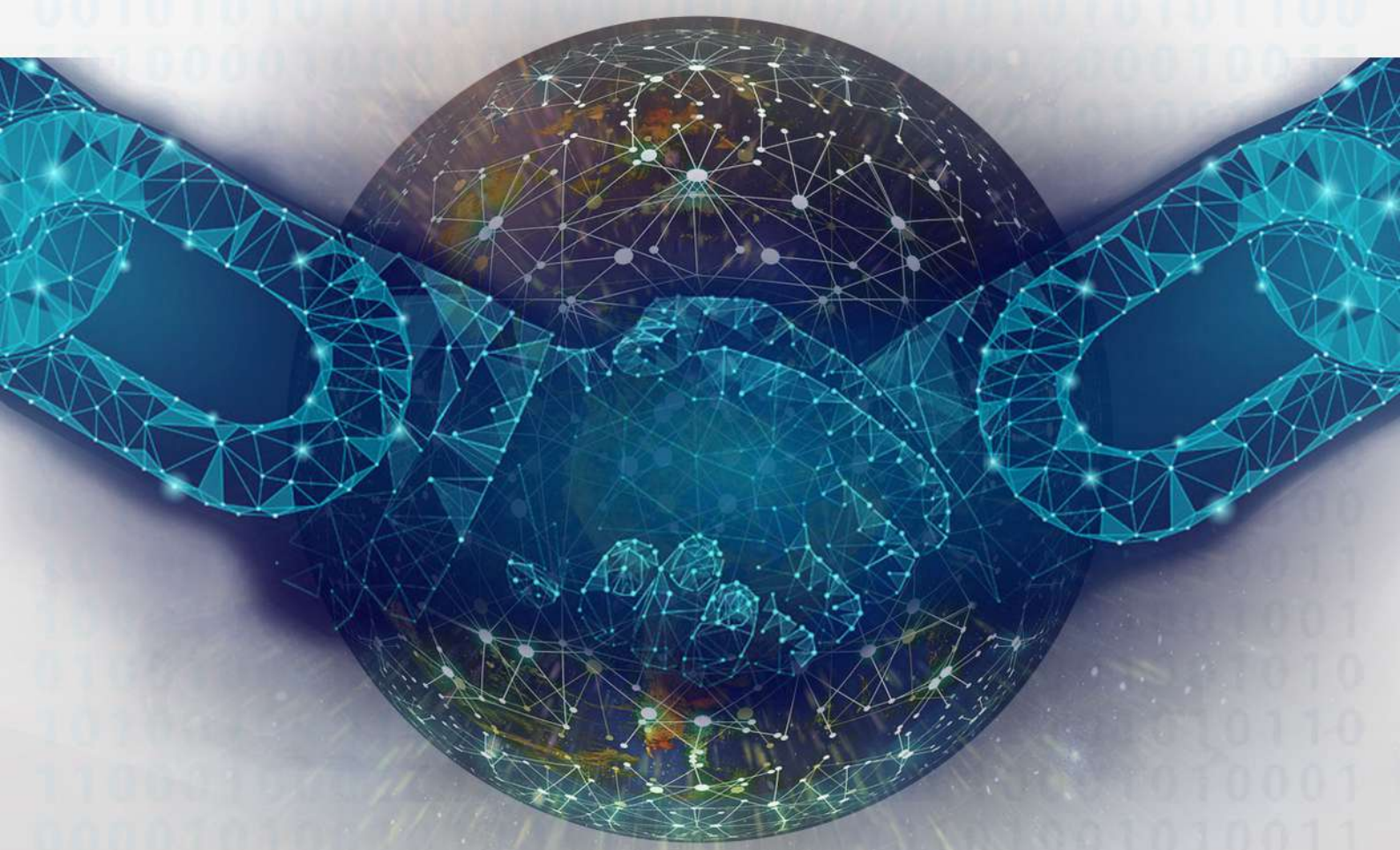


DEMOCRACIA TECNOLÓGICA.

Jersain Zadamig Llamas Covarrubias

Irving Norehem Llamas Covarrubias

DEMOCRACIA TECNOLÓGICA

Jersain Zadamig Llamas Covarrubias.

Irving Norehem Llamas Covarrubias.

NOTA PRELIMINAR **4**

CAPÍTULO I. De la democracia **5**

Formas de democracia 9

Democracia directa 9

Democracia representativa 12

Democracia semidirecta 14

Democracia liquida 16

La era de la información y la comunicación 19

Cambios disruptivos en la sociedad democrática 21

Las 3G: Gobierno, Gobernabilidad y Gobernanza 24

El protocolo de Dios 28

CAPÍTULO II. De las relaciones e interacciones democráticas **31**

Identidad digital 31

P2P: Persona a Persona 34

P2M: Persona a Máquina 34

M2M: Máquina a Máquina 35

Bots sociales 36

Procesos 39

Voto electrónico 39

Tipos de votos 40

Proceso de convergencia 42

C.E.R.E.B.R.O. 42

Datos 44

Información 45

Redes sociales electorales 46

Noticias falsas (fake news) 50

Dataismo 53

Modelo CIA 54

Big data 55

Caso cambridge analytica 56

Objetos 59

Internet de las cosas (IoT) 59

Transhumanismo y posthumanismo 62

Cyborg político-electoral 65

Inteligencia artificial 68

Caso Sophia 70

Caso Michihito Matsuda 73

Quinto poder tecnológico 75

CAPÍTULO III. Blockchain **78**
Términos Preliminares 79
Antecedentes del Bitcoin 82
Blockchain desconectada 84
Visión general 92
Mecanismos de consenso 102
Proof of work 102
Mineros 103
Solo Mining 105
Pool Mining 105
Proof of stake 105
Chain-based 107
Byzantine Fault Tolerance style (BFT-style) 107
Ataque del 51% 108
Tipos de clientes 109
Full client 110
Lightweight client 110
Clientes web 110
Clientes de escritorio 110
Clientes móviles 111
Tipos de wallets 111
Creación 111
Aleatorias o no deterministas 111
Deterministas o con semilla 111
Determinista jerarquica o HD 112
Semillas y mnemónicos (BIP-39) 113
Almacenamiento 113
Hot wallets 114
Exchanges 114
Escritorio 115
Cold wallets 115
Wallets fisicas 115
En papel 115
En el cerebro 115
Multi firma 116
Forks 116
Soft fork 116
Hard fork 117

Tipos de blockchain 118
Públicas 119
Sin permiso 119
Con permiso 119
Privadas 120
Sin permiso 120
Con permiso 120
Híbridas 120
Side chains 120
Smart Contracts 122
DAO’s 123
Aplicaciones Descentralizadas o DApps 124
Halving 125
Democracia con Blockchain 127
Referencias 129

NOTA PRELIMINAR

Antes de comenzar con la lectura de esta obra, es oportuno mencionar al lector que dicha publicación tiene la finalidad de explicar de manera general, los cambios en la sociedad y la democracia por medio de la tecnología, ya que se abordarán diversos temas actuales que han causado controversias, así como posibles escenarios futuros. En relación a la palabra democracia, es menester señalar que este concepto ha sido y será debatido durante mucho tiempo, es así como se abordará de manera muy genérica aplicada a la vida cotidiana, dejando fuera todo concepto abstracto y siendo conscientes que podrán existir otros encuadres epistemológicos y antítesis al respecto, pero que la idea principal no es mirar al pasado, en cambio si al futuro; a la construcción de una democracia tecnológica.

Las palabras democracia y tecnología son parte del lenguaje común en la vida cotidiana, pues reflejan situaciones de la vida pública y forma de gobernar, por lo que se pretendió transformar conceptos muy complejos, incluso hasta abstractos a un lenguaje muy sencillo y llano, por medio de ejemplos y diagramas, esto con el fin de que sea una herramienta para la sociedad en su día a día, inclusive para concientizar ante los nuevos cambios disruptivos que nos prepara el futuro.

Por último, se hablará mucho de la obra publicada por esta editorial en el año 2018, titulada "Internet ¿Arma o Herramienta?", donde tenemos el honor de ser autores de la misma, la cual puede ser consultada desde los siguientes hipervínculos: http://www.publicaciones.cucsh.udg.mx/kiosko/2018/internet_arma_o_herramienta_Ebook.pdf o de http://www.bit.ly/InternetEbook. Esto con el fin de dar continuidad a lo investigado, propuesto y no abordar los temas de la democracia con la tecnología de una manera aislada, pues dicha obra está enfocada en la ciberseguridad y los ciberderechos, pilar fundamental en la integridad, confidencialidad y disponibilidad de la información, herramienta que ha servido para para crear bases de confianza en la tecnología y por ende en las instituciones democráticas.

CAPÍTULO I. De la democracia

Durante cientos de años el tema de la democracia siempre ha sido discutido de forma interminable, tomando diferentes encuadres epistemológicos sin poder llegar a una teoría ecléctica. La única realidad, es que todas las personas tienen ciertos acuerdos respecto a este concepto, relacionándola con otras palabras, por ejemplo con pueblo, libertad, soberanía y autodeterminación.

No debe entenderse sólo a lo que marque la ley, pues debe tomarse en cuenta toda la doctrina que esta palabra conlleva, ya que a pesar de que en el mundo del derecho existen dos componentes en las normas que son las reglas y los principios, en estos dos tipos de normas se aplican dos procedimientos diferentes, a saber, en las reglas la subsunción y en los principios la ponderación. (Alexy, 1997). La democracia no debe entenderse como una regla que es una locución sentenciadora que solo cabe el cumplirse o no cumplirse, ni de un principio abstracto que debe cumplirse de la manera más óptima. Es así, como no debe observarse solo lo que la ley marque, ésto sin promover el arbitrio o el desacato de ésta misma, al contrario, pues debe observarse como un estilo de vida y respeto a las libertades e instituciones desde la costumbre y la lucha por los derechos, en una generalidad y abstracción que sea resultado de legitimidad y eficacia de un buen funcionamiento de la sociedad.

