

Blockchain:

contexto económico y de negocios

Carlos Castro-Iragorri

La tecnología

Blockchain: una conjunto de tecnologías que permiten garantizar la integridad de un registro de datos



Consensus

PoW, PoS, POET, RaFT,
BFT, PBFT



Crypto/Security

PKI, HASH, SHA-256,
zk-SNARK, HE, ECC, EXDSA,
SGX



Ledger Concepts

Mining, Blocks,
Forks, Parents, Uncles,
Merkle Trees



Platform Concepts

Nodes, Oracles,
Notaries, Wallet, Smart
Contracts

Blockchain: estructura conceptual

- Registro (base datos) digital compartido, descentralizado, integridad historial de las transacciones. Replicada en tiempo real.
- Seguridad criptográfica, identificación/autenticidad.
- Arquitectura P2P (sistemas distribuido) vs servidor/cliente.
- Gobernanza: mecanismo de consenso, garantizar consistencia datos entre nodos. Reglas de validación (usuario y transacciones), incentivos,....

La configuración de estos elementos nos lleva a diferentes tipos de tecnologías de registro distribuido y en particular blockchain.

Objetivo del curso

Conocer cada una de las tecnologías y entender cómo (Martin) y **porque (Carlos)** se unen.

- Seguridad (mensajes y datos)
- **Consenso.**
- Criptografía.
- **Registros (bases de datos).**
- **Sistemas distribuidos** y redes.

Tipos de registros (bases de datos)

Información que contiene

- Registros de propiedad: trazabilidad propiedad objetos físicos o digitales.
- Registros de derechos: derechos autor.
- Registros de acuerdos o compromisos.

Procesos que soportan

- Sincronización (reconciliadas): contabilidad, liquidación de pagos.
- Trazabilidad de negociación: auditoria, publicaciones académicas.

Sistemas distribuidos

Colección de procesos autónomos que se comunican para lograr un objetivo computacional común.

- Juegos en línea multi-usuario (Fortnite, League of Legends...).
- Sistemas de control industrial (química, energías, petróleo, alimentos).
- Multithreading en procesadores (computación, transacciones).

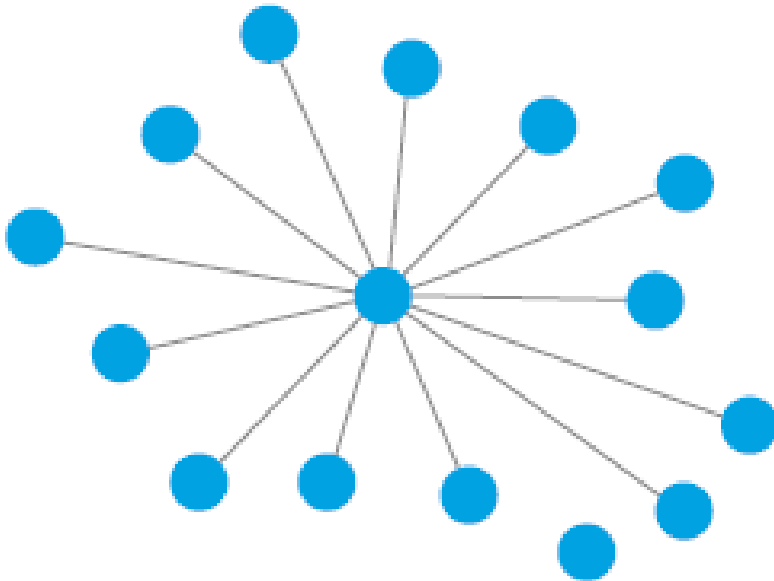
Registros distribuidos

En un sistema distribuido podemos compartir un registro compartido (*Distributed Ledger*)

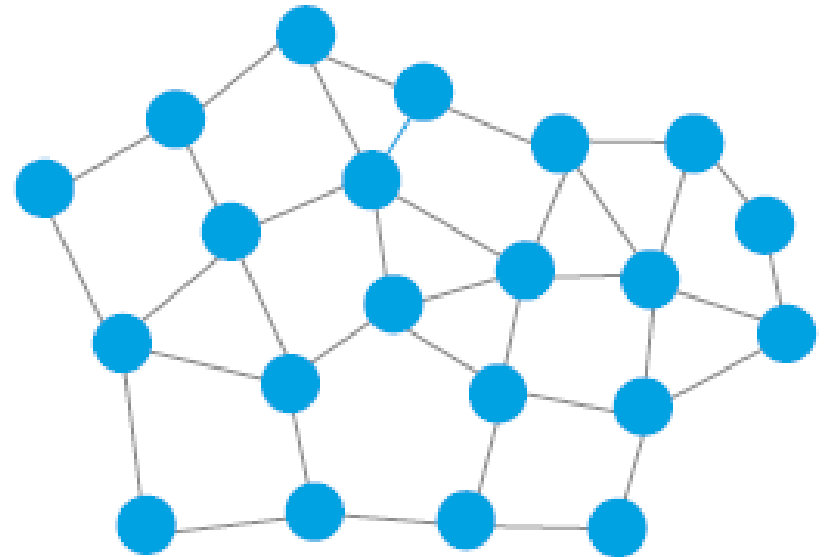
- Centralizado: copia autorizada, único administrador (identidad e integridad). Reservas aerolíneas.
- Replicado: varias copias con suscripción a actualizaciones, único administrador. Redes de tarjetas de crédito.
- Distribuido: varias copias, conjunto de nodos comparte actividades de administración.

