**Especialización en blockchain**

1)Conceptos Básicos previos a investigación

Creator: Satoshi Nakamoto (No one knows if he is a person or a group of people)

¿Qué es blockchain?

Dando permiso a la información digital para ser distribuida, pero no copiada, la tecnología de blockchain esta creando la columna vertebral de un nuevo tipo de internet. Originalmente ideado para “dinero digital”, más específicamente para “Bitcoin”, la comunidad tecnológica ha encontrado otros usos potenciales.

“El blockchain es un incorruptible libro mayor de transacciones económicas que pueden ser programados para registrar no solo transacciones financieras sino virtualmente todo lo de valor” – Don & Alex Tapscott, autores de “Blockchain Revolution” (2016)

Un blockchain es, en términos simples, una serie de registros inmutables de data sellados en el tiempo que es manejado por un grupo de computadoras que no le pertenecen a ninguna entidad. Cada uno de estos **bloques de data** o **bloques** están asegurados y unidos a cada uno usando **principios criptográficos** o **cadenas**.

Entonces, ¿qué es tan especial y porque decimos que tiene las capacidades de interrumpir la industria?

La red de blockchain no tiene una autoridad central – es la definición misma de sistemas democratizados. Desde que es un libro mayor compartido e inmutable, la información esta abierta a cualquiera y cualquiera puede verla. Por lo tanto, cualquier cosa que es construida en el blockchain es por naturaleza transparente y toda persona envuelta responsable por sus acciones.

2)Explicación del blockchain

Un blockchain carga **un costo de no transacción** (una infraestructura que cuesta, pero las transacciones no). El blockchain es una manera ingeniosa de pasar información de A a B de una manera totalmente automatizada y segura.

Proceso:

1. Una parte en una transacción inicia el proceso creando un bloque.
2. Este bloque esta verificado por miles, tal vez millones de computadoras distribuidas alrededor de la red.
3. El bloque, una vez verificado es agregado a una cadena, que es almacenado alrededor de la red, creando no solo un único registro, sino un único registro con una historia única. (lo que hace que, para falsificar un solo registro, se debería falsificar la cadena completa con sus millones de instancias, lo que es virtualmente imposible).

\*Bitcoin utiliza este modelo para transacciones monetarias, pero puede ser desplegado en muchas otras maneras.

Ejemplo:

Piense en una compañía de ferrocarriles.

Compras unos tickets en el app o la web de la compañía.

La compañía de tarjetas de crédito toma un tiempo para procesar la transacción.

Con blockchain, no solo el operador de ferrocarril ahorraría en las cuotas de procesamiento de las tarjetas de crédito, pues podría mover el proceso de tickets completo al blockchain.

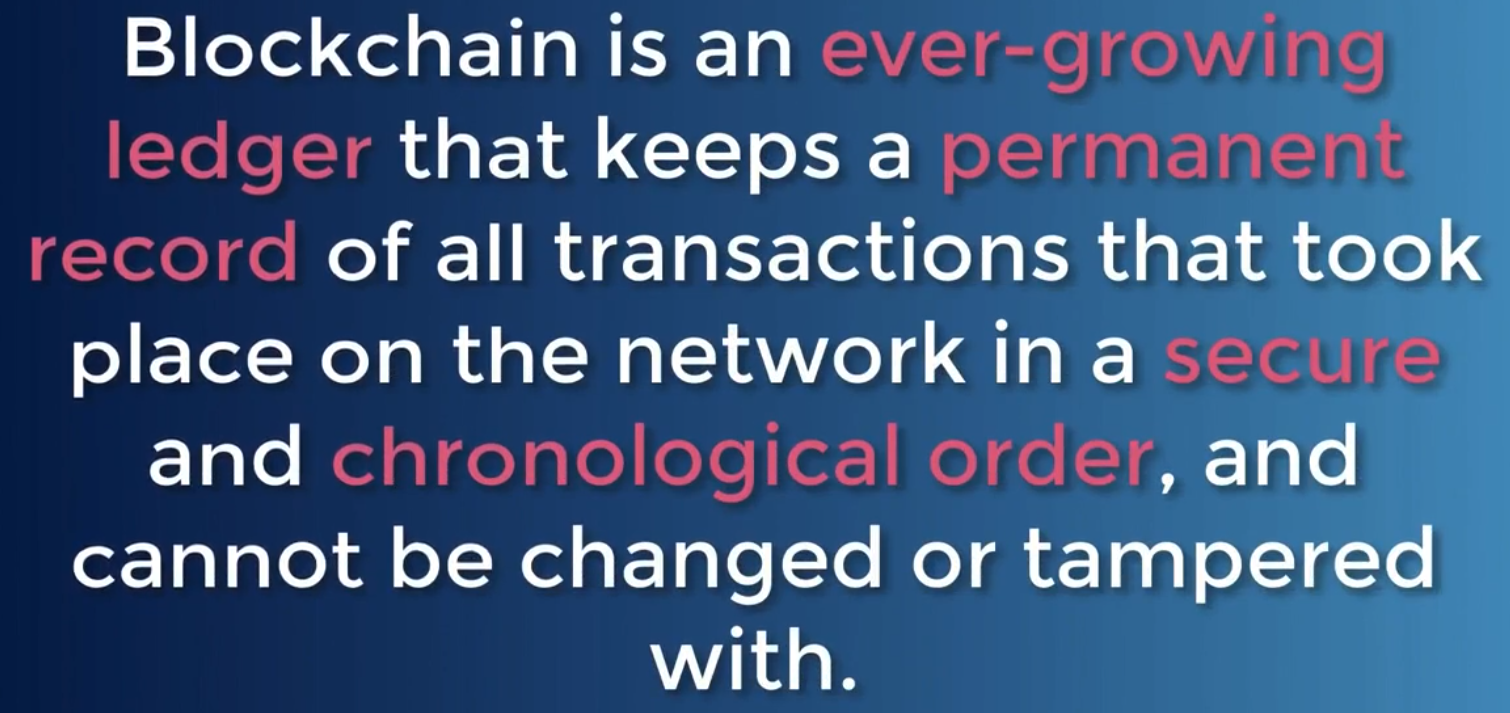
Las dos partes en la transacción son la compañía de ferrocarriles y el pasajero.

