**Etiquetado de tiempo confiable para Blockchain** https://github.com/gperezalba/TFM

## RESUMEN

En este TFM pretendemos desarrollar nuevas metodologías de desarrollo de la tecnología blockchain usando el tiempo como primitiva fundamental. Se pretende desarrollar una solución de etiquetado de tiempo descentralizado y trazable a referencias internacionales (tiempo UTC), que se ejecute en el procesador de forma confiable y segura. Se estudiará como esto permite desarrollar distintas aproximaciones en las pruebas de trabajo con objeto de mejorar la escalabilidad de la tecnología blockchain y su impacto en aplicaciones futuras.

## Conocimientos recomendados:

programación en c/c++, s.o. Linux.

Equipos:

Pc de proposito general + tarjetas Rasp Berry Pi

INDICE

1. Introducción
   1. Motivación del proyecto

Ganancia de popularidad de las criptomonedas

Los últimos años la popularidad se la lleva blockchain también

Actualmente existen varias limitaciones sin resolver de esta tecnología

Problema de escalabilidad (PoW)

Desperdicio de electricidad(PoW)

No descentralización por las minning pools

Etc

* 1. Objetivos

El problema que se pretende atajar es el de la escalabilidad

Blockchain con PoW es un método para ordenar transacciones con cuyo orden todos estén de acuerdo

No se usa el Timestamp ya que los actores (mineros) no son conocidos (no se puede confiar) y no se tiene la certeza de que usen el tiempo real de su reloj, y además, no se tiene la certeza de que los relojes de los mineros estén bien sincronizados.

Si se pudiera solventar lo anterior se podría hacer uso del Timestamp para un PoW más eficiente

Trustzone+Autenticación/Cifrado junto con software de trazabilidad de tiempo

* 1. Materiales y métodos

Trustzone

Autenticación y cifrado de código

R2CGGTTS

Se necesita dispositivo con ARM…RaspberryPi3

* 1. Organización de la memoria

1. Estado de la técnica
   1. Trazabilidad (código d Pascale de Fraigne)

Señal GPS

Satélites en common view

Trazabilidad a lab(k) o UTC

Fichero CGGTTS

* 1. Revisión de tecnologías blockchain

¿Qué es y cómo funciona blockchain?

Funciones hash, cifrado de clave asimétrica…

¿Qué es minar un bloque?

Algoritmos de consenso (PoW, PoS)

Problemas

Problema escalabilidad cuando PoW por los 10 min no reducibles por incremento forks

Mala descentralización por minning pools

Problemas de PoS (reparto de la riqueza desigual, seguiría estando mal descentralizado porque elegirían los que más token tienen)

Latencia de la red

* 1. Trusted Code

1. Desarrollo de un software de análisis de trazabilidad
   1. Integración “bonita” del código de Pascale
2. Desarrollo de software confiable en Zedboard
   1. Ejemplo de referencia
3. Propuesta blockchain basado en tiempo confiable

PoW: orden de paqs en base al trusted timestamp

Se mencionó que pow era un mecanismo para ordenar txs o bloques

El algoritmo dicta que hay que quedarse con la cadena más larga… por tanto sólo se puede decidir en base a la longitud de la cadena. Si se hace uso del timestamp se puede hilar más fino pudiendo reducir tiempo de pow sin que aumenten los forks

PoS: Proof of Traceability (Trabajo future?????????????)

En lugar de que la probabilidad de minar el siguiente bloque dependa de tu riqueza, dependería de lo bien sincronizado con la red que estés.

1. Integración y resultados experimentales
2. Conclusiones
   1. Revisión de objetivos y conclusiones
   2. Valoración personal
   3. Trabajo futuro
3. Bibliografía
4. Apéndices (coste del proyecto, diagrama gant, .…).

## BIBLIO

- Código confiable:

https://software.intel.com/es-es/sgx/details

https://developer.arm.com/technologies/trustzone

https://forums.xilinx.com/t5/Xcell-Daily-Blog-Archived/Secrets-of-the-ARM-TrustZone-in-the-Zynq-All-Programmable-SoC/ba-p/454128

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

- "trusted-timestamp service"

- Trazabilidad de referencias GNSS

- Uso de Trustzone o SGX para el códgo de trazabilidad, etiquetado y/o sincronización (ptp/ntp??)

https://forums.xilinx.com/t5/Xcell-Daily-Blog-Archived/Secrets-of-the-ARM-TrustZone-in-the-Zynq-All-Programmable-SoC/ba-p/454128

https://developer.arm.com/technologies/trustzone

https://software.intel.com/es-es/sgx/details

- Smart contract basado en "trustedtimestmamps software".

# Introducción

## Motivación del Proyecto

En el año 1992, tras una reunión en Sillicon Valley, Timothy C. May publica el manifiesto cripto-anarquista que da origen al movimiento Cyberpunk. Este movimiento social es el origen de una revolución de carácter libertaria cuyo principal objetivo es reducir la intervención del Estado a su mínima expresión. Se consideraba que la protección birndada por el Estado en la relación y acuerdos entre individuos, podía ser brindada de una manera más libertaria y eficiente por la tecnología. Dicho movimiento siembra las premisas de un proyecto que surge años después, el proyecto Bitcoin.

