**La tecnología subyacente a las cuatro revoluciones**

**Yadran Eterovic S**

Director, Departamento de ciencia de la computación Escuela de Ingeniería – P. Universidad Católica de Chile

Blockchain es una consecuencia de un camino que se viene desarrollando hace mucho tiempo, demostrar que esta tecnología esta nuestro alcance, se encuentra ad-portas, desde el punto de vista personal del director estas tecnologías han sido protagonistas de las 4 revoluciones industriales.

Estamos rodeados de redes inalámbricas, muchas de las comodidades que hoy conocemos son gracias a la computación, en cuanto a su capacidad de manejar grandes volúmenes de información sin practicante equivocarse.

Se encuentran en educación, comercio, entretenimiento, investigación, entre otros.

El equipo computacional promedio tiene una duración de 50 años, esto es producto de gente que esta mas allá de vender un equipo para generar una ganancia, sino que va más allá al momento de perfeccionar la eficiencia.

En la PUC se encuentra el IBM 620 el cual tenia 64 kb de memoria.

Esta es una realidad realmente palpable, el diseño según la ley de Moore, este señor es uno de los creadores de Intel, Moores Law, el numero de transistores en un circuito integrado, va incrementando de manera exponencial, desde 1000 transistores a los 10000 millones de transistores.

En el mundo de la computación se utiliza la abstracción todos los equipos están hechos en base a la abstracción, en el sentido que usamos una capa de servicios básicos fundamentales llamado el nivel de la lógica digital, y sobre esta se construye una segunda capa, y luego una tercera, de esta manera se pueden controlar los niveles de manera independiente.

Lo que es común se hace muy rápido, se privilegia lo que es común, como por ejemplo sumar 1, sumar 1 es común en los programas, el 1 se hace eficiente debido que se repite constantemente.

Paralelismo, varias CPU trabajando de manera paralela para resolver una misma tarea.

Pipelining y predicción, no se espera que se termine todas las tareas va por etapas cumpliendo, desde la inicial a la final.

Que sucede cuando tenemos una condición en pipelining, las personas detrás de estas cosas lograr adivinar, hoy en día se logra un 95% de acierto.

Pequeño volumen, rapidísimo acceso un ciclo de CPU, gran volumen discos magnéticos muchísimos ciclos de CPU, para almacenar una gran cantidad de información, esto es la jerarquización de las memorias CPU.

Confiabilidad vía redundancia, la tecnología raramente presenta errores en sus decisiones, por lo que se debe tener contingencias para cada caso.

Algoritmo, secuencia de pasos que resuelve un problema de principio a fin, esto no es únicamente consecuencia de la llegada de los computadores, en el año 1448, Johann Gutenberg promovió el alfabetismo, y finalmente ocurrió la primera revolución industrial, Se iba copiando y traduciendo del griego y el arabe al latín y luego al español, todo era manuscrito en esa época y aparte no todo el mundo sabia leer o escribir lo que era para la elite de la civilización, la imprenta cambia este paradigma NO SOLO FUE LA IMPRENTA QUIEN GUIO LA REVOLUCION, FUERON LOS ALGORITMOS,

Los numero romanos que utilizaba Gutenberg y el problema es que estos sugieren es que no siguen ninguna regla fija o reglas arbitrarios como los palos a la izquierda o derecha, sumar era difícil por lo tanto multiplicar era aún más difícil, había que recurrir a un experto en ábacos, en la **India** se inventaron diferentes numero como decimal posicional, tiene una regla clara de como se pueden realizar aplicaciones aritméticas con ellos de manera más fácil.

Un matemático persa que trabajaba en Bagdad que se llama la casa de la sabiduría, estudiar leer y entender la filosofía griega el se preocupo de la matemática, utilizando la aritmética india que la encontró realmente eficiente, se preocupo de escribir los métodos, para sumar, multiplicar, raíz cuadrada y obtuvo los dígitos de PI, para hacerlo un método automatizado, el nombre algoritmo en honor a Al Khwarizmi.

Leonardo de Pisa – Fibonacci- se da cuenta del potencial de estos métodos para generar valores, por lo tanto Fibonacci y Al Khwarizmi, se puede utilizar las operaciones aritméticas.