Topología de la red

Centralizado/ Replicado



Distribuido




Gobernanza en sistemas distribuidos

- En un registro distribuido y descentralizado hay una responsabilidad compartida (nodos) con respecto al proceso de registro de la información.
- Requiere un nivel de **confianza** entre los participantes o un mecanismo para garantizar que aun en presencia de nodos maliciosos el sistema funciona.
- Mecanismos:
 - Explícitos: nodos especializados y con un mandato.
 - Implícitos: reglas de juego y compatibilidad de incentivos.

Confianza vs administración de riesgo

“Distributed ledgers are often promoted as technologies to create trust, or even to democratise trust. This is wrong. Distributed ledgers are tools to enable us to more effectively manage risk.” Deloitte (2016)

Aproximación más pragmática que dogmática.
Soluciones potenciales  La tecnología.



Ventajas de los registros distribuidos

- Accesibilidad e interoperabilidad de la información.
- Visibilizar y validar la información.
- Mejorar la visibilidad no necesariamente incrementa la confianza,.... Pero
- Si permite monitorear y administrar mejor los riesgos.

Ventajas de los registros distribuidos

Situaciones en que esta habilidad para administrar mejor los riesgos favorece las soluciones distribuidas vs descentralizadas:

- Desintermediación: financiamiento comercial.
- Múltiples jurisdicciones: difícil acordar un registro centralizado.
- Cumplimiento: auditorias, impuestos.

Contexto económico

La economía colaborativa (Sundararajan, 2016)

1. Mercados grande: creación de mercados que permiten el intercambio de bienes y servicios (antiguos y nuevos) aumentando los niveles de actividad económica.
2. Capital de alto impacto: permite nuevas oportunidades para la (re-)utilización (*slack assets*) de activos, competencias,.., dinero y tiempo de tal forma que se puedan utilizar a su capacidad completa.

La economía colaborativa

(Sundararajan, 2016)

3. Redes colaborativas en vez de instituciones centralizadas y jerárquicas: la oferta de capital y trabajo es proporcionada por organizaciones o individuos descentralizados (P2P) vs corporaciones; los mercados futuros (marketplaces) pueden ser gobernados por redes colaborativas en vez de entidades centralizadas.
4. Relaciones laborales: Líneas difusas entre: personal y profesional; empleo completo y casual. Desafío en seguridad social.

La economía colaborativa: Taxonomía



Capacidad de ofrecer el servicio:



- Trayectos durante un día.
- La plataforma crea lo equivalente a una red de vías férreas utilizando activos subutilizados y una infraestructura existente.
- 21 países en Europa e India.
- Transporta más personas diariamente que algunas redes ferroviarias.
- 1,6 millones de toneladas menos de CO2.

By Jeremiah Owyang
jeremiah@CrowdCompanies.com
@jowyang, March 2016

WORKER SUPPORT

LEARNING

WELLNESS & BEAUTY

MONEY

GOODS

HEALTH

SPACE

FOOD

LOGISTICS

SERVICES

ANALYTICS AND REPUTATION

CORPORATIONS AND ORGANIZATIONS

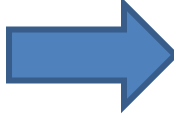

VEHICLE SHARING

UTILITIES

MUNICIPAL

EMPOWERED PEOPLE MAKERS, CO-CREATORS, CROWDFUNDERS, PEERS, CUSTOMERS

Impactos económicos

- Mayor impacto en factores de producción (capital, trabajo, utilización).
- Mayor variedad de bienes y servicios  mas consumo  mas crecimiento.
- Cambios en los mercados de activos (mayor uso).
- Alteración (perdida) de economías de escala, organizaciones que producen mas eficientemente.
- Promesa de crecimiento inclusivo.

La tecnología el principal motor

- *Digital enablers*: dispositivos móviles, banda-ancha, redes sociales.
- Mover la provisión de bienes y servicios a estructuras descentralizadas y basadas en relaciones sociales en vez de jerarquías (Benkler, 2001).
- Otros factores: urbanización (Norteamérica 82%; Latinoamérica y Caribe 80%; Europa 73%).