[Manifiesto cripto-anarquista]

El 1 de noviembre de 2008 se publica un artículo/White-paper titulado “Bitcoin: A Peer-to-Peer Electronic Cash System”. El autor (o autores) del artículo/White-paper, que se esconde bajo el alias Satoshi Nakamoto, decide publicarlo en una lista de correo sobre criptografía. Este es uno de los primeros documentos en los que se menciona el término *Blockchain.* Se describe como una tecnología creada con el propósito de llevar a cabo el proyecto de Bitcoin. Blockchain surge de la ingeniosa combinación de distintas técnicas creadas años atrás en el campo de la informática y la criptografía. Apoyándose en los ideales del movimiento Cyberpunk, se describe al Bitcoin como una moneda digital gobernada por unas reglas criptográficas que controlan su gestión y emisión. La tecnología blockchain garantiza el correcto funcionamiento de los aspectos clave de las criptomonedas: la puesta en circulación de la moneda y el mecanismo de gasto que garantiza que una moneda no pueda ser gastada varias veces. Anteriores monedas digitales habían intentado resolver estos dos problemas sin éxito. El proyecto Bitcoin, cuya base tecnológica es blockchain, es la primera criptomoneda capaz de resolverlos de manera totalmente descentralizada.

[Whitepaper bitcoin]

El problema del mecanismo para poner en circulación la moneda digital tiene su origen en el proyecto de Adam Back llamado HashCash. El proyecto tenía como objetivo combatir el correo *spam* haciendo uso de la técnica conocida como prueba de trabajo. La prueba de trabajo consiste en un problema matemático de resolución compleja pero cuya verificación es muy sencilla. El aspecto clave de la prueba de trabajo radica en que la dificultad del problema a resolver se puede ajustar. Es vital para cualquier moneda digital que la emisión de la misma sea predecible y constante en el tiempo. La regulación de la dificultad de la prueba de trabajo es el mecanismo por el cual se consigue ajustar la puesta en circulación. Las redes blockchain que hacen uso de la prueba de trabajo permiten que el usuario que antes resuelva uno de estos problemas cree una determinada cantidad de nuevas monedas. El resto de usuarios de la red procederá a la sencilla verificación de la solución del problema antes de comenzar a buscar la solución a otro de estos problemas.

Para resolver el segundo problema se necesita que los usuarios de la red sean capaces de conocer el último estado consensuado de la blockchain. Gracias a esto, los usuarios de la red serán capaces de determinar sin un usuario de la red es el poseedor de cierta moneda. En otras palabras, los usuarios de la red pueden verificar si un usuario en concreto está realizando un doble gasto de una determinada moneda o no. El trabajo del investigador Nick Szabo sobre la tolerancia a fallos bizantinos se convierte en la pieza clave para que los usuarios de la red lleguen al consenso sobre el último estado global de la blockchain.

[Tema 1 Alberto Toribio Intro a blockchain curso UNIR]

La tecnología blockchain permite a los usuarios de la red tener un registro válido, inalterable y consensuado de todas las transacciones realizadas. Los bloques de la cadena contienen la información relativa a esas transacciones, es por esto que a menudo se denomina a la blockchain como libro contable.

El 3 de enero de 2009 Satoshi Nakamoto crea el primer bloque de la cadena de Bitcoin conocido como bloque génesis. Desde ese momento se han estado creando nuevos bloques de la cadena y nuevos bitcoins ininterrumpidamente. Sin embargo, la popularidad de Bitcoin no ha sido la misma desde entonces. Durante los primeros años sufrió varios altibajos tanto en popularidad como en el precio. No fue hasta finales de 2017 cuando su popularidad y precio comenzaron a incrementarse de manera exponencial. Entre 2009 y 2017 surgen muchas otras criptomonedas y proyectos basados en Bitcoin y blockchain.

El proyecto con mayor repercusión que hizo ver las posibilidades que ofrecía la tecnología blockchain más allá de Bitcoin fue Ethereum. El proyecto Ethereum, bajo el liderazgo de Vitalik Buterin, surge en 2014 con el objetivo de crear una nueva red blockchain. La red Ethereum, además de registrar todas las transacciones de su propia moneda digital (el Ether), registra pequeños programas informáticos llamados Smart Contracts. Los usuarios de la red, además de estar de acuerdo en las transacciones que se realizan en la red, deben estar de acuerdo en los despliegues de los Smart Contracts y de los resultados de la ejecución de los mismos. Con los resultados de la ejecución de los Smart Contracts ocurre exactamente igual que con las transacciones de monedas, si la mayoría de la red está de acuerdo el resultado pasa automáticamente a ser válido.

