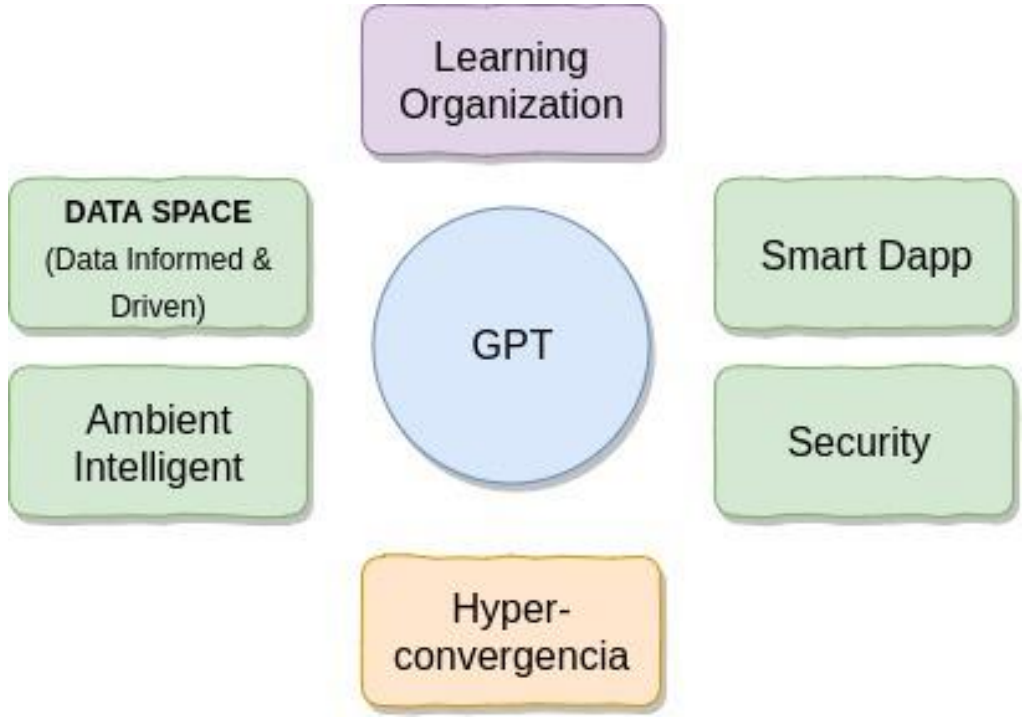
linkedin.com/in/victor-martinez-bahillo-758ab320

@vthot4

Versia Tecnologías Emergentes.

Tecnologías de Utilidad General (GPTs).

- Presentan un amplio margen de mejora sobre las tecnologías existentes.
- Posibilitan una amplia variedad de usos en un extenso número de sectores y áreas de aplicación.
- Dependen a la vez del desarrollo de una serie de innovaciones o tecnologías complementarias.



(*) Visión propia.

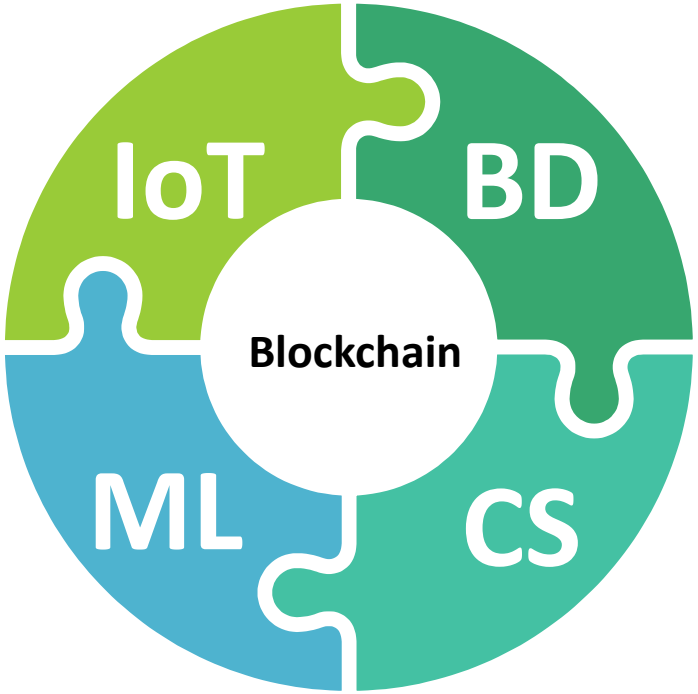
Versia Tecnologías Emergentes.

Internet of things

- Machine to Machine (M2M).
- Smart City platforms.
- Trazabilidad.

Machine Learning

- Modelos de análisis de cadenas.
- Análisis de Silos de Cadena.
- Sistemas antifraude.



Big Data

- Integridad de análisis.
- Análisis de patrones de transacciones.
- Auditorías.

Cyber Security

- Arquitecturas KSI.
- Arquitecturas sin contraseña.
- Decentralization del DNS.

¿Qué vamos a ver?

INTRODUCCIÓN

Problemáticas a resolver.

REDES PRIVADAS

Hyperledger, Alastria, Ethereum.

FUTURO

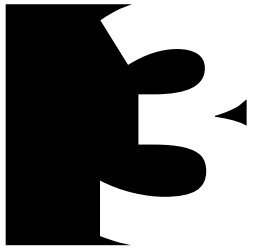
DAGs

BLOCKCHAIN

Definición.

INDUSTRIA 4.0

DUDAS Y PREGUNTAS

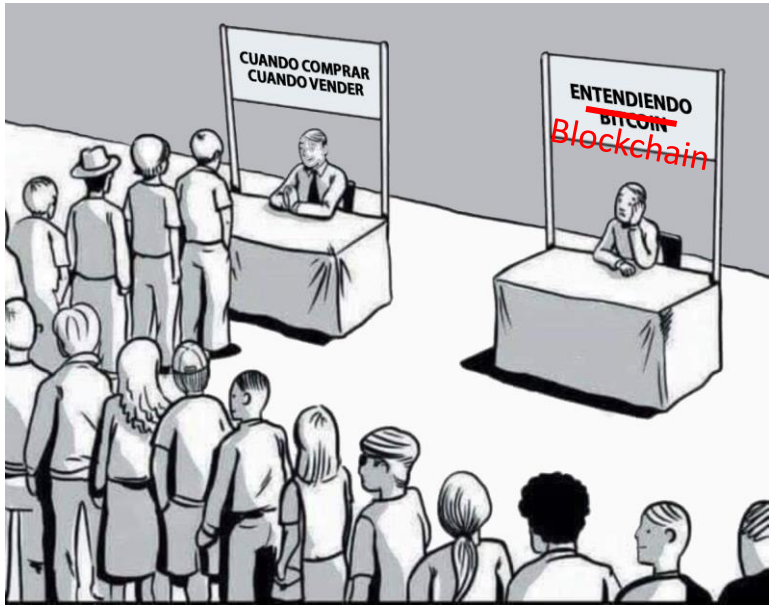


REDES PÚBLICAS

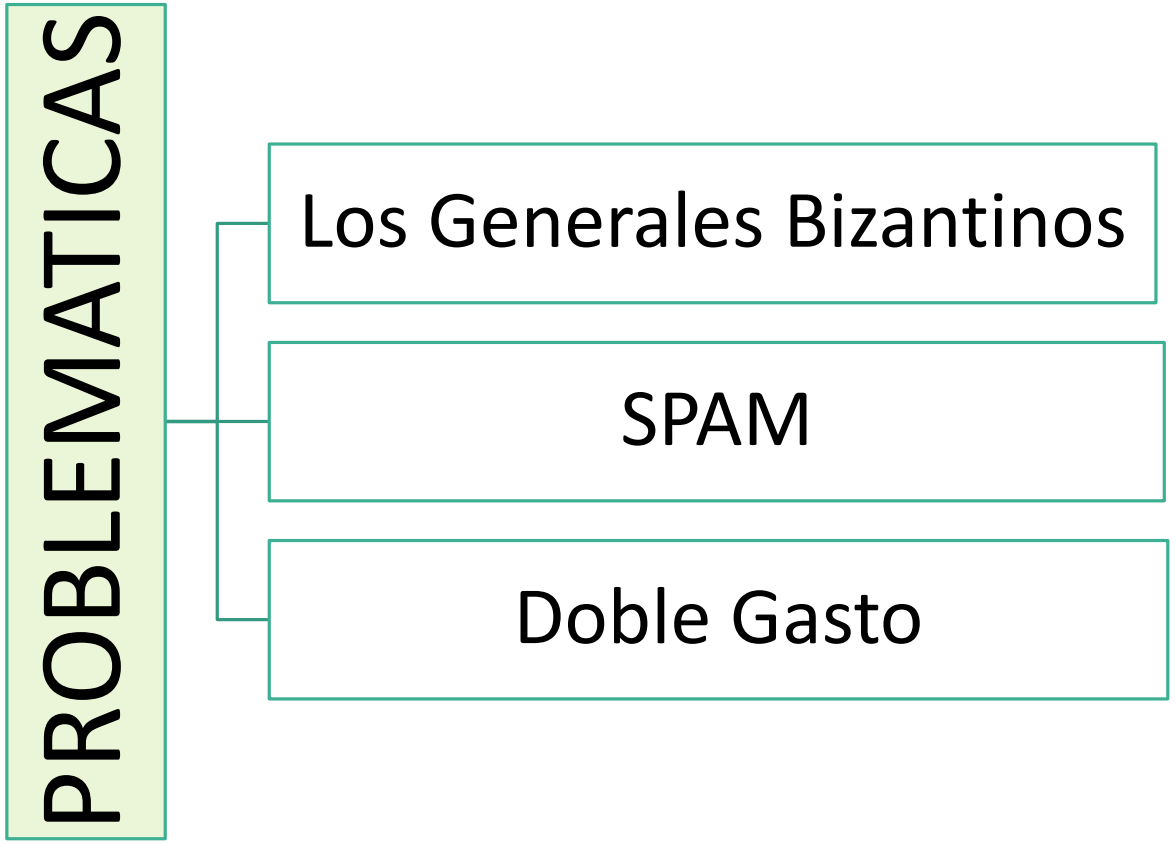
Bitcoin, Ethereum, Monero,..

CASOS DE USO

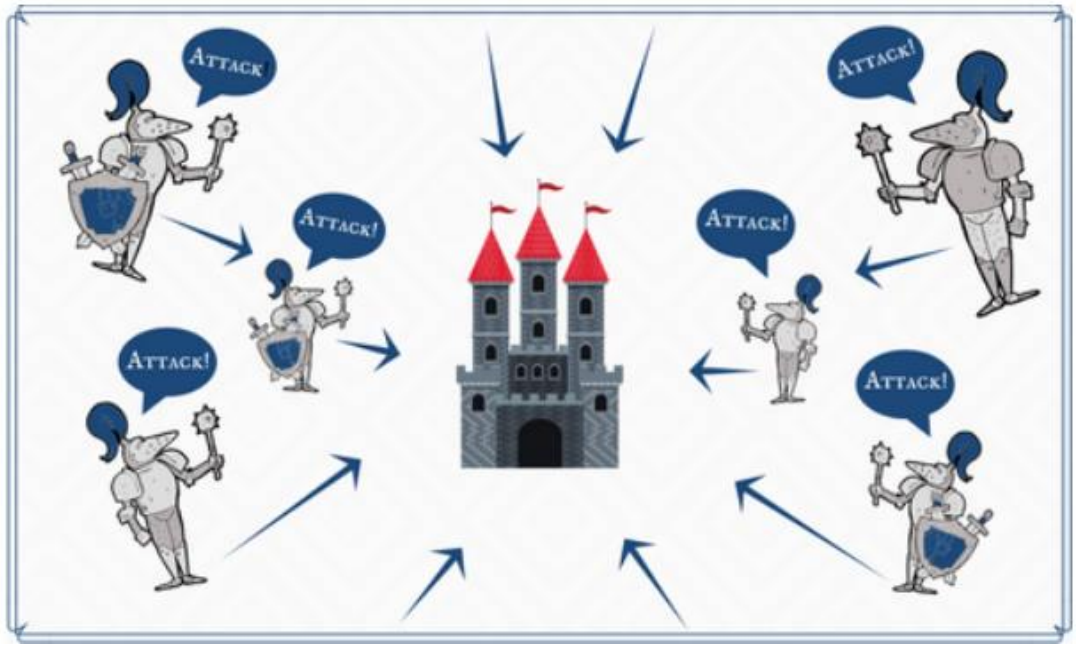
Introducción



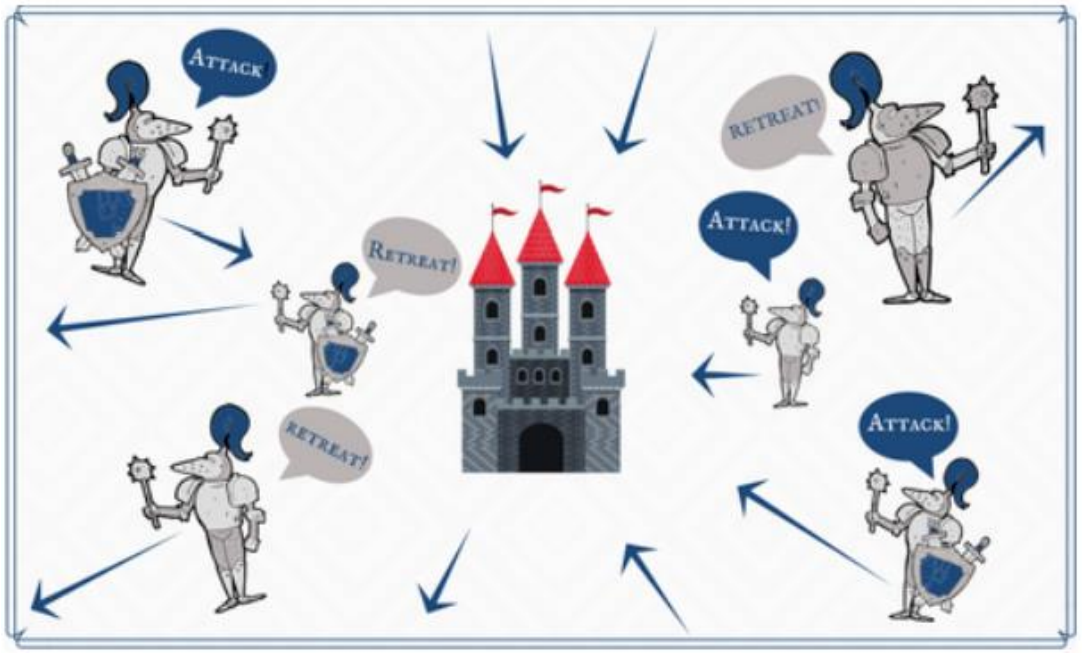
Problemáticas clave.



Problemática. Los generales bizantinos.



TODOS LOS GENERALES DE ACUERDO



FALLO DE UNIFICACIÓN DE ACCIÓN

SOURCE: https://keyholesoftware.com/wp-content/uploads/Blockchain-For-The-Enterprise-Keyhole-White-Paper.pdf

https://web.ua.es/en/recsi2014/documentos/papers/bitcoins-y-el-problema-de-los-generales-bizantinos.pdf

Propuesta Solución. Generales Bizantinos.