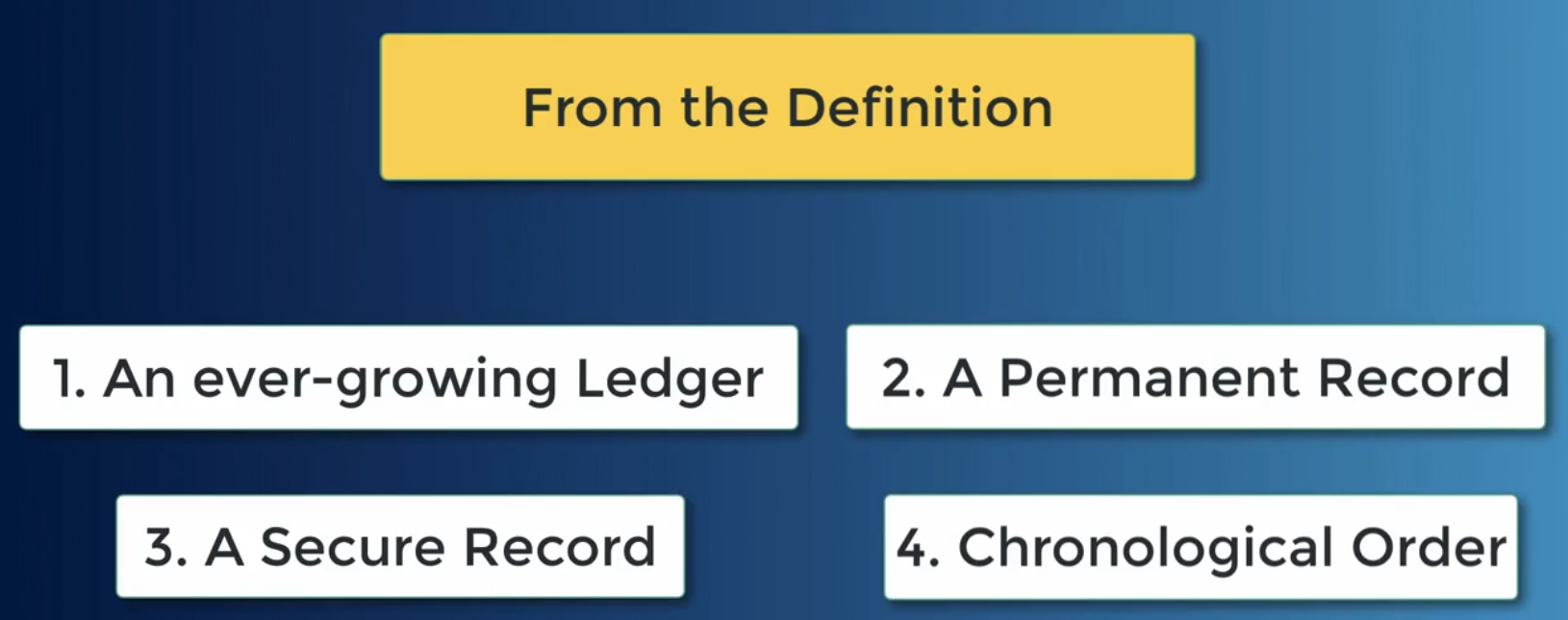
El ticket es el **bloque**, que será agregado a un blockchain de tickets.

Sólo como una transacción monetaria en blockchain es única, registros independientemente verificables e infalsificables (como bitcoin), como un ticket puede ser.

El último ticket blockchain es también un registro de todas las transacciones, por decir, la ruta del tren, o incluso la red completa de trenes, incluyendo cada ticket vendido, cada viaje tomado.

La llave aquí es que es **gratis**, No solo el blockchain se puede transferir o almacenar dinero, **pero también puede reemplazar todos los procesos y modelos de negocio que confían en cargar un pequeño monto por transacción.** O cualquier otra transacción entre dos partes.





