



Universidad Nacional Autónoma de México

Facultad de Ingeniería

División de Ingeniería Eléctrica

## Blockchain: Contratos Inteligentes (Smart Contracts)

Asignatura: Cómputo Móvil

Grupo: 02

Semestre: 2022-2

Fecha de realización: 18 de febrero del 2022

Profesor: Ing. Marduk Pérez de Lara Domínguez

Por: **García Serrano Héctor Mauricio**

Tarea: #1

## Introducción

Blockchain es un término que ha cobrado bastante popularidad en los últimos años, al ser un tema relativamente joven hay muchas interpretaciones diferentes de qué es y en qué consiste, realmente son pocos los que conocen el término y lo que lo rodea a la perfección. No es para menos que cause revuelo, pues con la llegada de la primera Blockchain de la mano del Bitcoin en el 2009 y los primeros “papers” sobre Bitcoin en 2008, se ha cambiado el paradigma de las transacciones, la seguridad informática, criptografía, economía, etcétera.

Resumiendo, a grandes rasgos, Blockchain es una base de datos descentralizada (distribuida) y pública que registra en bloques de datos información sobre, por ejemplo, transacciones de criptomonedas, etc. Dichos bloques son consecutivos y crecientes, al igual que los eslabones de una cadena están vinculados, cada bloque hace referencia al anterior. Todos los bloques se encuentran fuertemente protegidos contra cambios mediante algoritmos criptográficos.

Desde hace algunos años la tecnología Blockchain ha sido aprovechada para resolver múltiples problemas, el más popular es la descentralización del dinero mediante criptomonedas. Sin embargo, este documento se centra en la implementación de esta tecnología en los contratos comunes que conocemos, como: contratos de compraventa, de prestación de servicios, de suministros, etc. Para ello haré un pasaje rápido sobre lo que es Blockchain y cómo ha evolucionado hasta hoy, como se categoriza, su relevancia en la Ing. En computación, cómo se programan los Smart Contract y como podría llevarse al cómputo móvil.

## Desarrollo

El término Blockchain toma fuerza en 2008 junto a la aparición por primera vez de Bitcoin en el documento técnico de divulgación científica publicado bajo el seudónimo de Satoshi Nakamoto, el documento se llama “Bitcoin: A Peer-To-Peer Electronic Cash System”. Este documento y el nombre del “autor” son una historia legendaria dentro de la computación y seguramente en la historia de la humanidad, dado que es un nombre falso y hasta la fecha no se sabe quién es el autor de ese documento, en pocas palabras, no se sabe quién fue quién inició la primera criptomoneda y la primer blockchain, mismo que actualmente estaría en el top de las personas más ricas del mundo, pues en el momento que redacto este documento, 1 Bitcoin equivale a \$40596,60 dólares americanos, la o las personas que lo crearon en 2009 tienen las primeras criptomonedas y se tiene registro que estas nunca se han movido.

Es curioso que la palabra Blockchain no aparece en dicho documento, pero se plasmaron las bases del funcionamiento de Bitcoin y con ello las de la primera blockchain. Pero una cosa que hay que tener presente es que esta tecnología es la

combinación de muchas otras y en total es el resultado de aproximadamente 40 años de investigaciones en cuanto a redes de datos y criptografía, principalmente y avance computacional.

Hablo del avance de la computación porque en 1990 un científico en computación; Stuart Haber y un físico; W. Scott Stornetta dejaron plasmadas las primeras ideas de una blockchain, pues aplicaron técnicas de criptografía a manera de cadena de bloques para proteger documentos digitales de cambios, eliminación o alguna otra modificación. Este primer trabajo inspiró a otros proyectos predecesores del Bitcoin que no vieron la luz al igual que esta famosa criptomoneda, proyectos como: Digicash, Hashcash, Bitgold, B-Money, entre otros y junto al de Haber y Stornetta no pudieron despegar gracias a limitaciones tecnológicas de sus épocas y algunos otros problemas.

Se puede ver como es que funciona una blockchain analizando la historia de Bitcoin pues con esta criptomoneda se pasó de la teoría a la práctica, una implementación que no cayó como los proyectos ya mencionados, al contrario, está obteniendo un éxito impresionante.