Appears in the *Proceedings of the Third Symposium on Operating Systems Design and Implementation, New Orleans, USA, February 1999*

Practical Byzantine Fault Tolerance

Miguel Castro and Barbara Liskov
Laboratory for Computer Science,
Massachusetts Institute of Technology,
545 Technology Square, Cambridge, MA 02139
{castro,liskov}@lcs.mit.edu

Abstract

This paper describes a new replication algorithm that is able to tolerate Byzantine faults. We believe that Byzantine-fault-tolerant algorithms will be increasingly important in the future because malicious attacks and software errors are increasingly common and can cause faulty nodes to exhibit arbitrary behavior. Whereas previous algorithms assumed a synchronous system or were too slow to be used in practice, the algorithm described in this paper is practical: it works in asynchronous environments like the Internet and incorporates several important optimizations that improve the response time of previous algorithms by more than an order of magnitude. We implemented a Byzantine-fault-tolerant NFS service using our algorithm and measured its performance. The results show that our service is only 3% slower than a standard unreplicated NFS.

and replication techniques that tolerate Byzantine faults (starting with [19]). However, most earlier work (e.g., [3, 24, 10]) either concerns techniques designed to demonstrate theoretical feasibility that are too inefficient to be used in practice, or assumes synchrony, i.e., relies on known bounds on message delays and process speeds. The systems closest to ours, Rampart [30] and SecureRing [16], were designed to be practical, but they rely on the synchrony assumption for correctness, which is dangerous in the presence of malicious attacks. An attacker may compromise the safety of a service by delaying non-faulty nodes or the communication between them until they are tagged as faulty and excluded from the replica group. Such a denial-of-service attack is generally easier than gaining control over a non-faulty node.

http://pmg.csail.mit.edu/papers/osdi99.pdf

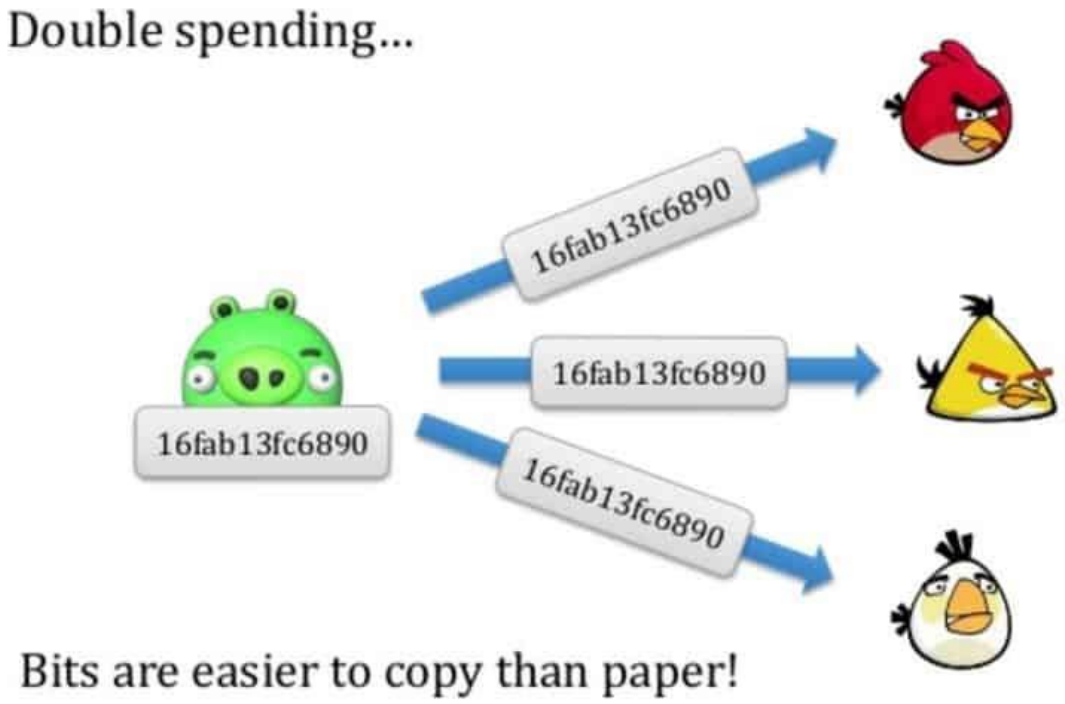
Problemática. SPAM.

Propuesta Solución. SPAM.

HASHCASH

ADAM Back, 1997

Problemática. Doble Gasto.



Source: https://coinsutra.com/bitcoin-double-spending/

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.

https://bitcoin.org/bitcoin.pdf

Propuesta Solución. Doble Gasto.

Bitcoin v0.1 released

Satoshi Nakamoto | Fri, 09 Jan 2009 17:05:49 -0800

Announcing the first release of Bitcoin, a new electronic cash system that uses a peer-to-peer network to prevent double-spending. It's completely decentralized with no server or central authority.

See bitcoin.org for screenshots.

Download link:
http://downloads.sourceforge.net/bitcoin/bitcoin-0.1.0.rar

Windows only for now. Open source C++ code is included.

- Unpack the files into a directory
- Run BITCOIN.EXE
- It automatically connects to other nodes

If you can keep a node running that accepts incoming connections, you'll really be helping the network a lot. Port 8333 on your firewall needs to be open to receive incoming connections.

The software is still alpha and experimental. There's no guarantee the system's state won't have to be restarted at some point if it becomes necessary, although I've done everything I can to build in extensibility and versioning.

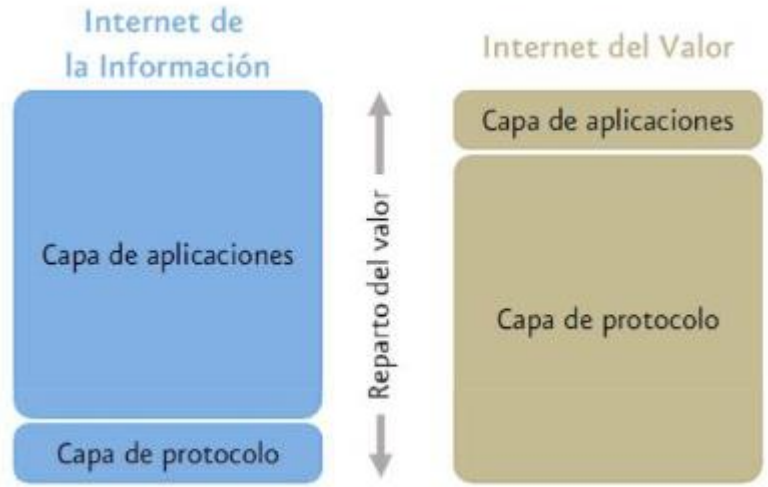
BLOCKCHAIN

Blockchain. Ledger.

- ***Ledger distribuido***.
  - Historia de todas las transacciones.
  - Sólo añadir, pasado inmutable.
  - Distribuida y replicada.
- ***Criptografía***.
  - Integridad del ledger.
  - Autenticidad de la transacción.
  - Privacidad de las transacciones.
  - Identidad de los participantes.
- ***Consenso.***
  - Protocolo descentralizado.
  - Control compartido tolerante a fallos.
  - Validación transacciones.
- ***Lógica de negocio***.
  - Lógica embebida en el ledger. (***Smart contracts***)

Blockchain. Definición

> *“ Definiremos Blockchain como una tecnología de registros distribuidos, protegidos criptográficamente y agrupados secuencialmente en bloques inmutables”.*

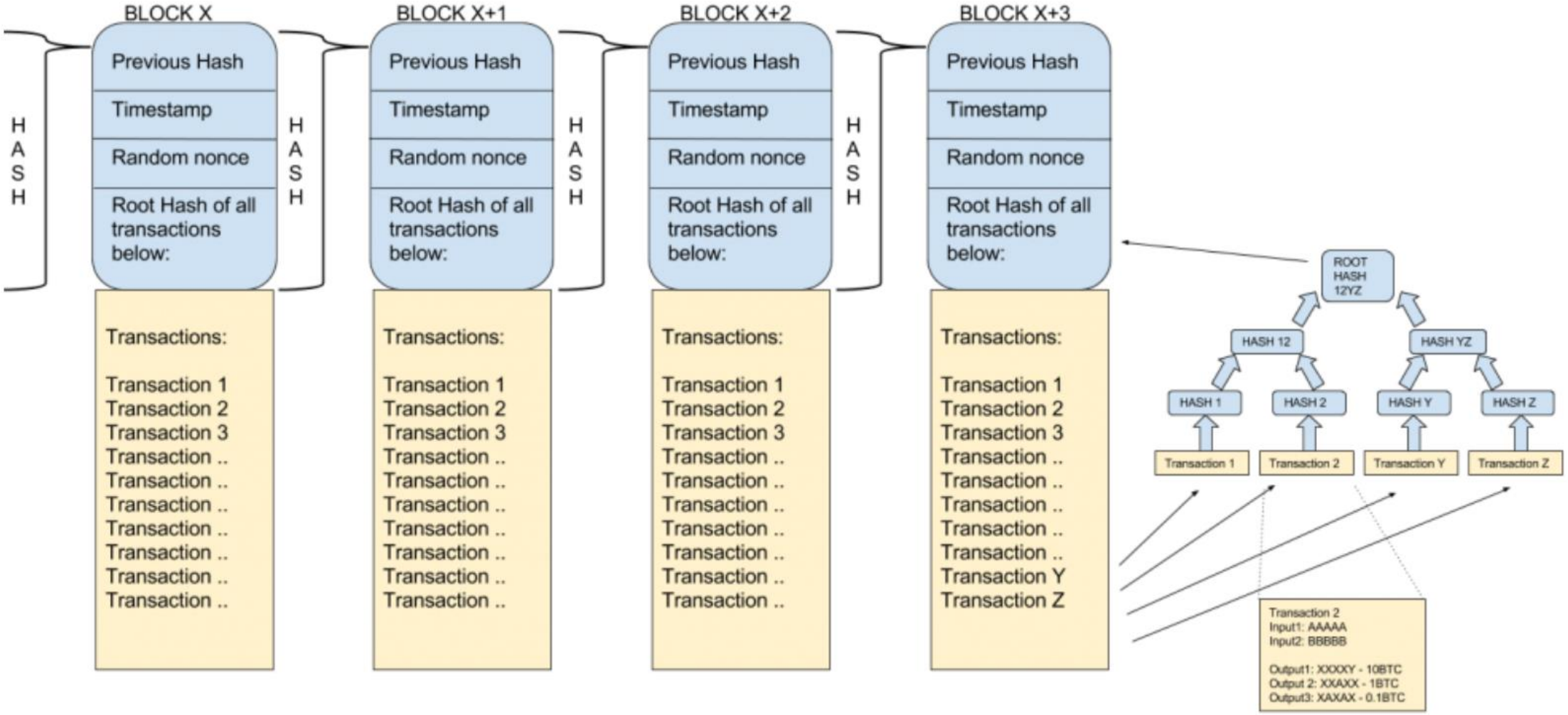


CARACTERÍSTICAS:

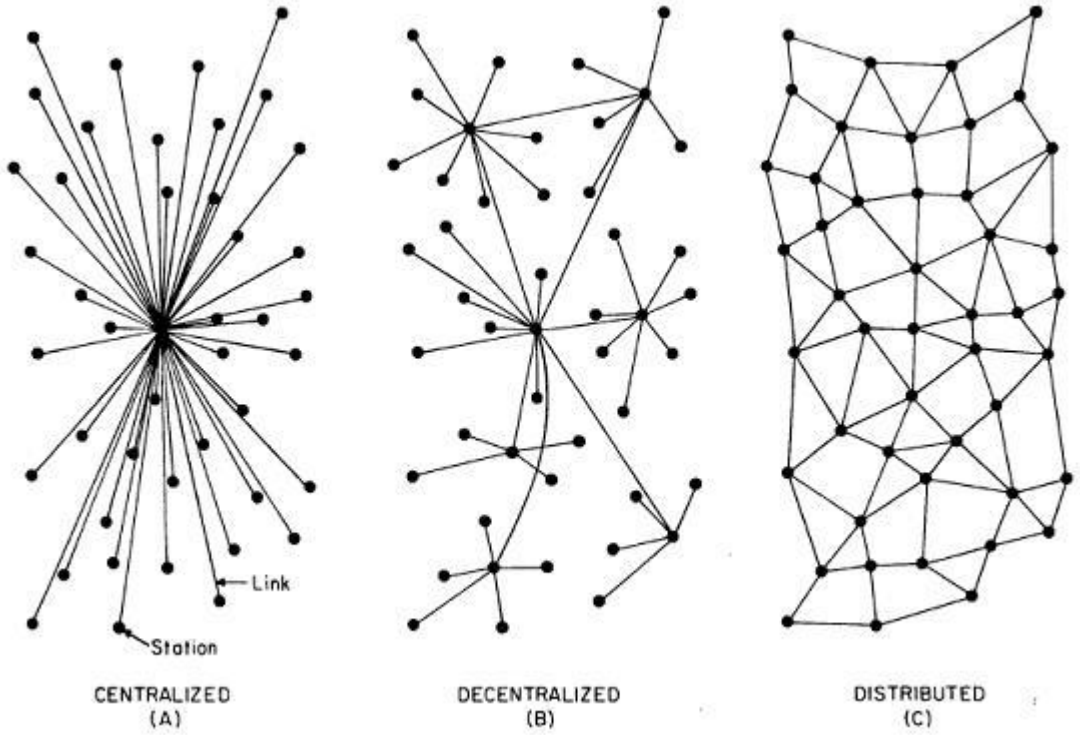
- Distribuida.
- Inmutable.
- Transparente.
- No Repudio.
- Homomórfico.

Teorema CAP: Disponibilidad y tolerante a fallos pero sin consistencia

Blockchain. Bloques.



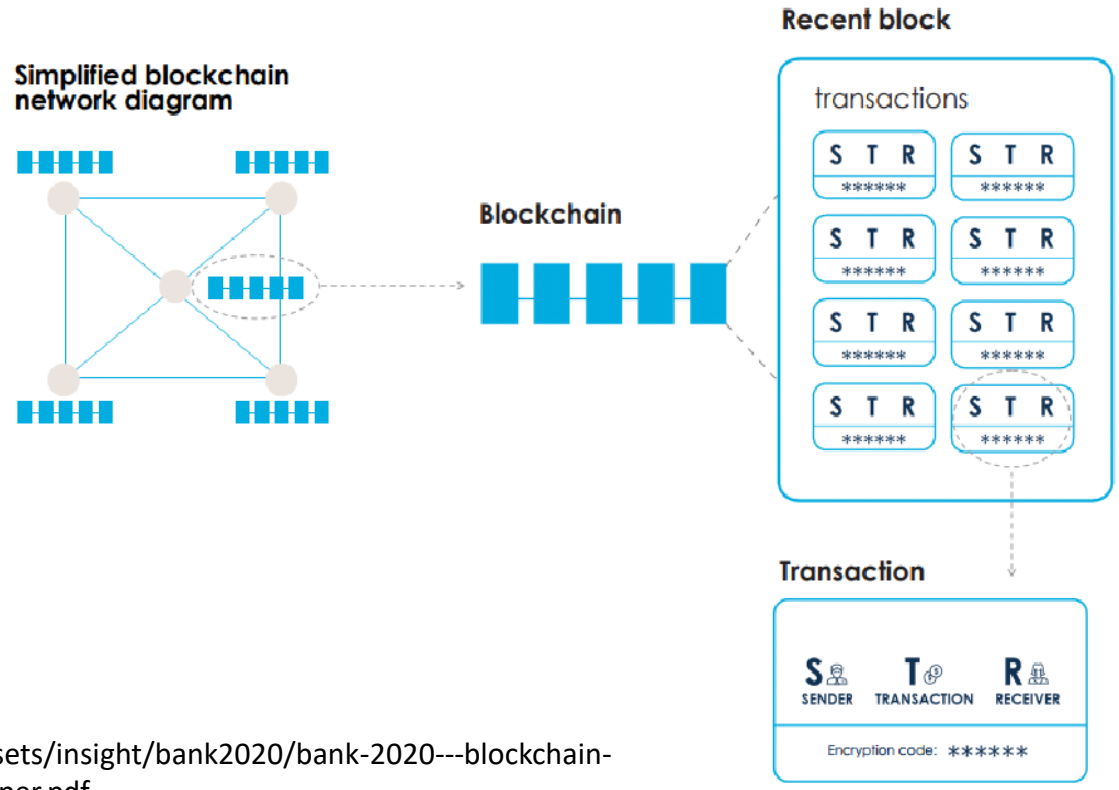
Blockchain. Malentendidos.