Definir la democracia es algo complejo, etimológicamente viene del griego antiguo y acuñado en Atenas, significa *dḗmos* que es pueblo y *kratía* que es poder, es decir el poder del pueblo. Una definición sencilla es la que dicta la Real Academia Española, expresando que la democracia es la «forma de gobierno en la que el poder político es ejercido por los ciudadanos». Por otra parte el diccionario Oxford la define como el «sistema político que defiende la soberanía del pueblo y el derecho del pueblo a elegir y controlar a sus gobernantes».

La democracia desde siempre ha indicado una entidad política, una forma de Estado y de gobierno; y ésa sigue siendo la acepción primaria del término. En una manera literal o

etimológica, teniendo el concepto de poder popular, «las democracias deben ser lo que dice la palabra: sistemas y regímenes políticas donde el pueblo es el que manda» (Sartori, 2012)

Existen otros conceptos más contemporáneos, por ejemplo, para Ferrajoli (2011), un exponente de la famosa democracia constitucional, dice que es «la institución política cuyo estatuto es una constitución democrática...es cualquier democracia dotada de constitución».

Por otra parte Dahl (1999), menciona como criterios de un gobierno democrático: «la participación efectiva, igualdad de voto, comprensión ilustrada, control de la agenda, inclusión de los adultos», es decir, que exista una comunicación política entre los miembros, donde todos los votos se cuentan como iguales, así como una instrucción sobre las políticas y sus consecuencias. Los miembros deben tener la oportunidad de participar en la agenda y por supuesto los adultos deben gozar de los derechos de ciudadanía.

A *prima facie* cuando se habla de democracia, el primer pensamiento que se puede asociar es el de unas elecciones, pues de una manera tradicional las figuras de democracia y participación ciudadana, son fáciles de asociar con las prerrogativas de los ciudadanos de votar y ser votados, materializandose en su raíz etimológica que el poder es del pueblo, esto bajo un sistema electoral establecido y un sistema de partidos. Sin embargo, en la actualidad eso solo es una pequeña parte de una democracia, ya que se ha convertido en una forma de gobierno, incluso en una forma de vida del día a día, pues no es nada raro que los derechos civiles y políticos fueron los primeros derechos o conocidos como aquellos de primera generación, ya que estos llevan el rumbo del país.

No es ajeno tener en consideración, que también se tiene que escuchar a las minorías en la toma decisiones pues son importantes en la lucha de poder, sin embargo la decisión colectiva o mejor dicho la unanimidad no existen ni en la naturaleza, pues realmente quien gobierna para todos no gobierna para nadie, siempre habrá diferencias y habrá que tomar las mejores decisiones de la

mayoría, o mejor llamada para entender la democracia y la tecnología *Blockchain*, la famosa palabra llamada “consenso” visto desde un sentido amplio.

Durante la presente investigación se utilizará en reiteradas ocasiones la palabra "consenso", pues realmente es un elemento esencial del funcionamiento de la red *Blockchain*, ya que por medio de este se logra la validez de las transacciones, asegurando la integridad y copias de la información, razón por lo cual tendremos que parar un momento en explicar el consenso visto desde una óptica democrática. A la vez también hay que considerar los conceptos de “centralizado”, “descentralizado” y “distribuido” que se abordará en su momento desde una óptica más técnica, pues la propia naturaleza de *Blockchain* apunta a ser un instrumento totalmente democrático.

Ahora bien, separamos los conceptos de mayoría, consenso, centralizado, descentralizado y distribuido. En cuestión democrática en una primera acepción debemos entender el consenso como un principio de mayoría, donde existan pluralidad de ideas y personas, que a pesar de que por naturaleza no se puede llegar a la unanimidad, las decisiones deben tomarse con el máximo consenso posible, es decir con la decisión de la mayoría. De manera puntual, esto es una democracia mayoritaria, también conocida como «modelo Westminster» (Lijphart, 2000), de manera analógica podríamos decir que es un sistema “distribuido”.

En una segunda acepción más estricta, existe un modelo de democracia de consenso el cual no podría ser similar al consenso en *Blockchain* que sí es mayoritario. Este modelo es en sociedades heterogéneas, con diferencias muy marcadas, por ejemplo religión, lenguaje o cultura, es decir «se trata de optimizar la amplitud de la mayoría gobernante obteniendo acuerdos con los sectores minoritarios» (Zipper, 1995), un ejemplo es que el «ejecutivo debe contar con representantes de los grupos lingüísticos más numerosos»(Lijphart, 2000). Esto nace con el fin de prevenir la preponderancia de un grupo específico en el poder, a esta democracia llamada de consenso, también de manera analógica podríamos decir que es un sistema “descentralizado”.

Brevemente, para no perder el hilo de las ideas, a lo que respecta a una *Blockchain* pública, el consenso descentralizado significa que todos los cambios requieren la aceptación de la mayoría. El consenso se llega por medio de algoritmos, en este caso solo mencionaré dos, el primero por las pruebas de trabajo, también conocido en inglés como *Proof of Work*, donde de todos se hace la operación matemática por los mineros en igualdad de circunstancias. Por otra parte se encuentra el algoritmo por pruebas de participación, en ingles *Proof of stake*, donde tienen más votos quienes poseen más reputación por participación en la red (por la cantidad de *tokens* que demuestren poseer), todo esto se abordará a detalle más adelante.

A continuación se muestra un gráfico de sistemas centralizados, descentralizados y distribuidos:

Imagen realizada por Rautopia [CC BY-SA 4.0 (https://creativecommons.org/licenses/by-sa/4.0)]

Para concluir, se podría hablar de Roma y Grecia, de manera más contemporánea de los Estados Unidos de América, de las caídas de los imperios y de las luchas por los derechos de primera generación, o mejor llamados civiles y políticos, no obstante eso sería una gran tarea que afortunadamente cumplen los antropólogos e historiadores, que son la memoria del Estado con la tarea de recabar todo lo acontecido, con el fin de que no volvamos a repetir los mismos errores.

Por todo lo anterior, dicha obra tiene el objeto de abordar brevemente la democracia y sus formas, pero incluyendo un gran contenido de los nuevos paradigmas y tecnologías disruptivas actuales como el *Blockchain*, *Big Data* e Inteligencia Artificial, que serán las herramientas principales que marcarán el rumbo de los países y el mundo.

Formas de democracia

Hablar de los tipos de democracia es algo teóricamente rápido, pues existe una gran cantidad de autores que hacen referencia a clasificaciones basándose desde aspectos de representación, hasta cuestiones económicas o políticas. Dicho tema da lugar para crear colecciones muy robustas en las bibliotecas, pudiendo hablar por ejemplo de democracia constitucional, formal, material, base, política, social, participativa, deliberativa, económica, interactiva, liberal, parlamentaria, religiosa, soberana. Por lo que a lo que este estudio no pretende abarcar en su totalidad las formas de democracia, sino dar un parteaguas a la democracia y las tecnologías de la Información y Comunicación (TIC's), razón por lo cual solo se abordarán las principales: directa, representativa, semidirecta y líquida.

Democracia directa

La democracia directa, o democracia radical o pura, es una forma donde no existen representantes y el poder es ejercido directamente por el pueblo, esto materialmente en una asamblea donde todos asisten, como antecedente está grecia y se prevé que sólo puede llevarse a cabo en comunidades donde existen pocos habitantes, por el problema de tiempo y reunión en un mismo lugar. Debe quedar muy claro que esta democracia no admite representantes, pues los habitantes pueden tomar las decisiones en colectividad.

Rousseau (1762), al respecto dice:

> La soberanía no puede ser representada por la misma razón de ser inalienable; consiste esencialmente en la voluntad general y la voluntad no se representa: es una o es otra. Los diputados del pueblo, pues, no son ni pueden ser sus representantes, son únicamente sus comisarios y no pueden resolver nada definitivamente. Toda ley que el pueblo en persona no ratifica, es nula. El pueblo inglés piensa que es libre y se engaña: lo es solamente durante la elección de los miembros del Parlamento: tan pronto como éstos son elegidos, vuelve a ser esclavo, no es nada. El uso que hace de su libertad en los cortos momentos que la disfruta es tal, que bien merece perderla.

Concluye Rousseau que no ha existido ni existirá jamás una verdadera democracia, pues enumera unos principios que debería de reunir para presunto gobierno como:

- Primeramente, un Estado muy pequeño, en donde se pueda reunir el pueblo y en donde cada ciudadano pueda sin dificultad conocer a los demás.
- En segundo lugar, una gran sencillez de costumbres que prevenga o resuelva con anticipación la multitud de negocios y de deliberaciones espinosas;
- Luego mucha igualdad en los rangos y en las fortunas, sin lo cual la igualdad de derechos y de autoridad no podría subsistir mucho tiempo; y
- Por último, poco o ningún lujo, pues éste, hijo de las riquezas, corrompe tanto al rico como al pobre, al uno por la posesión y al otro por la codicia; entrega la patria a la molicie, a la vanidad, y arrebata al Estado todos los ciudadanos para esclavizarlos, sometiendo unos al yugo de otros y todos al de la opinión.