Al primer bloque de una cadena de bloques se le llama bloque génesis. Un bloque almacena muy poca información, pero es información única y sobre una transacción, a continuación, describo un poco de los campos que cada uno almacena:

- Bloque anterior y siguiente: si hablamos de una cadena de bloques debe haber una manera de unirlos, pues estos datos son Hashes, o identificadores únicos de los bloques anterior y siguiente, en el caso del génesis el Hash del anterior es nulo.
- Dificultad: la dificultad matemática del calcular el bloque.
- Recompensa: es la recompensa en Bitcoin de haber minado dicho bloque, esta recompensa va disminuyendo mientras más crece la cadena de bloques. Si hablamos de que es una base de datos distribuida, entonces hablamos de muchos ordenadores con la misma información y cada que se requiere calcular un nuevo bloque muchos ordenadores compiten por realizar el cálculo, al ganador se le da la esta recompensa. Como dato curioso; existe un límite establecido de Bitcoin en el documento de Satoshi Nakamoto, este es de 21 millones.
- Información relevante de la transacción como: fecha y hora, valor, tamaño, peso, versión, número de transacción, etc.

Durante mucho tiempo Bitcoin era irrelevante en el mundo, no fue hasta 2017 que despegó de manera impresionante gracias a muchos factores, pero hasta ese entonces lamentablemente gran parte de la totalidad de usuarios de la criptomoneda eran vendedores del mercado negro online o dentro de la Deep Web para compraventa de artículos y servicios ilícitos. Esto gracias a las bondades de manejar transacciones

descentralizadas por medio de Bitcoin pues no podían ser rastreados. Gracias a esto Bitcoin (BTC) tenía muy mala reputación y es que además de todo eso no era fácil conseguir la moneda, con el paso del tiempo y la entrada de las casas de cambio que facilitaban la adquisición de BTC la criptomoneda se volvía más popular porque también estaba haciendo millonarios a muchas personas que confiaban en ella e invertían en enormes centros de hardware para poder calcular el siguiente bloque de la cadena, todos esos factores la llevaron a su primer pico importante en 2017. Sin embargo, sólo era (y sigue siendo) sostenida por la apuesta de empresas e inversionistas (especulación).

Gracias a que muchos hablaban de ese proyecto surgieron personajes interesantes, el que nos sirve para hablar de contratos inteligentes es Vitalik Buterin; este chico a sus 19 años se interesó en la investigación sobre BTC, en pocas palabras se clavó de manera técnica y no solo para obtener criptomonedas, comenzó publicando artículos y en especial uno de ellos marcó una nueva etapa en las criptomonedas y más concreto en blockchain. Vitalik hablaba de una nueva criptomoneda llamada “Ethereum” que ofrecía más posibilidades que Bitcoin y con ello comenzó a tener gente interesada en el proyecto quienes en conjunto le dieron forma. Claro que un proyecto necesita financiación, por lo que Vitalik hizo la primera ICO sobre Bitcoin de toda la historia, básicamente ofrecía Ether a cambio de BTC y claro que hasta ese momento Ether (que es el nombre de la criptomoneda de Ethereum) no existía, era una promesa para cuando terminara el desarrollo, con esa convocatoria recaudaron suficiente para poder lanzar el concepto en 2013 y fue hasta el 2015 que se calcula el primer bloque, el bloque génesis de Ethereum.

¿Y cuál es la relevancia de Ethereum en esta historia?, que con ella comenzó la era de las aplicaciones blockchain o descentralizadas. Ethereum puso sobre la mesa los contratos inteligentes (Smart Contract) y con ellos la creación de ICOs de manera muy sencilla, ya hablamos un poco de lo que es un ICO, básicamente una préstamo o promesa de pago, pues desde ese momento comenzaron a surgir muchos proyectos de criptomonedas que buscaban financiación como lo hizo Vitalik desde ese entonces hasta ahora han surgido miles de nuevas criptomonedas y un enorme campo de especulación.

Ethereum a diferencia de Bitcoin propone transacciones más allá como transacciones de acciones, archivos digitales, terrenos, productos reales y demás, con ello permite aplicar varios casos de uso descentralizado dentro de la misma plataforma blockchain, se le conoce como blockchain pública, lo anterior comenzó a impactar sobre áreas como el comercio electrónico, energía, gobierno, entre otras diferentes a las que ya se había impactado con Bitcoin (financiera, bancaria, etc.).