"La cadena de bloques es una red P2P en la que todos los nodos son iguales entre sí dando como resultado un sistema distribuido resiliente."

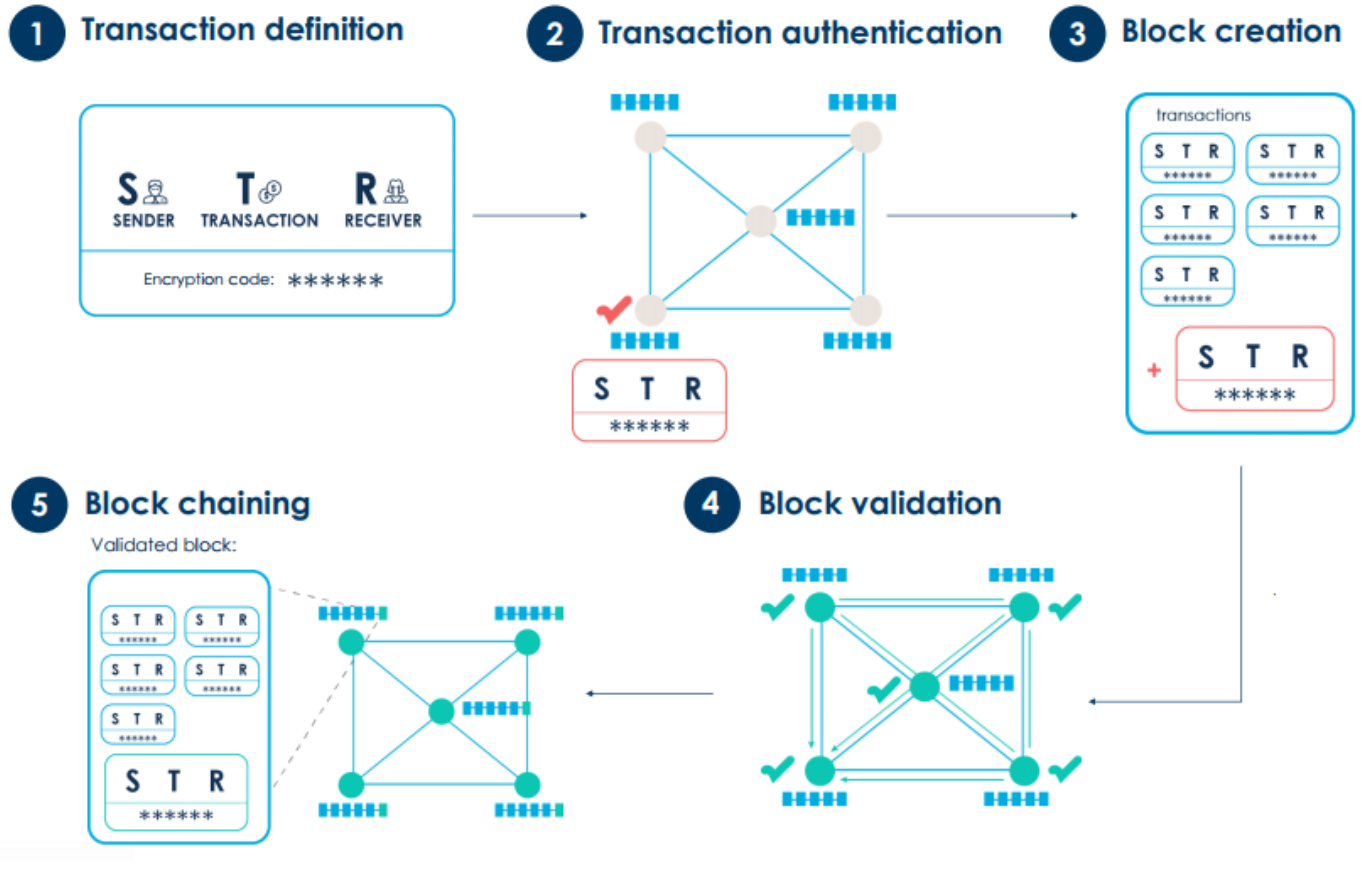
"Sistema distribuido que proporciona la descentralización de las entidades autoritativas."

Blockchain. Componentes.

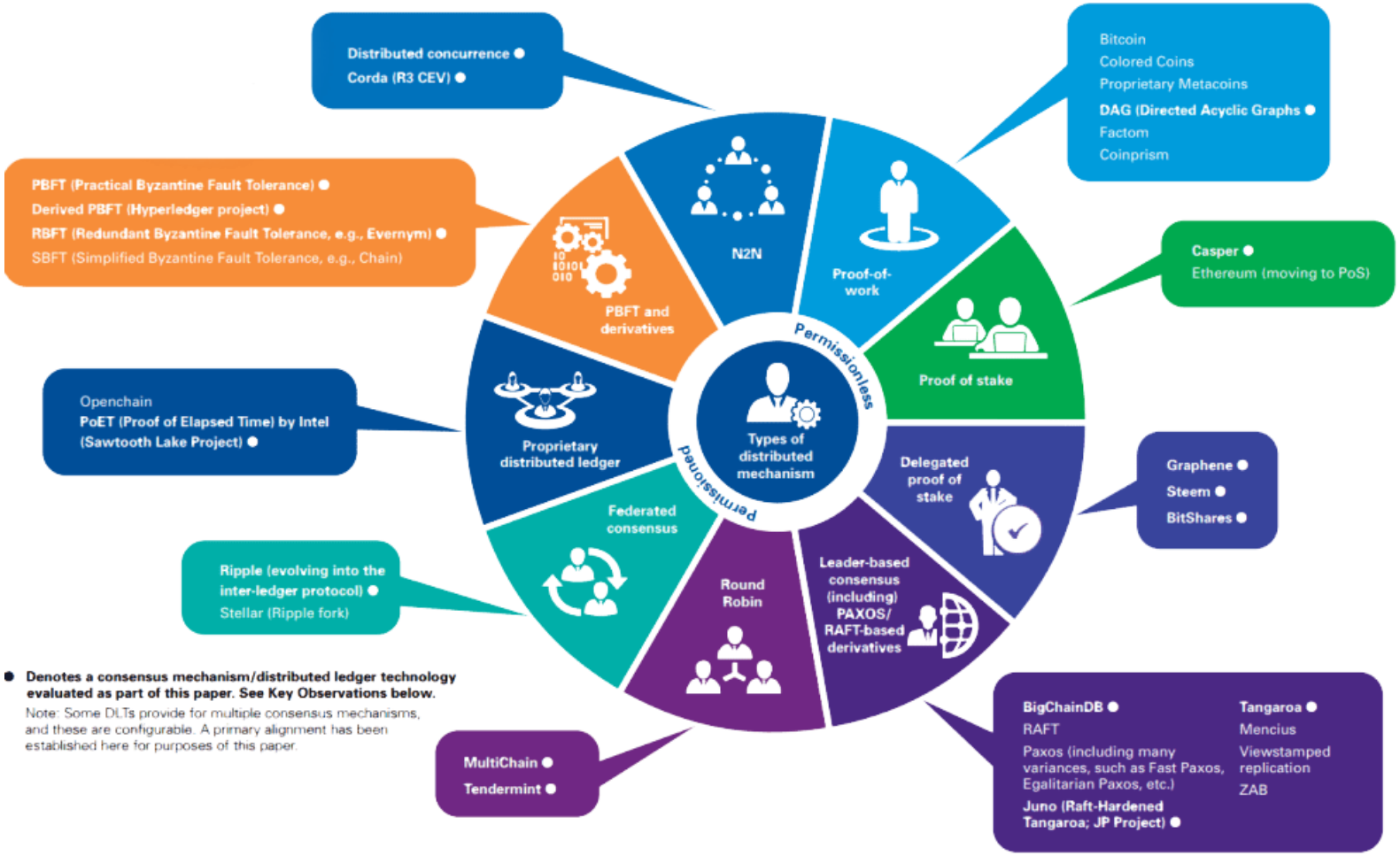


SOURCE: https://www.evry.com/globalassets/insight/bank2020/bank-2020---blockchain-powering-the-internet-of-value---whitepaper.pdf

Blockchain. Funcionamiento.



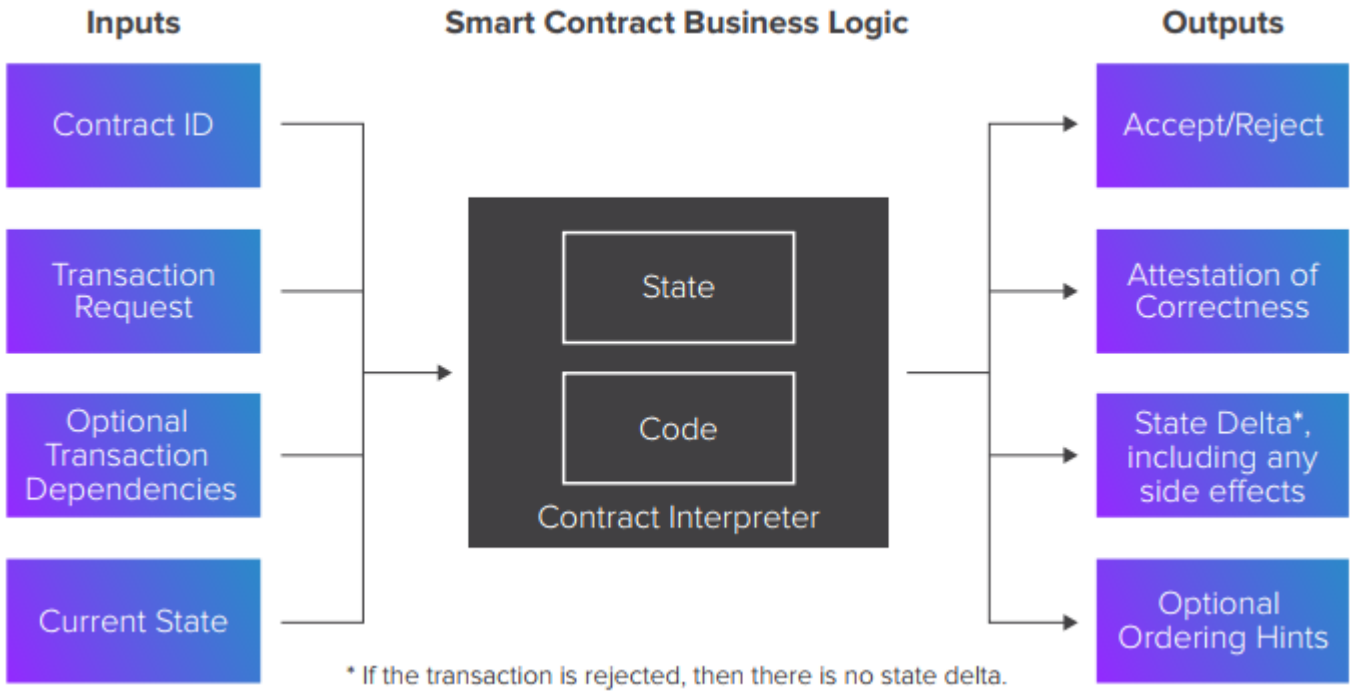
SOURCE:
https://www.evry.com/globalassets/insight/bank2020/bank-2020---blockchain-powering-the-internet-of-value---whitepaper.pdf



Blockchain. Consenso.

Source: https://assets.kpmg.com/content/dam/kpmg/pdf/2016/06/kpmg-blockchain-consensus-mechanism.pdf

Blockchain. Smart Contract.



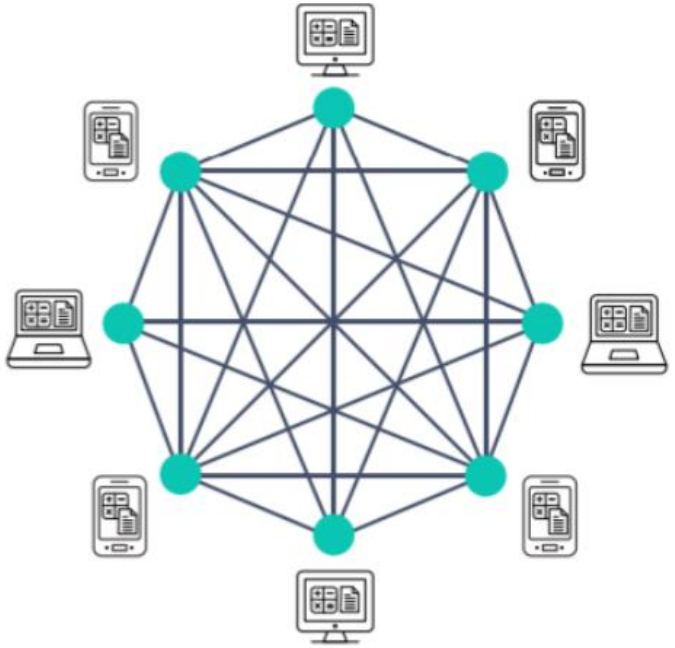
Source: Hyperledger_Arch_WG_Paper_2_SmartContracts.pdf

"El programa puede definir reglas y consecuencias estrictas del mismo modo que lo haría un documento legal tradicional, pero a diferencia de los contratos tradicionales, también puede tomar información como input, procesarla según las reglas establecidas en el contrato y adoptar cualquier medida que se requiera como resultado de ello"

Javier Sebastián, BBVA Research

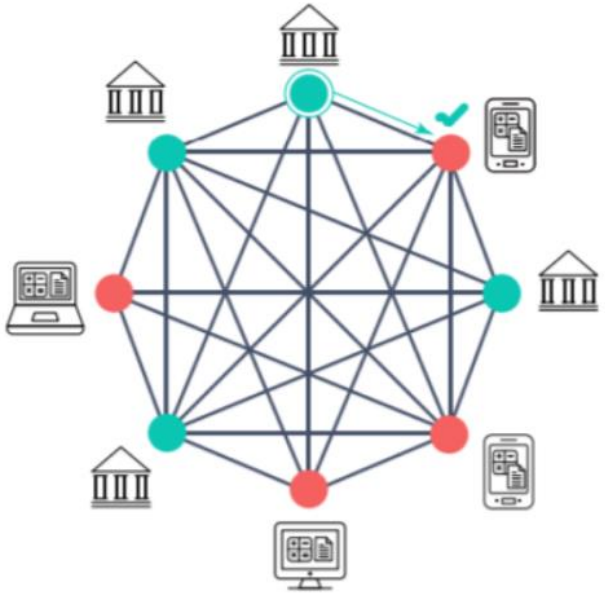
Blockchain. Privadas vs Públicas.

RED PÚBLICA



Nodos Validadores de la red.

RED PRIVADA



Nodos Validadores de la red.