A la vez Norberto Bobbio (1986) dice que:
Si por democracia directa se entiende estrictamente la participación de todos los ciudadanos en todas las decisiones que le atañen, ciertamente la propuesta es insensata. Es materialmente imposible que todos decidan todo en sociedades cada vez más complejas como las sociedades industriales modernas.

La democracia directa o pura vista desde una manera muy radical y anarquista, pudiera entenderse como el rechazo total de una representación política, llegando a ser una sociedad sin gobierno. La desventaja material que por medio de la tecnología se puede superar es el de la practicidad y eficiencia, pues lo digital siempre es mucho más económico que las papeletas impresas, aunque esto no significa que es gratis el servicio. Pero realmente existe un elemento más, que quizá la tecnología no pueda superar, y es la posibilidad de que el ciudadano se adhiera totalmente a los asuntos democráticos que todo se convierta en político, que solo exista la educación ciudadana provocando fatiga, desinterés o apatía.

De todo lo anterior, es necesario precisar que la tecnología *Blockchain* no viene a romper el paradigma actual, en una inclinación hacia una democracia directa y pura de manera radical, aunque sí pudiera lograrse, pero lo importante es que necesita existir un equilibrio, pues siguiendo a Bobbio (1986):

«El exceso de participación, que produce el fenómeno que Dahrendorf llamó, desaprobando, del ciudadano total, puede tener como efecto la saturación de la política y el aumento de la apatía electoral. El precio que se debe pagar por el compromiso de pocos es frecuentemente la indiferencia de muchos. Nada es más peligroso para la democracia que el exceso de democracia.»

Es así pues cómo la tecnología puede ayudar en todas las formas de democracia. Tal como lo mencionaba Rodotá (2014), que la llamaba «los derechos políticos de la plaza virtual». Mostrando como antecedente que:

> Mediados los años noventa, modelando el sistema político según las sugerencias de Alvin Toffler, un político estadounidense, Newt Gingrich propuso la transición hacia un «Congreso virtual» que debería sustituir al Senado y a la Cámara de representantes, otorgando a todos los ciudadanos el derecho a decidir sobre las leyes mediante el voto electrónico.

Se sintetiza que la democracia directa puede ejercerse por medio de las tecnologías de la información y comunicación (TIC’s), pero tendría que plantearse las ventajas y desventajas así como mantener un equilibrio para no caer en anarquismo.

Gráfico hecho con iconos realizados por Freepik en www.flaticon.com. Licencia Creative Commons BY 3.0 (CC 3.0 BY). http://creativecommons.org/licenses/by/3.0/

Democracia representativa

La democracia representativa, también es conocida como democracia indirecta, es donde los gobernantes son electos popularmente. Bien se dice que la soberanía radica esencialmente en el pueblo, pero este al tener su derecho originario de decidir sobre todo, delega o deriva su derecho subjetivo a otra persona llamada representante. De una manera muy llana, es donde el pueblo no gobierna, pero si elige a los representantes que lo hacen.

Bobbio (1986) menciona que la primera equivocación de la que debemos liberarnos es que "democracia representativa" signifique lo mismo que "Estado parlamentario", es decir «En términos generales la expresión "democracia representativa" quiere decir que las deliberaciones colectivas, es decir, las deliberaciones que involucran a toda la colectividad, no son tomadas directamente por quienes forman parte de ella, sino por personas elegidas para este fin; eso es todo».

A lo que refiere la democracia representativa, es el «Estado en el que el órgano central es representativo (o por lo menos central, en principio, aunque no siempre de hecho). A dicho órgano llegan las instancias y de él parten las decisiones colectivas fundamentales», Por ejemplo

México es una república con sistema presidencialista y no por eso deja de ser un Estado representativo.

Siguiendo a Bobbio (1986):

> En otras palabras, un Estado representativo es un Estado en el que las principales deliberaciones políticas son realizadas por los representantes elegidos no importa si los órganos donde se efectúan tales deliberaciones sean el Parlamento...Las democracias representativas que nosotros conocemos son democracias en las que por representante se entiende una persona que tiene las siguientes características: a) en cuanto goza de la confianza del cuerpo electoral, una vez elegido ya no es responsable frente a sus electores y en consecuencia no es revocable; b) no es responsable directamente frente a sus electores, precisamente porque él está llamado a tutelar los intereses generales de la sociedad civil y no los intereses particulares de esta o aquella profesión.

Se podría decir que el defecto principal de la democracia representativa, y sea una posible razón para una transición por medio de la tecnología a la directa, es que en la formación de esa representatividad, independientemente de convertirse en una demagogia, internamente se forman pequeños grupos de poder, es decir pequeños grupos de personas que deciden entre sus propios intereses, y no se convierte en un gobierno con los mejores representantes, sino con gobiernos con representantes que deciden sobre quienes siguen en el poder e intereses personales, o estados degenerativos con gobiernos de muchedumbres desvirtuando la voluntad general.

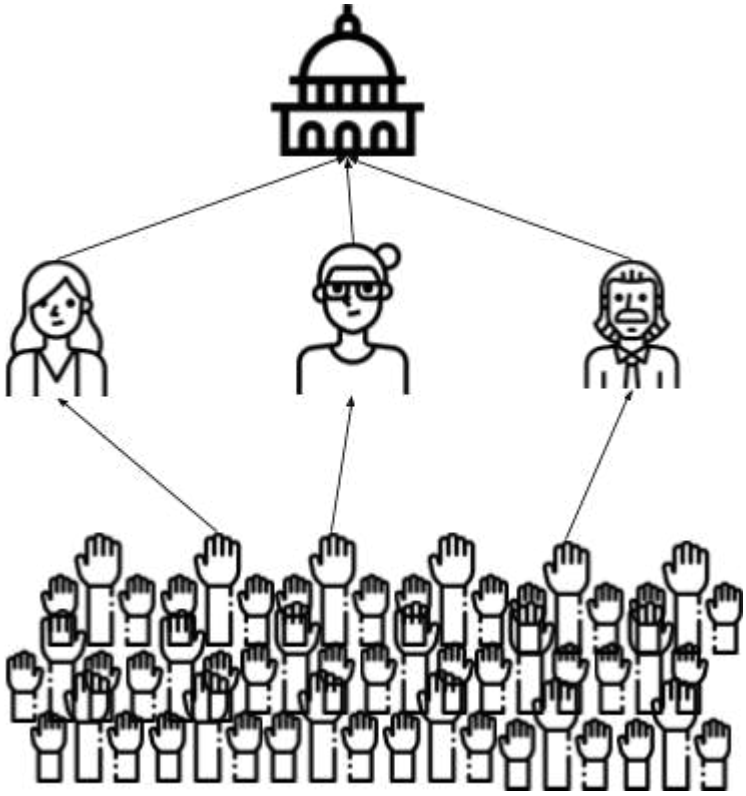


Gráfico hecho con iconos realizados por Freepik y monkik en www.flaticon.com. Licencia Creative Commons BY 3.0 (CC 3.0 BY). http://creativecommons.org/licenses/by/3.0/

Democracia semidirecta

La democracia semidirecta, también conocida como democracia participativa, es la forma donde el pueblo se expresa de manera directa por medio de instrumentos de participación. La participación de la sociedad es un pilar fundamental de la legitimidad de los regímenes democráticos y su reconocimiento es importante para la participación política de las personas en los asuntos públicos.

Los representantes son elegidos de igual manera por medio del voto, pero los ciudadanos aún mantienen su soberanía, pudiendo tener acciones populares y tomar participación en la agenda pública mediante instrumentos o mecanismos que las mismas leyes garanticen. Esta debe establecerse en la Constitución como en alguna legislación especial.

Dahl dice que en las características de la democracia está el elemento de la inclusión de los adultos, que se encuentra en nuestra constitución federal de la siguiente manera:

> *Artículo 34. Son ciudadanos de la República los varones y mujeres que, teniendo la calidad de mexicanos, reúnan, además, los siguientes requisitos:*
> *I. Haber cumplido 18 años, y*
> *II. Tener un modo honesto de vivir.*

Es decir únicamente los ciudadanos mexicanos son aquellas personas que han cumplido 18 años de edad y tienen un modo honesto de vivir, dejando fuera a los nacionales menores de edad; sin embargo este paradigma evoluciona y la forma democrática se amplía a un estilo de vida, pues basándonos en la fuente de la legislación, en el Estado de Jalisco existía un Código Electoral y de Participación Ciudadana, que a *prima facie* por contener derechos y obligaciones en materia electoral se pensaría que es ley para únicamente los ciudadanos, pero en la transición progresista cambió su denominación de ‘participación ciudadana’ a ‘participación social’, es así como la ley se denominó Código Electoral y de Participación Social del Estado de Jalisco, contemplando no solo a los ciudadanos sino a toda la sociedad en general para los asuntos e instrumentos garantizados.

Dichos instrumentos de democracia directa y en un nuevo auge hacia una democracia más participativa, pueden llevarse a cabo diversos instrumentos de participación vecinal, democrática, ciudadana o social. Por ejemplo el mismo Código Electoral y de Participación Social de Jalisco contempla el Gobierno abierto; Plebiscito; Referéndum; Ratificación constitucional; Iniciativa popular; Iniciativa Popular municipal; Presupuesto participativo; Revocación de mandato; Consulta Popular; Contraloría Social; Cabildo abierto; y Juntas municipales.

Es necesario precisar que la democracia semidirecta no es la solución a los problemas de la democracia representativa, pues claramente los ciudadanos pueden determinar quienes son sus gobernantes pero esto no rebasa los objetivos principales en la agenda, pues a pesar de que se

toma en cuenta a los gobernados en esta democracia semidirecta o participativa, sigue faltando un cambio cultural y de acción en los asuntos públicos.

