Universidad de los Andes
Facultad de Ingeniería

FOROS ISIS

Departamento de Ingeniería de Sistemas y Computación

Aplicaciones Blockchain: Clases y Desarrollo

Jimmy Chung Tong – Director de Tecnología

Luis Javier Parra Bernal – Director de Estrategia

infoprojects

1ER FORO DE BLOCKCHAIN

Tipos de aplicaciones en Blockchain

"La maquina de confianza"

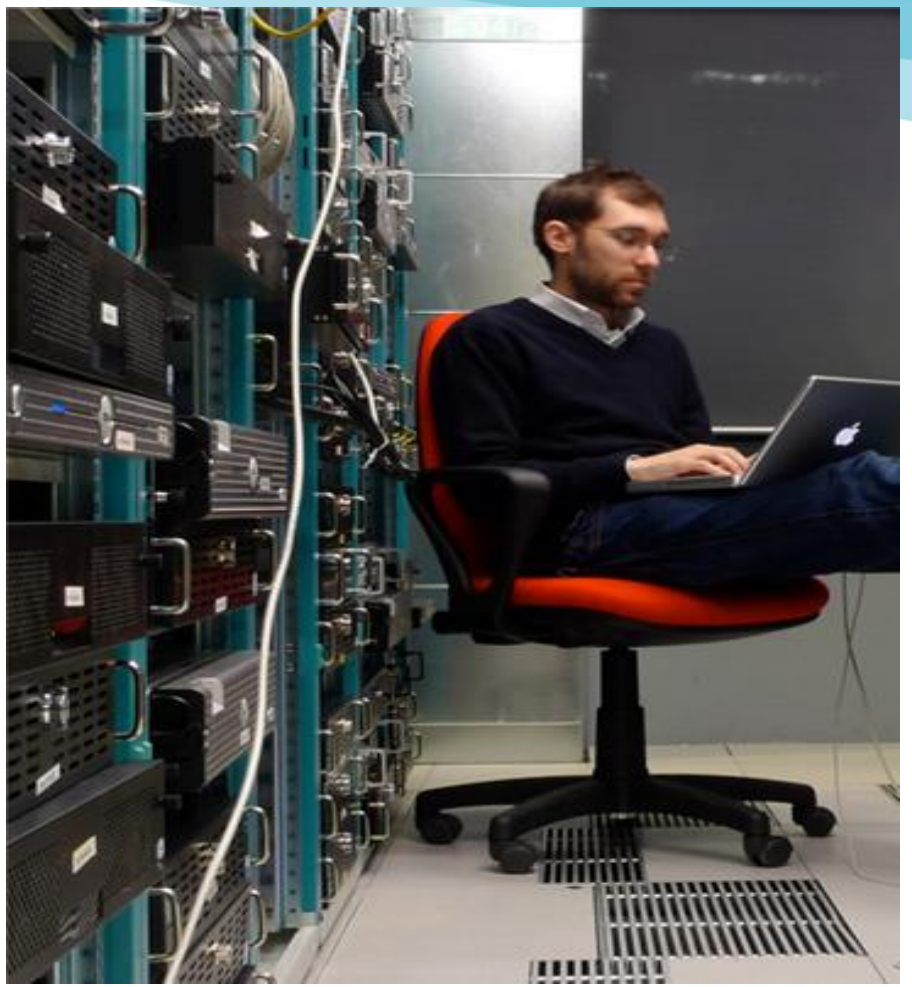
- Autoría:
  Firma digital (autenticidad y no repudio).
- Integridad:
  Inmutable (inalterable e imborrable).
- Sellado de tiempo:
  Fecha cierta.
  Sin Time Stamping Authority.

Seguridad de la información

Mitiga riesgos internos:

- Historial y log de accesos a bóvedas, data centers u otras zonas restringidas.

- Backups: integridad.



Prueba de autoría/conocimiento

Prueba concluyente de autoría o conocimiento (texto, audio, video) en una fecha determinada:

Propiedad intelectual/patentes.

NDAs.

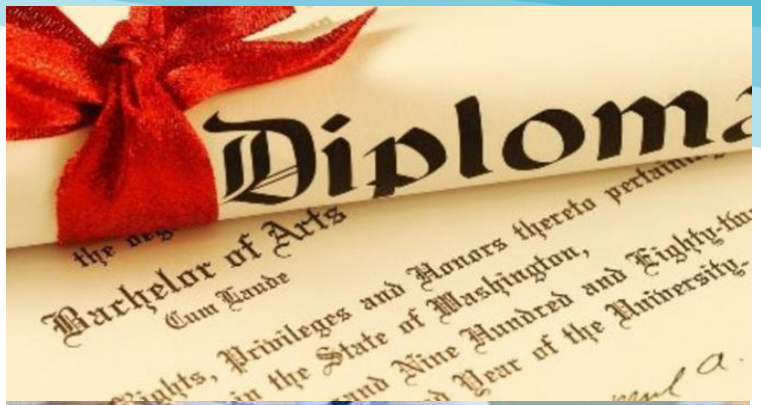
Escribano digital

Si tuviésemos a nuestra disposición un escribano digital, que a muy bajo costo certifique la documentación que queramos, las 24 horas del día, los 7 días de la semana...

¿Para qué lo usaríamos?

Títulos y certificados

- Impide falsificación.
- Evita fraude interno futuro.
- Simplifica/agiliza verificación.



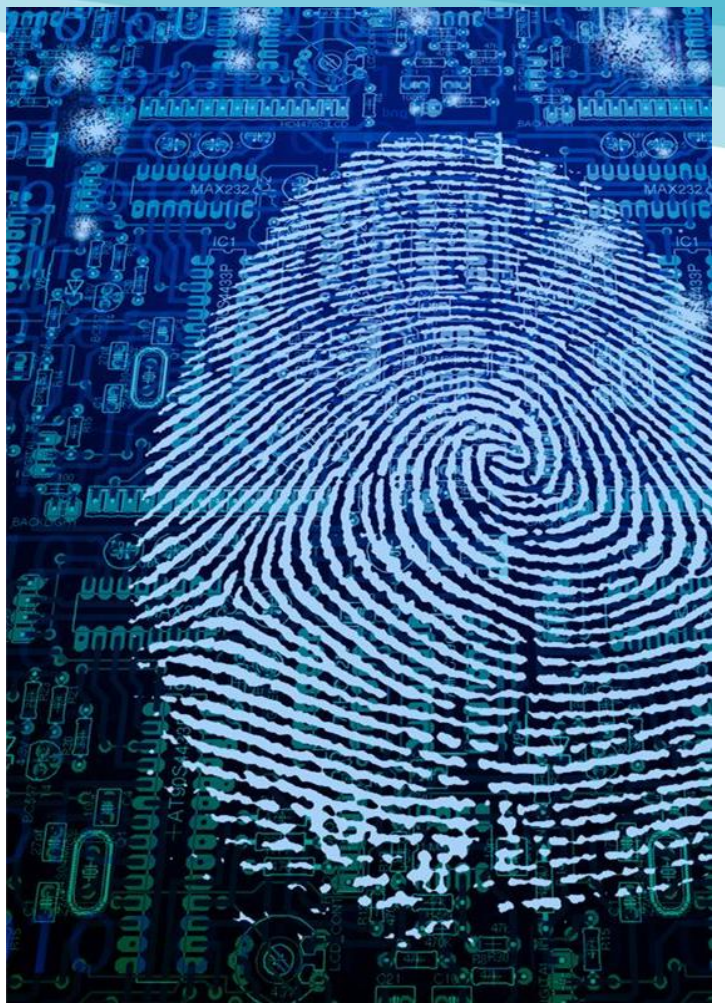
mit media lab

CESYT DESDE 1978 calidad en educación

HOLBERTON school()

Firma digital e identidad

- Firma digital potenciada (smart signing, imposibilidad de reemplazo de firmas).
- Integración con documentos de identidad digitales.
- Distintas plataformas pueden compartir identidad sin un repositorio propio de datos y de identificador único.