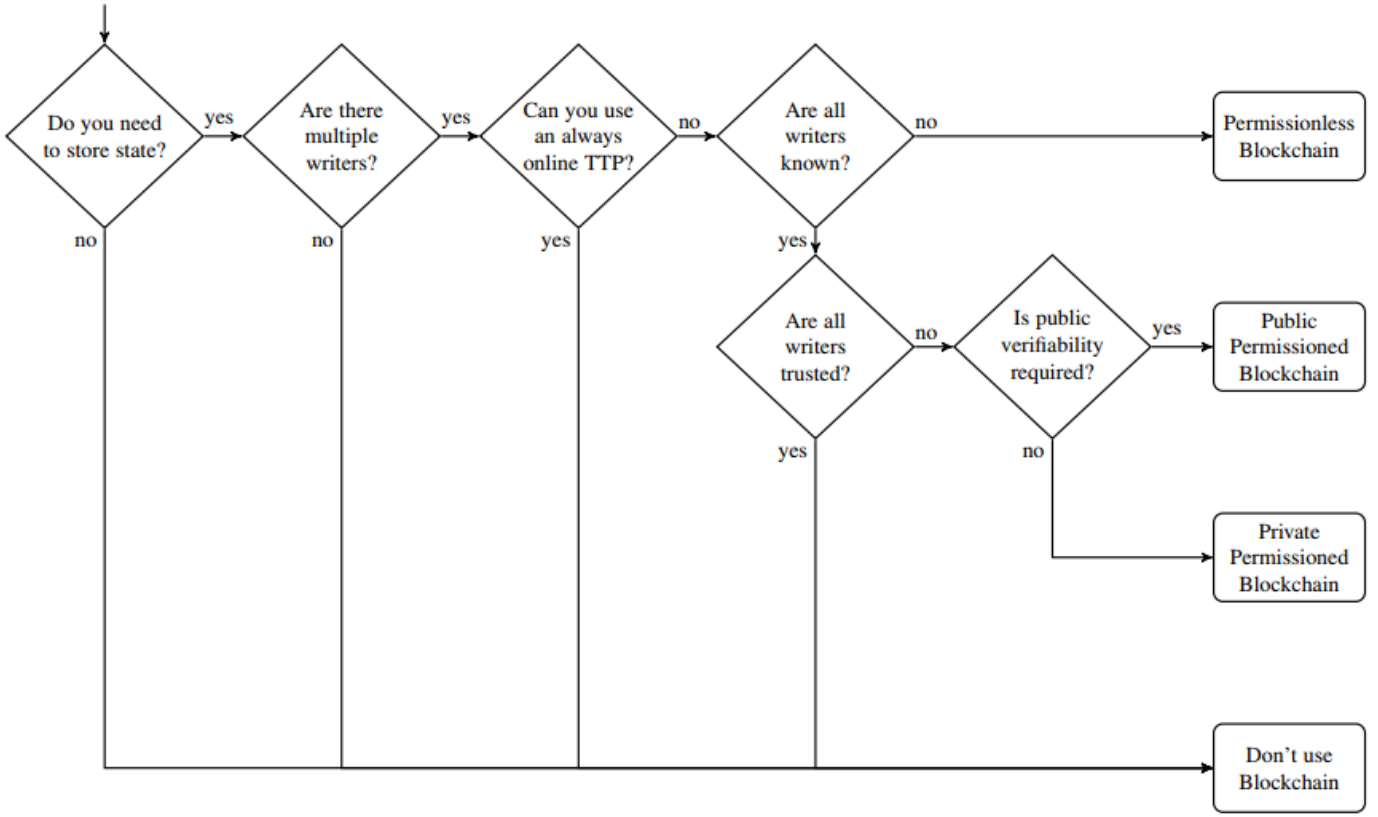
Nodos miembro. Inician/reciben transacciones

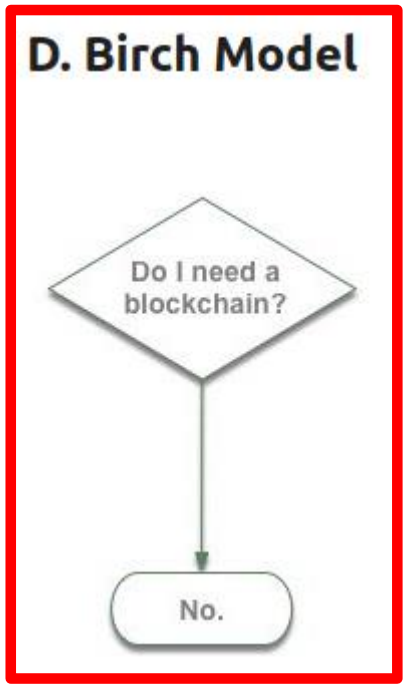
Blockchain. Privadas vs Públicas.

	PRIVADA	PÚBLICA
Acceso de los usuarios al registro de transacciones.	PERMISIONADO	PÚBLICO
Acceso de los usuarios como participante de la red.	CERRRADO	ABIERTO
Estructura de una red de nodos.	DISTRIBUIDO	DESCENTRALIZADO
Acceso de los usuarios al contenido de las transacciones	ANÓNIMO	ANÓNIMA/ PSEUDOANÓNIMO
Velocidad validación transacción	RÁPIDA	LENTA
Ejemplos	HYPERLEDGER, QUORUM, R3	BITCOIN, ETHEREUM, DASH

http://bitfury.com/content/5-white-papers-research/public-vs-private-pt1-1.pdf
http://bitfury.com/content/5-white-papers-research/public-vs-private-pt2-1.pdf

¿Necesitas Implementar Blockchain?





(*) Source: Karl Wüst, "Do you need a Blockchain?", https://eprint.iacr.org/2017/375.pdf

Blockchain. Posibles usos.

Soberanía digital
Desintermediación
Confianza
Seguridad
Transparencia

SANIDAD

- Gestión de expediente médico.
- Seguridad y confidencialidad de nuestros datos.

IOT

- Seguridad comunicación M2M.
- Compartición de datos.
- Smart City.

FINTECH

- Nuevos modelos de negocio.
- Reducción de costes de intermediarios.

SEGUROS

- Pago por el uso que se haga del vehículo.
- El vehículo puede negociar la contratación del seguro.

BIENES DIGITALES

- Autoría y pertenencia.
- Reducción de costes de intermediarios.

OPENDATA

- Participación ciudadana.
- Voto electrónico.

CADENA DE SUMINISTROS

- Detección de falsificación y manipulación.
- Simplifica la transmisión de información entre los participantes.

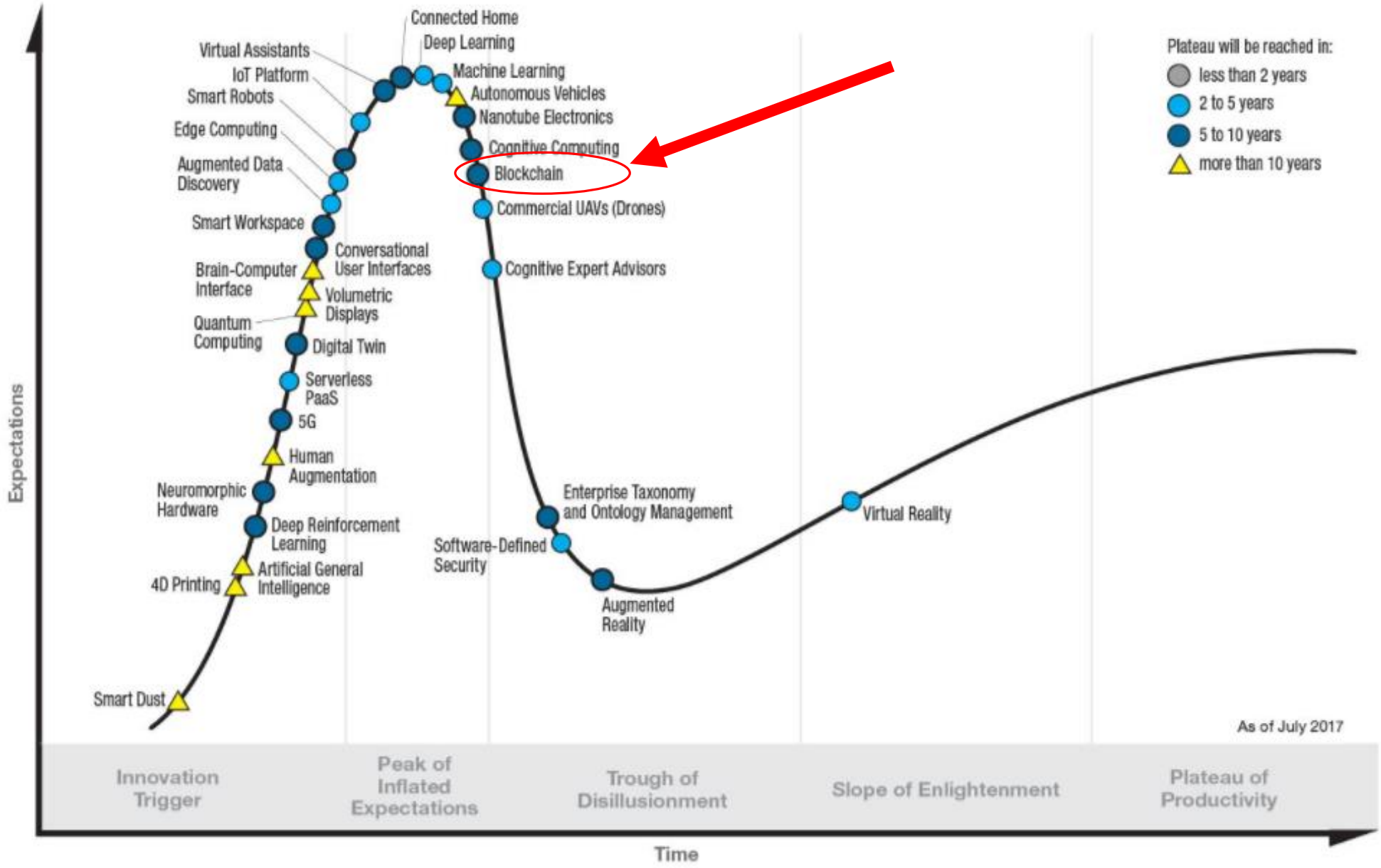
IDENTIDAD

- Identidad Digital.

SEGURIDAD

- Defensa

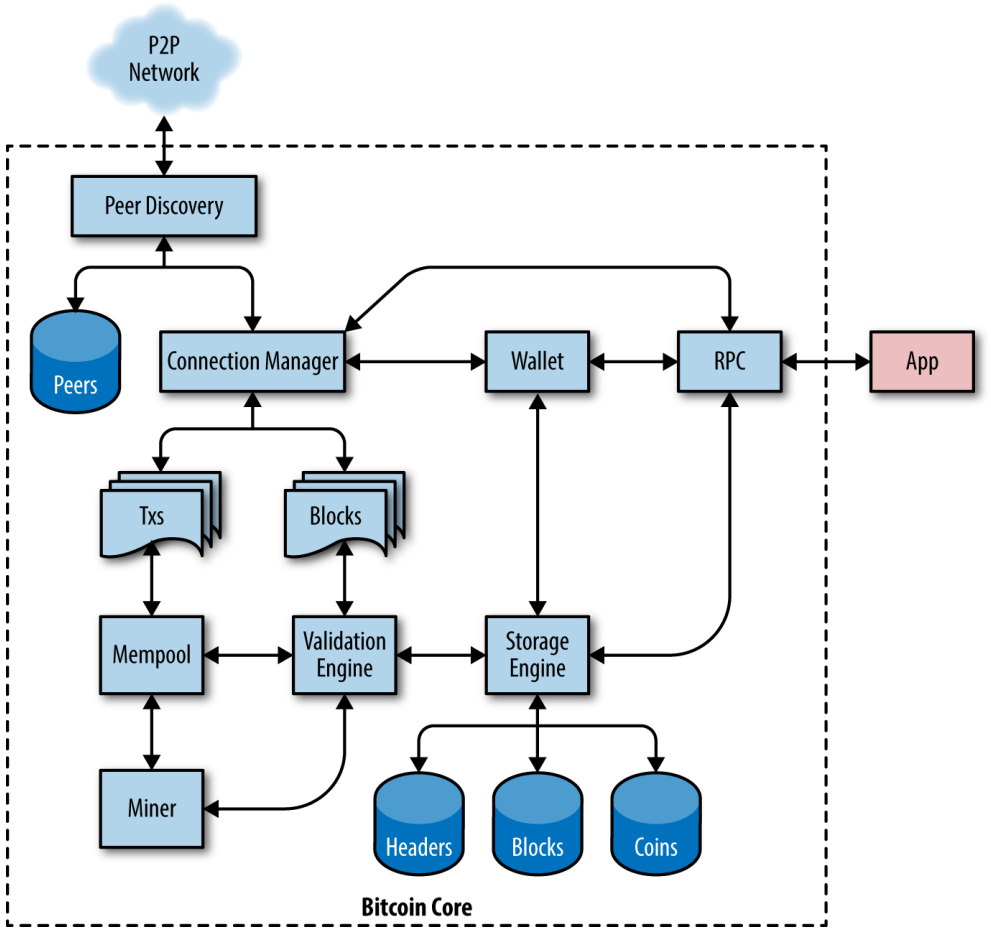
Ciclo Hype


Connected Home
Deep Learning
Virtual Assistants
IoT Platform
Machine Learning
Smart Robots
Autonomous Vehicles
Edge Computing
Nanotube Electronics
Augmented Data Discovery
Cognitive Computing
Blockchain
Smart Workspace
Commercial UAVs (Drones)
Conversational User Interfaces
Brain-Computer Interface
Cognitive Expert Advisors
Volumetric Displays
Quantum Computing
Digital Twin
Serverless PaaS
5G
Human Augmentation
Neuromorphic Hardware
Enterprise Taxonomy and Ontology Management
Deep Reinforcement Learning
Virtual Reality
Software-Defined Security
Artificial General Intelligence
4D Printing
Augmented Reality
Smart Dust
Plateau will be reached in:
less than 2 years
2 to 5 years
5 to 10 years
more than 10 years
Expectations
As of July 2017
Innovation Trigger
Peak of Inflated Expectations
Trough of Disillusionment
Slope of Enlightenment
Plateau of Productivity
Time