Oportunidades y retos de Blockchain

- El próximo *Digital Enabler*?
- Puede ser porque en una economía colaborativa y descentralizada debemos garantizar procedencia (origen, autenticidad, propiedad,..)
- Tecnologías detrás de la nueva generación de **mercados P2P que son las plataformas descentralizadas** (Red, Sistema de incentivos, Seguridad).
- Cuál es la captura de valor en la descentralización: re-agregación de valor, si seguimos el patrón de los orígenes de internet.

Intersecciones economía colaborativa y blockchain

Desintermediar los mercados
colaborativos.

- [OpenBazaar](#) (bitcoin) vs Amazon
- [La'Zooz](#) vs Uber
- Bee Token vs Airbnb

Criterios para preferir una solución blockchain

Consideraciones

- Cuando se necesita una Blockchain?
- Hay varios tipos de tecnologías de registro distribuido.
- Tecnologías alternativas.
- Viabilidad de los proyectos basados en tecnologías blockchain
 - Incertidumbre
 - Permanencia y sostenibilidad de la red.
 - Análisis costo-beneficio.

Usted necesita un blockchain?

<http://doyouneedablockchain.com/>

Based on Wüst, Karl, and Arthur
Gervais. "[Do you need a
Blockchain?](#)" *IACR Cryptology ePrint
Archive* 2017 (2017): 375.

Sin permisos, Blockchain publica

- Transacciones procesadas (teoricamente) por todos los nodos.
- Transacciones son completamente visibles (lectura abierta).
- Gran cantidad de nodos
 - Ethereum: 13,978
 - Bitcoin: 9,563.
- Beneficios: escritura y lectura abierta, distribución autentica del registro, resistente a la censura, autenticidad del registro garantizado por la regla de minado (>51%)

Con permisos, Blockchain privada

- Transacciones procesadas por algunos nodos (especialización de nodos).
- Transacciones pueden ser visibles o privadas.
- Distribución local de la red: dentro de una(s) organización(s).
- Beneficios: Empresas u organizaciones quieren guardar control sobre su información y transacciones, transacciones mas rápidas, mejor escalabilidad, soporte, consenso eficiente.
- Hyperledger



Blockchain Privadas vs Publicas

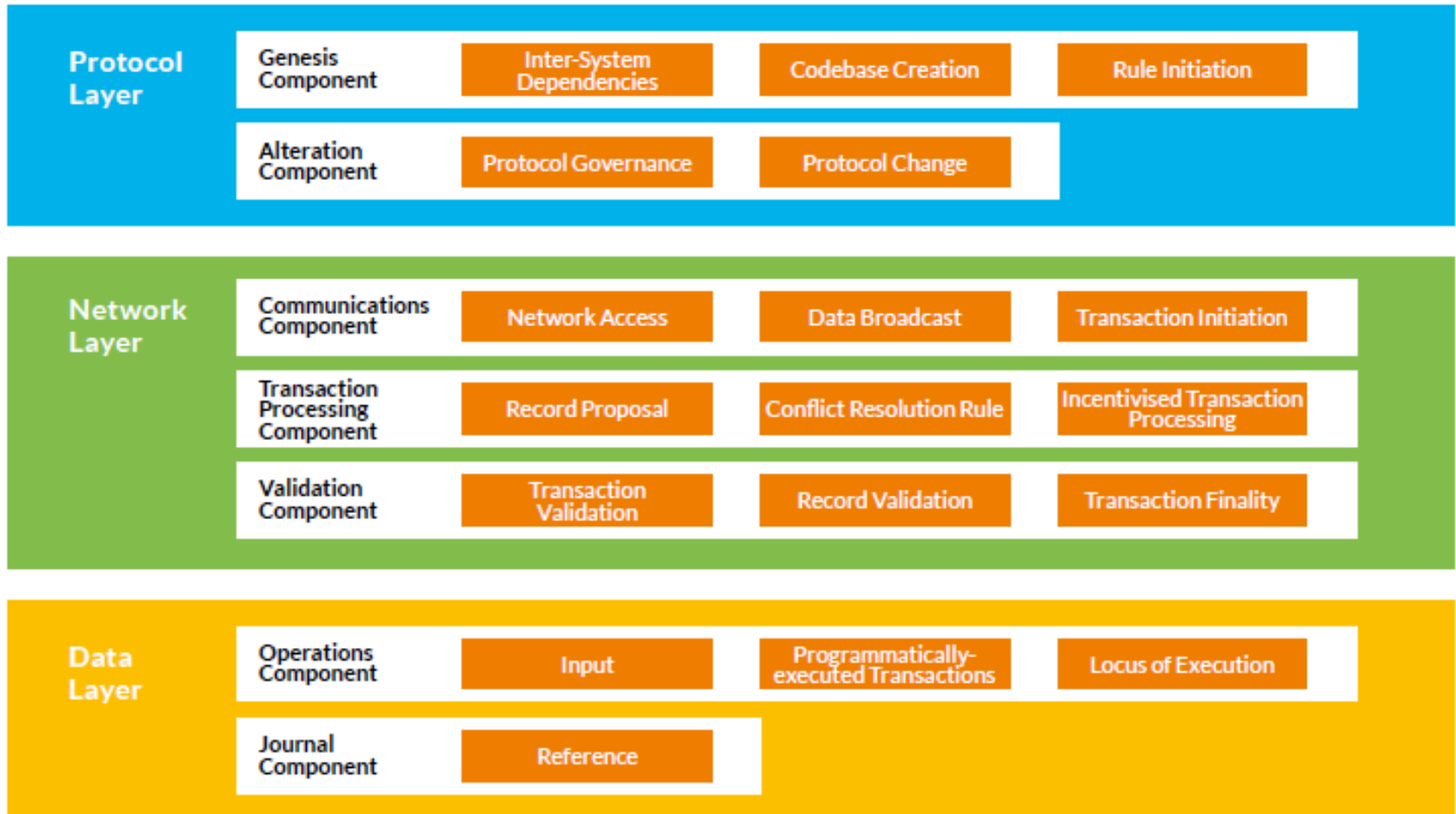
	Public (Permissionless)	Private (Permissioned)
Access to Ledger	Open Read/Write	Permissioned Read/Write
Identity	Anonymous	Known Identities
Security and Trust	Open Network (Trust Free)	Controlled Network(Trusted)
Transaction Speed	Slower	Faster
Consensus	POW/POS	Proprietary or Modular
Open Source	Yes	Depends on Blockchain
Code Upkeep	Public	Consortium or Managed
Examples	Ethereum, Multichain	R3 Corda, Quantum, Hyperledger