Transparencia gubernamental

Gobierno abierto: mayor control ciudadano en DD.JJ. y transparencia en cualquier otra documentación que así lo requiera.

Rendición de cuentas: trazabilidad en partidas presupuestarias.

Plataforma de voto electrónico.

Mercado de capitales

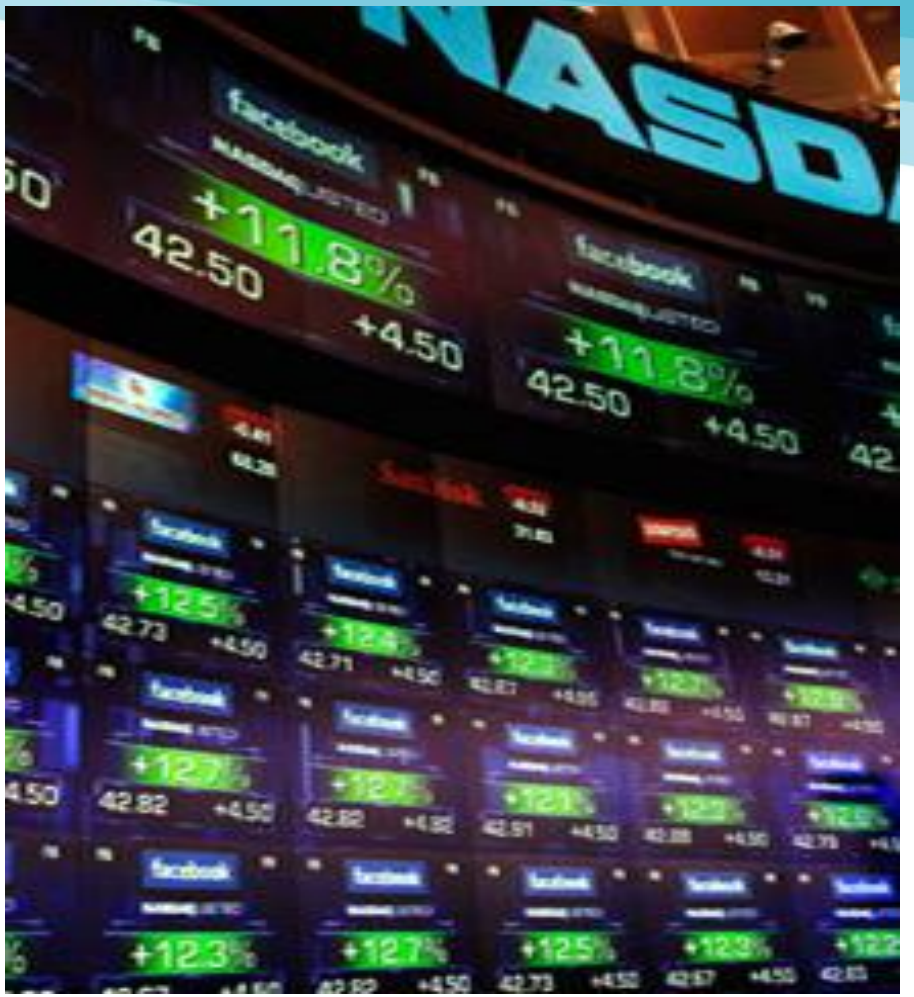
Settlement inmediato.

Registro consolidado.

Auditoría consolidada.

Reducción de riesgo.

Eficiencia.



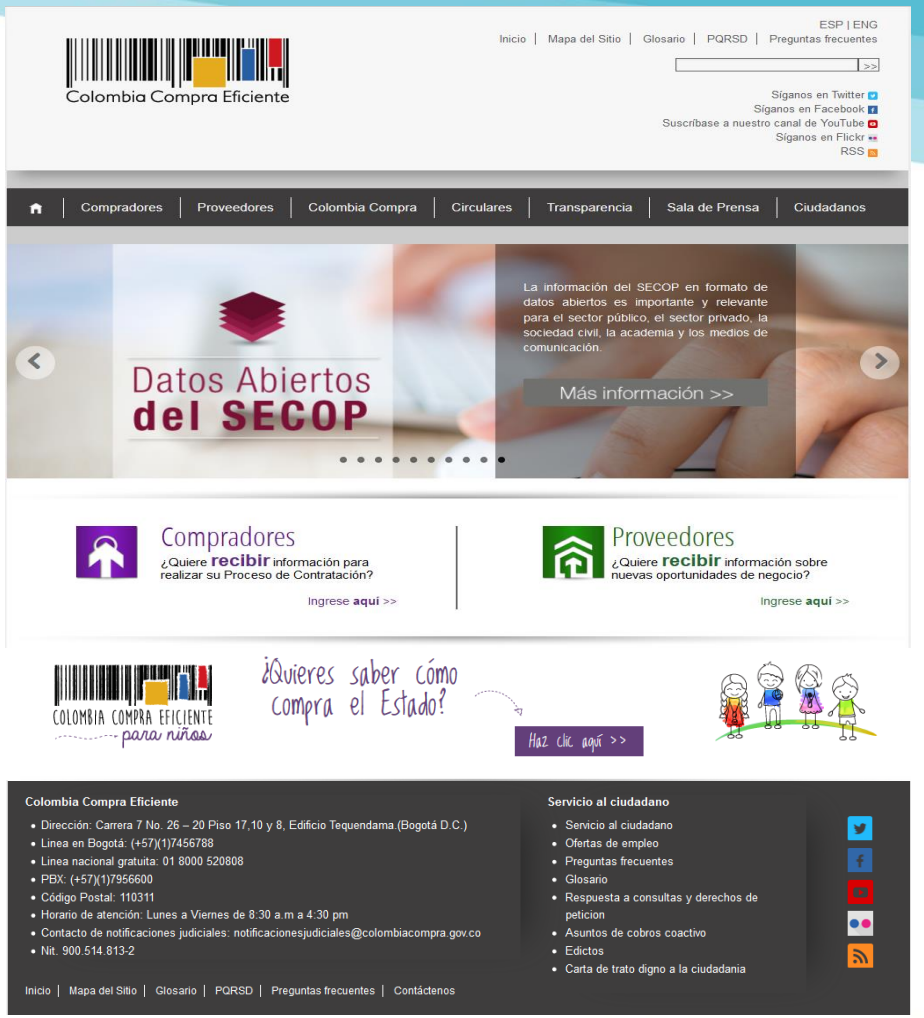
Compras y licitaciones

Confianza: sobre/plataforma web/matemática.