La forma en que es posible la ejecución de aplicaciones de blockchain, formalmente llamadas DApps, que no solo sean transacciones es mediante la Ethereum Virtual

Machine (EVM), muy similar al concepto de la Java Virtual Machine (JVM), es la base para ejecutar Smart Contract en Ethereum. El lenguaje por excelencia para Ethereum se llama Solidity, este es un lenguaje de programación similar en sintaxis a JavaScript y que se considera “Turing Complete”, por lo que cualquier lenguaje de Turing es capaz de crear Smart Contract, que por ahora veamos como un script de programación capaz de fungir como intermediario en un contrato de cualquier índole ejecutándose de manera automática en caso de ocurrir un evento. Todos los scripts de Ethereum (DApps) se ejecutan de manera distribuida en la EVM como sistemas P2P de manera efectiva, claro que el desarrollar una DApp y subirla a la red Ethereum no es gratis, dado que muchísimos nodos (mineros) son los encargados de mantener viva la red se cobra un “precio de gas” debido al gasto de procesamiento por parte de los mineros, gracias a esto Ethereum es autosustentable y puede sostenerse ofreciendo estos servicios.

Ahora que ya entendimos la cadena de bloques, muy por encima, pero lo suficiente, entremos en materia de ¿qué es un Contrato Inteligente o Smart Contract?, Muchos dicen que no es un contrato y tampoco es inteligente y esto es porque se trata de un Script informático que puede ejecutarse de manera autónoma y automática de acuerdo con parámetros programados y al estar en una blockchain lo realiza de manera transparente, inmutable y segura. Pero entonces, ¿de dónde surge el nombre de “Contract” ?, esto es porque su objetivo principal es llevar a cabo un acuerdo entre dos o más partes interesadas sin la necesidad de intermediarios como pudiesen ser abogados, notarios, etc., por ello decíamos que son autónomos, porque no dependen de una autoridad que lo haga cumplir. Otro aspecto implícito en el anterior es el ahorro de mucho dinero en la elaboración de contratos escritos, ahorra tiempo, permite la negociación entre partes de distintos países y evita malas interpretaciones.

El término de contrato inteligente surgió en la década de los 90 con un criptógrafo llamado Nick Szabo quién realizó publicaciones detalladas de los Smart Contract, lamentablemente fue muy adelantado a su época pues no existían los medios para llevarlo a cabo.

Estos contratos inteligentes contienen la declaración de las características a cumplir de un contrato o reglas del juego, pasan a digital lo que sería un contrato como se conocía hasta ahora, con todo lo que se debe cumplir para otorgar un bien remunerado a manera de criptomonedas o validar algo. El motivo por el que aún no han sustituido completamente la forma tradicional de hacerlos es porque existe ignorancia e incertidumbre sobre estos, al igual que sucedía con las criptomonedas en sus inicios, y es que al no haber autoridad intermediaria la responsabilidad recae en el desarrollador del script puesto que se debe prestar mucha atención en la etapa del desarrollo de los contratos al no ser modificables una vez sean parte de la cadena de bloques. De hecho, el único problema que puede surgir en un contrato sería problema del diseño de este y/o del desarrollador, error de programación.

Los Smart Contract pueden ser utilizados por personas, pero también por otros programas para validar y llevar a cabo procesos de hecho, en las criptomonedas hay contratos inteligentes implícitos, pero no era posible desarrollarlos para fines distintos (porque en Bitcoin ya se podía, un ejemplo son los ICOs) hasta la llegada de Ethereum.

Otras características de los Smart Contract nos las menciona Rojo:

- *Públicos: Ya que se almacenan en la Blockchain y cualquiera puede acceder a la misma.*
- *Inmutables: Están almacenados en la Blockchain por lo que no se pueden cambiar.*
- *Configurables: Una vez subes el contrato a la Blockchain, únicamente su dueño (...) puede cambiar ciertas variables.*
- *Comunicativos: Los Smart Contract se pueden invocar entre ellos.*
- *Distribuido: Son los mineros quienes los ejecutan por lo que su procesamiento puede ser realizado por cualquiera, esto elimina cualquier intento de censura o burocracia ya que no se puede controlar quien lo ejecuta, a qué país pertenece y qué leyes se aplican allí. (...). (Rojo, 2009, p.106)*

En su inicio, los Smart Contract presentaban un problema, cómo iba a saber el programa cuando se cumplían ciertas condiciones que se relacionaban con información externa a la Blockchain, fue a mediados de 2019 cuando aparece Chainlink, la primera red de oráculos descentralizada que venía a resolver el problema ayudando a los contratos inteligentes a obtener información de bancos de datos externos; como valores de divisas, precios de productos, resultados de partidos, clima, o sea, APIs. Las posibilidades se ampliaron mucho y con ello llegó el concepto de Oráculos, los oráculos son software que obtiene información casi de cualquier lado y la traduce en idioma que el Smart Contract entienda y pueda accionar o decidir.