REDES PUBLICAS

BITCOIN, ETHEREUM, MONERO

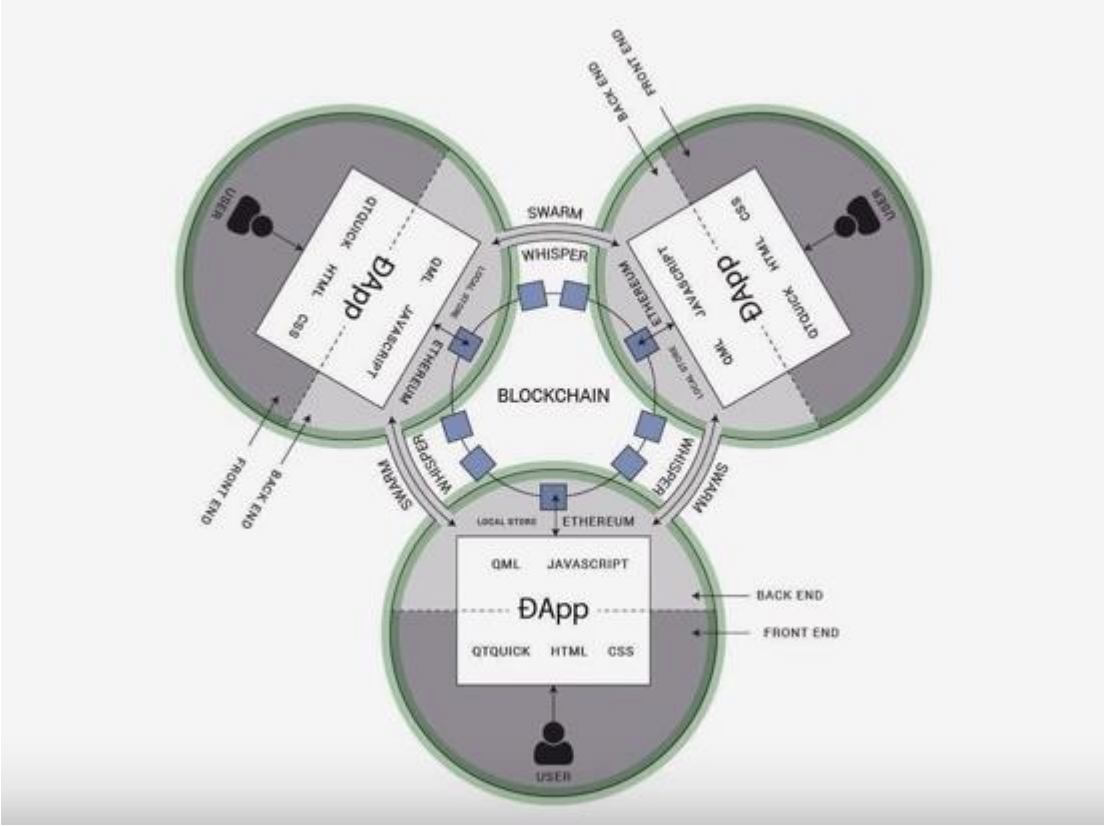
BITCOIN

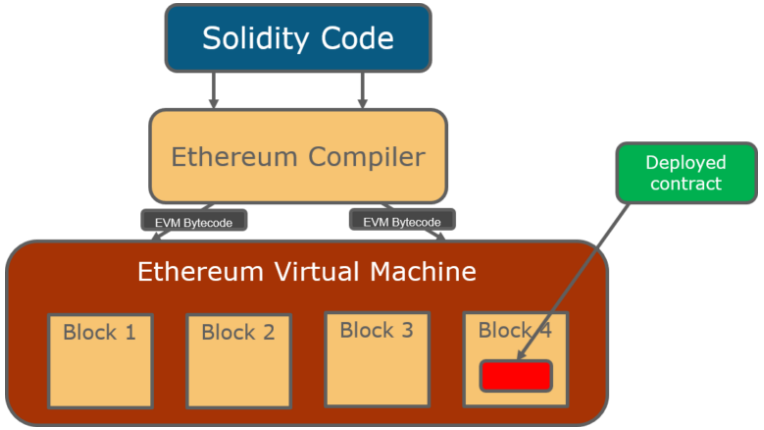


Source:
https://github.com/bitcoinbook/bitcoinbook/blob/develop/ch03.asciidoc

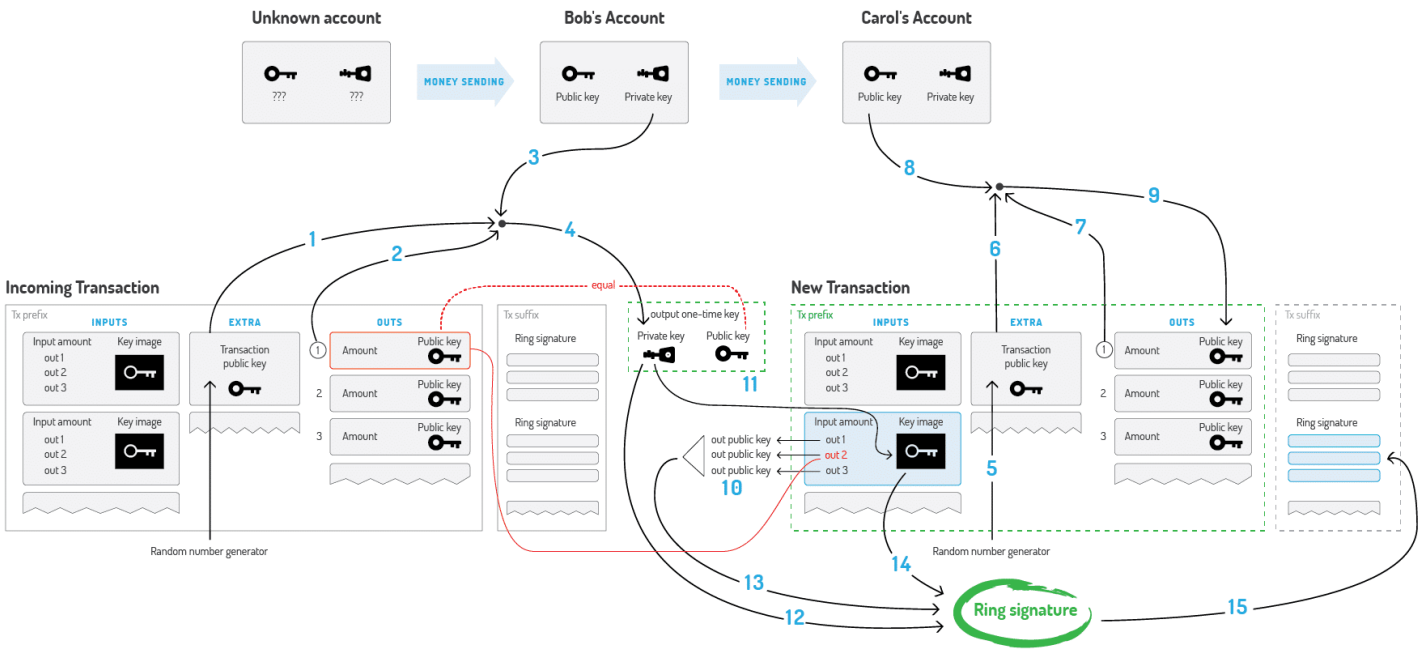
Ethereum

ethereum





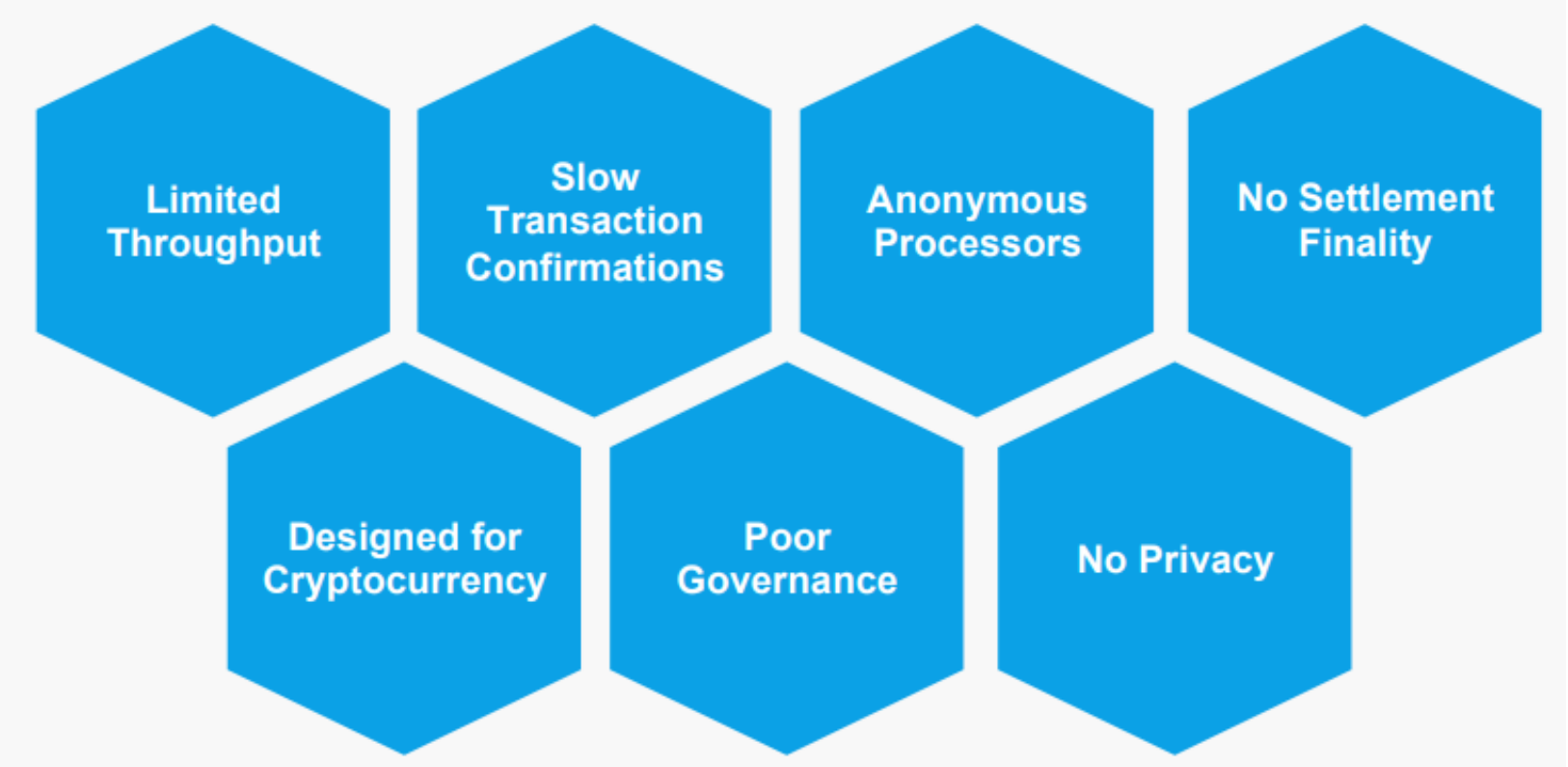
Monero (XMR)


Unknown account
Bob's Account
Carol's Account
MONEY SENDING
MONEY SENDING
???
???
Public key
Private key
Public key
Private key
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
Incoming Transaction
New Transaction
Tx prefix
INPUTS
EXTRA
OUTS
Tx suffix
Input amount
Key image
out 1
out 2
out 3
Transaction public key
Amount
Public key
Ring signature
equal
output one-time key
Private key
Public key
out public key
out public key
out public key
Random number generator
Random number generator
Ring signature

REDES PRIVADAS

HYPERLEDGER, ETHEREUM, ALASTRIA, NEM

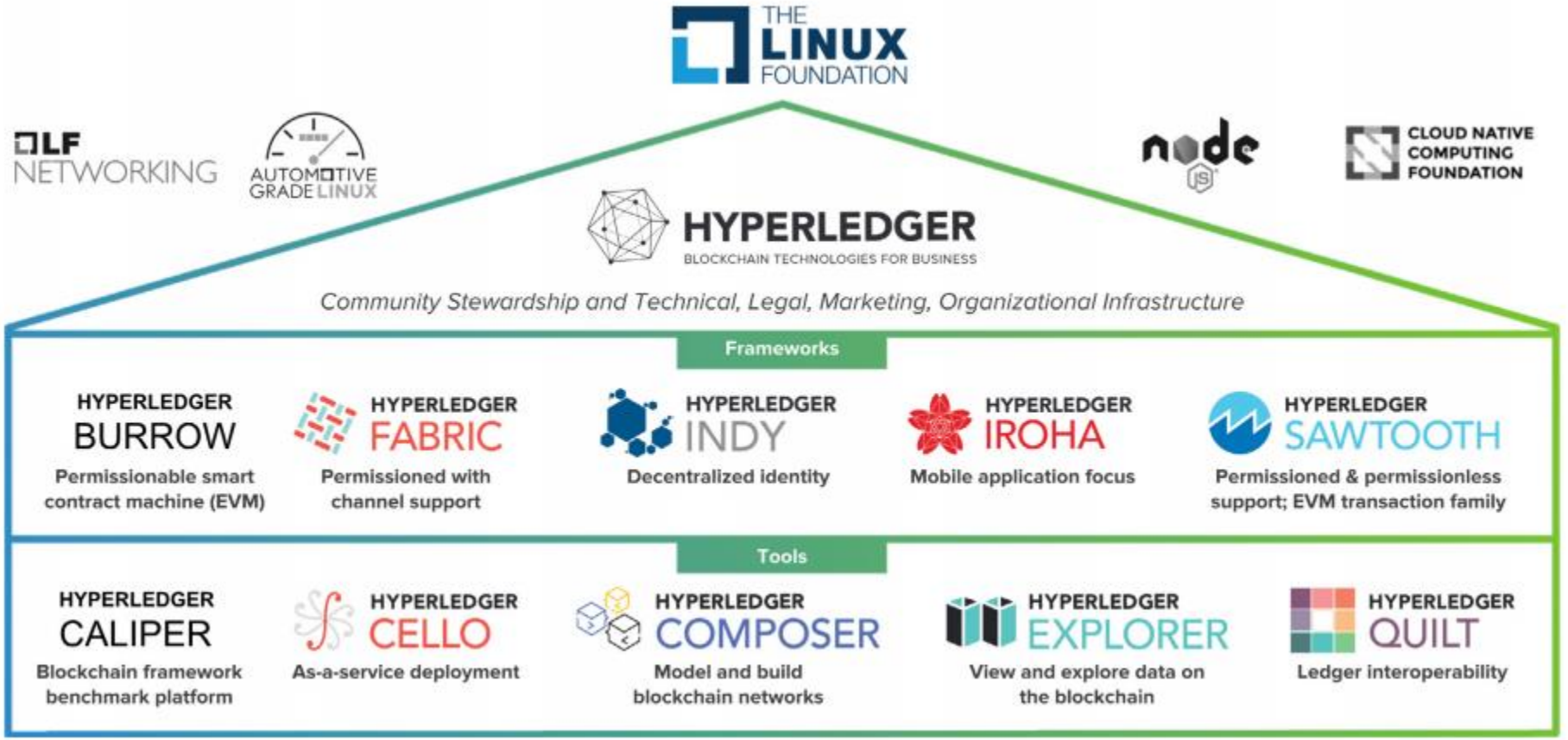
Problemáticas



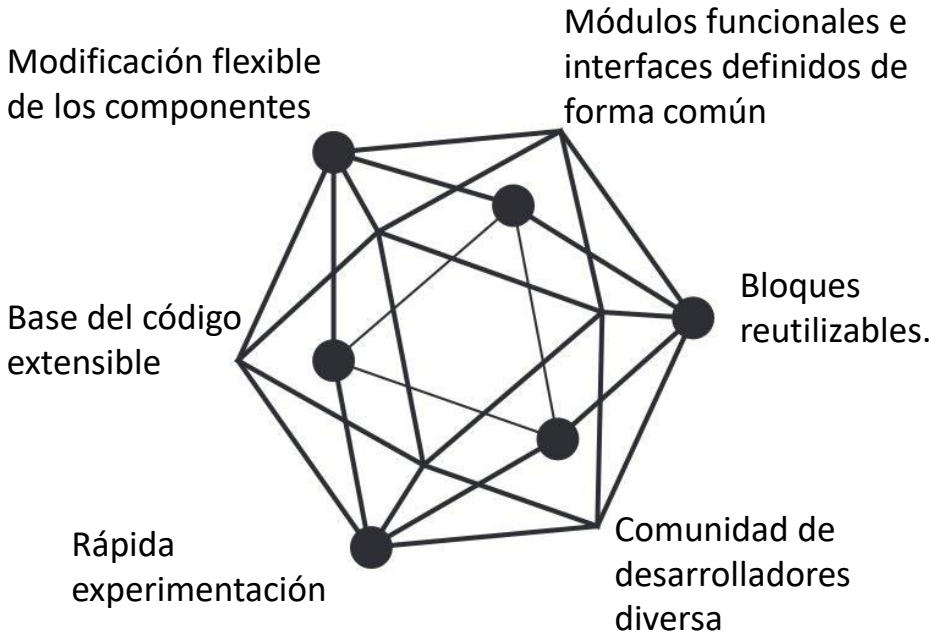
Hyperledger

> *"El papel más valioso que el proyecto Hyperledger puede desempeñar es servir como una **fuente confiable** para la comunidad de desarrollo de software de **fuente abierta**, innovadora y orientada a la calidad; y el crear **componentes y plataformas modulares** de código abierto; todos enfocados en DLT y tecnologías de contratos inteligentes. Si Hyperledger puede forjar una **marca** que sea ampliamente vista como la plataforma de implementación 'segura' predeterminada **para los equipos empresariales**, y ser vista como un gran hogar para la colaboración activa en torno a las nuevas tecnologías, entonces creo que podemos decir 'misión cumplida'".*
>
> ***Brian Behlendorf (Director Ejecutivo de Hyperledger)***

Hyperledger



Hyperledger



Arquitectura de Capas:

- Capa de Consenso.
- Capa de Smart Contract.
- Capa de comunicación.
- Capa de abstracción de almacenamiento.
- Capa de abstracción de la criptografía.
- Servicio de identidad.
- API's.
- Capa de interoporabilidad.