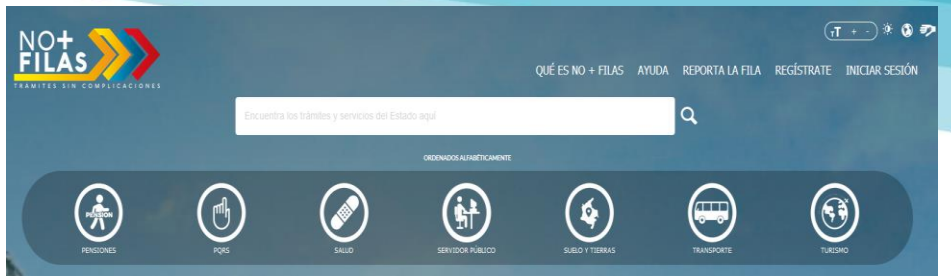
Mayor transparencia (registro público y auditable).

Menor posibilidad de fraude o corrupción.

- Privacidad de las ofertas durante el concurso.
- Oferentes no adjudicados, y ciudadanos de tratarse de un gobierno, pueden verificar la autenticidad del proceso.
- No más necesidad de terceros de confianza.
- Estricto cumplimiento de plazos.
- El pliego y las ofertas presentadas son inalterables.
- Imposibilidad de presentar múltiples ofertas en paralelo.



Trámite y sellado digital



Hoy el ciudadano no tiene prueba de lo que realiza en un portal de gobierno.

Un número de trámite, o un documento PDF fácilmente editable, no le permite demostrar de manera fehaciente que realizó una gestión ante un organismo público (el trámite digital se puede perder/“traspapelar” o adulterar sin que el ciudadano tenga prueba inequívoca del mismo).

Títulos de propiedad

Hernando de Soto
@ReadingSignals

The official account of Peruvian economist, President of @ILDthinktank and author of 'The Mystery of Capital'. *Run by ILD staff

Lima, Peru
ild.org.pe

Hernando de Soto Follow
@ReadingSignals

How Blockchain Could Help Strengthen Developing Nations ild.org.pe/ild-in-the-new … via @ILDThinkTank

Hernando de Soto Follow
@ReadingSignals

Georgia to Store Real Estate Documents in Blockchain System with Bitfury Group and Hernando de Soto ild.org.pe/ild-in-the-new … - @ILDThinkTank

How Blockchain Could Help Strengthen Developing Nations

INVESTOR'S BUSINESS DAILY NEWS

"Forget the details, all the facts that are needed to be able to see what belongs to whom, and have the degree of certainty that you need to make transactions in a market economy remain to be done," said Hernando de Soto, an economist from Peru who has researched property rights and their relationship to economic development.

De Soto is working with the Bitfury Group, a tech company whose advisory board includes a variety of former U.S. government officials, on a pilot project to develop a Blockchain-based land registry in the Republic of Georgia.

Forbes

Personal Finance / #CuttingEdge
FEB 7, 2017 @ 09:52 AM 8,713 VIEWS

The First Government To Secure Land Titles On The Bitcoin Blockchain Expands Project

WOMEN@FORBES

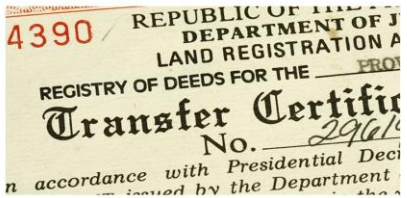
Laura Shin, CONTRIBUTOR
I cover Bitcoin, blockchain, fintech, personal finance and career FULL BIO

Republic of Georgia to Develop Blockchain Land Registry

Stan Higgins (@mpmcsweeney) | Published on April 22, 2016 at 16:44 GMT

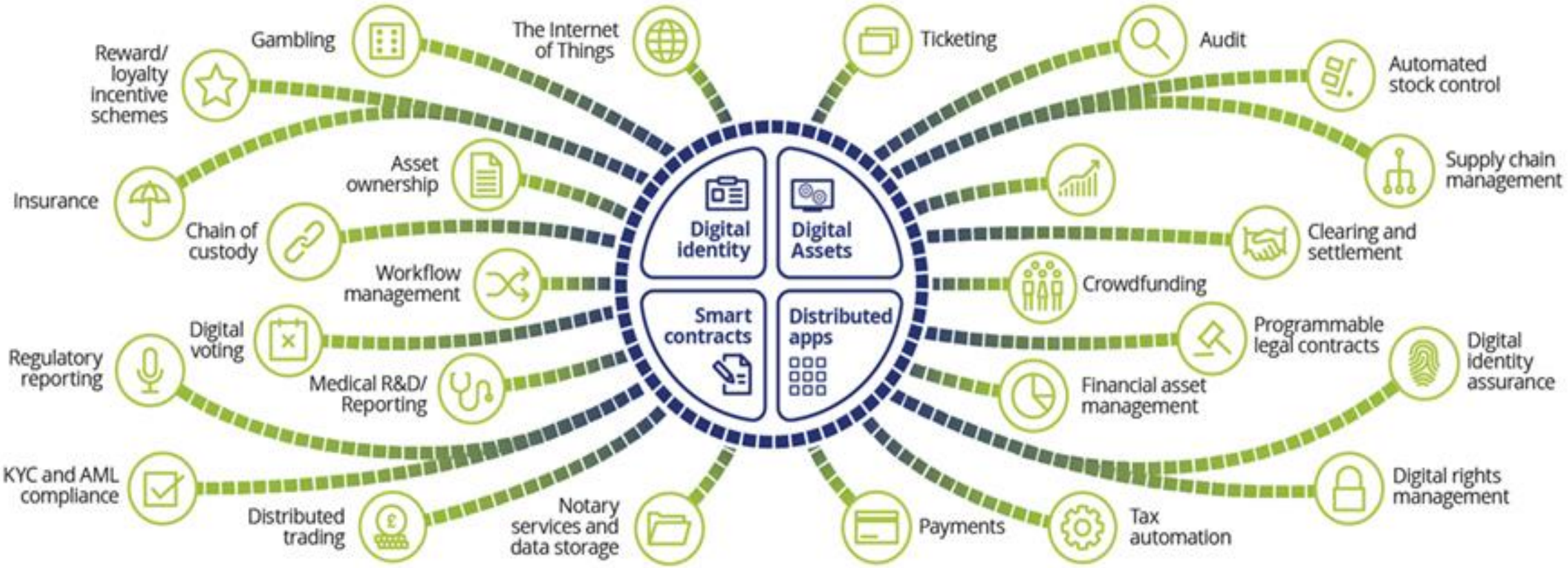
Chicago's Cook County to Test Bitcoin Blockchain-Based Property Title Transfer