Transacciones por segundo, VISA: 24,000

	Block Generation Time	Transactions Per Second (tps) ²³
Bitcoin	10 minutes	Average 3 tps (Max: 7 tps)
Corda	n/a	> 500 tps
Ethereum	10-19 seconds	Average 15-20 tps, but no theoretical limit
Fabric	variable	> 10 tps
Multichain	Configurable (≥ 2 seconds)	Configurable
Neo	15 seconds	10,000 tps
NXT	1 minute	12 tps
Quorum	50 mSec	>500 tps
Sawtooth	Configurable	>500 tps







Mercy Corps (2018). BLOCK BY BLOCK A Comparative Analysis of the Leading Distributed Ledgers
 University of Waterloo (Mayo 3, 2019) Hyperledger Fabric blockchain from 3,000 to 20,000 transactions per second (TPS).

Marco de referencia para DLT



Rauschs, M. et al (2018). Distributed Ledger Technology Systems: A Conceptual Framework, University of Cambridge

Tipos de Blockchain/DLT

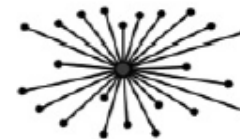
							
GOVERNANCE	Anarchic	✓					
	Hierarchical		✓				
	Dictatorship			✓			✓
	Federation				✓	✓	
NETWORK ACCESS	Open	✓	✓	✓			
	Semi-open				✓		
	Closed					✓	✓
TRANSACTION PROCESSING	Decentralised	✓	✓				
	Semi-centralised			✓	✓	✓	
	Centralised						✓
INCENTIVES	Intrinsic	✓	✓				
	Extrinsic			✓	✓	✓	✓
REFERENCE	Endogenous	✓					
	Hybrid		✓	✓	✓		
	Exogenous					✓	✓

Rauschs, M. et al (2018). Distributed Ledger Technology Systems: A Conceptual Framework, University of Cambridge