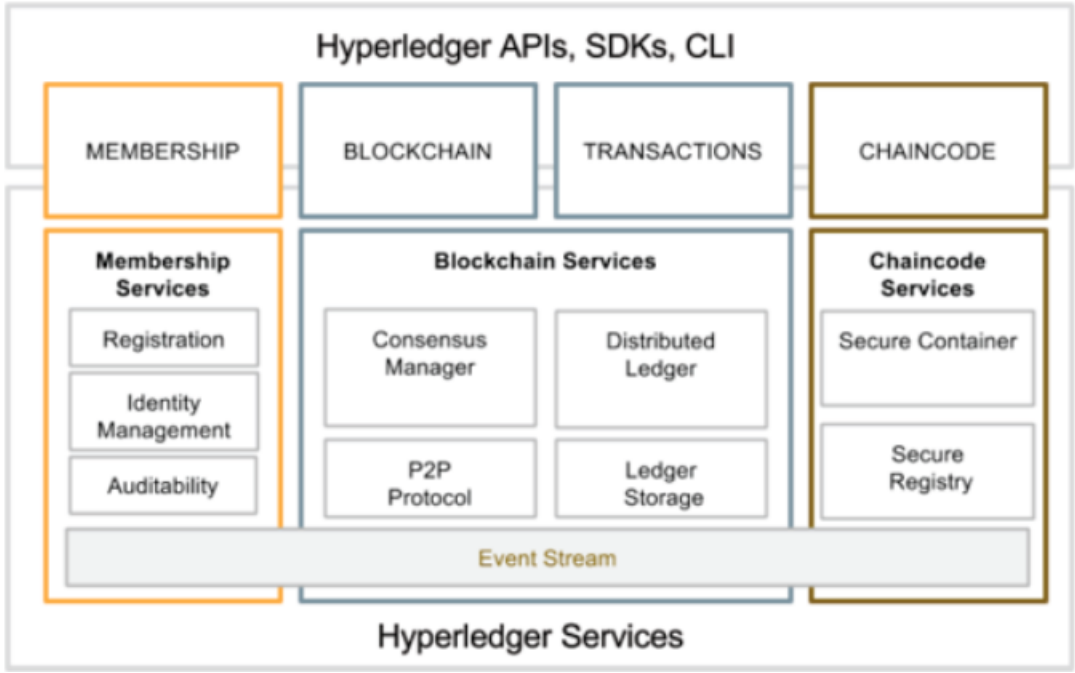
https://www.hyperledger.org/wp-content/uploads/2017/08/Hyperledger_Arch_WG_Paper_1_Consensus.pdf

Hyperledger

La interfaz de Hyperledger es el REST API

Manejo de la Identidad, privacidad, confidencialidad y auditabilidad.

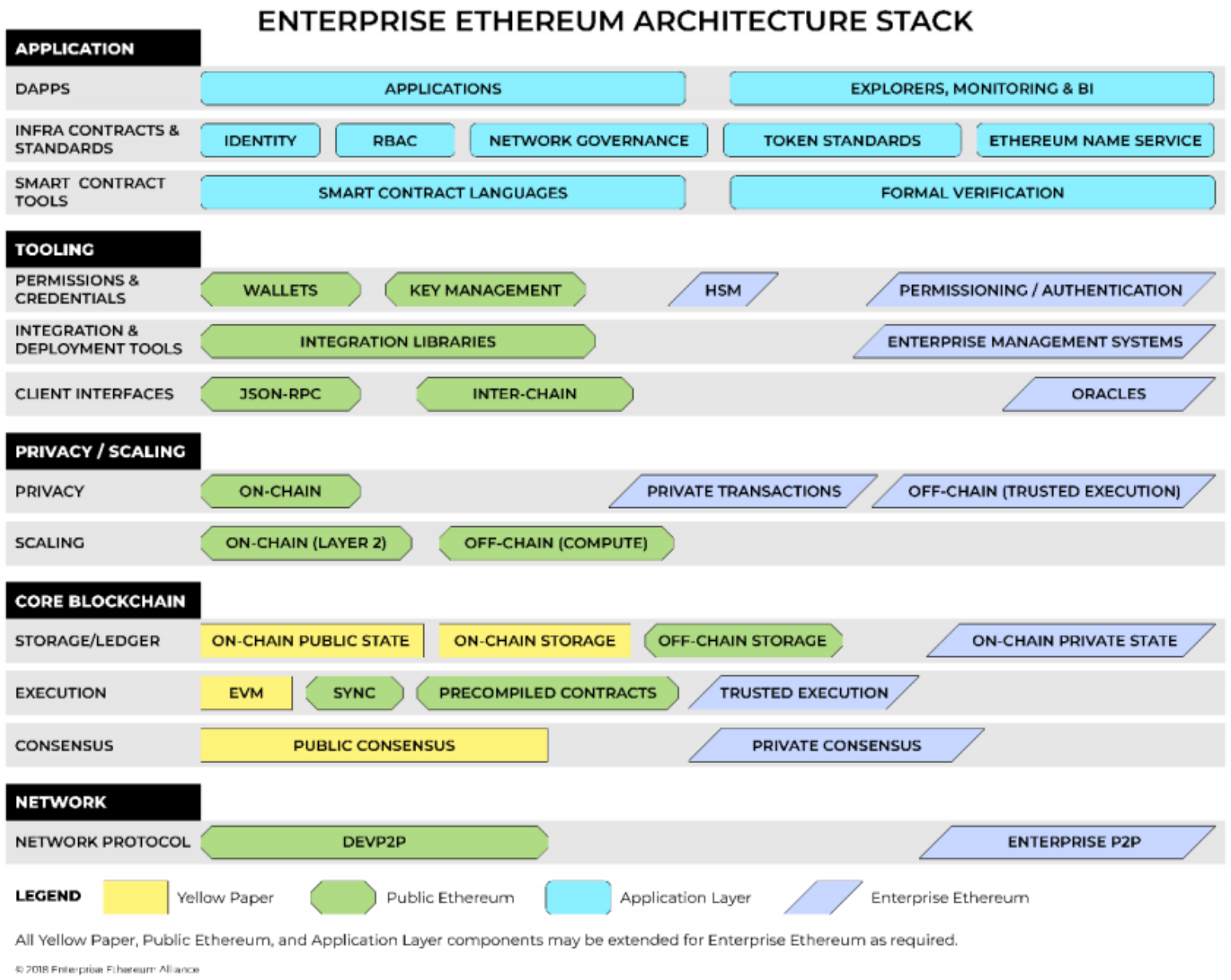
Infraestructura basada en PKI para permitir Blockchain permisionadas



Ejecución de Smart Contracts en nodos validados de forma ágil y segura.

SDK con soporte para Go, Java y Node.js

Maneja el layer distribuido mediante protocolo peer-to-peer, construido sobre HTTP/2.
Diferentes consensos. Por defecto PBFT/Sieve

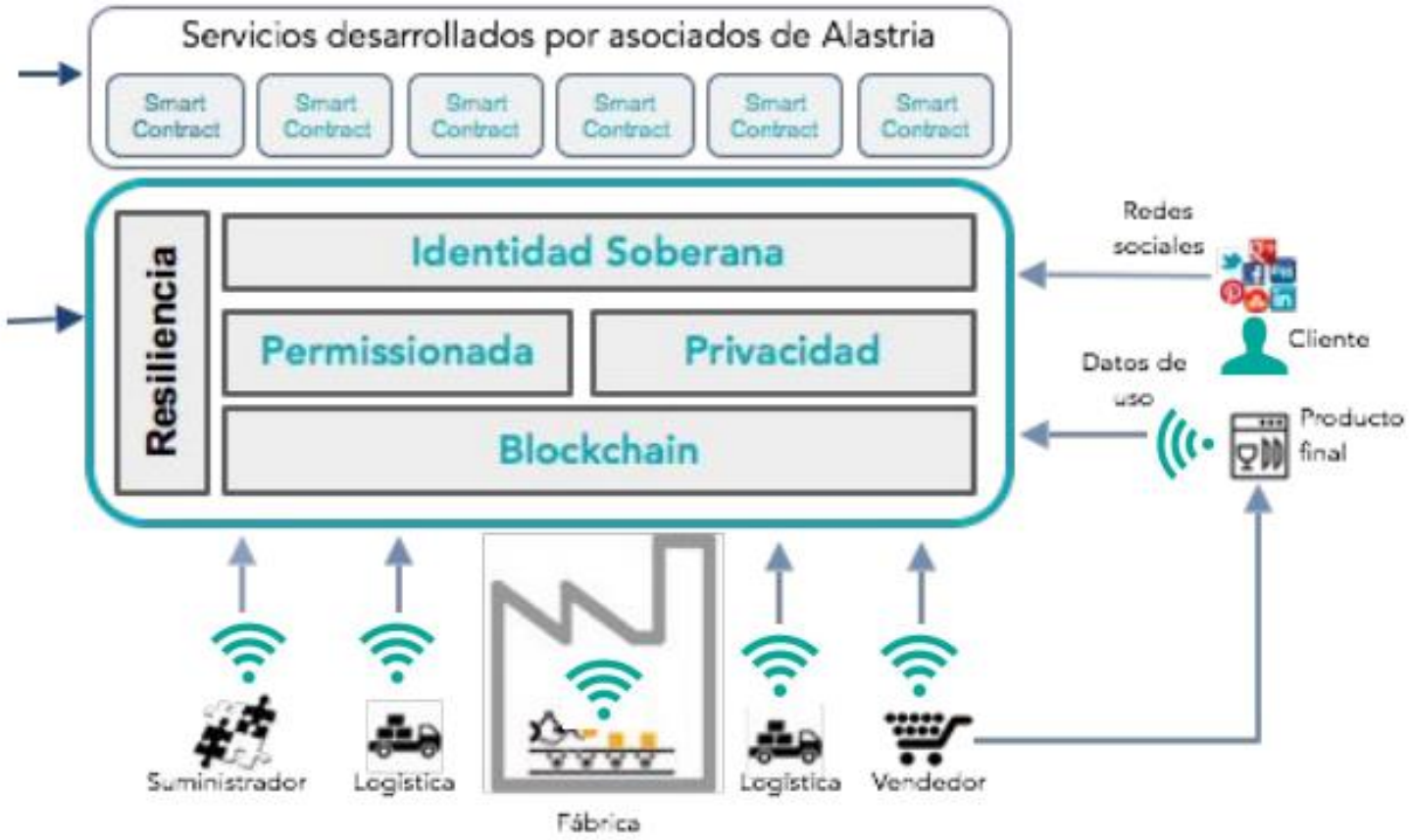

ENTERPRISE ETHEREUM ARCHITECTURE STACK
APPLICATION
DAPPS
APPLICATIONS
EXPLORERS, MONITORING & BI
INFRA CONTRACTS & STANDARDS
IDENTITY
RBAC
NETWORK GOVERNANCE
TOKEN STANDARDS
ETHEREUM NAME SERVICE
SMART CONTRACT TOOLS
SMART CONTRACT LANGUAGES
FORMAL VERIFICATION
TOOLING
PERMISSIONS & CREDENTIALS
WALLETS
KEY MANAGEMENT
HSM
PERMISSIONING / AUTHENTICATION
INTEGRATION & DEPLOYMENT TOOLS
INTEGRATION LIBRARIES
ENTERPRISE MANAGEMENT SYSTEMS
CLIENT INTERFACES
JSON-RPC
INTER-CHAIN
ORACLES
PRIVACY / SCALING
PRIVACY
ON-CHAIN
PRIVATE TRANSACTIONS
OFF-CHAIN (TRUSTED EXECUTION)
SCALING
ON-CHAIN (LAYER 2)
OFF-CHAIN (COMPUTE)
CORE BLOCKCHAIN
STORAGE/LEDGER
ON-CHAIN PUBLIC STATE
ON-CHAIN STORAGE
OFF-CHAIN STORAGE
ON-CHAIN PRIVATE STATE
EXECUTION
EVM
SYNC
PRECOMPILED CONTRACTS
TRUSTED EXECUTION
CONSENSUS
PUBLIC CONSENSUS
PRIVATE CONSENSUS
NETWORK
NETWORK PROTOCOL
DEVP2P
ENTERPRISE P2P
LEGEND
Yellow Paper
Public Ethereum
Application Layer
Enterprise Ethereum
All Yellow Paper, Public Ethereum, and Application Layer components may be extended for Enterprise Ethereum as required.
© 2018 Enterprise Ethereum Alliance

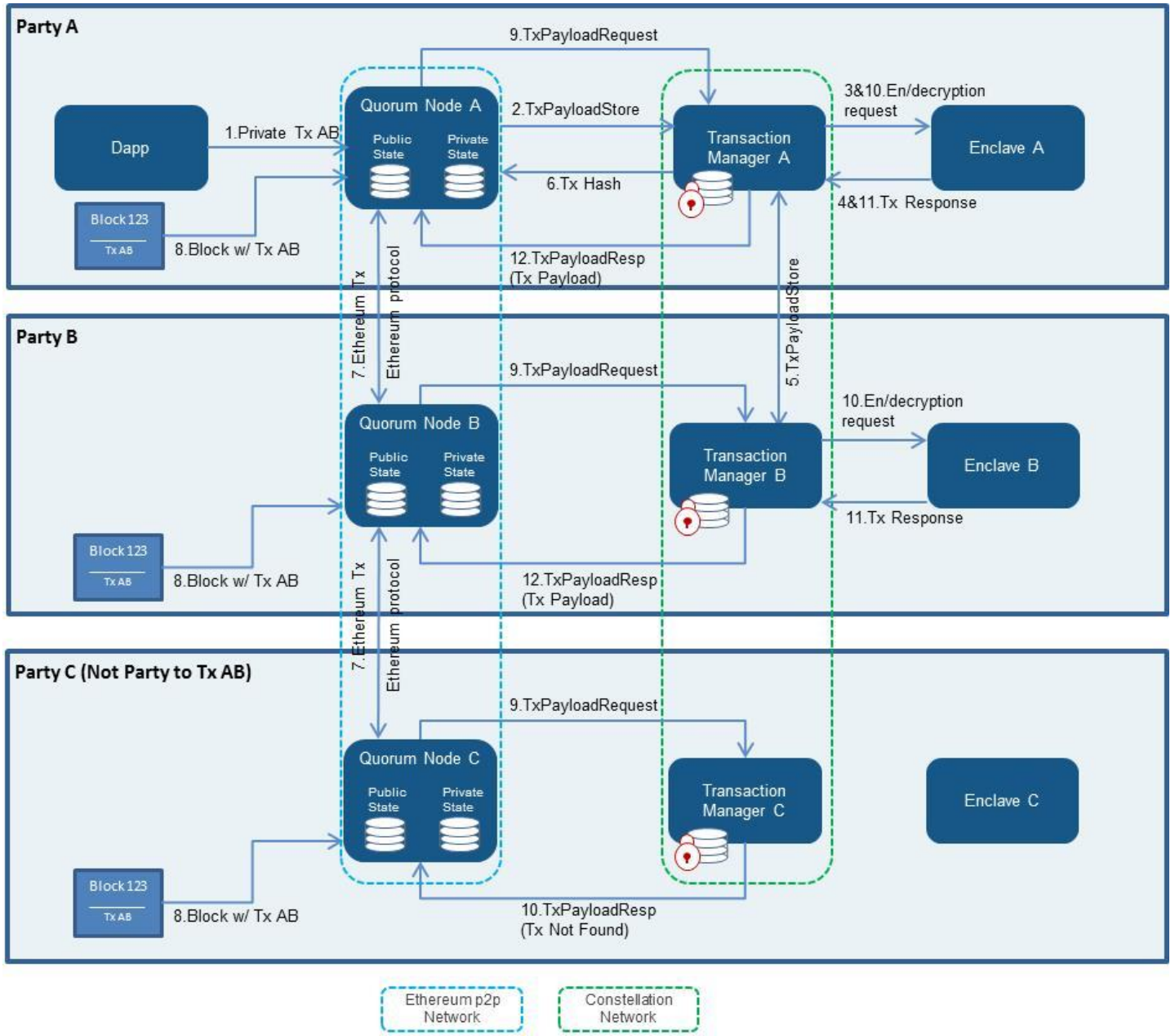
Ethereum

Alastria.