Oct 6, 2016 11:47 AM EST by Kyle Torpey



1ER FORO DE BLOCKCHAIN

En general

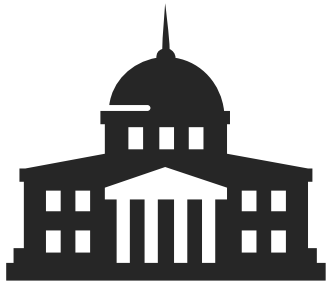


Fuente: Deloitte/uk

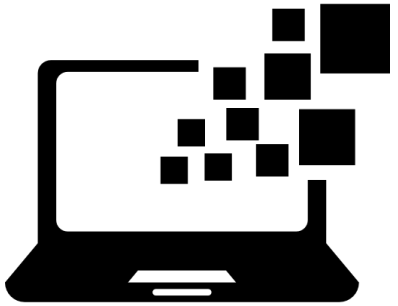
Uso de la tecnología Blockchain en varias industrias

Servicios Financieros

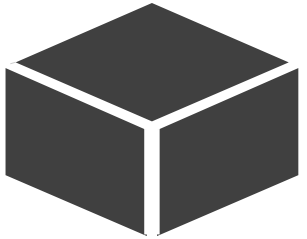
Industria de la salud



Organizaciones públicas y de impacto social



Tecnología, medios y telecomunicaciones



Consumidor y productos industriales

Startups basados en Blockchain han atraído tanto capital de inversión como lo que consiguieron las empresas de Internet en sus inicios

El sector financiero busca expandir el acceso a los servicios financieros optimizando la eficiencia

Aplicaciones potenciales de Blockchain

- Compensación y Liquidación en procesos post-negociación para agilizar procesos.
- Billeteras digitales
- Transferencias punto-a-punto (e.g., transferencias monetarias, consignaciones)
- Contratos inteligentes
- Algoritmos de negociación automáticos

Señales del mercado

- Abra está re-imaginando los pagos P2P sin costos ni cuentas para incrementar la inclusión financiera
- Align Commerce (ahora Veem) simplifica el ciclo facturación-pago para pequeños negocios negociando en la moneda local
- Ethereum, Digital Note, y Bitcoin desarrollaron criptomonedas digitales
- Digital Asset, desarrolla para ASX todo su Sistema de post negociación en Blockchain

Digital Asset Holdings

Caso de estudio destacado:

Digital Asset Holdings hace reingeniería de la "infraestructura" en servicios financieros.

- Digital Asset Holdings construye herramientas de procesamiento distribuídos, encriptados, y completos sobre Blockchain para mejorar la eficiencia, seguridad, conformidad y velocidad en el cumplimiento
- La compañia es liderada por Blythe Masters, un ex ejecutivo de JPMorgan, y recientemente ha adquirido varios startups en Blockchain

La industria de la salud busca mejorar resultados, incrementar la coordinación y maximizar la eficiencia

Aplicaciones potenciales de Blockchain

- Registro electrónico seguro de registros médicos
- Cumplimiento y verificación de servicio en seguros de salud
- Administración de quejas – reducción de tiempos de procesamiento e identificación de quejas fraudulentas

Señales del mercado

- El Startup BitHealth implementó una solución para asegurar la identidad y registros de salud a través del Blockchain
- Philips Healthcare ha mostrado interés en el startup Tierion, solución que recolecta datos, los registra en el Blockchain, y los conecta con otras aplicaciones de negocio

Caso de estudio destacado:

HealthNautica.com factom

HealthNautica y Factom hacen que los registros medicos sean más seguros…

- El servicio de mantenimiento de registros de Factom basado en Blockchain se ha asociado con el mayor proveedor de servicios medicos en Estados Unidos llamado HealthNautica, para desplegar una solución para los registros médicos digitales en Blockchain
- HealthNautica espera que integrando la tecnología basada en Blockchain ayudará a asegurar la integridad de documentos altamente sensibles dentro de su campo de estudio, tales como: disputas de procesos de facturación y reclamos, registros médicos, información de calendario de cirugías, etc.

Universidad de los Andes
Facultad de Ingeniería

FOROS ISIS

Departamento de Ingeniería de Sistemas y Computación

Organizaciones públicas y de impacto social buscan incrementar el acceso a sus servicios y mejorar eficiencia y transparencia

Aplicaciones potenciales de Blockchain

- Administración de registros públicos
- Administración de identidad
- Inclusión financiera y servicio social
- Ayudas humanitarias
- Protección contra el fraude y la corrupción
- Administración de subsidios en tiempo real
- Títulos y Certificados de estudios

Señales del mercado

- El candidato a la alcaldía de Londres propuso "MayorsChain" para monitorear las finanzas de la ciudad
- Onename espera proveer ID oficiales para aquellos que no disponen de un ID del gobierno
- Ambisafe proveerá un sistema nacional de votación a prueba de fraudes
- El partido político liberal danés, Liberal Alliance, fue primero en el mundo en usar Blockchain para elecciones internas
- Signatura, prove una plataforma sencilla para firmar y notarizar documentos en blockchain.

Caso de studio destacado:

factom

Honduras está digitalizando títulos de tierras…

- Honduras ha experimentado disputas en marcha de títulos sobre la tierra dentro de sus comunidades, lo que ha causado conflictos y desórdenes por décadas
- El gobierno de Honduras se asoció con Factom Inc., para digitalizar su proceso de titulación de tierras. El sistema en Blockchain prevendrá el fraude continuado sobre la titulación de tierras en Honduras.
- Aunque el proceso actualmente está detenido, se espera pueda continuar en cualquier momento.
- **República de Georgia** (Bitfury Group), **Suecia** (ChromaWay), **Condado Cook** de Chicago(Velox), han lanzado proyectos similares.

1ER FORO DE BLOCKCHAIN

Organizaciones del sector Telecomunicaciones, Media y Tecnología, enfrentan retos relacionados a la privacidad creciente, ciber seguridad y amenazas a la propiedad intelectual

Aplicaciones potenciales de Blockchain

- Contratos inteligentes para automatizar la ejecución de contratos, como pagos de regalías y/o Propiedad Intelectual (PI)
- Internet de las Cosas (IoT) para facilitar transmisiones y transacciones punto-a-punto entre dispositivos usando Blockchain

Señales del mercado

- IBM y Samsung se asociaron para lanzar una prueba de concepto para ADEPT, un sistema construído sobre Blockchain para Internet de las Cosas (IoT)
- Compañias como Uber y Airbnb pueden sufrir disrupciones – La'Zooz provee una plataforma basada en Blockchain para compartir viajes que no requieren un intermediario como Uber para validar y aprobar las transacciones

Caso de studio destacado:

PeerTracks y UJO reconstruyen la industria musical en el Blockchain…

- Los creadores publican información de propiedad y establecen las políticas en el Blockchain
- Contratos inteligentes permiten que cualquiera use el contenido registrado siempre y cuando cumplan las condiciones pactadas en la política
- Los pagos se entregan a los respectivos participantes al instante usando moneda digital
- **Spotify** adquirió Mediachain Labs para distribuir los derechos de autor con la música que proporciona el servicio de Spotify.