Campos potenciales de aplicación:

-Dinero (bancos, transacciones, etc)

-IOT (Internet of things)

-Comercio electrónico

(compra y venta de objetos entre personas sin tener que pagar comisiones)

(check open bazar)

-Caridad y donaciones

-Campañas electorales y los votos

**Resumen**

**Index**

\*Deben haber 3 papers.

Mi enfoque va a ser el usar Internet Of Things.

1)Applications of Blockchain Technology beyond Cryptocurrency. (<https://arxiv.org/abs/1801.03528> )

2)A Review on the Use of Blockchain for the Internet of Things

(<https://ieeexplore.ieee.org/abstract/document/8370027> )

3)A blockchain future for internet of things security: a position paper. (Mandrita Banerjee, Junghee Lee, Kim-Kwang Choo)

(<https://www.sciencedirect.com/science/article/pii/S2352864817302900> )

4)IoTChain: A blockchain security architecture for the Internet of Things (<https://ieeexplore.ieee.org/abstract/document/8377385> )

Resumen de las fuentes

1. <http://www.aetic.theiaer.org/archive/v2/v2n1/p1.html>

Blockchain es la tecnología detrás del **sistema de la** **criptomoneda Bitcoin**, es considerada para ser atractivo y crítico para garantizar una seguridad mejorada y (en algunas implementaciones, no rastreables) privacidad para diversas aplicaciones en muchos otros dominios – Incluyendo el ecosistema del Internet de las Cosas (IoT). Investigación intensiva nos esta conduciendo a que en academias e industria apliquen tecnología Blockchain en múltiples aplicaciones. Proof-of-Work, un puzle criptográfico, juega un rol vital en asegurar los Bitcoin manteniendo un libro digital de transacciones, que es considerado como incorruptible.

Blockchain usa una clave pública (PK) para registrar la identidad de los usuarios, que provee una capa extra de privacidad. No solo en criptomonedas se ha adoptado con éxito el blockchain (BC) siendo implementado, pero también en **multifacéticos sistemas no monetarios** como: Sistemas de almacenamiento distribuido, Prueba de ubicación, Cuidado de la Salud, Votación descentralizada, entre otros. Recientes artículos y proyectos/aplicaciones fueron encuestados para evaluar las implementaciones de BC para seguridad mejorada, para identificar retos asociados y para proponer soluciones para sistemas de seguridad mejorados con blockchain habilitado.

1)Resumen de la intro:

Este paper desea resumir la literatura de la implementación de blockchain y técnicas de libros digitales parecidas en varios otros dominios más allá de su aplicación en criptomonedas y dibujar las conclusiones adecuadas.

Blockchain es una tecnología relativamente nueva, un ejemplo representativo de investigación es presentado, abarcando los últimos 10 años, a partir de los primeros trabajos en este campo.

Blockchain es la tecnología detrás del **sistema de la** **criptomoneda Bitcoin**, es considerada para ser atractivo y crítico para garantizar una seguridad mejorada y (en algunas implementaciones, no rastreables) privacidad para diversas aplicaciones en muchos otros dominios – Incluyendo el ecosistema del Internet de las Cosas (IoT). Investigación intensiva nos esta conduciendo a que en academias e industria apliquen tecnología Blockchain en múltiples aplicaciones. Proof-of-Work, un puzle criptográfico, juega un rol vital en asegurar los Bitcoin manteniendo un libro digital de transacciones, que es considerado como incorruptible.

Blockchain usa una clave pública (PK) para registrar la identidad de los usuarios, que provee una capa extra de privacidad. No solo en criptomonedas se ha adoptado con éxito el blockchain (BC) siendo implementado, pero también en **multifacéticos sistemas no monetarios** como: Sistemas de almacenamiento distribuido, Prueba de ubicación, Cuidado de la Salud, Votación descentralizada, entre otros. Recientes artículos y proyectos/aplicaciones fueron encuestados para evaluar las implementaciones de BC para seguridad mejorada, para identificar retos asociados y para proponer soluciones para sistemas de seguridad mejorados con blockchain habilitado.

1. Fundamentos tecnológicos de Blockchain

Aquí se describirá brevemente los fundamentos en la tecnología detrás de blockchain. Un blockchain comprende dos diferentes componentes:

1. **Transacción**: Una transacción, en un blockchain, representa la acción desencadenada por el participante.
2. **Block**: Un bloque, en un blockchain, es una colección de registros de datos de transacciones y otros detalles asociados como la secuencia correcta (correct sequence), marca de tiempo desde la creación (timestamp of creation), etc.

El **BC** puede ser ambos, **público** o **privado**, dependiendo del alcance de su uso.

Un **blockchain público permite que todos los usuarios con permisos de escritura y lectura** como con Bitcoin, pueden acceder a él. Sin embargo, **hay algunos blockchain públicos que pueden limitar el acceso a solo lectura o escritura**.

También están los blockchain privados que limitan su acceso a solo participantes confiables seleccionados, con el objetivo de mantener los detalles ocultos de los usuarios.

~~Es particularmente pertinente entre instituciones gubernamentales y preocupaciones entre hermanos aliados o sus subsidios.~~

Uno de los mayores beneficios del blockchain es que la tecnología de su implementación es **pública**. Cada entidad participante posee y actualiza un registro completo de transacciones y los bloques asociados. La data permanece sin alteraciones, como cualquier cambio se podría ver públicamente. La data en los bloques son encriptados por una llave privada (private key) y por lo tanto no pueda ser interpretar por todos.