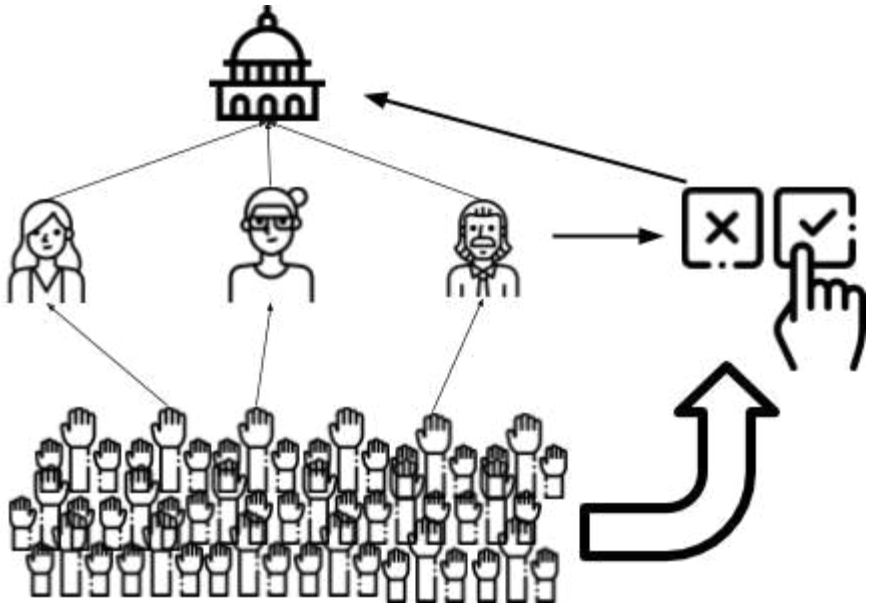


Gráfico hecho con iconos realizados por Freepik y monkik en www.flaticon.com. Licencia Creative Commons BY 3.0 (CC 3.0 BY). http://creativecommons.org/licenses/by/3.0/

Democracia liquida

Al conocer las formas de democracia que se han abordado anteriormente; directa, representativa y semidirecta, la democracia líquida es algo sencillo de entender, pero antes de entrar al tema es necesario determinar ciertos puntos. Primero, visto desde diversas ópticas el derecho a votar es un derecho absoluto; es decir oponible a terceros, puede concebirse como un derecho originario pues emana de un titular y/o derivado pues se le otorga a alguien más, en este caso a los representantes. Independientemente si la voluntad o el interés son elementos esenciales en la toma de decisiones, la realidad es que existe un interés tutelado en la legislación, pero debe existir un reconocimiento interno de voluntad para ejercerlo.

Behrens, Kistner, Nitsche y Swierczek comentan que con democracia líquida (también conocido como poder delegado), los votantes pueden delegar el poder de voto a otros votantes, pero también pueden optar por anular las delegaciones y votar directamente. Además, los

participantes pueden cambiar de delegación en cualquier momento. La delegación es transitiva, una votación puede pasar a través de varios enlaces de delegación antes de que se cuente sobre un tema. (Citado por Hardt & Lopes, 2015)

Por otra parte el proyecto Democracy.earth (2018), ha contribuido con una lista de formas de votar en dicha democracia:

- **Voto directo:** se permite al votante tomar decisiones directamente como democracia directa.
- **Delegación básica:** Se puede delegar el voto a alguien, ejemplo: Alicia le delega su voto a Bob y él puede ejercerlo mientras tenga acceso y no sea revocable.
- **Delegación de etiqueta limitada:** Alicia puede delegar votos a charlie bajo la condición específica de que sólo en ciertos asuntos, por ejemplo votar en solo asuntos de medio ambiente.
- **Delegación transitiva:** Si Bob recibió los votos de Alicia, puede delegar en Frank. Esto genera una cadena de delegaciones, es decir el voto delegado es de nuevo delegado.
- **Voto principal:** Si Bob usó los votos delegados que recibió de Alicia, pero ella tiene una opinión diferente sobre un tema determinado, ya que es la dueña de su propio voto, Alicia puede anular la decisión de Bob.
- **Voto público:** Referido a que el titular del voto tiene el derecho de saber como su delegado ha votado sobre un tema determinado.
- **Voto secreto:** método que puede hacer que las transacciones de voto no sean rastreables para el votante, esto indispensable cuando existe un alto riesgo de coerción.

Una democracia líquida se basa en un modelo de representación dinámica que funciona con un enfoque de abajo hacia arriba: los ciudadanos pueden elegir libremente dentro de su gráfico social (amigos, colegas, familiares) a quién quieren tener como representantes en un conjunto específico de temas. Es la forma más flexible de gobierno democrático que puede construirse con tecnología digital, operando como un híbrido que permite el voto directo o delegado en cualquier momento. (Democracy.earth, 2018)

A *prima facie,* pareciera que la democracia representativa y directa son polos opuestos, ya que el debate antiguo y contemporáneo es sobre la legitimidad, ya sea por el reconocimiento a las instituciones y su participación en estas, pero a la vez es necesaria la satisfacción ante un estilo de vida democrático. Es así como la medida de representación y los instrumentos de participación social muestran un panorama que es la democracia líquida.

En ocasiones, hacer políticos todos los asuntos no es la mejor opción, pues como se ha mencionado anteriormente puede crear fatiga a los ciudadanos, por otra parte no todos los temas son de interés para los votantes, ya sea por decisión personal o porque no se están informados sobre el tema que se podría discutir y someter a votación. La democracia líquida nace tomando lo mejor de la democracia directa y representativa, ya que permite al gobernado decidir si quiere votar directamente o delegar a un representante su decisión. En pocas palabras la democracia líquida, es la democracia directa con la opción de poder delegar el voto.

La diferencia con la democracia directa o democracia pura, es que las decisiones son examinadas por el parlamento, ya que esto no extingue la representación, a la vez que se puede decidir si participar en las decisiones o delegarse a otra persona.

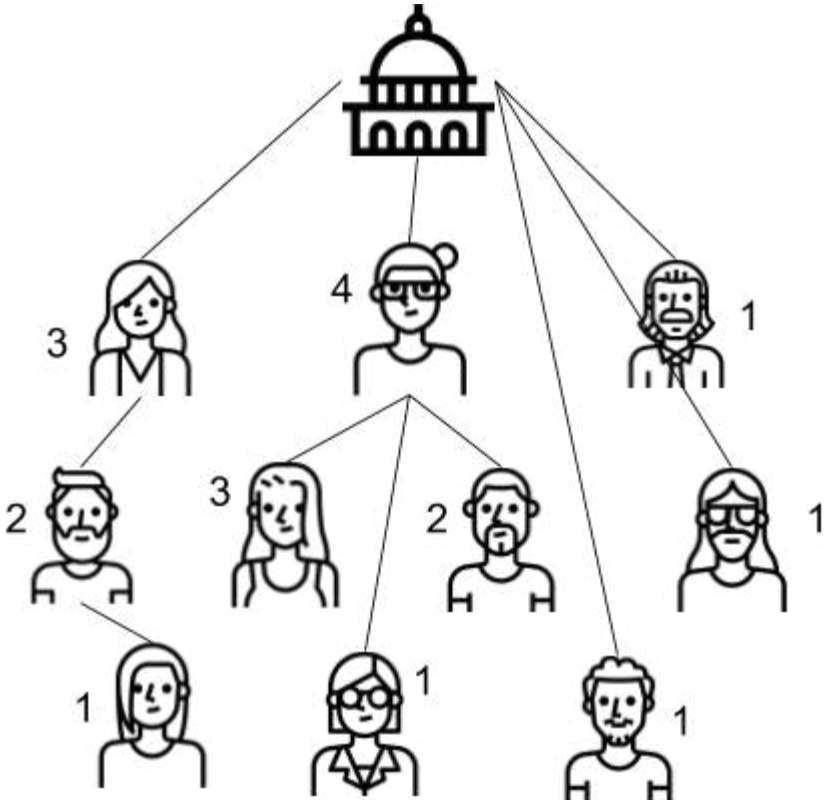


Gráfico hecho con iconos realizados por Freepik y monkik en www.flaticon.com. Licencia Creative Commons BY 3.0 (CC 3.0 BY). http://creativecommons.org/licenses/by/3.0/

La era de la información y la comunicación

La nueva era tecnológica, con el uso de las TIC's tecnologías de la información y comunicación, han realizado diversos cambios en la sociedad, especialmente en las relaciones sociales y ahora digitales, siendo un componente trascendental para todos los elementos del Estado, pues el intercambio, la conectividad, las interacciones tecnológicas son la energía del desarrollo.

Nos encontramos en un momento histórico en el cambio del paradigma de la sociedad y la tecnología, donde somos más que una simple generación viviendo en la era de la comunicación y la información. La tecnología ha permeado en todo lo relacionado con este mundo de manera tangible e intangible, automatizando las relaciones entre personas, procesamientos, datos e inclusive objetos, emergiendo una nueva forma de vivir y dando pauta a un futuro tecnológico con saltos de «humanismo a *tecnohumanismo*, de *homo sapiens* a *homo deus*» (Harari, 2016).

La tecnología disruptiva de innovación y la fuerte demanda de las nuevas generaciones, hacen tambalear los pilares de las instituciones y democracias tradicionales, pues es difícil engañar y no rendir cuentas a una sociedad tan conectada, que con su rapidez, eficacia y sus canales multidireccionales de comunicación, hacen que exista una retroalimentación en todo ejercicio de gobernabilidad.