Compañías del sector de Consumidores y Productos Industriales enfrentan presiones debido a la evolución de las expectativas de los clientes

Aplicaciones potenciales de Blockchain

- Acuerdos inteligentes, para hacer que las Cartas de Crédito sean mas rápidas, baratas y mejores
- Libros distribuídos para mejorar el rastreo y verificar la autenticidad de productos
- Información en tiempo real acerca de la demanda y uso de productos

Señales del mercado

- La plataforma de Alibaba **TaoProtect** le permite a los comerciantes reportar violaciones a las patentes
- **BlockVerify** trabaja para proveer una solución anti-piratería para cadenas de suministro, incluyendo farmacia, items de lujo, diamantes y electrónicos. La plataforma puede identificar productos falsos, mercadería robada, bienes cambiados, y transacciones, marcas y PI fraudulentas

Caso de studio destacado:

Everledger está haciendo "sonar" el Blockchain…

everledger

- La industria de diamantes enfrenta un problema costoso de fraude y robo. Cerca del 65% de los reclamos fraudulentos pasan sin ser detectados, a un costo anual de USD 3 billones
- Everledger en asociación con las certificadoras de diamantes, aseguradoras y autoridades policiales se unieron para digitalizar diamantes y colocar la información en el Blockchain. Actualmente, cerca de 1 millón de diamantes están en el registro.
- Minoristas como eBay y Amazon podrán revisar el inventario de los vendedores en su plataforma usando esta huella digital

Smart Contracts

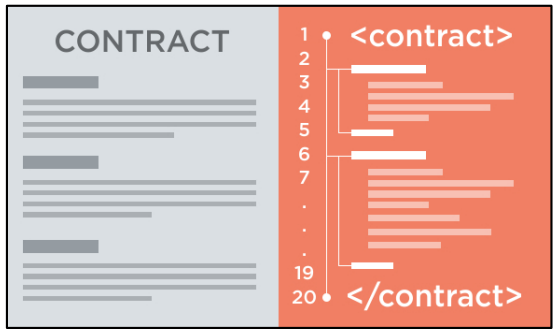
Universidad de los Andes
Facultad de Ingeniería

FOROS ISIS

Departamento de Ingeniería de Sistemas y Computación

1ER FORO DE BLOCKCHAIN

Smart contracts



- Contrato definido mediante software que automatiza y garantiza su cumplimiento.
- Eliminan al sistema judicial como intermediario.
- Son almacenados en un blockchain y ejecutados por su red de nodos.
- Requieren que el dinero sea un token digital.
- Internet de las cosas (IoT)/Ethereum/RSK/Lisk.

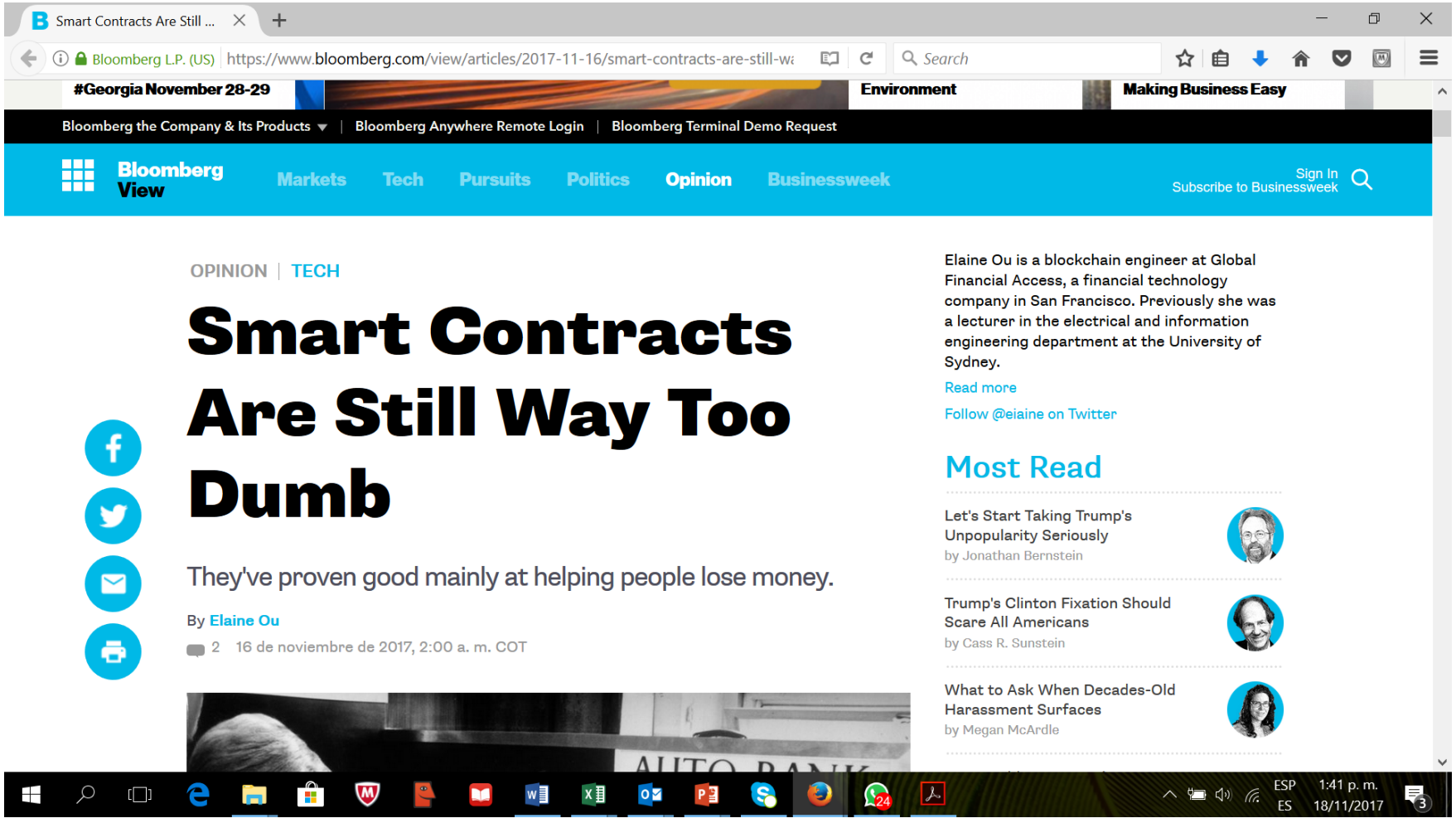
Interrogantes acerca de Smart Contracts

- Costos
- Incentivos
- Tradeoff: Almacenar y ejecutar en un solo lugar
- Reducción del riesgo operacional
- Cláusulas con personas involucradas
- Arbitraje