La llegada de los oráculos trajo excelentes noticias, pero surgió un problema de filosofía, esto centraliza las aplicaciones pues aparece un *tercero*, dependen del oráculo además de depositar la confianza en este software mismo que puede ser corrompido por los dueños de este, hackeado o simplemente que el servicio presente una falla. Nuevamente, gracias a la popularidad de los contratos inteligentes, rápidamente aparecieron proyectos como Orisi y Oraclize que consultan a muchos oráculos la información, la combina y por mayoría decide, lo cual descentraliza un poco.

Actualmente Ethereum no es la única blockchain donde funcionan las DApps y los Smart Contract, también tienen soporte y hay aplicaciones funcionando en EOS, Tron, Solana, Neo, Avalanche, Binance Smart Chain, Bitcoin, entre otros. El tema es completamente joven y va en evolución, muchas empresas famosas y proyectos nuevos van saliendo en busca de seguir desarrollando esta tecnología, gracias al interés y la popularidad siguen apareciendo nuevas aplicaciones de estos contratos, como mencioné antes, nos

encontramos en una etapa donde esto no lo vemos tan a la mano, pero se está trabajando bastante en ella. Un problema que surge es la falta de atención o velocidad de resolución en cuanto al tema legal, son contados los países donde se ha puesto el tema en la mesa y en general sobre las criptomonedas para regular, prohibir o permitir. Específicamente sobre los Smart Contract, se encuentran en un área gris legalmente hablando, puede ser legal pero quizá no es correcto. Otro debate actual y muy común sobre Blockchain en general; es su exagerado gasto energético, pues es bien sabido que los cientos de miles o incluso millones de nodos requieren mucha energía eléctrica para el procesamiento del cálculo de los bloques, además de que las famosas granjas de minería generan calor.

¿Esta tecnología es relevante para la ingeniería en computación?, claro que lo es, muchas empresas están apostando por el desarrollo de estos scripts o contratos inteligentes, por lo que se requieren programadores especialistas en algoritmos, Solidity, redes de datos, desarrollo de Backend, de microservicios, incluso con conocimientos de economía, finanzas y derecho. Blockchain gira alrededor de la criptografía, las redes de datos descentralizadas, del hardware de alto rendimiento, etcétera. Se trata de un tema que a nosotros como ingenieros en computación nos incumbe, el interés dependerá de cada persona, pero se están abriendo un panorama de posibilidades y nosotros tenemos las herramientas técnicas para poder con ello.

Viendo como pueden ser relevantes los Smart Contract, desde el punto de vista del cómputo móvil, es un panorama muy amplio. Si estos nos permiten negociar y realizar transacciones con otras personas y/o empresas de manera libre abre muchas puertas principalmente desde el e-commerce para PyMES las transacciones se verían más al alcance de todos mediante el celular, el dinero podría fluir más rápido incluso entre países, podría una persona contratar proveedores para importación y exportación mediante aplicaciones destinadas a este comercio ahorrando muchísimo dinero. Y no estoy contando las aplicaciones ya existentes como juegos que manejan compras en la aplicación mediante criptomonedas, aplicaciones para compraventa de NFTs y demás que al manejar criptos llevan Smart Contract implícitos.

Una hipótesis de aplicación podría ser una para las elecciones de nuestro país. Leí de algunos casos de Bit2Me en donde se puede aplicar esto a las votaciones democráticas de un país donde los votantes únicamente seleccionarían el Smart Contract de un político que más les convenció y que este previamente desarrolló un contrato inteligente plasmando como se van a repartir recursos, así desde el celular la gente podría votar sin tener que ir hasta una casilla en su entidad, formarse, llenar las boletas, manchar su dedo, etcétera. Ahorraría tener que capacitar a funcionarios de casilla, papel para las boletas, tinta, pagos a representantes de partido y una infinidad de gastos llevando todo a una simple App donde el votante entre, visualice las propuestas de sus políticos y solo presione un botón con la mejor opción que decida elegir. Los beneficios de manejar esto sobre una blockchain ahorrarían un gasto que, al menos en México, es



gigantesco, además de que los votantes pueden estar seguros de que su voto sigue siendo libre y secreto, los partidos estarán tranquilos al saber que no hay posibilidad de fraude al no ser contados los votos por humanos, además de que cada votante podría entrar con la cuenta asociada a su monedero de criptomonedas lo cuál haría más seguro el voto pues no sería fácil crear “bots” para inclinar los votos hacia cierto candidato y/o partido.