Los miembros **compiten** en las aplicaciones

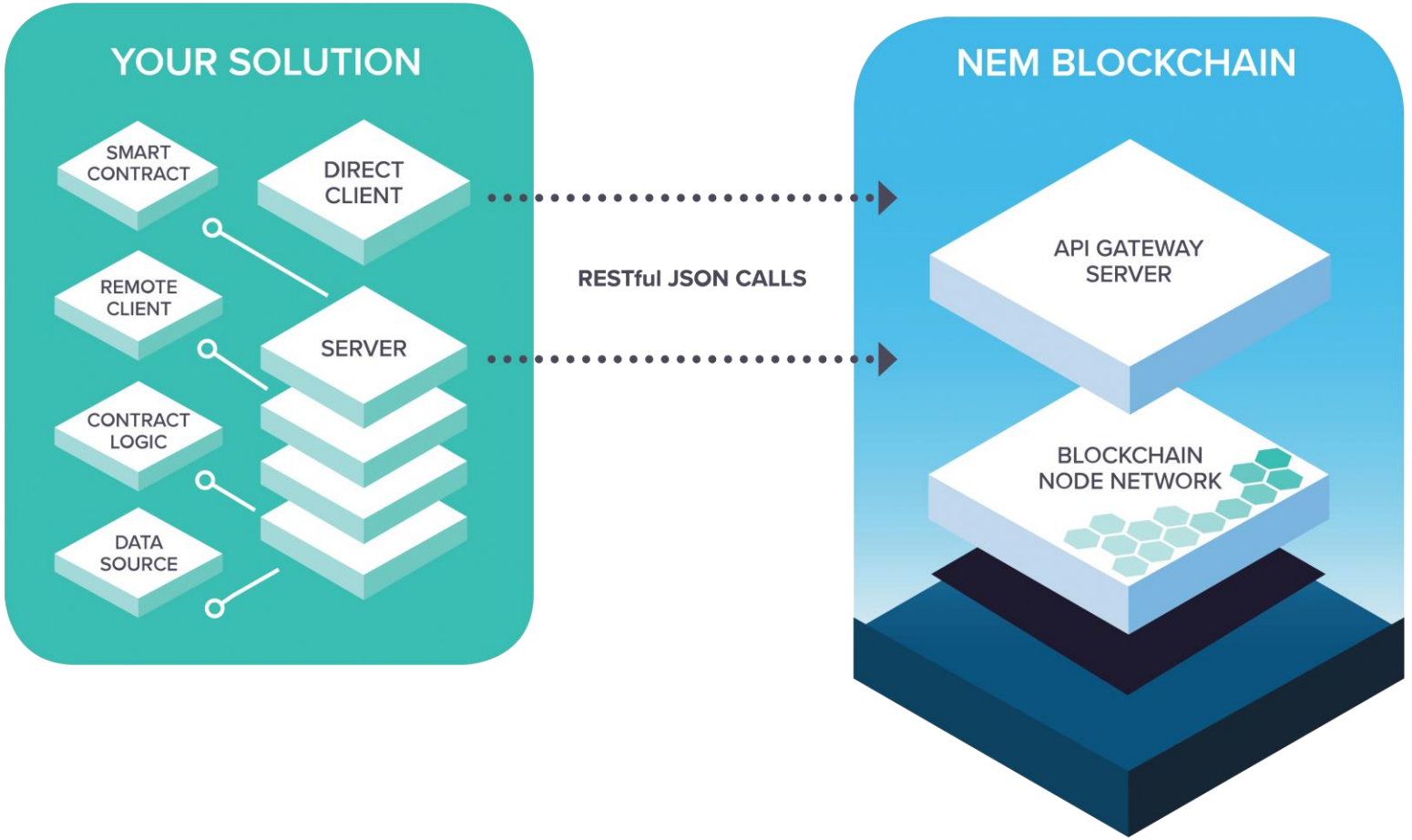
Los miembros **colaboran** en la infraestructura




Party A
9.TxPayloadRequest
Quorum Node A
Public State
Private State
2.TxPayloadStore
Transaction Manager A
3&10.En/decryption request
Enclave A
Dapp
1.Private Tx AB
6.Tx Hash
4&11.Tx Response
Block 123
Tx AB
8.Block w/ Tx AB
12.TxPayloadResp (Tx Payload)
7.Ethereum Tx
Ethereum protocol
5.TxPayloadStore
Party B
9.TxPayloadRequest
Quorum Node B
Public State
Private State
Transaction Manager B
10.En/decryption request
Enclave B
11.Tx Response
Block 123
Tx AB
8.Block w/ Tx AB
12.TxPayloadResp (Tx Payload)
7.Ethereum Tx
Ethereum protocol
Party C (Not Party to Tx AB)
9.TxPayloadRequest
Quorum Node C
Public State
Private State
Transaction Manager C
Enclave C
Block 123
Tx AB
8.Block w/ Tx AB
10.TxPayloadResp (Tx Not Found)
Ethereum p2p Network
Constellation Network

Alastria.

NEM


YOUR SOLUTION
SMART CONTRACT
DIRECT CLIENT
REMOTE CLIENT
SERVER
CONTRACT LOGIC
DATA SOURCE
RESTful JSON CALLS
NEM BLOCKCHAIN
API GATEWAY SERVER
BLOCKCHAIN NODE NETWORK

Blockchain & Industria 4.0

Industria 4.0

«la integración técnica de los sistemas ciber-físicos en la manufactura y logística y en el uso de internet en los procesos industriales»

(Kagermann et al., 2013: 14).

Blockchain en la industria 4.0

TRAZABILIDAD.

SMART CONTRACT

Blockchain en la industria 4.0

Casos de uso en el IoT de platan:

- Registros de datos de sensores.
- Identificación de dispositivos.
- Intercambio de datos.
- Descentralización y resiliencia.
- Autonomía de los dispositivos mediante Smart contract.

Tecnalia. Laboratorio industrial blockchain.

> **El centro de investigación y desarrollo tecnológico facilitará a las pymes el acceso a este sistema que garantiza la seguridad y la eficiencia de las transacciones digitales**

Este laboratorio industrial permitirá experimentar en tres áreas fundamentalmente:

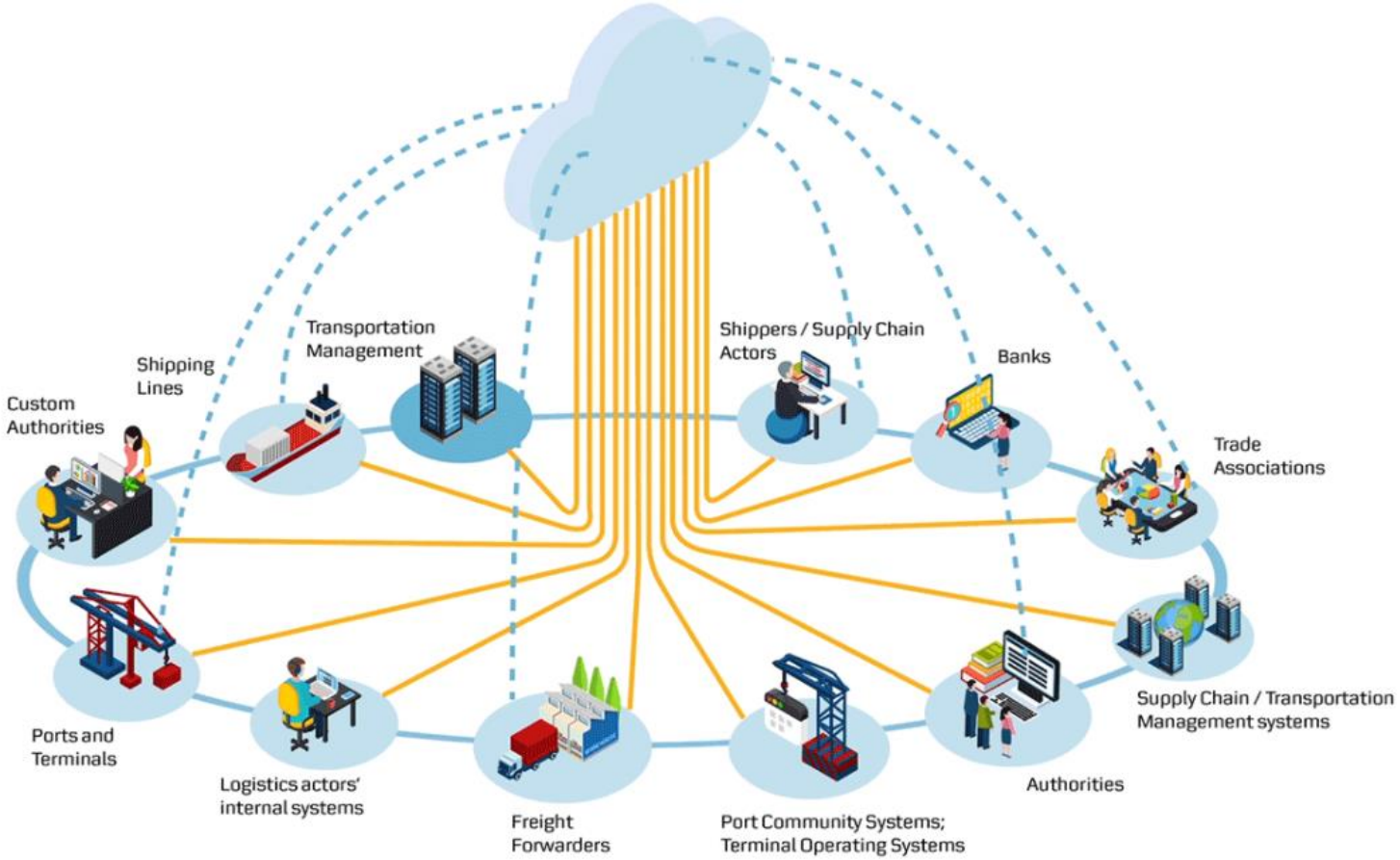
- Industria 4.0
- Socioeconomía
- Protección de la propiedad intelectual

ENTERPRISE ETHEREUM ALLIANCE

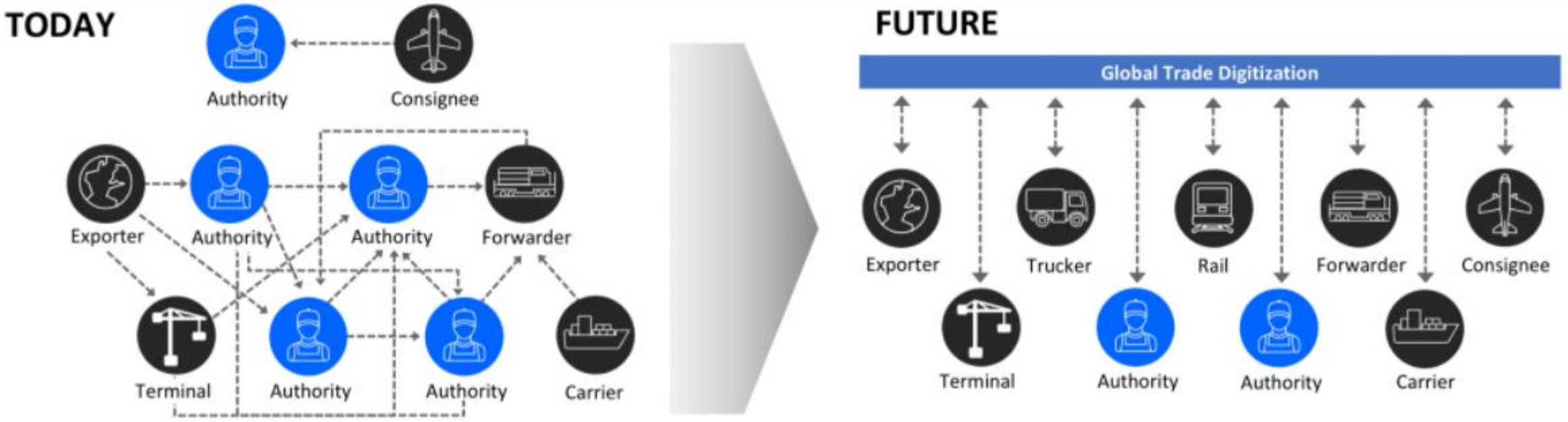
HYPERLEDGER GENERAL MEMBER

CASOS DE USO

Maersk e IBM. Cadena e suministro.

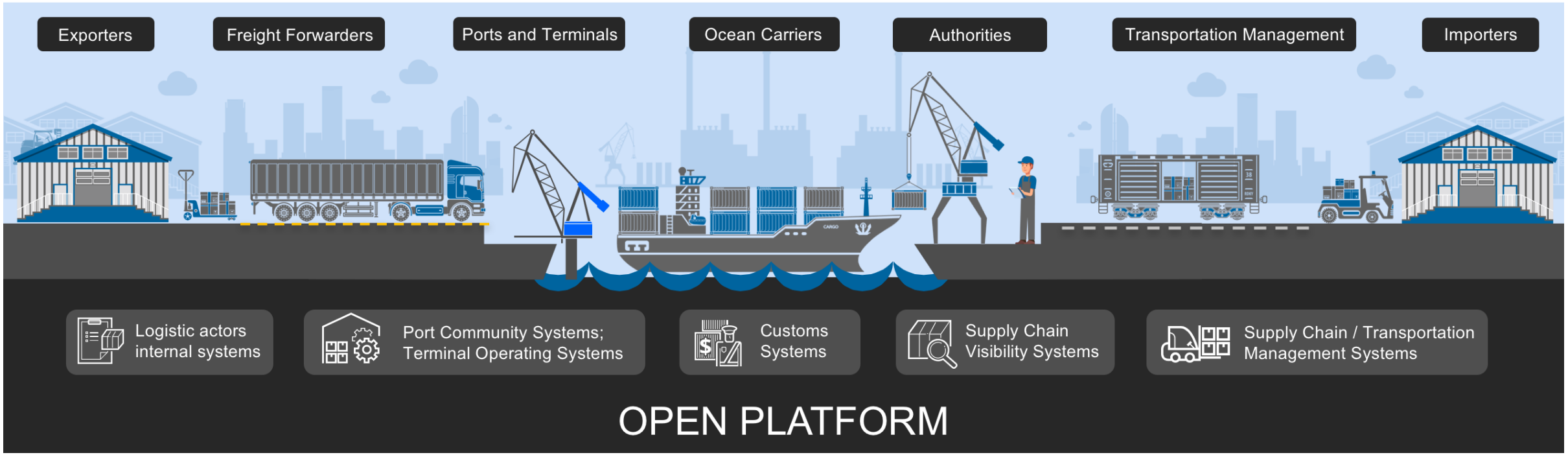


Maersk e IBM. Cadena e suministro.