Es así pues, que la actual forma de democracia se pone en duda, naciendo un nuevo modelo de dirigir el rumbo de la sociedad, dejando atrás el pensamiento tan desinteresado del voto y prerrogativas del ciudadano, creyendo que los votos no deciden nada, ya que al final los que cuentan los votos son quienes deciden todo. Es así como las instituciones como objetos inanimados tienen una metamorfosis para convertirse en las mismas personas, portando en sí mismos el propio sistema digital.

En el término de Gobernabilidad y Democracia, el *Blockchain* abre un catálogo de preguntas sobre ¿Quiénes están a cargo de esta tecnología? ¿Realmente todos podemos participar? ¿Qué son elecciones justas? ¿Cómo es el proceso de voto contemporáneo? ¿Qué implicaciones legales conllevan usar *Blockchain*?, ¿Es una mejora electoral o pone en peligro la democracia?. Y de forma sencilla se podría contestar que nadie está a cargo ya que de manera distribuida y por defecto no hay necesidad de tener un mando, convirtiendo a la sociedad en general en nodos para así llegar a un consenso por medio de algoritmos y acordar automáticamente los resultados del proceso.

La concepción del nacional, ciudadano y extranjero quedan en meras teorías socio-políticas, pues al conectarse a Internet solo existe una nación que radica en la libertad y el conocimiento. El famoso «leviatán» de Hobbes (1651) quedará a la dispensa de los peces que hacen la corriente. El viejo dicho de Cicerón y retomado por Walzer (2001) «Inter arma silent leges: cuando las armas hablan, callan las leyes», queda solo en una leyenda porque el código fuente se convierte en ley interrumpible, inmutable y único, creando una nueva revolución digital.

Ya no es difícil concebir lo que pudiera pasar en un futuro, porque se han desarrollado tanto los avances tecnológicos, que todo lo que sea imaginable puede ser real, pero independientemente del progreso tecnológico, es necesario detenernos y analizar un tema muy importante que pudiera salvar al mundo o empeorarlo, y es preguntarnos ¿Es necesario o conveniente cambiar el paradigma actual y reemplazar todo mecanismo social contemporáneo para crear una verdadera confianza basada en la tecnología distribuida y descentralizada?.

Máxime a que el código fuente es ley, nos encontramos en el justo momento de decidir, pues quizá por el momento no todos los problemas sociales se resuelven con tecnología, pero las humanidades tendrán que tomar la responsabilidad de ser guía a los avances tecnológicos.

Cambios disruptivos en la sociedad democrática

Entre la normatividad, facticidad, legitimidad, vigencia y validez encontramos contenido para justificar a la sociedad democrática, pero existe un tema de gran trascendencia en la actualidad como lo es la «reconstrucción interna del derecho» (Habermas, 1998). En los discursos políticos se escucha la idea de refundar o transformar, ¿pero hasta donde llega este discurso?, mientras siguen los debates de lo que sería lo mejor para una nueva sociedad democrática, la tecnología no espera y está realizando una reconstrucción el Estado y la democracia.

Abraham Lincoln, en su discurso de Gettysburg dijo que «...el gobierno del pueblo, por el pueblo y para el pueblo no desaparecerá de la Tierra». Palabras dulcísimas desde 1863 que dan aliento al alma por prometer una libertad y determinación. Pero a pesar de esta máxima, el único gobierno que podemos encontrar y la tierra de la libertad es el Internet y la tecnología, pues los ciudadanos no sienten que sus instituciones políticas sean una expresión de su voluntad y que protegen sus derechos fundamentales, careciendo la legitimidad, es decir, de esa capacidad administrativa para mantener la idea y respeto a las instituciones públicas encaminadas al bien de la sociedad en general. Se ha llegado a los extremos de promover el no votar como resistencia, pensando que es

un modelo de debilitar a las instituciones, confundiendo la libertad con el libertinaje, el derecho con la obligación.

Es así como *Blockchain* entra en la vida de las personas como una pequeña luz en la oscuridad, pudiendo recuperar la confianza en las instituciones por la integridad de la información que se procesa al ser inmutable y registrarse en todos los bloques, sin necesitar de un tercero con posibles intereses, totalmente transparente sin menoscabo de una privacidad ante las posible represalias y su seguridad por medios criptográficos.

El mayor cambio que ha tenido la sociedad con las tecnologías de la información y comunicación, lo dice su propio nombre, es la misma información que se transmite y las formas de comunicación. El filósofo Habermas (1987), acuña el concepto de la «acción comunicativa», como una teoría crítica de la modernidad, observando la importancia de la interacción social del ser humano, basada en principios lingüísticos, culturales y racionales, con elementos de inteligibilidad, verdad, rectitud y veracidad.

Es así como la sociedad por medio de la tecnología va cambiando radicalmente con canales unidireccionales, bidireccionales y multidireccionales. El primer canal de comunicación unidireccional, entre gobernante y gobernado ya no es eficaz en los tiempos modernos, es decir, cuando una forma de gobernar simplemente envía órdenes y el receptor que son los gobernados simplemente la reciben.

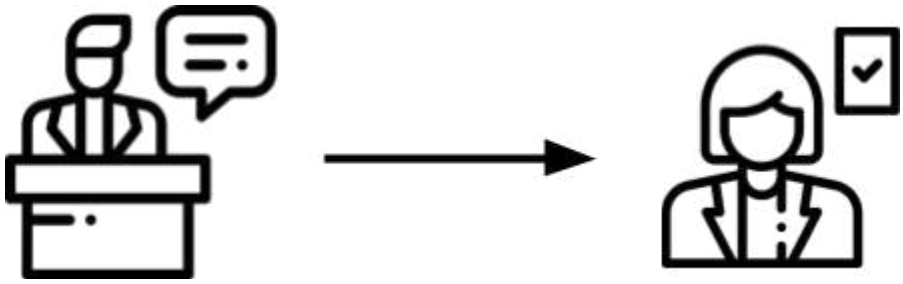


Gráfico hecho con iconos realizados por Freepik en www.flaticon.com. Licencia Creative Commons BY 3.0 (CC 3.0 BY). http://creativecommons.org/licenses/by/3.0/

Podría definirse como meramente transmitir información, donde el emisor que es el gobernante envía dicha información al receptor que es el gobernado, es una expresión de subordinación total donde la opinión no tiene vehículo para viajar.

En segundo término está la comunicación bidireccional, donde el emisor que es el gobernante envía un mensaje por medio de un canal al receptor que es el gobernado, y este que lo recibe puede enviar una retroalimentación.

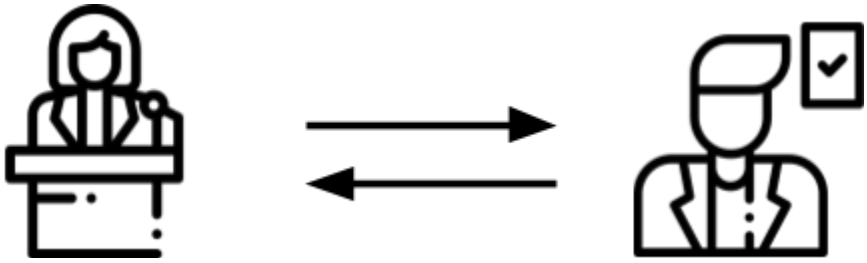


Gráfico hecho con iconos realizados por Freepik en www.flaticon.com. Licencia Creative Commons BY 3.0 (CC 3.0 BY). http://creativecommons.org/licenses/by/3.0/

Como última comunicación está la multidireccional, que su propio nombre lo dice que va a todas las direcciones, siendo todos emisores y receptores al mismo tiempo. Esto significa más que un emisor envíe un mensaje a un receptor, incluso si se permite la retroalimentación que podŕia ser como escuchar su voz, esto es una interacción completa infinita, compartiendo ideas y construyendo a favor del consenso.

Icono realizado por Eucalyp en www.flaticon.com. Licencia Creative Commons BY 3.0 (CC 3.0 BY). http://creativecommons.org/licenses/by/3.0/

Pero la pregunta es ¿esto es suficiente?. A pesar de que contamos con infraestructura, conectividad, accesibilidad y comunicabilidad, pareciera que todo sigue igual, pues en las comunicaciones existe la censura, violaciones de privacidad, usuarios inexistentes como *bots*, información falsa que entorpecen la comunicación, y protocolos no fiables que no garantizan la disponibilidad de la información. Es así como *Blockchain* llegó para quedarse, donde los códigos fuente sean ley.

Las 3G: Gobierno, Gobernabilidad y Gobernanza

En la actualidad las famosas 3G, de Gobierno, Gobernabilidad y Gobernanza, aunado a un buen gobierno abierto y transparente, han sido pilares fundamentales en las nuevas sociedades de la información y comunicación.

Conforme pasa el tiempo, nos damos cuenta que los bienes y servicios proporcionados por el Estado, son una sobrecarga difícil de sostener por las instituciones públicas, ya sea por el déficit presupuestal o crecimiento poblacional. Es así como la naturaleza de los conceptos de distribución y descentralización acompañados de la tecnología *Blockchain*, emergen como una red de confianza, inmutable y transparente, que cambia radicalmente todo proceso de gobernar, haciendo mecanismos e instrumentos de participación de manera más horizontal. La figura de un Estado paternalista donde este se debía de hacer cargo absolutamente de todo, cumpliendo con las mejoras y funciones de gobernar en un canal unidireccional de comunicación, y que solo los gobernados reciban el mensaje sin emitir una retroalimentación, actualmente ya solo queda como un antecedente por ser anacrónico.