## Conclusiones

Se me ocurren más aplicaciones como algunas con plantillas para poder realizar contratos inteligentes desde el teléfono solo seleccionando las reglas a seguir en el contrato y que por detrás se genere el contrato tomando la selección de las partes. En fin, es un abanico de posibilidades las que esta tecnología nos arroja.

Como mencionaba, se encuentra en una etapa joven con un futuro muy alentador por delante, claro, sin dejar pasar y estudiar el impacto sobre el medio ambiente que tienen las Blockchain y las regulaciones sobre estas, pues lamentablemente se está avanzando mucho en nuevas tecnologías, pero nuestras leyes van muy lentas y eso puede provocar grandes conflictos a mediano plazo, como ya se ha visto en otras.




En lo personal, me sentía bastante abrumado por el bombardeo que se vive actualmente de información, que más bien es des información sobre las criptomonedas, pues se me hacía bastante interesante, pero me daba pereza adentrarme en un mundo donde parece que todos saben mucho. En realidad, después de esta investigación me di cuenta de que hace falta mucha enseñanza sobre esto, desde nuestra facultad hasta al público en general que muchas veces invierte en bruto en las blockchain gracias a la recompensa inmediata, pero es un mundo que hay que entender para poder adentrarse en él.

Después de la investigación me he quedado con ganas de saber más e incluso quizá tener un acercamiento profesional con el desarrollo en Solidity sobre Blockchain, no me cierro a nada pues es la tecnología de moda y no solo eso, suena bastante bien el posible futuro.

## Referencias

- Singhal, B., Dhameja, G., & Panda, P. S. (2018). Beginning blockchain: a beginner's guide to building blockchain solutions. Apress.
- Rojo, M. I. (2019). Blockchain: fundamentos de la cadena de bloques (Primera edición). Ediciones de la U.
- Biscontini, T. (2020). Blockchain (technology). Salem Press Encyclopedia of Science.
- Bit2Me Academy. (2022, 4 febrero). Smart Contracts: ¿Qué son, cómo funcionan y qué aportan? Recuperado 17 de febrero de 2022, de <https://academy.bit2me.com/que-son-los-smart-contracts/>



- Binance Academy. (2020, 16 noviembre). Blockchain. Recuperado 17 de febrero de 2022, de <https://academy.binance.com/en/glossary/blockchain>
- BBVA Communications. (2017, 4 diciembre). De Alan Turing al ‘ciberpunk’: la historia de «blockchain». BBVA NOTICIAS. Recuperado 17 de febrero de 2022, de <https://www.bbva.com/es/historia-origen-blockchain-bitcoin/>
- Blockchain School for Management. (2021, 13 diciembre). Lenguajes de programación para aplicaciones blockchain. Formación en Blockchain Management y Engineering. Masters Big Data Business Intelligence y Data Science. Recuperado 19 de febrero de 2022, de <https://www.bsmexecutive.com/lenguajes-de-programacion-para-aplicaciones-blockchain/>
- Google. (s. f.). Bitcoin (BTC) Price, Real-time Quote & News. Google Finance. Recuperado 18 de febrero de 2022, de <https://www.google.com/finance/quote/BTC-MXN?sa=X&ved=2ahUKEwi5-emCwIj2AhVEJEQIHWSSCpEQ-fUHegQIDhAS>
- Inversor Global [Inversor Global TV]. (2021, 12 agosto).  Que son los CONTRATOS INTELIGENTES - Cripto en tu idioma #32 [Vídeo]. YouTube. <https://www.youtube.com/watch?v=oliv7vZfx50>
- Mi Camino Financiero. (2021, 13 junio).  Que es un CONTRATO INTELIGENTE en criptomonedas  smart contracts blockchain en español [Vídeo]. YouTube. <https://www.youtube.com/watch?v=IPaeOB1A1No>
- EL TIEMPO Casa Editorial [EL TIEMPO]. (2021, 12 octubre). ¿Qué son? Y ¿para qué sirven los contratos inteligentes Blockchain? | #ConsultorioJurídico [Vídeo]. YouTube. <https://www.youtube.com/watch?v=oDNl9QbhFb0&t=420s>