Source: https://www.ibm.com/blogs/blockchain/2018/01/digitizing-global-trade-maersk-ibm/

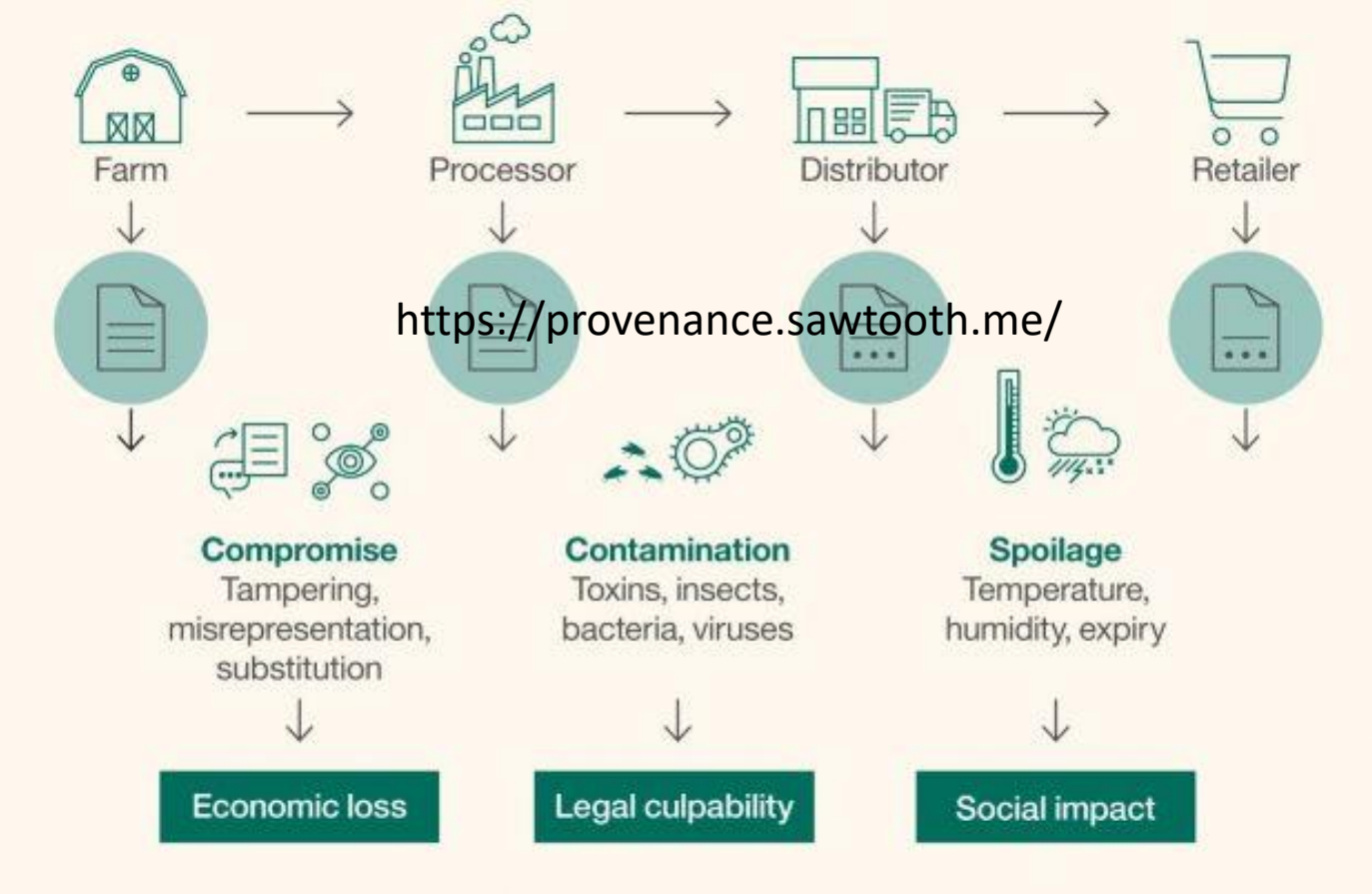
Maersk e IBM. Cadena e suministro.



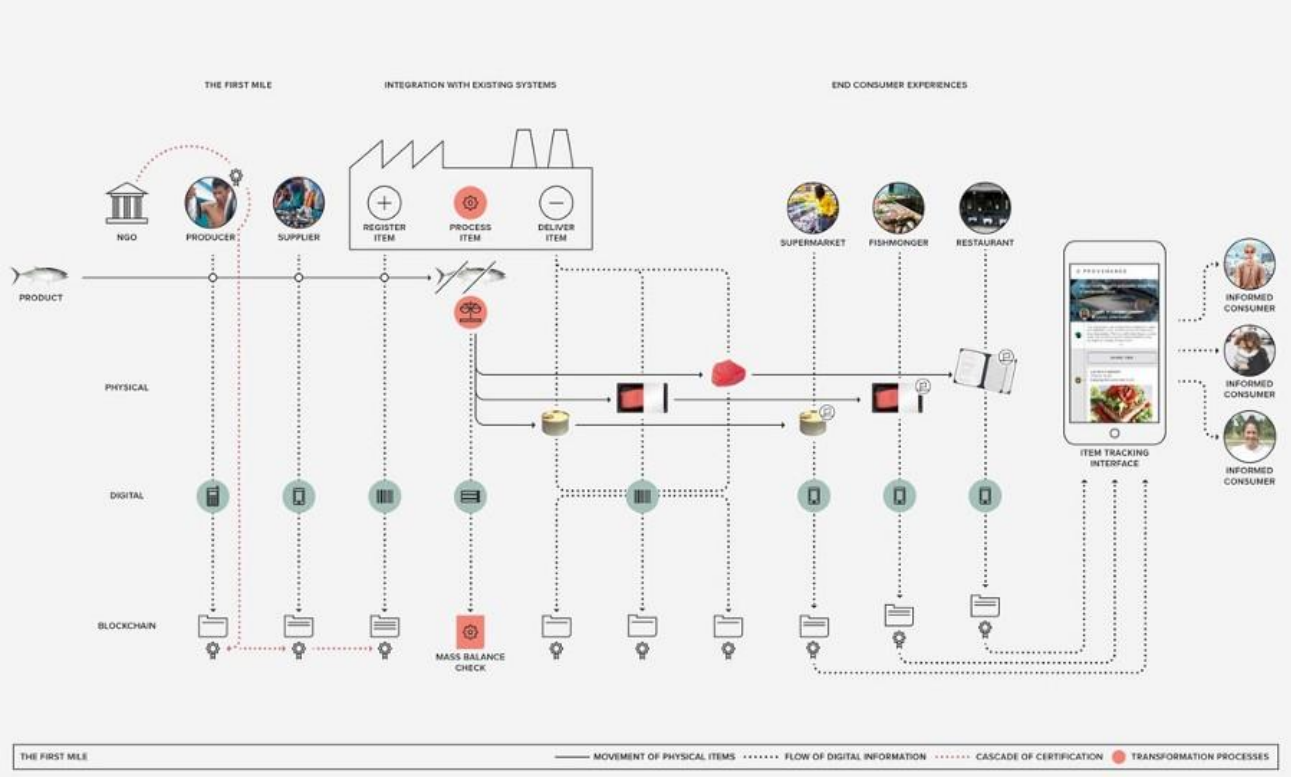
Source: https://www.ibm.com/blogs/blockchain/2018/01/digitizing-global-trade-maersk-ibm/

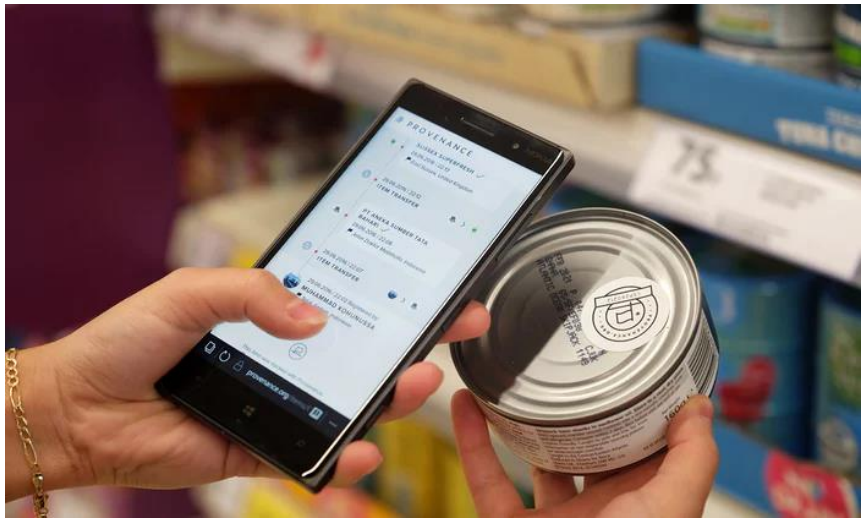
Mercatrace. Trazabilidad de productos

IBM and Walmart.



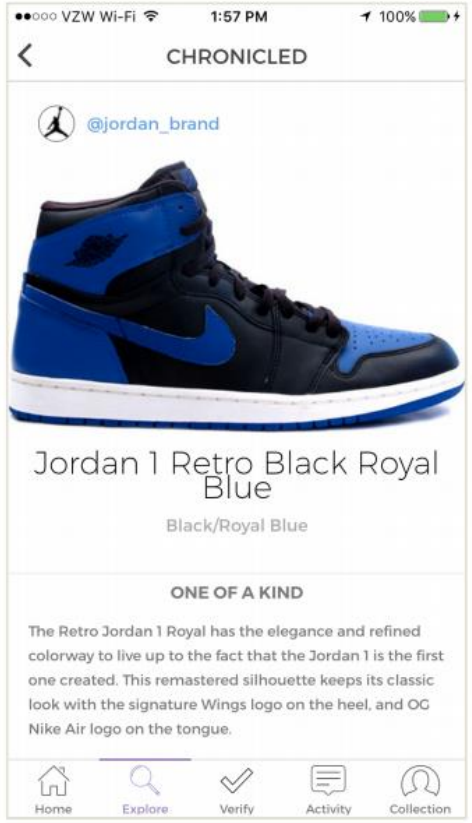
Provenance. Trazabilidad de productos.





https://provenance.sawtooth.me/

Chronicled. Luchando contra la falsificación.



Banco de alimentos de la ONU.

La ONU sustituye a los bancos por la blockchain para el Programa Mundial de Alimentos

Javier Ruiz BLOCKCHAIN ETHEREUM 19 febrero 2018

Blockchain, la tecnología detrás del bitcoin y el resto de monedas digitales, está encontrando un nicho completamente alejado del mundo de las finanzas: la ayuda humanitaria.

ZF, UBS e IBM llevan blockchain a los pagos dentro del vehículo

FUTURO

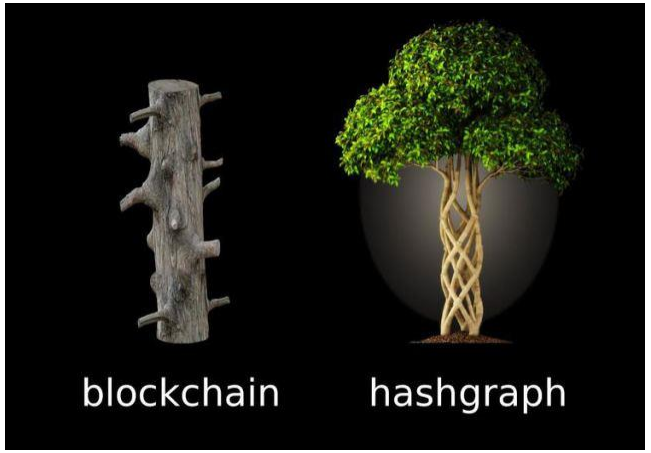
Problemáticas

- Escalabilidad limitadas.
- Privacidad limitada.
- Falta de verificación formal del contrato.
- Restricciones de almacenamiento.
- Mecanismos de consenso insostenibles.
- Falta de gobierno y estándares.
- Herrameintas inadecuadas.
- Amenaza de la computación cuántica.

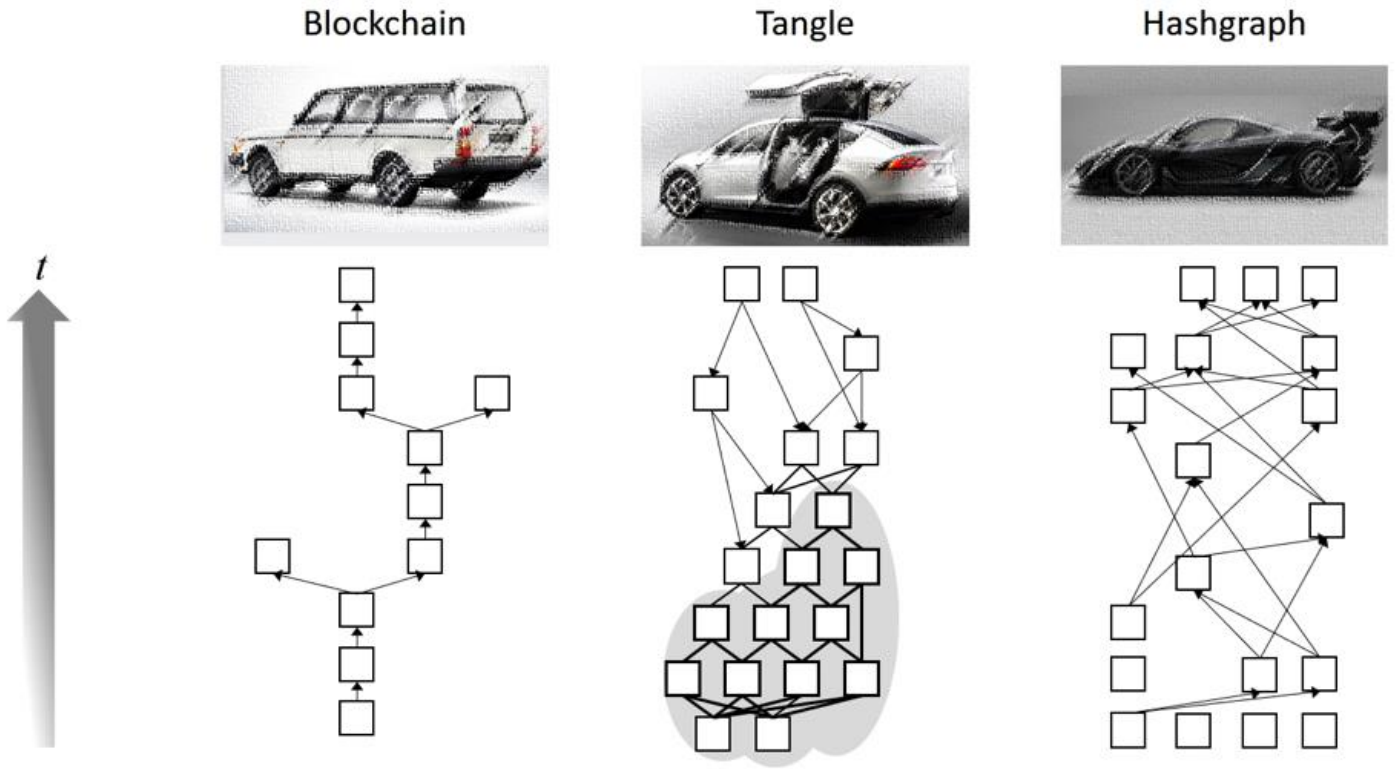
Nuevas plataformas.

IOTA

Hedera™
Hashgraph



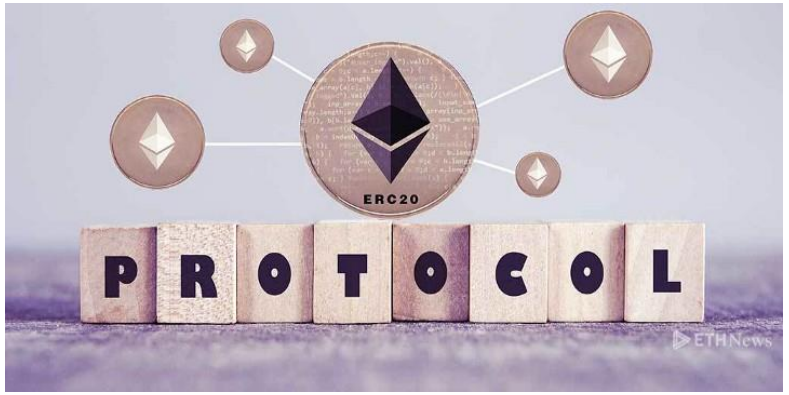
DAG



	Blockchain	Tangle	Hashgraph
Technology	Block chain	Directed acyclic graph	Directed acyclic graph
Copyright	Open source	Open source	Patented
Consensus	Proof of Work: SHA256-Hash	Proof of Work: check of Tangle tip	Virtual voting
Openness	Public ledger	Public ledger	Private ledger
Applications	Bitcoin	Iota	Swirlds
Efficiency (tps)	3-4	500-800	> 250,000

RETOS

ESTANDARIZACIÓN



ERC-20, ERC-223, ERC-721,….

IDENTIDAD

HYPERLEDGER
INDY

MUCHAS GRACIAS

“Estudia como si nunca fueras a aprender bastantes bastante, como si temieras olvidar lo aprendido”

Confucio

“Me lo contaron y lo olvide;
lo vi y lo entendí;
lo hice y lo aprendí”

Confucio

“No importa lo lento que vayas mientras no te detengas”

Confucio