Otra ventaja enorme de la tecnología blockchain es que es **descentralizada** en el sentido que:

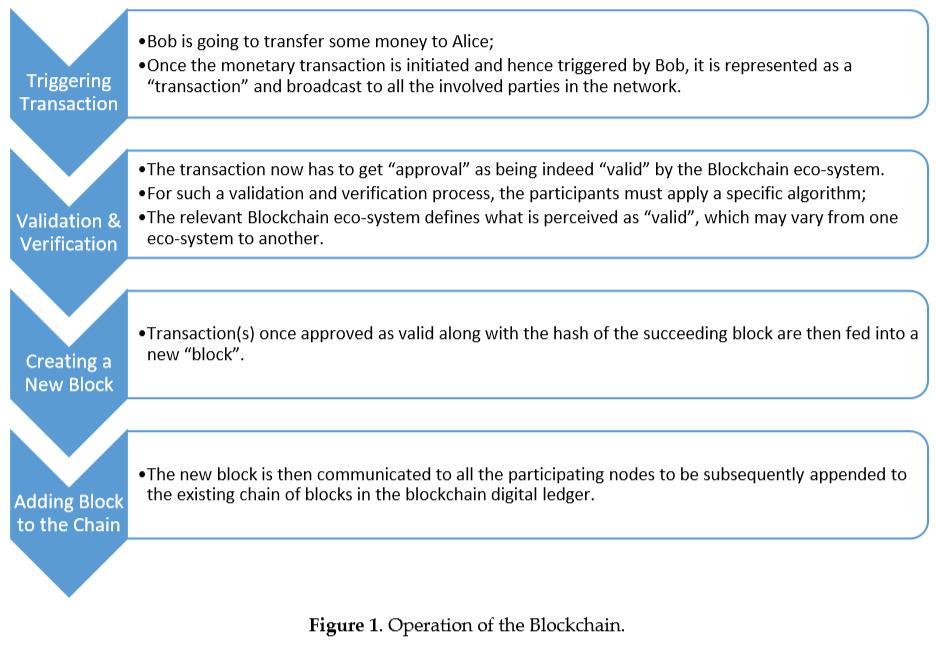
* No hay solo un aparato que registre la data (transacciones y bloques asociados). Ellos están distribuidos entre todos los participantes de la red apoyando el blockchain.
* Las transacciones no están sujetos a aprobación de ninguna autoridad o tener que cumplir un set de reglas específicas, implica una confianza sustancial para llegar a un consenso.
* La seguridad en general del ecosistema de blockchain es otra ventaja. El sistema solo permite que nuevos bloques sean adjuntados. Desde que los bloques anteriores son públicos y distribuidos, ellos pueden ser alterados o revisados.

Para una nueva transacción que pueda ser agregada a la cadena existente, esta debe ser validada por todos los participantes del ecosistema relevante del blockchain. Para tal proceso de validación y verificación, los participantes deben aplicar un algoritmo específico.

El ecosistema relevante del blockchain define que es percibido como **“válido”**, que debe variar entre un ecosistema y otro. **Un numero de transacciones, aprobadas por el proceso de validación y verificación, están empaquetados juntos en un bloque.** El recién preparado bloque es luego comunicado con todos los otros nodos participantes para que sean adjuntados a las cadenas de bloques existentes. Cada bloque sucesivo comprende un hash, una huella digital única, de la anterior.

Ejemplo de una transacción usando blockchain:

* Bob quiere transferirle dinero a Alice.
* Una vez la transacción es iniciada y por lo tanto activada por Bob, esta es representada como una **“transacción”** y emitir a todas las partes envueltas en las redes.
* La transacción ahora tiene que ser “aprobada” siendo de hecho “válido” por el ecosistema blockchain.
* Una vez la transacción o transacciones son aprobadas como validas con el hash de bloque exitoso son alimentados en un nuevo “bloque” y comunicados a todos los nodos participantes para ser adjuntos subsecuentemente a las cadenas de bloques existentes en el libro digital de blockchain.



1. Uso de blockchain más allá de las Criptomonedas.

El internet aún falla en términos de seguridad y privacidad, especialmente cuando viene de FinTech y E-commerce.

* Blockchain, la tecnología detrás de las criptomonedas trajo adelante una nueva revolución proporcionando un mecanismo para transacciones Peer-to-Peer(P2P) sin necesidad de un cuerpo intermediario como bancos comerciales. BC valida todas las transacciones y preserva un registro permanente de ellos mientras se asegura que cualquier información relacionada con la identificación de los usuarios se mantienen en incognito. Toda la información personal de los de los usuarios es retirada mientras justifican todas las transacciones. Esto se logra al conciliar la colaboración masiva mediante la acumulación de todas las transacciones en un libro digital basado en un código de computadora. Aplicando blockchain o técnicas de criptomoneda parecidas, los usuarios no necesitan confiar en el otro ni necesitan un intermediario, la confianza es manifestada dentro de un sistema de redes descentralizadas.