En este momento todos los miembros de una sociedad pertenecientes a la red, forman parte de los procesos en las tomas de decisiones, empoderando a los individuos mediante la descentralización de la autoridad en *lato sensu*. Las personas por medio de su identidad digital, además de agentes de cambio, son agentes del *software*. El tradicional contrato social (Rousseau,

1762) de admitir la existencia de autoridad política y orden social, evoluciona y se convierte en un contrato social más inclusivo, es decir, en un contrato inteligente de sociedad.

En un comienzo, la tecnología de *Blockchain* podría utilizarse en automatizar aún más los servicios gubernamentales en relación a la conservación, manejo y gestión de documentos públicos que en la práctica son muy tardados de conseguir, suprimiendo la interacción personal e identificación individual por la certeza de la red. En la actualidad, *Blockchain* sigue evolucionando y cada vez se le encuentran múltiples actividades en diferentes sectores.

La mayoría de proyectos de *Blockchain* son *software* libre y de código abierto, es decir que cualquier persona es libre de usar, distribuir, construir proyectos basados en el código de alguna *Blockchain*, además de ser un libro distribuido que guarda todo lo que procesa por medio de bloques permitiendo una transparencia y confianza de que no serán modificados los valores que corren sobre esta red. También *Blockchain* gana la confianza de las personas, pues al no tener la necesidad de un tercero para aprobar movimientos y ser registrados en la cadenas, aunado a que es un libro de registros que no se deja corromper. La ciencia criptológica no es una novedad en este siglo XXI, sin embargo la razón teleológica de esta tecnología hace que sus principios sean potencializadoras para permitir beneficios en áreas de gran impacto en todas las áreas humanas.

Brevemente, como ya hemos abordado en la obra Internet ¿Arma o Herramienta?, el Gobierno es un elemento del Estado, conformado por personas llamadas gobernantes que dirigen la función política administrativa de un territorio, al ejercer ese gobierno es por medio de la gobernabilidad, ya que en esta acción se pretende crear un estado que permita a las autoridades elaborar e implementar políticas públicas, así alcanzando metas, proyectos y programas para ejercer el gobierno. La gobernanza, yendo un poco más lejos, es una construcción de desarrollo en cuestión de los sectores públicos, privados y civiles para coordinar, pedir, investigar, negociar, motivar, conocer, resolver y tener una satisfacción en general entre los procesos democráticos y la rendición de cuentas.

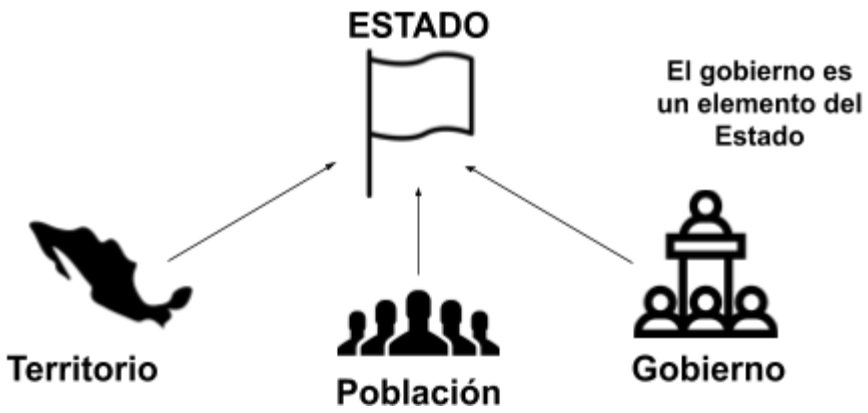


Gráfico hecho con iconos realizados por Freepik, Gregor Cresnar & Smashicons en www.flaticon.com. Licencia Creative Commons BY 3.0 (CC 3.0 BY). http://creativecommons.org/licenses/by/3.0/

Gobernabilidad es la acción de gobernar, es esa capacidad administrativa, técnica y política con la que se cuenta para dar solución a los intereses de la sociedad

Gráfico hecho con iconos realizados por Freepik, Eucalyp & monkik en www.flaticon.com. Licencia Creative Commons BY 3.0 (CC 3.0 BY). http://creativecommons.org/licenses/by/3.0/

La Gobernanza, de acuerdo a la RAE es el “Arte o manera de gobernar que se propone como objetivo el logro de un desarrollo económico, social e institucional duradero, promoviendo un sano equilibrio entre el Estado, la sociedad civil y el mercado de la economía”, es decir es una

construcción de desarrollo en cuestión de los sectores públicos, privados y civiles para coordinar, pedir, investigar, negociar, motivar, conocer, resolver y tener una satisfacción en general entre los procesos democráticos y la rendición de cuentas.

Gráfico hecho con iconos realizados por Freepik en www.flaticon.com. Licencia Creative Commons BY 3.0 (CC 3.0 BY). http://creativecommons.org/licenses/by/3.0/

Explicado todo lo anterior respecto a las 3G: Gobierno, Gobernabilidad y Gobernanza, entramos a un nuevo cuestionamiento, considerando a la democracia y tecnología, entonces nos preguntamos ¿será que la confianza descentralizada y despersonalizada implica una gobernanza mejorada?.

Escuchar las palabras descentralizado y distribuido a *prima facie* asociamos a la confianza, pues es la antítesis de lo centralizado, de ese posible poder desmedido que en su patología es un despotismo. Es así como la descentralización y distribución debe abordarse de la manera más amplia y no solo meramente en la perspectiva tecnológica, es decir que las funciones y procesos realmente se descentralicen y distribuyan entre el sector público, privado y civil, en una verdadera democracia tecnológica.

Por ejemplo, el sector público pudiera implementar tecnología *Blockchain* pero en una red propia, donde estos tengan la mayoría de los *nodos* de la red para realizar las validaciones y

transacciones. Esto es un grave error y demagogia, pues un modelo donde solo el sector público tiene la infraestructura de *Blockchain* de manera centralizada lo convierte en un sistema posiblemente manipulable, violando la confidencialidad, integridad y disponibilidad de la información.

Por lo tanto el sistema de *Blockchain* en una verdadera democracia tecnológica es de distribución y descentralización optimizada, donde la manipulación sea prácticamente imposible, dejando fuera a cualquier entidad individual involucrada en el mantenimiento de la red, distribuyendo a los *nodos* en todos los sectores posibles en el ámbito del sector público, privado y sociedad civil.

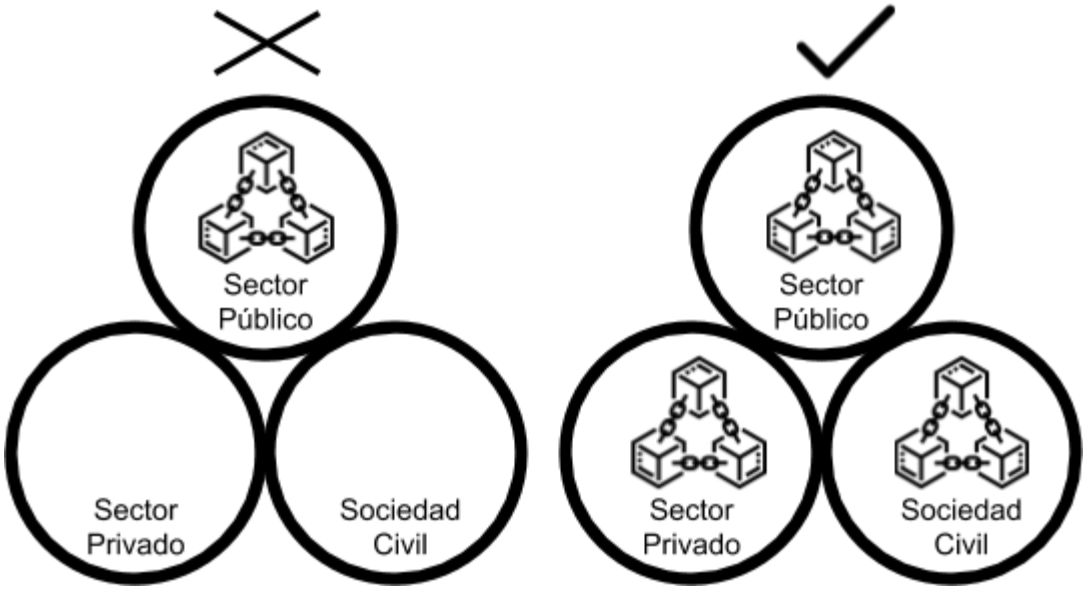


Gráfico hecho con iconos realizados por Freepik en www.flaticon.com. Licencia Creative Commons BY 3.0 (CC 3.0 BY). http://creativecommons.org/licenses/by/3.0/

El protocolo de Dios

Rousseau (1762) dijo: «si hubiera un pueblo de dioses, se gobernaría democráticamente, un gobierno tan perfecto no conviene a los hombres». Es así como la concepción de una verdadera democracia indica a convertirse en algo perfecto, en busca de personas realmente virtuosas. Sin embargo al no ser deidades, es necesaria la relación con los humanos y seres vivos en general, creando armonía en un orden social y natural.

Primero tendríamos que separar la oración “Protocolo de Dios”. Comenzando con la palabra “Dios” y sin entrar a detalle ni debate, el autor Victor Hugo (1862), lo define de una manera muy romanticista, comentando que:

«El Eclesiástico os llama Todopoderoso; los Macabeos os nombran Creador; la Epístola a los Efesios os llama Libertad; Baruch os nombra Inmensidad; los Salmos os llaman Sabiduría y Verdad; Juan os llama Luz; los reyes os nombran Señor; el Éxodo os apellida Providencia; el Levítico, Santidad; Esdras, Justicia; la creación os llama Dios; el hombre os llama Padre; pero Salomón os llama Misericordia, y éste es el más bello de vuestros nombres»

La realidad es que independientemente de la concepción de cada uno, este concepto va relacionado con lo celestial, supremo, omnipotente, omnipresente, omnisciente. El punto medular aquí, es que todos confían en Dios o en sus Dioses.