Historiadores mencionan que si las cosas no fuesen así el avance de la tecnología seria menor, debido a la velocidad ya que la tecnología y el sistema aritmético Indio decimal posicional.

Los computadores modernos fueron desarrollados unos 700 años después, incluyen explícitamente posicional en sus bits, palabras y unidades aritméticas, estamos utilizando técnicas que existen hace años, el desarrollo tecnológico les debe su desarrollo a todas estas aplicaciones.

Los equipos no son magia ni productos de la casualidad, cada paso que da un sistema computacional esta calculado y se sabe exactamente que es lo que tiene que ocurrir, ha sido concebido implantando por personas, esta tecnología computacional del siglo 20, es lo que permite la revolución industrial la 3° que es computacional y la 4° que es la actual en cuanto a blockchain.

**Algoritmos desarrollados últimamente**

**Algoritmos Numéricos**

Para poder buscar eficientemente se debía tener un orden eficiente y bien hecho, todos querían plasmar su fama en un desarrollo de un nuevo algoritmo de ordenación, por lo que empiezan a aparecen los algoritmos:

* **Búsqueda** (back tracking)
* **Ordenación** (dividir y conquistar)
* **Grafos** (Programación dinámica y algoritmos codiciosos)

Hoy en día los computadores procesan mas texto que numero, la gran mayoría de los e quipos convencionales se preocupan más de imágenes y texto, todo se traduce a bits, como podemos abordar este problema de manera informática con estrategias algorítmicas, tenemos diferentes estrategias, back tracking revisar el camino si llego al limite retrocedo y busco otro camino, como por ejemplo encontrar la ruta más corta.

Aparecieron los algoritmos más directamente responsables de la cuarta industrial:

* **Page Rank**
* **Indexación** (Google motores de búsqueda) se creo en base al ranking de páginas, lo que hace es recorrer una vez la web para identificar que pagina es mejor que las demás, dentro de la internet.
* **Criptografía de Clave Publica**, como yo me comunico contigo sin haberte conocido sin que nadie sepa que es lo que estoy comunicando, Amazon no sabe quién soy yo ni mi equipo sabe quién es Amazon, como para ingresar los numero de las tarjetas de créditos, la criptografía se utilizaba en ámbitos militares por lo que eran secretos militares.
* **Firma digital**

Compresión de información y códigos de correctores de errores, es un tributo a las personas que están detrás de todo esto

Preguntas algoritmos, ¿Es correcto? ¿Cuánto tiempo ejecutarlo? Y ¿podemos mejorarlo?

Finalmente todo a la tecnología computacional rápida y eficiente y los algoritmos fruto del ingenio humano necesitar poder aplicarse a la realidad mediante

Software, es muy difícil convertir una idea en un programa computacional que funcione de manera correcta, D. Knuth Tek es un producto de principio a fin por Knuth, una de las acciones más importantes, quizás, es el hecho de que el software es difícil “Los procesos de desarrollo de software es muy riguroso hasta los métodos más fáciles.

* **Cascada**
* **Mejoramiento Iterativo**
* **Espiral**
* **RUP**
* **Scrum**
* **XP (Extreme Programming)**

En febrero de 2001 un grupo de 17 líderes de toda la industria se reunió en el Ski resort Snowbird, porque les ha ido bien, las personas y las interacciones son más valiosos es que las herramientas y procesos, por lo que se debe comunicar entre los integrantes para que estos aporten el equipo, es mas valioso el SW que funciona que la documentación, ellos privilegian la interacción del cliente por lo que si le va bien también le va bien al creador del SW, no dejemos esto en manos de los abogados ni contratos, ojala se pueda colaborar de manera activa.

Métodos agiles no rechazaba los cambios los aceptamos e incorporémoslos a nuestros procesos, sin que estos se conviertan en un caos, esta es la contribución mas reciente de los algoritmos, todo esto proceso es producto del trabajo de las personas, lo que hemos hecho y seguimos haciendo, como bitcoin, inteligencia artificial, conocer todas estas disciplinas pueden lograr.