**Blockchain aparece para ser el paradigma de “Máquina de confianza” ideal.**

* En el ambiente de la nube, la historia de creación de cualquier objeto de datos en la nube y sus operaciones subsecuentes realizadas luego son registradas por el mecanismo de estructura de datos de “Procedencia de Datos”, que es un tipo de metadata en la nube. Es muy importante proveer la mayor seguridad a la procedencia de datos para asegurar la privacidad de los datos, forense y responsabilidad. Liang et al expuso un blockchain basado en arquitectura confiable de procedencia de datos en la nube, ‘ProvChain” que es totalmente descentralizada. La adopción de blockchain en un ambiente en la nube puede proveer una fuerte protección contra registros que pueden ser alterados permitiendo una mayor transparencia, así como la responsabilidad adicional de datos. Esto también aumenta la disponibilidad, integridad, privacidad y últimamente el valor de los propios datos de procedencia.
* En el ecosistema de Internet de las Cosas (IoT), la mayoría de las comunicaciones son en la forma de interacciones Máquina a Máquina (M2M). Establecer confianza entre las máquinas participantes es un gran reto que la tecnología IoT aún no cumplido ampliamente. Blockchain puede actuar como catalizador en este sentido, permitiendo una mayor escalabilidad, seguridad, confiabilidad y privacidad. Esto puede ser alcanzado al desplegar teconologia blockchain para realizar seguimiento de billones de aparatos conectados en el ecosistema IoT y usado para activar o coordinar el proceso de transacciones. Aplicando blockchain en el ecosistema de IoT también puede aumentar la confiabilidad haciendo un solo click en un Punto único de fallo (SPF). Los algoritmos criptográficos que se usan para encriptar los bloques de data al igual que las técnicas de hashing podrían proveer mejor seguridad. Esto debería demandar más poder de procesamiento que es de lo que los dispositivos IoT sufren. Investigación es requerida para sobreponerse a estas limitaciones actuales.
* Considera la aplicación de tecnología blockchain a una completa revisión de la economía digital. Asegurando y manteniendo la confianza es ambos la principal e inicial preocupación de la aplicación del blockchain. BC puede también ser usado para reunir información de transacciones de manera cronológica y secuencial, como debería ser visto como un enorme sistema de sellado de tiempo en la red. Por ejemplo, NASDAQ usa su “Linq Blockchain” para grabar sus transacciones de valores privados. Mientras tanto “Depository Trust & Clearing Corporation” (DTCC, USA) esta trabajando con Axoni para implementar servicios de liquidación financiera como asuntos post-comercio e intercambios. Reguladores también son interesantes para las habilidades de habilidad BC para ofrecer seguridad, privacidad y seguimiento en tiempo real de las transacciones.

1. El Futuro de Blockchain

De acuerdo a “Gartner Hype Cycle for Emerging Technologies 2017”, blockchain aún permanece en la región de “Peak of Inflated Expectation” (Pico de expectativa inflada) con previsión de alcanzar la platea entre “5 y 10 años”. Esta tecnología se muestra bajando hacia la región del “Canal de la desilusión”. Debido a la gran adopción del blockchain en el enorme rango de aplicaciones más allá de las criptomonedas, los autores de estos papers están proveyendo un cambio en la clasificación de “entre 5 a 10 años” a “entre 2 y 5 años” para alcanzar maduración. Blockchain posee un gran potencial en empoderamiento de los ciudadanos de los países en desarrollo puede ser ampliamente adoptados por aplicaciones E-Gobernancia para manejo de identidad, transferencia de propiedades de activos de bienes preciosos (oro, plata y diamantes), atención médica y otros usos comerciales, así como en la inclusión financiera. Sin embargo, esto dependerá fuertemente de las decisiones políticas nacionales.

1. Conclusión

En conclusión, la aplicación del concepto y tecnología blockchain ha crecido más allá de la generación de Bitcoin y transacciones. Las propiedades de seguridad, privacidad, traceabilidad, procedencia de datos y el sellado de tiempo inherentes han visto su adopción más allá de sus áreas de aplicación iniciales. El blockchain y sus variantes son ahora usadas para asegurar cualquier tipo de transacción, sean comunicaciones humano a humano o máquina a máquina. Su adopción parece ser seguro especialmente con aparición global del Internet de las Cosas (IoT). Hay aplicaciones descentralizadas alrededor del ya establecido internet global que también es muy atractivo en términos de asegurar la redundancia de datos y, por lo tanto, la supervivencia.

El blockchain ha sido identificado especialmente por ser adecuado en naciones en desarrollo donde aseguran la confianza es de gran preocupación.