En lo que respecta la palabra protocolo, en cuestión tecnológica, este va relacionado con las comunicaciones. Es un conjunto de reglas que sirven para transmitir los datos, se establecen procesos de comunicación, por ejemplo el protocolo de transferencia de hipertexto, en inglés *Hypertext Transfer Protocol* conocido como *HTTP*, que sirve como comunicación en la transferencia de información a través de la red informática mundial WWW (*World Wide Web*).

Un problema muy importante tanto para las personas y los protocolos de comunicación es la confianza, puesto que en el intercambio de información, se presentan problemas de seguridad y desconfianza, que en un plano material se acude ante jueces, notarios o autoridades certificadoras, mientras que de manera inmaterial es utilizada la criptografía.

Nick Szabo que escribió sobre los contratos inteligentes, en inglés *smart contracts* que se abordarán en el capítulo dedicado a *Blockchain*, realizó un documento que llamó «*The God Protocols*» (1997), es decir el protocolo de Dios. Este autor dice que imaginemos un protocolo ideal, tendríamos al tercero más confiable que uno pueda imaginar, pues Dios está de lado de

todos, precisa que con un protocolo fiable, con un protocolo de Dios, «todas las partes enviarán sus aportes a Dios. Dios determinaría confiablemente los resultados y devolvería los resultados»

Es así como llega *Blockchain* a nuestras vidas, demostrandonos que somos parte de Dios, en consecuencia que la democracia puede ser efectiva, reconociendo a las instituciones y participando con estas, esa cadena de bloques nos permite saber lo que es verdad y es la materialización del concepto abstracto de conciencia colectiva.

CAPÍTULO II. De las relaciones e interacciones democráticas

Las Tecnologías de la Información y Comunicación (TIC's) han formado las nuevas bases de una democracia, creando procesos con mayor importancia y que la legitimidad prevalezca con más valor, siendo un pilar fundamental contemporáneo. Es así, como las relaciones democráticas las abordaremos por: sujetos, procesos, datos y objetos. Se explicarán las nuevas relaciones, acciones, experiencias y oportunidades que la tecnología ha brindado y podría tomar como desafíos y promesas en el precedente de la democratización tecnológica.

Sujetos

Como primer bloque están los sujetos, por no hablar solo de personas. En esta era de la información todos estamos conectados, en una primera etapa los usuarios comienza a usar tecnología, interactúan y se comunican.

Identidad digital

Una primera concepción sobre lo que es la identidad digital, es toda nuestra información que se encuentra en la red, como nombre completo, fecha de nacimiento, domicilio, sexo, estado civil, grados de estudio, etc. Es decir, en un sentido amplio todo lo que nos hace identificables por medio de las TIC's. Esto no es nada raro y podría ser un tema que abarcara asuntos de derechos a la identidad, libre información, privacidad, intimidad, anonimato, reputación en la red, pero lo cierto es que constantemente utilizamos servicios con los cuales tenemos que interactuar, y por los modelos de seguridad de la información es necesario identificarse y autenticarse para demostrar quienes somos, por la misma razón existen incidentes de ciberseguridad en relación al robo, suplantación y usurpación de identidad en la red.

Ahora con la tecnología *Blockchain*, se puede tomar este control, siendo verdaderos dueños de nuestros datos e identidad digital, una identidad soberana, inmutable y más segura que cualquier sistema actualmente existente.

Hagamos un análisis muy sencillo, cuando entramos a la red social de facebook, ingresamos nuestras credenciales que puede ser correo electrónico o teléfono celular y una contraseña, es un sistema básicamente con una autenticación de algo que solo nosotros sabemos. La pregunta es ¿Esto es poseer la identidad?, en sentido estricto no, pues solo se posee una contraseña y esta puede ser tomada por alguien más. El segundo punto es, el procesamiento de dicha información pasa por servidores de terceros y puede ser vulnerable, además no es determinable por nosotros.

Entonces ¿qué es tener identidad digital?, esto es controlar nuestra información, tenerla de manera actualizada, seleccionar la información que prefiramos mantener privada, la transportación de los datos en todos los servicios. En cuestión democrática la identidad digital serviría para un sistema de votación en el momento de la autenticación de cada persona, facilitando y promoviendo elecciones honestas, también en lo gubernamental, los servicios burocráticos que a veces suelen ser tardados, serán más eficientes, fáciles y rápidos, garantizando que solo la información que se requiere esté a la disposición.

El tema se encuentra en demasiado auge, de hecho la empresa transnacional IBM, dentro de sus soluciones en *Blockchain* ha dicho que «Transformando la identidad digital en una identidad de confianza. Conozca cómo IBM *Blockchain* Trusted Identity ™ está uniendo fuerzas con otros para construir la capa de entidad descentralizada perdida de Internet» (IBM, s.f.), dicha entidad de confianza está basada en un enfoque descentralizado para la gestión de la identidad. Emerge puesto que los individuos u organizaciones no tienen control sobre sus propias identidades, tratando la información sin consentimiento desde sistemas centralizados. Es así como se proponen identidades seguridad y de alta disponibilidad con infraestructura basada en *Blockchain*.

Continuando con el proyecto de IBM, toma asuntos de importancia y estándares normativos que permiten intercambiar atributos de claves públicas, privadas e identidades. Menciona como pilar la identificación y autenticaciones descentralizadas, credenciales verificables y gestión de claves,

además de mencionar la existencia de comunidades como lo son *Hyperledger Indy*, *Hyperledger Fabric* e *Identity.foundations.*

Este concepto debe quedar muy claro, es importante entenderlo. Retomemos unas preguntas ¿que es la identidad digital en *Blockchain*? ¿cuales son sus ventajas? ¿que diferencia hay con los sistemas de identidades electrónicas actuales?. De manera sencilla se podría decir que se trata de limitar la información a terceros, hacerla realmente soberana y confiable.

Por ejemplo en los lugares que solo permiten el acceso a personas mayores de edad, en el caso de México es de 18 años de edad. Para esto hay varios documentos para identificarse, pero la credencial de elector expedida por el Instituto Nacional Electoral (INE) es la más usada, entonces si accedemos a un bar ¿cuál es el único dato que necesita saber la persona que da acceso?, solamente que eres mayor de edad y ya, el resto de los datos como nombre, domicilio, CURP, firma son irrelevantes para la persona del acceso.

Es así, como con el sistema en *Blockchain* se limita la información que se muestra, promoviendo el derecho a la identidad digital, anonimato y encriptar la información como lo reiteramos en el capítulo de Derechos Digitales en la Obra titulada Internet ¿Arma o Herramienta?. Si te piden un nombre, debe ser necesario solo mostrar el nombre, si te piden tu domicilio solo es necesario mostrar tu domicilio. La ventaja es que los sistemas médicos, gubernamentales o empresariales puedan tener una relación con la cadena de bloques, e independientemente al lugar que vayamos esta información esté al alcance para su uso, teniendo el control de acceso a qué datos.

De una manera más formal es como todas las instituciones de salud coordinan la verificación de la identidad de una manera confiable, es como un banco gestiona el préstamo con la identificación emitida por un gobierno, o también como un gobierno se coordina con empresas y compañías, todo en una identidad soberana, identidad en *Blockchain*, descentralizada y de confianza.

En una aplicación real y contemporánea el mejor ejemplo es el país de Estonia, donde en *e-estonia.com* se comenta que a diferencia de muchos otros países, todos los estonios, independientemente de su ubicación, tienen una identidad digital emitida por el estado. Gracias a esto, Estonia está a años por delante de los países que aún intentan averiguar cómo autenticar a las personas sin contacto físico. En este país, cada persona puede proporcionar firmas digitales utilizando su tarjeta de identificación, Mobile-ID o Smart-ID, para que puedan identificarse y utilizar los servicios electrónicos de forma segura.

Otro proyecto es *Smart Nation Singapore*, que además de crear un mejor futuro de la mano con la tecnología, en conjunto el gobierno, empresas, sociedad, buscando la innovación, este proyecto implementa un sistema de identidad digital para que los residentes y empresas de Singapur realicen transacciones digitales con el gobierno y el sector privado de manera conveniente y segura. Cabe destacar que estará operativo en 2020.

P2P: Persona a Persona

El concepto *zoon politikón* creado por el filósofo Aristóteles, es una expresión de animal político o animal cívico. Es decir el hombre y el animal son sociales por naturaleza, pero el humano se relaciona políticamente, formando más que muchedumbres a las civilizaciones y organizando la forma y orden en las ciudades. Es así como el ser humano en sus relaciones, solo se puede desarrollar plenamente en sociedad y necesita vivir con otras personas, mediante organizaciones.

Esto quiere decir que la misma naturaleza del ser, así como las transiciones del estado natural al estado civil, son temas que explican cómo existe una comunicación de Persona a Persona (P2P), en cuestiones políticas y democráticas.

P2M: Persona a Máquina

El lenguaje de las máquinas es en sistema binario, solo son unos y ceros, es decir podríamos decir “hola” y las máquinas podrían interpretar ”10010111101111”. Esto quiere decir que se necesita un decodificador, así como lenguajes de programación y aplicaciones que sirvan como medida de comunicación entre las personas y las máquinas.