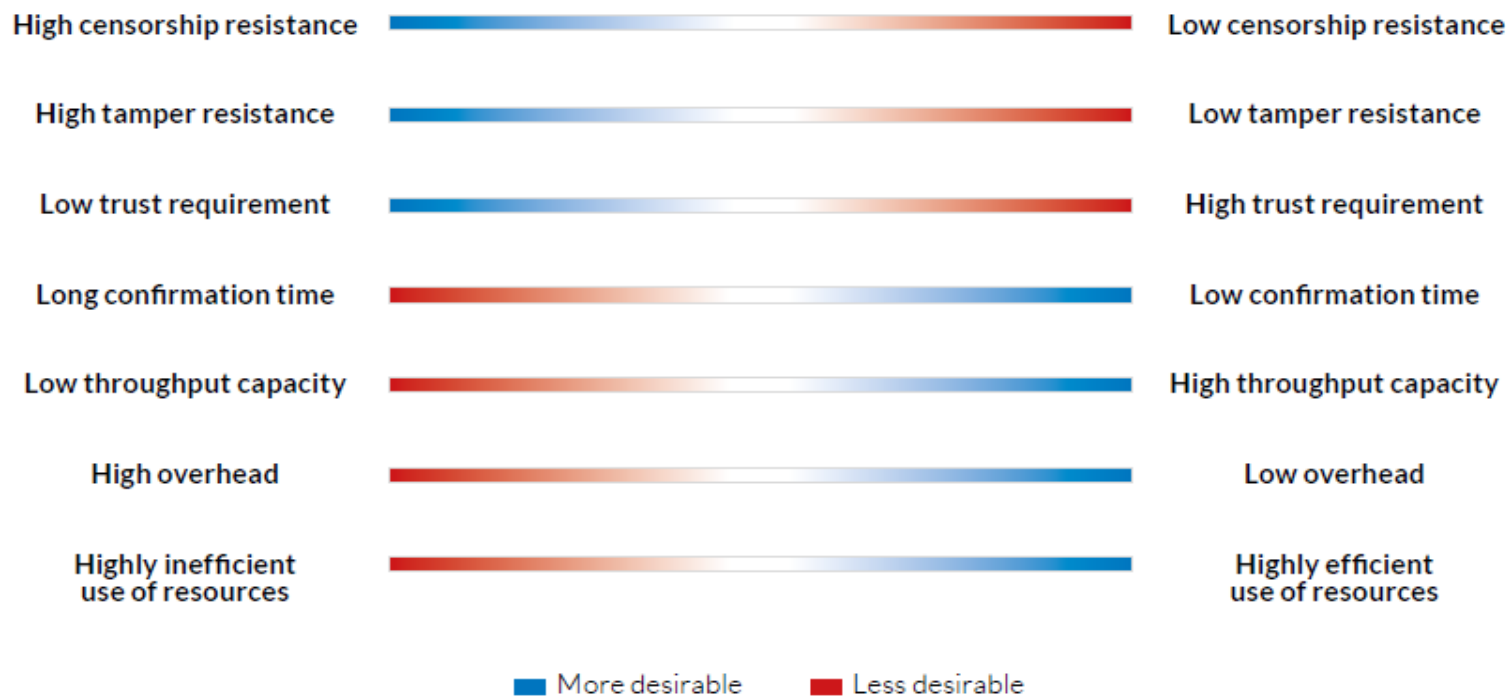
Tecnologías Alternativas



Fully Decentralised System



Fully Centralised System



Rauschs, M. et al (2018). Distributed Ledger Technology Systems: A Conceptual Framework, University of Cambridge

Consideraciones para adoptar una solución blockchain

Viabilidad: Incertidumbre

Estrategias de emprendimientos (Gans, Stern, Wu, 2019) criterios que llevan a una decisión.

1. Existe mas de un camino a seguir (libertad).
2. Restricciones a seguir todos los caminos.
3. Valor de la idea es incierto (distribución de probabilidad).
4. Aprendizaje ruidoso del valor de una idea, la alternativa estratégica y la relación entre las dos.
5. Regla de parada: Evaluar dos (valor esperado equivalente ex-ante), escoger una.

Viabilidad: Incertidumbre

Paradoja del emprendedor (*path dependence*):

“clasificar estrategias alternativas (viables) requiere un conocimiento que solo se puede adquirir a través de la experimentación, pero la experimentación necesaria para resolver la incertidumbre genera algún nivel de compromiso que le cierra puertas a algunas estrategias”.

- Proyectos Blockchain (riesgos)
 - Escoger la plataforma equivocada.
 - Caso de uso débil.

Viabilidad: permanencia y sostenibilidad de la red

Sin permisos

- La red existe (Bitcoin, Ethereum,...).
- Incentivos (verificación, minado, procesamiento) la hacen sostenible?
- Concentración de nodos.
- Gobernanza establecida.
- Costos marginales de utilizar la red.