2)A Review on the Use of Blockchain for the Internet of things

3) A Blockchain Future to Internet of Things Security: A Position Paper

Abs:

El internet de las cosas (IoT) se encuentra cada vez más en contextos civiles y militares, que van desde “ciudades inteligentes” a “redes inteligentes” a “Internet de las cosas médicas” a “Internet de vehículos” a “Internet de las cosas militares” a “Internet de campo de batalla”. En este paper se presenta soluciones de seguridad IoT publicadas desde Enero del 2016. Se tomaron una cantidad de observaciones, incluyendo la falta de datasets disponibles públicamente que pueden ser usados en las comunidades de investigación y práctica. Dada la naturaleza potencialmente sensible de los conjuntos de datos del tipo IoT, hay una necesidad de desarrollar un standard para mostrar los datasets IoT entre las comunidades de investigación y de práctica y otras partes interesadas relevantes. Luego, se plantea el potencial de la tecnología blockchain para facilitar el intercambio seguro de conjuntos de datos del tipo IoT (por ejemplo, usar blockchain para garantizar la integridad de los conjuntos de datos compartidos) y asegurar los sistemas de IoT, antes de presentar dos enfoques conceptuales basados en blockchain. Concluimos este documento con nueve posibles preguntas de investigación.

1)Intro:

**Technologies have changed the way we live, particularly in our data-driven society.** Esto es debido a los avances en tecnología de semiconductores y comunicación, que permite que multitudes de dispositivos puedan conectarse en una red proveyéndonos maneras de conectar y comunicar entre máquinas y humanos. Esta tendencia también se conoce como Internet of Everything, que comprimido seria “Internet of Things” (IoT), “Internet-of-Medical-Things” (IoMT), “Internet-of-Battlefield-Things” (IoBT), “Internet-of-Vehicles” (IoV) y muchos más. Dada la omnipresencia de cada dispositivo en tu sociedad (ejm: ciudades inteligentes, redes inteligentes y sistemas de cuidado de la salud inteligentes), seguridad y privacidad son dos de las mayores preocupaciones. En 2014 se reportaron más de 750000 dispositivos de consumo fueron comprometidas a distribuir **phishing** y **spam emails.** En las **aplicaciones de data sensible** como **IoMT o IoBT la seguridad de la data, sistemas y dispositivos, como la privacidad de la data y el calculo de datos** es crucial. Tratar con un sistema puede ser resultado de una medida de seguridad que no esta bien pensada. Por ejemplo, en un típico hospital civil o militar, los equipos de información tecnológica (IT) generalmente tienen el control de la red completa incluyendo los dispositivos de punto de salida y los dispositivos IoMT (básicamente, cualquier dispositivo con una dirección IP). No es realista esperar que el equipo IT sea familiar con cada dispositivo individual conectado, a pesar de ello, ellos tienen la capacidad de administrador para instalar parches, acceder a dispositivos y a su data remotamente, entre otras cosas.

**¿Qué pasa si en el medio de una operación medica uno de los dispositivos IoMT administrando medicinas se apaga y reinicia luego de que un parche es aplicado remotamente por el sistema de administración IT?**

Podría resultar un caos en los quirófanos, como el equipo quirúrgico no tendrá idea de que pasa en ese momento a tiempo. Sin mencionar, el trauma o sus potenciales consecuencias al paciente (Ejm: Privar al paciente de oxigeno podría resultar un daño cerebral u otra fatalidad). En otras palabras, las cosas pueden ir “Pear-shaped” muy rápido en una situación aparentemente normal como aplicar parches y los dispositivos reiniciándose a sí mismos.

En este paper se hablarán sobre técnicas de seguridad que fueron diseñadas para o son aplicables para IoT, publicado en ingles en Enero 2016. Aplazaremos la encuesta de técnicas de privacidad de IoT como trabajo futuro. Los siguientes artículos están ordenados en enfoques reactivos y proactivos, y los podríamos categorizarlos en

i)Sistema de detección de intrusiones (IDS)

ii)Sistema de prevención de intrusiones (IPS)

iii)Enfoque de seguridad colaborativa

2)Encuensta de los IoT existentes y enfoques de seguridad relacionados

2.1) Técnicas de detección y prevención de intrusiones

Los diseñadores de malware de la actualidad y los ciber atacantes son innovadores y estan en constante búsqueda de eludir las medidas existentes (Ejm: Generando diferentes versiones de malware usando mutaciones).

La mayoría de los enfoques IDS e IPS están diseñados para detectar intentos de accesos no autorizados y ataques distribuidos de denegación de servicio (DDoS). Por ejemplo, Alsunbul et al, presentado como un sistema de defensa de redes para detectar y prevenir intentos de acceso no autorizados generando dinámicamente un nuevo protocolo para reemplazar el protocolo standard. El objetivo es el confundir los intentos de escaneo. El camino de la red también es cambiado periódicamente para prevenir intentos no autorizados y escaneos de tráfico. La cantidad de paquetes generados puede ser excesiva. En el enfoque de Zitta, Neruda y Vojtech, Raspberry Pi 3 es usado para asegurar frecuencia ultra altas (UHF), identificación de radio frecuencias (RFID), lectores que ejecutan el protocolo lector de bajo nivel (LLRP). Especificamente, **Fail2ban** y **Suricata** fueron seleccionados como la solución debido a sus funcionalidades y alta escalabilidad.

* Fail2ban soporta arquitecturas complejas, por lo que es manejable para desplegar en un ambiente en la nube con múltiples sensores y servidores.
* Suricata provee un mejor performance que Snort y permite procesamiento multithread que requiere el CPU multicore de un Raspberry Pi 3.
* Park y Ahn analizaron y compararon la detección y performance de Snort y Suricata cuando se trata con ataques DoS, y determinaron que Snort tiene un menor consumo de CPU. El multithread que Suricata provee mejor detección de performance entre un core y muchos cores.