Smart Contracts y Bitcoin

- Counterparty, XCP
- RootStock, Roots

Smart Contracts – Madurez



Universidad de los Andes
Facultad de Ingeniería

FOROS ISIS

Departamento de Ingeniería de Sistemas y Computación

Desarrollo de aplicaciones Blockchain

Luis Javier Parra Bernal

Director de Estrategia y Desarrollo de Negocios

infoprojects

1ER FORO DE BLOCKCHAIN

Desarrollo de aplicaciones Blockchain

Temas a cubrir

- Conceptos básicos
- Ambientes para el desarrollo de aplicaciones Blockchain
- Características generales de una aplicación Blockchain
- Pasos para desarrollar una aplicación Blockchain
- Ejemplos de ambientes de desarrollo

Conceptos Básicos

Modelo de tres capas

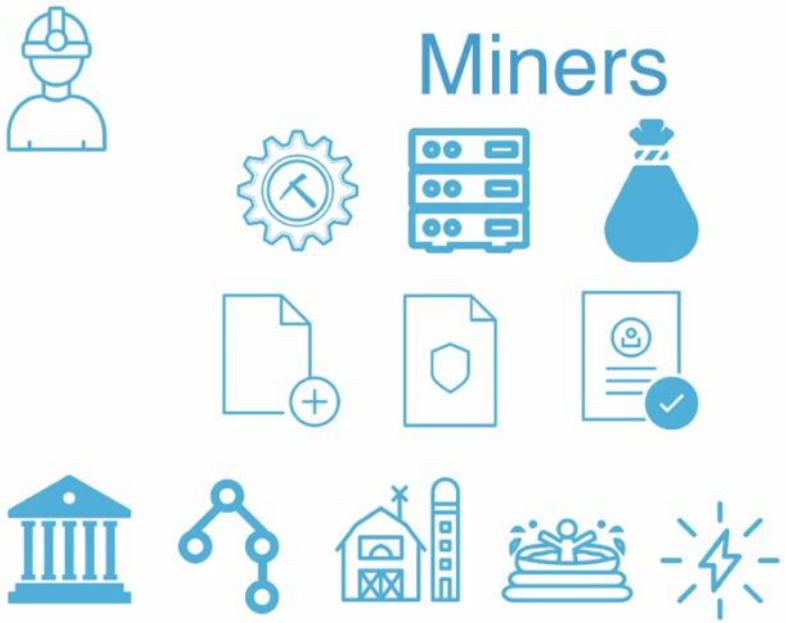
Usuarios, Mineros y Desarrolladores

Modelo de tres capas

Instancias	Red Principal (Network ID, Genesis Block), Red Paralela (Forks), Red de Pruebas, Redes Privadas, Redes Mixtas, …
Implementaciones	Bitcoin, Ethereum, Ripple, Eris, … OpenChain, Hyperlayer (Fabric, Sawtooth, Fabric, Iroha, Indy, Quilt, …), …
Características del Diseño	Distribución, Descentralización, Inmutabilidad, Privacidad, Anonimato, Consistencia, …

http://bit.ly/btc-wallets
http://bit.ly/eth-wallets

Billeteras (Client SW), Transacciones, Network, Cuentas, Libro diario, …



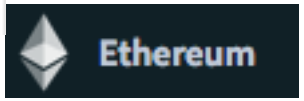
Algoritmo de consenso, Infraestructura, Recompensa, Registro, Criptografía, Firma, Teoría de juegos, …

Código, Colaboración, Lenguajes, Ambientes, …

1ER FORO DE BLOCKCHAIN

Ambientes para el desarrollo de aplicaciones Blockchain

Bitcoin
Ethereum
OpenChain
Hyperledger



- En constante evolución …
  - Más maduros: Bitcoin 2008, Ethereum 2014 (Solidity),
- Más nuevos: OpenChain Dic-2015 de la Linux Foundation
- Proyecto Hyperledger 2016
  - Multiples proyectos derivados: Fabric, Sawtooth, Iroha, Indy, Quilt, …
  - Miembros Premier: … ACCENTURE, AMEX, **IBM**, CISCO, BAIDU, **Intel**, HITACHI,…
  - Miembros Generales: … Deloitte, EY, Huawei, Nokia, **Oracle**, RedHat, VMware …
  - Miembros Asociados: … bancos, universidades, …
- Anuncio de Coco Framework Ago-2017 por parte de **Microsoft Azure.** Hace parte de Enterprise Ethereum Alliance

Proyectos Hyperledger

HYPERLEDGER

Proyecto	Iniciador - Lider	Diferencia Principal
Fabric	IBM	Canales Privados
Sawtooth	Intel	Consensus: Proof of elapsed time. Menos costoso
Indy	Sovrin Foundation	Identidad Digital compartible selectivamente
Burrow	Enterprise Ethereum Alliance	Permissioned smart contract interpreter (EVM)
Iroha	Japan Developers	C++ High Performance

Características generales de una aplicación Blockchain

1. Peer-to-Peer Network Distributed Descentralized Data Base
2. Node Software Client (Wallet) is your key to store a transacction in a blockchain
3. Distributed Ledger (List of ordered transactions)
4. Consensus Algorithm (Hash, Game process, No center point, Proof of …)
5. Smart contract language (Conditionals and Arithmetic, … Turing complete)
6. Crypto-currency (Reward, ...)
   - Durable, Portable, Accesible, Oferta limitada, Visible, Uniforme, Fusionable

Pasos generales para desarrollar una aplicación Blockchain

A tener en cuenta antes de iniciar …

- Es una nueva clase de sistemas de software que cumple las carácterísticas indicadas anteriormente
- La complejidad del manejo de las transacciones esta oculta en los ambientes de desarrollo
- El software cliente
- El lenguaje de los “contratos inteligentes” abstrae el registro y proceso de la lógica de las transacciones
- Identificar la aplicación
- Evaluar si la tecnología blockchain es la adecuada para la aplicación
- Seleccionar ambiente adecuado de los multiples existentes y en evolución

… pasos para el desarrollo …

- Definir el modelo de dominio (Entidades, Relaciones y Procesos)
- Preparar el ambiente
  - Crear contenedores
  - Instalar herramientas de desarrollo
  - Ejecutar el ambiente de red blockchain
- Crear la definición de la red (Identificador y bloque inicial)
- **Escribir la función de procesamiento de transacciones**
- Definir los reglas de control de acceso
- Generar el bloque inicial

… pasos para pruebas …

- Escribir las pruebas unitarias
  - RPC
- Implementar en el ambiente de pruebas local
  - Red Privada
- Implementar en el ambiente de la red blockchain
  - Red blockchain