Permissionadas

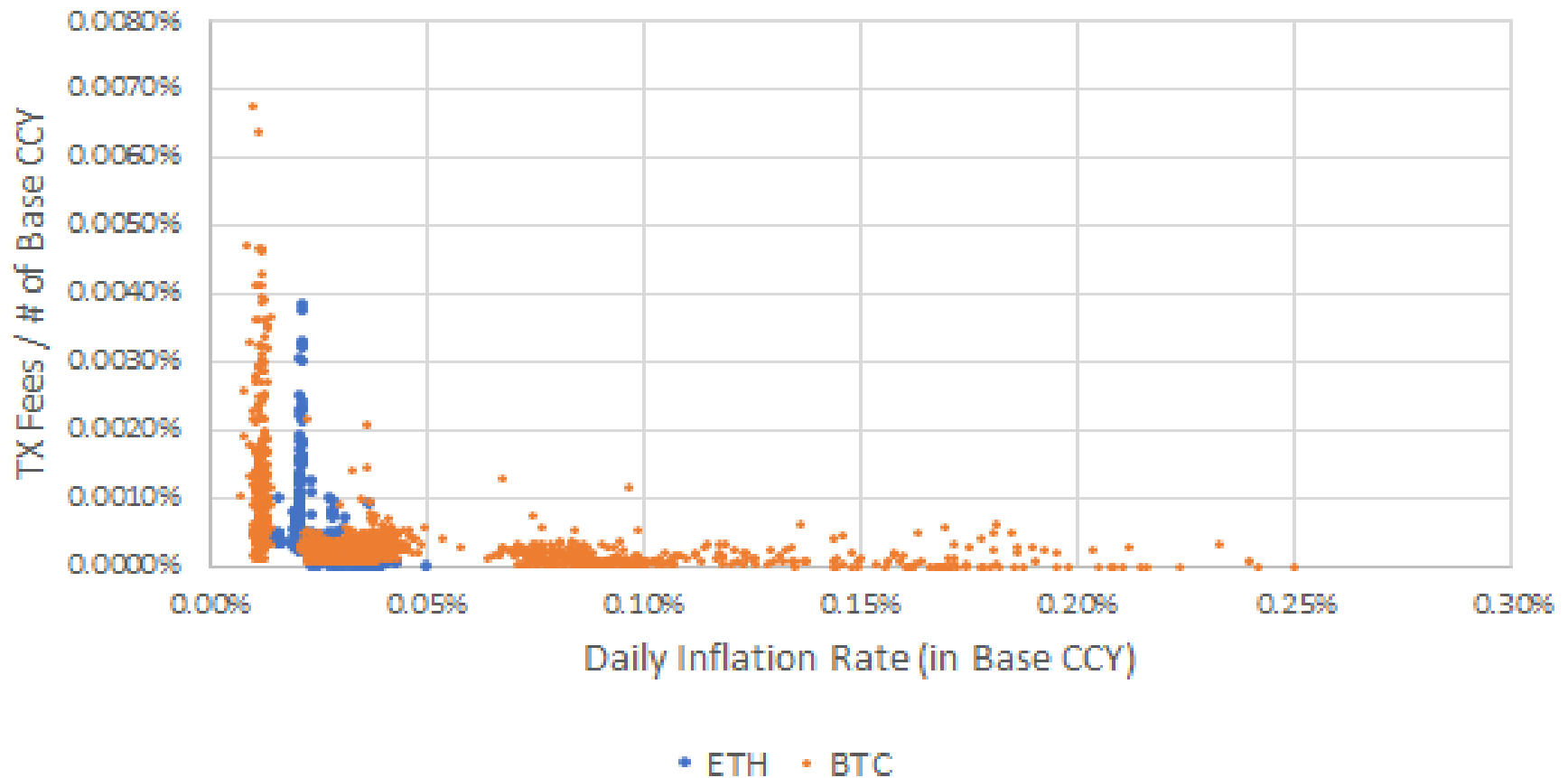
- Hay que crear un consorcio para crear nodos y canales de comunicación de la red.
- Incentivos hace parte de un modelo de negocio existente y en transito a una nueva tecnología.
- Gobernanza se debe establecer.
- Costos fijos altos de crear la red

Análisis costo-beneficio, Platt 2018

- La descentralización es costosa: redundancia y sincronización de los datos (red grande) y computacionalmente.
- La viabilidad económica no ha alcanzado las expectativas con respecto a la tecnología.
- La racionalidad económica para aplicaciones sobre blockchain publicas depende que tan importante es el interés de blindarse con respecto a la posibilidad de censura.

Costo marginal operar blockchain publica (minería/transacciones)