Que se puede hacer con esta tecnología a nivel empresarial, tanto blockchain e IoT, Netflix que tenemos día a día, ellos están cambiando su modelo negocio, están orientados un poco a IoT y bigData, para empezar la producción y ser asertivos en su mercado, hoy en día cuentan con productos IoT, es parte de la transformación digital en las empresas, a partir de esto, ¿que dicen los clientes que quieren?, ¿se preocupan de las rentabilidades, que piensan las organización que quieren sus clientes?, que esperan, las organización se creen grandes viene el startups, se fijan en números que hoy en día se cuenta con tantas herramientas exitosas, como Cryptomarket, Buda, Cornershop.

IoT, Hiper-Conectividad de los objetos físicos y virtuales a nivel mundial, blockchain Smart Contracto, Dinero Digital.

Iot: Internet of Things, hoy en día en toda parte se encuentra un sensor la idea principal de esto es tener esos datos, para ahora hacer algo realmente bueno con esto, ahí es donde entra IoT, esto no es mundo que está aislada, todas las tecnologías colaboran entre sí, IoT Business Ideas

* **Mobike Sistema de bicicletas**
* **Industria medica seguimiento.**
* **Deportes relojes con sensor de pulsaciones.**
* **Smart Cities, que pasa si tenemos todo en un servidor y la red se cae perdemos el acceso a información.**

6 mesas de gobiernos mesa medica ficha medica única, ya que en otros hospitales esta no tiene información.

Antes del 2005 todas las redes estaban centralizadas como las IoT, ahora se tiene acceso a las redes pero con problemas, en 2025 se estima que se pueda conectar con todo nuestro alrededor.

Definir una red de negocios identificable con participantes, activos y transacciones.

Requiere confianza mesas de consenso empresas publicas y privadas para sacar adelante un chile más tecnológico.

SupplyChain (Cadena de suministros), se propone un sistema de negocios, Walmart todos sus alimentos perecederos para que todos sus proveedores se sumen a esa red para contar con toda la información relacionada con la compra y venta a los proveedores, como llegada de productos, fechas, entre otras cosas.

Caso de negocio, estacionamientos cuando uno se estaciona no recordemos donde quedo el auto, falto algo en su interior, o el auto no está.

Para el momento de la denuncia tener información como antecedentes, en forma corporativa se puede saber el historial del auto.

Ficción o Realidad, la capital de Latinoamérica de lo que podría ser una Smartcities, california cantina para pagar cervezas con criptomonedas.

BlockChain, ¿La cuarta revolución industrial?

* **1 etapa:** Mecanización, poder del agua, steam power
* **2 etapa:** producción en masa, línea de ensamblaje, electricidad
* **3 etapa:** computación y automatización, procesar grandes volúmenes de información.
* **4 etapa:** Sistemas distribuidos IoT, poder tener dispositivos constantemente a una red, en base a blockchain.

**¿QUE ES BLOCKCHAIN’**

Seria un libro contable distribuido y abierto que permite grabar transacciones entre 2 partes de manera eficiente y en una forma verificable.

Como hacemos un registro de información permanente, gobiernos necesitan controlar sus ejércitos.

Y ¿cómo hacemos un registro de información digital permanente?

En el bloque se tienen un numero de transacciones y el nonce es los mineros que están descifrando, algoritmo de proof of work, es fácil saber si la información es correcta, es fácil verificar el hash de los bloques.

El registro digital más permanente hoy.

El blockchain es una base de datos ineficiente transformando un problema en la solución de las transacciones financieras.

Es primera vez en la historia de la humanidad en que podemos llevar un registro de información incorruptible.

Billeteras, Pago en Internet, Remesas, Robots de Arbitraje, Infraestructura para el manejo de llaves digitales, Servicio notariado de documentos.

Uber + Bitcoin + Inteligencia Artificial

Las remesas significan enviar y recibir dinero desde otro país, un 7% del dinero se va a PayPal, Westerunion, el E-Commerce vender un producto atraes de internet.

La gracia de esto es global no discrimina por país, no existe un punto central, debajo de Bitcoin, Smart contracts, voting, payments, blockchain, governance, identity, intert of things.

* **B2C**, servicios de valor a personas.
* **B2B**, Business to Business. (Empresa a empresa)

Email CryptoMKT: **daniel@cryptomkt.com**