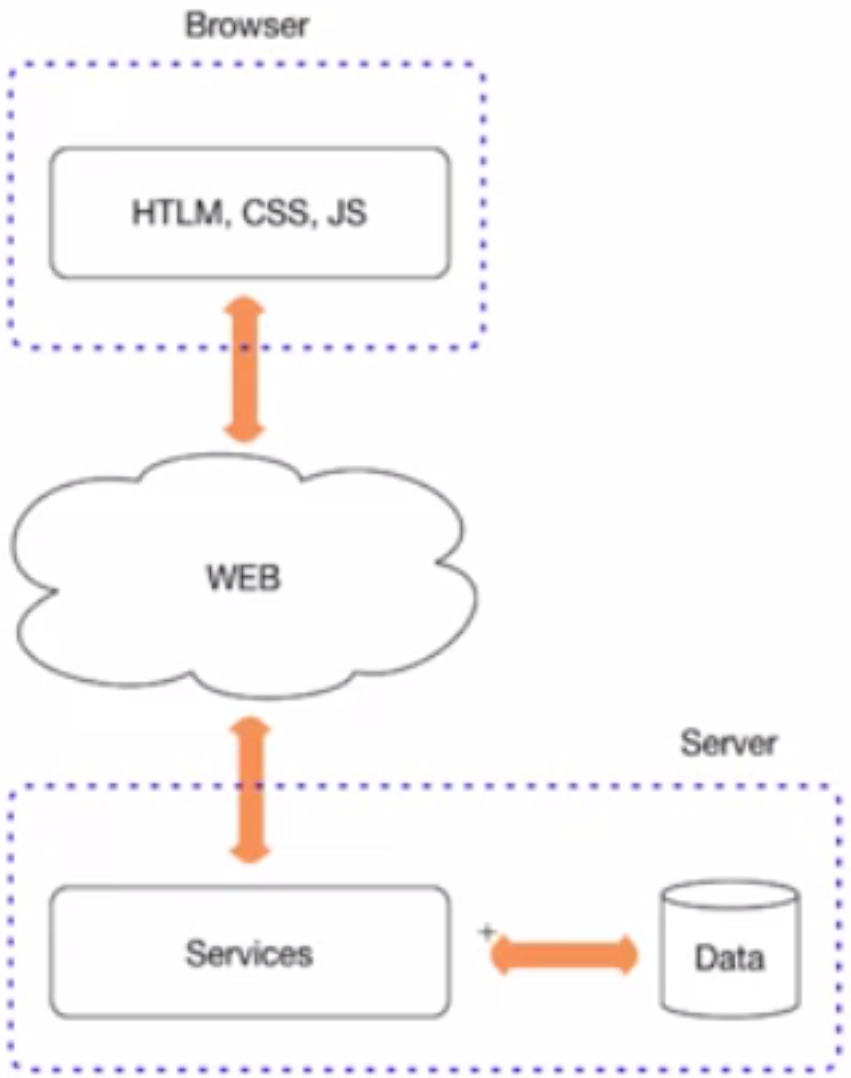
… pasos para puesta en producción …

- Generar el REST API para aplicaciones moviles
- General el esqueleto para las aplicaciones web