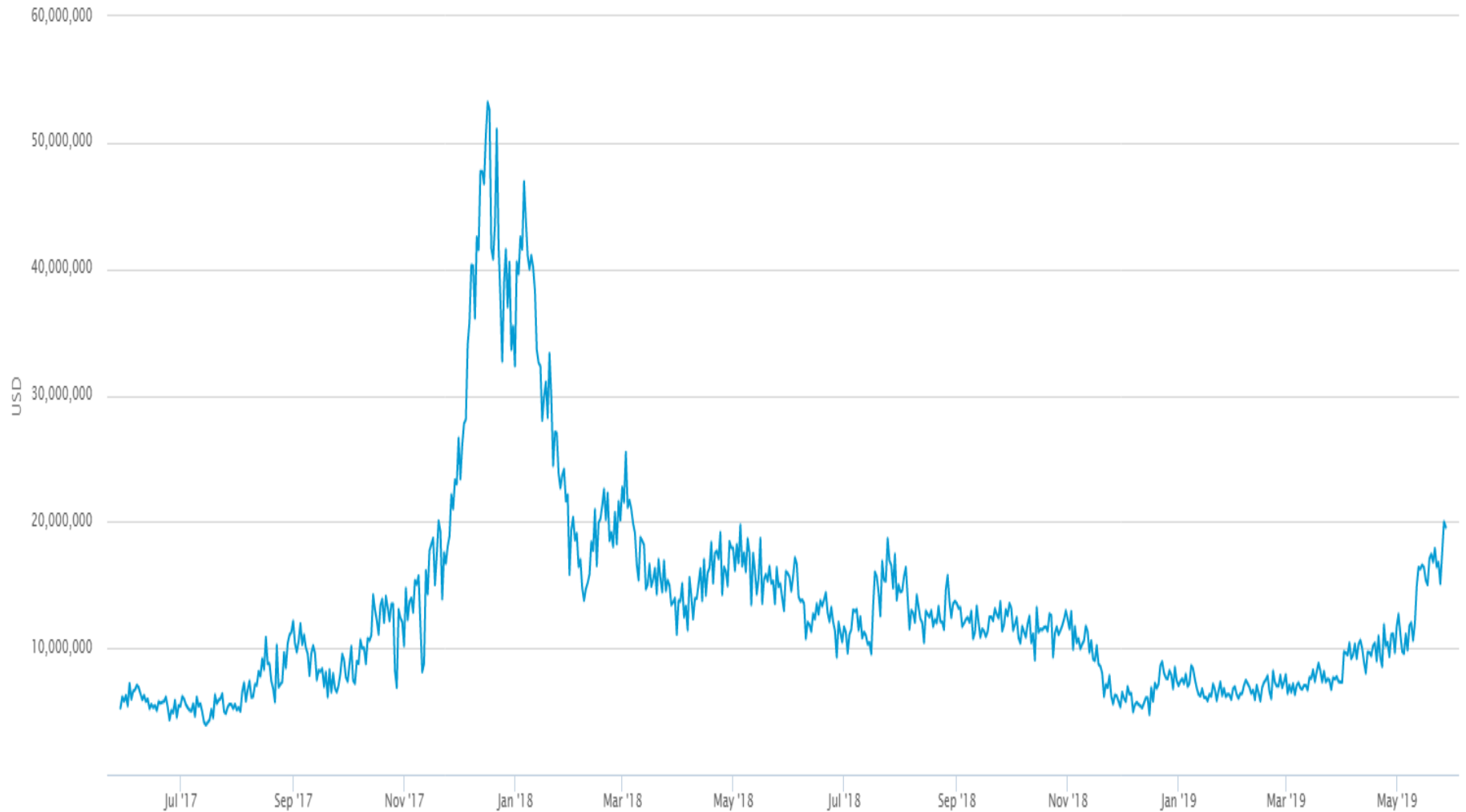
BTC & ETH Daily Inflation & TX Fees Paid as % of Monetary Base



Costo de las operaciones

- Operaciones básicas dentro de los nodos
 - Recolectar y validar transacciones.
 - Almacenamiento y disponibilidad.
- Supuestos
 - 4,320 bloques por mes (produce 1 cada 10min, 144 por dia..)
 - 100 millones de búsquedas sobre la base de datos.
 - 165/210 GB, tamaño BTC blockchain Abril 2018/2019.

Precio operación de la red BTC



Comparación de Costos

- BTC, \$20M
- ETH, \$30M
- Amazon AWS, \$200
- Tener en cuenta que es el global de operar la red sobre la cual pueden funcionar varios negocios.
- ¿Que hace la diferencia? Riesgo jurisdiccional.
- Cuál es el panorama para las blockchain permissionadas? Es difícil calcularlo, son proyectos cerrados.
- Comparación entre un caso de uso implementado en los dos tipos de blockchains.

Casos de Uso

Potencial vs implementacion

50+ BLOCKCHAIN REAL WORLD USE CASES

GOVERNMENT

Essentia develops world's first blockchain solution to manage international logistics hub together with Traffic Labs and the Finnish Government

essentia.one

IDENTIFICATION

Voter registration is being facilitated via a blockchain project in Switzerland spearheaded by Uport.

uport

MOBILE PAYMENTS

The blockchain ledger that Ripple uses has been latched onto by a group of Japanese banks, who will be using it for quick mobile payments.

ripple

INSURANCE

A smart contract-based blockchain is being used by Insurer American International Group Inc as a means of saving costs and increasing transparency.

AIG

ENDANGERED SPECIES PROTECTION

The protection of endangered species is being facilitated via a blockchain project that records the activities of these rare animals.



CARBON OFFSETS

IBM is using the Hyperledger Fabric blockchain in China to monitor carbon offset trading.

IBM

HYPERLEDGER

ENTERPRISE

Ethereum's blockchain can be accessed as a cloud-based service courtesy of Microsoft Azure.

Microsoft Azure

BORDER CONTROL

Essentia has devised a border control system that would use blockchain to store passenger data in the Netherlands.

essentia.one

SUPPLY CHAINS

IBM and Walmart have partnered in China to create a blockchain project that will monitor food safety.