Ahora se discutirán recientes detecciones de intrusión y otros sistemas preventivos. Para simplicidad, IDPS es usado para referirse a detección de intrusiones y sistemas de prevención en los siguientes papers

2.1.1) Clasificación por enfoques

La criptografía es un enfoque común y es usado para proveer confidencialidad e integridad de la data, como en el enfoque de las múltiples capas de seguridad reportada.

**Chang** y **Ramachandran** propusieron la solución de seguridad de múltiples capas para computación en la nube.

i)La primera capa de seguridad es el firewall y el acceso de control, diseñado para asegurar que solo usuarios autorizados y autenticados puedan acceder al sistema y a la data.

ii)La segunda capa es la administración de identificación e intrusión preventiva para asegurar a los usuarios identificar que será revisado otra vez y detectar cualquier archivo malicioso será removido.

iii)La tercera capa es cifrado convergente, que provee una póliza de seguridad de arriba hacia abajo.

Para evaluar el enfoque propuesto, los autores conducen un penetration test de 10 PB de datos en data centers. Sus hallazgos indican que el tiempo de recuperación de un intento de acceso no autorizado es un mínimo de 125 horas. **Makkaoui** propuso una red con multiples capas de seguridad y un modelo de privacidad (CSPM), que consiste en 5 capas, llamadas:

* Capa de Seguridad física y ambiental (PESL)
* Capa de Seguridad de la infraestructura en la nube (CISL)
* Capa de seguridad de red (NSL)
* Capa de data (DL)
* Capa de control de acceso y administración de privilegios (ACPML)

**Jin, Tomoishi y Matsuura** proveyeron un método mejorado de red virtual privada (VPN), autenticación usando un sistema de posicionamiento global (GPS). El método propuesto provee protección geo privada en dispositivos móviles. Un cliente VPN envía el valor hash de la información del GPS en lugar de enviar el valor bruto, asi se protege la geoprivacidad del cliente. En vez de proveer las coordenadas GPS, el área se brinda el área para registrar con un servidor de autenticación por cada cliente. Google maps fue usado para revisar la tasa de éxito de las coordenadas GPS del cliente de un área especificada, y la evaluación del autor resulta reportada con un rango de precisión de entre 99.29% y 92.96% para latitud y longitud, respectivamente.

**Olagunju and Samu** diseñaron un honeypot automatizado para la detección de intrusión en tiempo real, previniendo y corrigiendo al usar técnicas de administración centralizada del sistema de registro (también conocido como marionetas o maquinas virtuales). El sistema centralizado recolecta información de una dirección, tiempo y país de los atacantes. El enfoque reduce el esfuerzo manual requerido a modificar dinámicamente el sistema honeypot alto interactivo usando libremente tecnología existente y de código abierto. El protocolo de transferencia es útil atrayendo atacantes que deja rastros o evidencia de username, passwords y puertos fuente de varios países.

**Agrawal y Tapaswi** propusieron un honeypot basado en multiples capas de IDS para detectar y prevenir ataques de puntos de acceso no autorizados. El enfoque combina IDS existentes y honeypots para mejorar la precisión de los IDS existentes y comprende filtraciones, detección de intrusiones y honeypot. El sistema fue implementado en una pequeña red inalámbrica. Desplegando el sistema en la nube y adoptando técnicas de machine learning se puede mejorar el rendimiento general manteniendo un rango bajo de falsas alarmas y una baja sobrecarga del honeypot.

**Merlo, Migliardi y Spadacini** propusieron un mecanismo adaptativo que tiene en cuenta los errores de predicción y el trafico residual. Este modelo es evaluado usando un simulador de red y retrasa donde es calculado. El resultado indica solo un mínimo retraso es introducido, debido al análisis de seguridad. Este modelo carece de un algoritmo de predicción ideal, por lo que produce retraso en los paquetes por una falsa predicción.

**Ingre y Lemnaru** presentan un IPS contra cyber ataques y malware botnet. Proponen diferentes algoritmos de aprendizaje enfocándose en características seleccionadas y etapas de extracción y su evaluación indica un 98% de puntaje de predicción.

**2.1.2) Clasificación por estructuras de red**

**Yevdokymenko** diseño un metodo adaptativo para detectar y prevenir ataques activos en un sistema de telecomunicaciones.

**Abazari, Madani y Gharaee** propusieron un modelo que calcula amenazas basadas en el grafico de ataque ponderado. Específicamente, este es un modelo dinámico y proactivo de respuesta ante amenazas multipropósito diseñado para minimizar las amenazas y los costos. Otros métodos de optimización como algoritmos genéticos pueden ser implementados para responder rápidamente a amenazas óptimamente en el futuro.

**Yacchirena** desarrollo una red Wi-Fi corriendo en el sistema operativo Linux, usando Snort y Kismet como IDS e IPS, respectivamente. Penetration testings fueron conducidos con Backtrack 5 R3 usando Fern Cracker y Ettercap para estudiar la respuesta de los IPS. Integrando las funcionalidades de Snort y Kismet, en teoría, puedes mejorar el performance del sistema aumentando el rango de detección en las capas superiores de Kismet y redes Wi-Fi en Snort.