El nombre de Smart Contract puede llevar a equivocación. Sin embargo, los Smart Contracts no extienden todas las capacidades o características de un contrato convencional. Son programas informáticos que permiten programar una serie de instrucciones máquina propias de su máquina virtual (Ethereum Virtual Machine, EVM) para interaccionar con los datos que residen en memoria. Por lo tanto, la clase de tareas que podrán realizar los Smart Contracts será muy limitada.

Uno de los principales usos de los Smart Contracts es la creación de *tokens*. Un token es una unidad de valor que una organización crea para gobernar su modelo de negocio y dar más poder a sus usuarios para interactuar con sus productos, al tiempo que facilita la distribución y reparto de beneficios entre todos sus accionistas [william mougayar, the business blockchain]. El Smart Contract asociado a un determinado token será el encargado de programar el registro y la interacción que se tenga con el token en cuestión. En definitiva, se tendría un pequeño libro contable creado sobre un gran libro contable (la blockchain) [tema 1 UNIR].

La *tokenización* de activos abre un gran abanico de posibilidades, siendo su mayor práctica las ICOs (Initial Coin Offering). Permite una nueva forma de financiación a nuevas empresas. Consiste en la preventa de su propia moneda digital o token en representación de los servicios que dicha empresa prestará en el futuro. En el 2017 la financiación obtenida por empresas que han realizado esta oferta inicial de moneda supera los 5000 millones de euros [buscar dato real].

Tras toda esta serie de puntos de inflexión que han marcado el avance de la tecnología blockchain, es necesario citar los principales problemas, aún por resolver, entre los cuales se encuentra la principal motivación de este trabajo.

La raíz de la mayoría de problemas está en la prueba de trabajo. La dificultad de los problemas de la prueba de trabajo se ajusta constantemente para hacer que el tiempo que empleará el poder computacional de todos los usuarios de la red en resolver el problema sea constante. Este tiempo tiene que ser suficiente para que la solución al problema hallada por un usuario sea difundida a la mayoría de usuarios y se adquiera el consenso. Este tiempo dependerá de las características de la red blockchain en cuestión. Cada solución a un problema permite que se añada un nuevo bloque a la cadena que contendrá la información relacionada con las transacciones realizadas. Cada bloque tiene un tamaño máximo que dependerá de cada red blockchain. Se tendrá por tanto un tiempo de creación y un tamaño máximo prefijado. Esto se traduce en una tasa máxima de transacciones por segundo (tx/s) para cada blockchain. Notar que la dificultad de la prueba de trabajo se ajusta en base al poder computacional agregado de todos los usuarios para que el tiempo sea constante. Esto significa que no por añadir más poder computacional a la red se incrementará el número de transacciones por segundo. Si un sistema no aumenta su rendimiento cuando se le añaden más recursos al mismo se dice de este que no es escalable. Es por esto que las redes blockchain basadas en prueba de trabajo son ineficientes por diseño. En base a la definición que se tiene, no se podrá conseguir que sea escalable como tal. Sin embargo, se podrán realizar cambios en el protocolo para hacer que sea lo más eficiente posible. Estos cambios en el protocolo que hagan que se consiga la máxima eficiencia posible están aún por descubrir y diseñar.

La falta de escalabilidad da paso a otro de los principales problemas, el desperdicio de energía eléctrica. La reciente popularidad de las criptomonedas y las redes blockchain ha atraído el interés de muchas personas. Cada vez son más los usuarios que suman su poder computacional a la red con el objetivo de resolver los problemas de la prueba de trabajo. Sin embargo, el protocolo define que el tiempo empleado por el poder computacional agregado de todos los usuarios sea aproximadamente el mismo siempre. En otras palabras, si se aumenta el poder computacional de la red, aumentará también la dificultad de la prueba de trabajo. Este aumento de la dificultad se traducirá en un aumento de la energía eléctrica empleada en resolver la prueba de trabajo. El resultado siempre será la creación de un nuevo bloque de la cadena cada cierto intervalo de tiempo, la consecuencia directa que cuánto más poder computacional tenga la red, más energía eléctrica se empleará en el proceso.

Cuando un usuario encuentra solución a la prueba de trabajo, este obtiene la capacidad de crear cierta cantidad de nuevas monedas que se autoasignará. Esto ha provocado la creación de grupos que aúnan todo su poder computacional en un mismo usuario para así aumentar la posibilidad de encontrar la solución a la prueba de trabajo y por ende de recibir estas nuevas monedas creadas que posteriormente repartirán entre todos. Surge así un nuevo problema que atenta contra la descentralización de la red. En redes como la de Bitcoin, casi la totalidad de los nuevos bloques son incluidos a la cadena por tres de estos grupos. Se podría decir que estos tres grupos gobiernan la blockchain de Bitcoin. A esto se le suma que, si uno de estos grupos adquiere al menos el 51% del poder computacional de la red, este podrá incluir las transacciones que desee a su antojo. Esto se conoce como el ataque del 51%.

La gran cantidad de inconvenientes aún por solventar o mejorar motivan este trabajo. En el siguiente apartado se definirá más concretamente el problema que se pretende atajar en el trabajo y los objetivos del mismo.