IBM
Walmart

HEALTHCARE

A number of healthcare systems that store data on the blockchain have been pioneered including MedRec.

MEDREC

SHIPPING

Shipping is a natural fit for blockchain, and Maersk have been trialling a blockchain-based project within the maritime logistics industry.

MAERSK

REAL ESTATE

Blockchain is now being used to complete real estate deals, the first of which was conducted in Kiev by Propy.

PROPY

ENERGY

Essentia is developing a test project that will help energy suppliers track the distribution of their resources in real time, whilst maintaining data confidentiality.

essentia.one

LAND REGISTRY

Land registry titles are now being stored on the blockchain in Georgia in a project developed by the National Agency of Public Registry.

NATIONAL AGENCY OF PUBLIC REGISTRY

COMPUTATION

Digital Currency Group are helping Amazon Web Services examine ways in which the distributed ledger technology can help improve database security.

DIGITAL CURRENCY GROUP

ADVERTISING

New York Interactive Advertising Exchange has been experimenting with blockchain as a means of providing an ads marketplace for publishers.

NYIAX

BORDER CONTROL

Essentia is developing a blockchain project for border control that will allow customs agents to record passenger data from an array of inputs and safely store it.

essentia.one

JOURNALISM

Decentralized journalism, as enabled by blockchain technology, has the potential to prevent censorship and increase transparency, as Civil has shown.

CIVIL

WASTE MANAGEMENT

Waltonchain is using RFID technology to store waste management data on the blockchain in China.

WALTONCHAIN

ENERGY

Food importation is another industry where blockchain is proving its worth, with Louis Dreyfus Co trialling a soybean importation operation using this technology.

LDC

DIAMONDS

The De Beers Group is using blockchain to record the importation and sale of diamonds.

DE BEERS GROUP OF COMPANIES

FINE ART

By storing certificates of authenticity on the blockchain, it's possible to dramatically reduce art forgeries, as one blockchain project is proving.

Google
Alphabet

NATIONAL SECURITY

For the past two years, the US Department of Homeland Security has been using blockchain to record and safely store data captured from its security cameras.

U.S. DEPARTMENT OF HOMELAND SECURITY

TOURISM

In a bid to boost its tourism economy, Hawaii is examining ways in which blockchain-based cryptocurrencies can be adopted throughout the US state.

STATE OF HAWAII

TAXATION

In China, a tax-based initiative is using blockchain to store tax records and electronic invoices led by Miaocai Network.

MAOCAI NETWORK

ENERGY

Chile's National Energy Commission has started using blockchain technology as a way of certifying data pertaining to the country's energy usage as it seeks to update its electrical infrastructure.

CNE COMISION NACIONAL DE ENERGIA

RAILWAYS

Russian rail operator Novotrans is storing inventory data on a blockchain pertaining to repair requests and rolling stock.

NOVOTRANS

ENTERPRISE

Google is building its own blockchain which will be integrated into its cloud-based services, enabling businesses to store data on it, and to request their own white label version developed by Alphabet Inc.

Google
Alphabet

MUSIC

Arbit is a blockchain-based project led by former Guns N Roses drummer Matt Sorum seeking a fairer way to reward musicians for their creative efforts.

arbit

FISHING

Blockchain technology has been used to provide a transparent record of where fish was caught, as a means of ensuring it was legally landed.

FISHING

Implementaciones, realidad.

System	Deployments
Bitcoin	Intesa Sanpaolo
Corda	Finastra, GuildOne, Gemalto, GuildOne, TradelX, Tradewinds Market
Ethereum	Amazon, AXA Group, Daimler, Bank of America
Fabric	Maersk, Walmart, Oracle, AIA Group, Airbus, Northern Trust, ABN Amro, Swift, Allianz
Multichain	<u>See</u> , Notes on Interpretation, below
Neo	unknown
NXT	BNP Paribas, National Settlement Depository (NSD)
Quorum	Interbank Information Network (IIN), J.P. Morgan, National Bank of Canada
Sawtooth	T-Mobile, Tel Aviv Stock Exchange, State Bank of India, Vanig

Mercy Corps (2018). BLOCK BY BLOCK A Comparative Analysis of the Leading Distributed Ledgers

Trade Lens Maersk/IBM



TRADE+LENS



Everledger's solution for the diamond industry



Verifiable Organizations Network (VON)



Using the VON software stack based on Hyperledger Indy, any government service can issue digital licenses or permits for businesses like Mary's Eco Tours. And anyone can verify these digital licences and permits by checking the OrgBook for their jurisdiction.

Otros Casos

- Hyperledger
 - [Emission de bonos.](#)
 - [Blockchain Showcase.](#)
- Ethereum
 - [DaapRadar](#)
 - [Intercambio de tokens.](#)
 - [Mercados de Prediccion.](#)
- Corda
 - [MonetaGo](#)