**2.1.3) Clasificación por aplicaciones**

Muchos estudios han dedicado su investigación a varios dispositivos móviles inteligentes, como Smart phones.

**Vij y Jain** revisaron enfoques IDPS existentes para Smart phones. Ellos determinaron que las redes basadas en IDPS pueden hacer una emulación en tiempo real y facilitar la detección de archivos maliciosos antes de incluso descargarlos, al contrario de los que están basados en host IDPS. Por otro lado, los IDPS basados en host son menos costosos y no requieren mucho hardware dedicado. Normalmente, las redes basadas en IDPS son preferidas sobre las IDPS basadas en hosts.

**Saracino** diseño un detector de anomalías basada en comportamiento de multi niveles para dispositivos Android, diseñado para analizar y correlacionar muchas características en cuatro diferentes niveles de Android (kernel, aplicación, usuario y paquete). El detector propuesto identifica y bloquea amenazas sospechosas al detectar patrones de comportamiento específicos para un conjunto de amenazas de seguridad conocidas, y evalúa el riesgo de seguridad al verificar los metadatos de permiso y reputación solicitados, cada vez que se instala una nueva aplicación.

**Rashid** desarrollo un IPS inteligente para una casa equipada con una computadora con sistema de chip basada en el procesamiento de imágenes y la tecnología de identificación de voz para diferenciar entre huéspedes genuinos e intrusos. Esto abrirá la puerta para caras conocidas y autorizadas. Tanto para personas desconocidas como para aquellas que no están autorizadas, realizará una llamada de voz al propietario de la casa utilizando una aplicación de teléfono inteligente y se conectará con el visitante. Los visitantes pueden entrar a casa si el dueño aprueba el acceso. Si el dueño deniega el acceso al visitante, entonces el dueño también tiene la opción de llamar a la policía directamente.

**2.2) Técnicas de seguridad colaborativa**

La seguridad no puede funcionar de forma aislada, y en los últimos tiempos ha habido interés en el paradigma de la seguridad colaborativa debido a su potencial para detectar y prevenir una gama más amplia de ataques. En esta subsección se discutirá sobre enfoques de seguridad colaborativa.

Un numero de mecanismos de control de acceso multipartidista han sido propuestos en la literatura.

**Zhang, Patwa y Sandhu** propusieron un mecanismo de control de acceso para clientes en la plataforma Amazon Web Services (AWS), lo que facilita compartir información asegurada. Específicamente permite a organizaciones colaborar y comunicarse intercambiando su data segura con otras organizaciones durante un periodo de ciber ataques.

**Indumathi y Sakthivel** propusieron un IDS para MANETs, que usa el esquema de firmas digitales para eliminar colisión entre recibidores y transmisiones de poder limitadas y minimiza el rango de falsas alarmas.

**Sharman, Bhuriya y Singh** propusieron una técnica de encriptación hibrida usando RSA y el algoritmo de firma digital para alcanzar un alto rendimiento y seguridad, y reduce gastos generales en MANETs. El performance de las técnicas propuestas usando el protocolo de routing de asegurar el vector de distancia a pedido ad hoc (SAODV) es evaluado usando la herramienta de simulación de redes NS-2.

2.2.2) Clasificación por estructuras de redes

**Arya, Singh y Singh** estudiaron sobre ataques de agujero de gusano y ataques colaborativos de agujero negro en MANETs, y como detectar estos ataques usando ad-hoc confiables en algoritmos de routing en vector de distancia de demanda (AODV). Los valores confiables son calculados por estos dos escenarios de ataques usando varios parámetros (Ejm: Energía, relación de rendimiento y entrega de paquetes). La evaluación utilizando simulaciones NS-2.

**Saied** propuso esquemas colaborativos por tres diferentes redes, llamadas:

**-Ruteo**

**-Seguridad**

**-Radio en comunicaciones inalámbricas Ad-Hoc**

También discutieron dos soluciones de seguridad para manejar ataques internos. Estos son mecanismos de seguridad por diseño y mecanismos basados en la confianza. Este ultimo es más flexible y eficiente debido a sus procedimientos de seguridad autónomos; sin embargo, requiere entradas adicionales y aspectos de servicio para diseñar un modelo más claro basado en la situación.

**Pan** diseño una red de tipo honeypot basado en SDN para permitir a diferentes partes colaborar dinámicamente y desacoplar puertas de enlace y honeypots. También propusieron un mercado definido por software, HogMap, donde diferentes partes publicarán y suscribirán servicios de inteligencia de amenazas cibernéticas de manera flexible.

**2.2.3) Clasificación por aplicaciones**

**Ganesh and RamaPrasad** propuso un modelo de control de acceso multipartito junto con un sistema de evaluación y especificación de políticas multipartita para redes sociales en línea. También se propone un sistema de sondeo para lograr una resolución de conflictos multipartita eficiente y flexible. Se han estudiado diferentes problemas de seguridad en tres situaciones diferentes: Compartir el perfil de usuario, compartir relaciones y compartir contenido en OSN.