Ejemplos de ambientes de desarrollo

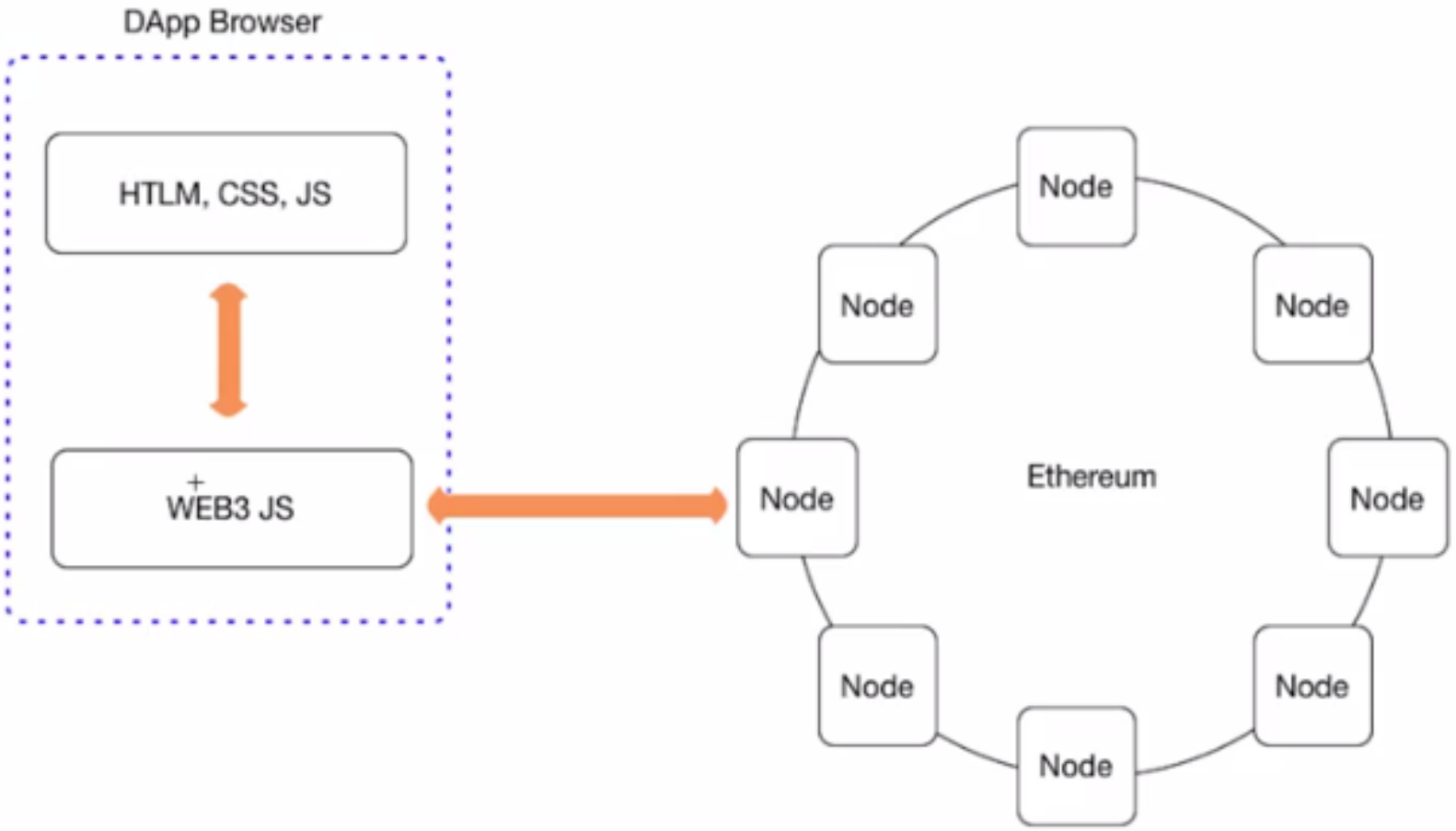
Ethereum

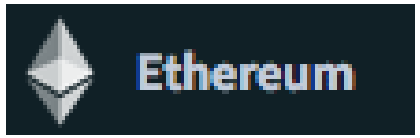
Hyperledger Fabric


Browser
HTLM, CSS, JS
WEB
Server
Services
Data

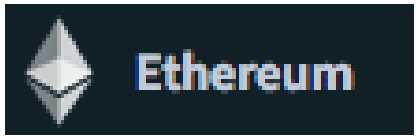
Ethereum

solidity





1. Preparación de ambiente:
   - Xcode, …
   - homebrew
   - nodeJS
   - testrpc
   - truffle
     - solc
     - geth

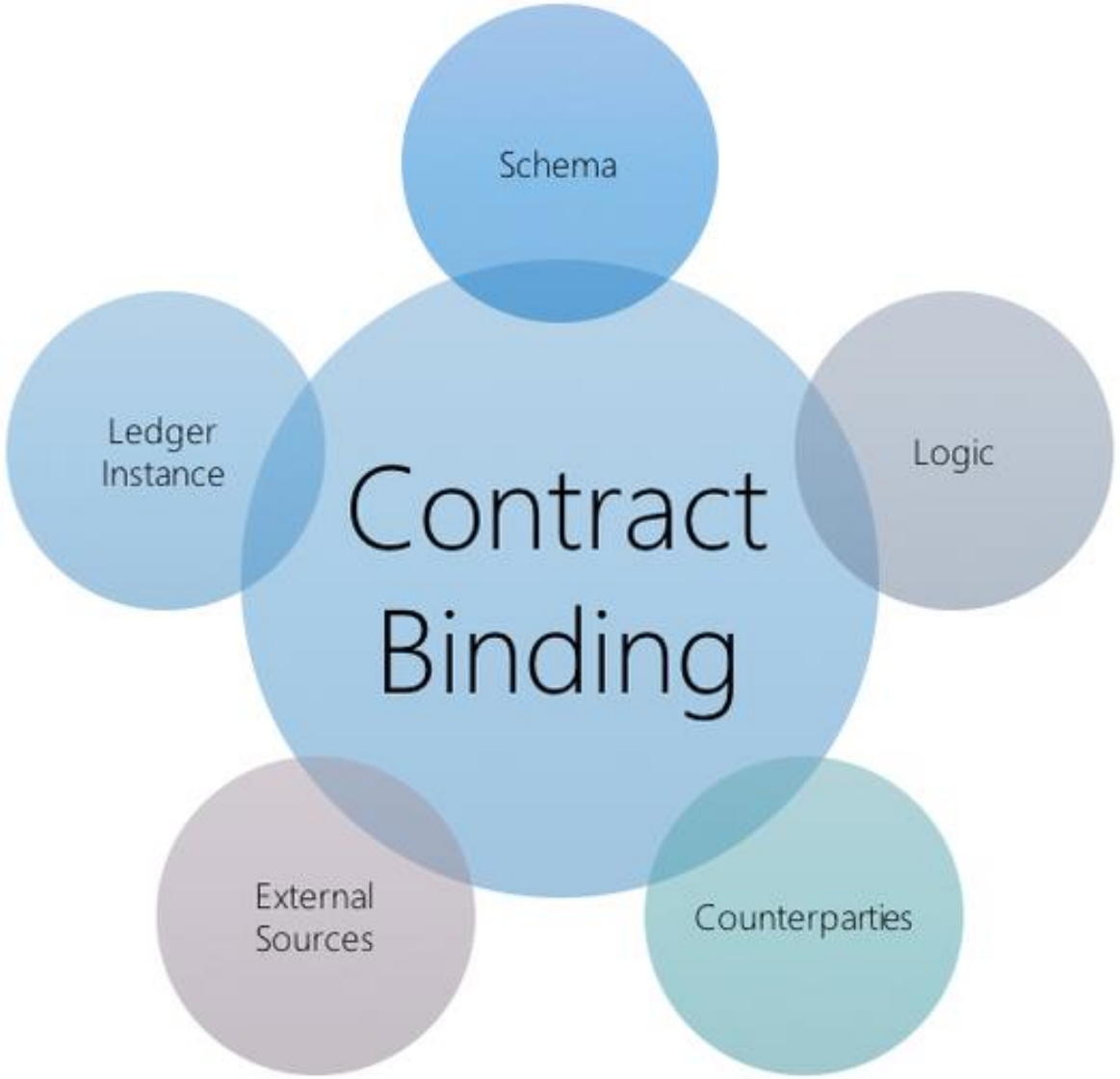


1. Crear una instancia de la red privada
   - Inicializar, Arrancar e Inspeccionar el nodo
2. Instalar el software cliente
   - Mist o Metamask
3. Escribir el programa (Contrato Inteligente)
   - Solidity … Viber
4. Compilar el programa
   - nodejs … capa de abstracción de conexión frontend y server
   - Solc … compilador de Solidity
   - Truffle … Ambiente de desarrollo (development framework)
5. Probar
   - testrpc

```
pragma solidity ^0.4.11;

contract GreetIngs {
    string message;

    function Greetings() {
        message = "I am ready!";
    }

    function setGreetings(string _message) public {
        message = _message;
    }

    function getGreetings() constant returns (string) {
        return message;
    }
}
```

HYPERLEDGER

Fabric



Velocidad, Volumen y Tamaño

Transaction speed

	Transaction recording	Transaction finality
Centralized API	~100ms	immediate
Bitcoin	10 minutes	6 blocks (1 hour)
Ethereum	17 seconds	12 blocks (~3.5 minutes)

Throughput (volume)

1MB/block
7 transactions/second

4 millions gas/block
20 transactions/second

Ø 2000 transactions/second
max 40000 transactions/second

Blockchain size

	Current size (April 2017)	Growth rate
Bitcoin	~112 GB	~4GB / month
Ethereum	~40 GB	~2GB / month

1ER FORO DE BLOCKCHAIN

Algunos términos

- **UTXO's**: Unspend Transaction Output Transacciones que han sido enviadas a un usuario y no han sido aún gastadas por ese usuario
- **Consensus Algorithm:** Proceso de arbitraje para determinar cuál nodo (minero) puede registrar el siguiente bloque, basado en teoría de juegos. Varios tipos de prueba: trabajo, participación, tiempo consumido.
- **Wallet (Node Software Client):** Software del cliente que registra una transacción en el blockchain.

Bibliografía

- Udemy Course: Getting Starting with Ethereum
- Hyperledger Composer Development Tutorial for Mac OS X
- IBM - DeveloperWorks Courses - Blockchain essentials
- Enterprise Smart Contracts, Marley Gray - Microsoft
- OpenChain Project
- Hyperledger Project
- What's the Difference Between the 5 Hyperledger Blockchain Projects? – Linda Hardesty
- Enterprise Ethereum Alliance
- https://hyperledger.githib.io/composer/installing/development-tools.html

Gracias

Jimmy Chung Tong – Director de Tecnología

Luis Javier Parra Bernal – Director de Estrategia

infoprojects