Con la llegada del Internet el ser humano puede hacer el uso de dispositivos para promover el gobierno electrónico e instrumentos de democracia, así como ejercer sus derechos fundamentales, pero esto no queda así, pues con la llegada del Internet de las Cosas (IoT) las interacciones con los dispositivos tecnológicos son más dinámicas, pues se establecen estrategias de tecnología con infraestructura digital para realizar interacciones coordinadas.

M2M: Máquina a Máquina

La comunicación de Máquina a Máquina (M2M), es de gran trascendencia para los procesos democráticos, antes de comenzar me parece interesante comentar como «Facebook apaga una inteligencia artificial que había inventado su propio idioma»(Jiménez, 2017), dicho proyecto fue para mejorar los chatbots de facebook, probaron con dos máquinas que mantenían una conversación, pero inesperadamente estas máquinas crearon su propio idioma, posteriormente decidieron apagarlos para no perder el control sobre estas. También «la IA de Google se ha inventado su propio idioma secreto» (Raya, 2016).

Retomando el tema principal, esto ha tenido gran trascendencia con el Internet de las cosas (IoT). Se podría decir que existe una interacción de Máquina a Máquina (M2M), cuando la tecnología permite a los dispositivos o máquinas en red intercambiar información y principalmente realizar acciones sin la asistencia manual de un humano cambia toda la realidad. Los millones de dispositivos y máquinas conectados en Internet y entre estos mismos se comunican, comparten, interactúan y automatizan procesos que podrían ser aburridos o incluso humanamente no adecuados por su constante repetición, convirtiendo hogares, ciudades y naciones inteligentes, donde todo esté conectado.

¿Cómo afectan las conexiones de Máquina a Máquina (M2M) a la democracia?, para esto es menester hablar sobre los *bots*.

Bots sociales

Un bot es una abreviatura de la palabra robot. De acuerdo a la Real Academia Española robot es del inglés robot, y este del checo robot, de robota 'trabajo, prestación personal', en su definición es «Máquina o ingenio electrónico programable que es capaz de manipular objetos y realizar diversas operaciones», así como relacionado a la informática es el «Programa que explora automáticamente la red para encontrar información».

Al respecto Fernández Calvo (2001) dice que Robot es:

> Palabra creada en 1920 por el escritor checo Karel Capek. Capek se basó en el cheko robota, que significa siervo, trabajador forzado, para referirse a cualquier máquina, de forma humana o no, que pudiera llevar a cabo tareas inteligentes. En la web se conoce como robot un programa que recorre la red llevando a cabo tareas concretas, sobre todo creando índices de los contenidos de los sitios, para alimentar los buscadores.

Específicamente los bots sociales o de las redes sociales influyen en las opiniones políticas y al respecto, el Instituto de Internet de la Universidad de Oxford realizó una serie de estudios sobre casos de propaganda computacional en 9 países diferentes, tomando a Estados Unidos, China, Rusia, Polonia, Brasil, Canadá, Alemania, Ucrania, Taiwán (Woolley & Howard, 2017).

En dicho estudio de la Universidad de Oxford se encontró que los *bots*, es decir cuentas automatizadas y otras formas de propagando en redes sociales son usadas por algunos países, principalmente en el tráfico de Twitter dominaban los *hashtags* asociados con partidos políticos influyeron en los espacios democráticos.

En el libro multicitado con anterioridad, publicado por sus servidores “Internet ¿Arma o Herramienta?” se dedica en el capítulo 8, a hablar exclusivamente de los *botnets* y ataques de denegación de servicio, pero ahora por lo que respecta a la cuestión democrática tenemos que preguntarnos ¿Los *bots* son un peligro para la democracia?. La primera cuestión que tendríamos

que identificar es que los *bots* no son personas, son máquinas, por lo tanto tendría que identificar y descalificar estas cuentas previo a que puedan influir en los discursos y expresiones políticas en Internet.

Ahora bien, el Internet es ese gran altavoz que nos permite hablar sobre todos los temas, participar en asuntos políticos y ejercer la libertad de expresión. Sin el Internet se podía engañar muy fácilmente a la sociedad, pues al no estar conectada era propensa a ser manipulada, pero en la actualidad cualquier cosa que suceda se puede grabarse y subirla a la red, y este es compartido por miles de personas, los usuarios discuten y alzan voz, teniendo un total alcance global siendo imposible ocultar información, claramente esto favorece a la construcción de la democracia y gobernanza.

Pero ¿Qué pasaría si los debates en las redes sociales se cayeran en cuestión de segundos?, por ejemplo, supongamos que socialmente el asunto de la democracia y la libertad de expresión con la tecnología se convierte en un asunto de la agenda pública y de interés general. Los usuarios utilizan y comparten el *hashtag #democraciatecnológica* en *Twitter* hasta llegar a ser una tendencia y salir en los destacados de esta red, posteriormente un ejército de *bots*, haciéndose pasar por humanos postean otro *hashtag* y secuestran el debate político, publicando *#comefrutasyverduras*, y solo así el *hashtag #democraciatecnológica* desaparece, llegando a menos personas promoviendo que las personas dejen hablar del tema. ¿Los *bots* destruyen la democracia?

En otro subcapítulo se abordarán las campañas electorales y redes sociales, pero con fines de estadística a continuación se mostramos un gráfico referente al número de *tweets* automáticos pro-Trump para cada *tweet* automático pro-Clinton alrededor de determinados períodos clave de la campaña electoral presidencial de los EE. UU. en 2016, cabe destacar que durante el día de las elecciones, cada *tweet* pro-Clinton automatizado obtuvo un promedio de 4.9 *tweets* pro-Trump.

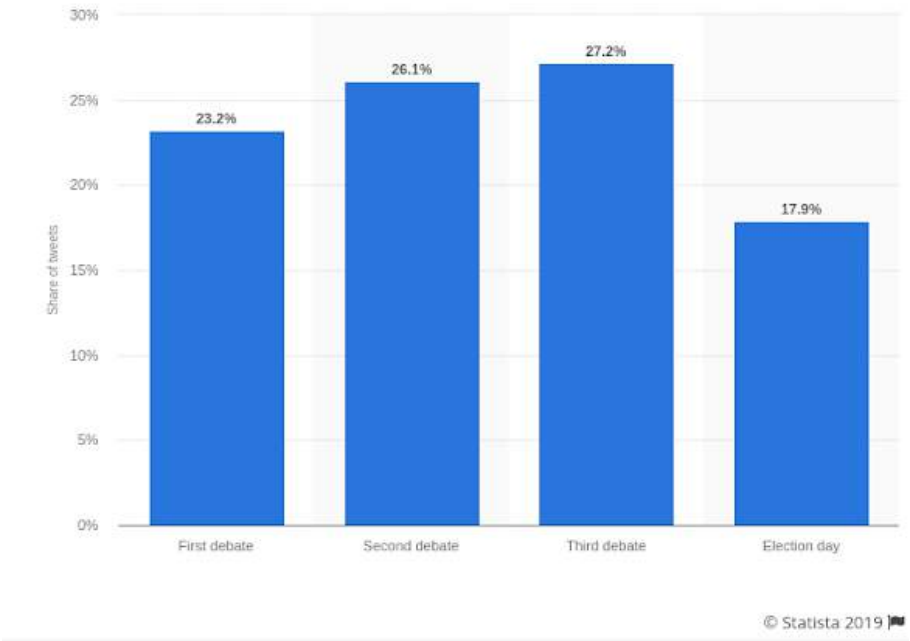


Gráfico obtenido de Statista (portal de estadisticas).

https://www.statista.com/statistics/699668/us-pro-trump-bot-tweets-during-campaign/

Retomando el asunto principal, California como siempre ha estado a la vanguardia de la tecnología, ha propuesto en el Congreso el *Bot Disclosure and Accountability Act of 2018* (California Legislative Information, 2018), una regulación respecto a la divulgación y responsabilidad de los *bots*, esto con el fin de establecer procesos de identificación, evaluación y verificación de la actividad de los programas de *software* automatizados o procesos destinados a suplantar o replicar la actividad humana en línea, con medidas preventivas y correctivas como eliminar contenido que no cumpla la reglamentación, luchando contra los actos engañosos.

La prohibición de los programas de *software* automatizados destinados a suplantar o replicar la actividad humana para la publicidad política en línea es un tema que deberá tratarse y discutirse con exhaustividad, la realidad es que los *bots* generan contenido y en consecuencia manipulan a la sociedad, siendo un gran problema para la democracia y para los derechos fundamentales.

Procesos

Los procesos, son un bloque trascendente, pues las reglas automatizadas hacen una adecuada armonía entre la información. Con esto se facilitan las interacciones entre las personas, datos y objetos, es decir de Persona a Persona (P2P), de Persona a Máquina (P2M) y de Máquina a Máquina (M2M).

Voto electrónico

Como aclaración no se abordará del voto electrónico por medio de *Blockchain*. Entonces nos enfocaremos brevemente en el voto electrónico tradicional, recalcar que es sin *Blockchain*. Esto es materia de debate, ya que por una parte existe una reducción de costos, agilidad de recuento de votos, mayor inclusión y participación si se cuenta con la infraestructura adecuada, sin embargo, desde otra perspectiva se abordan temas que pondrían en peligro la privacidad de las personas y la integridad y autenticidad de los procesos.

La automatización del voto electrónico en un sistema, debe garantizar además de la confidencialidad, integridad y disponibilidad de la información; el anonimato, privacidad de los usuarios, es decir, que los ciudadanos votantes tengan la certeza de que su voto será libre y privado, sin poder ser vinculados a la decisión que tomaron. Por ejemplo, en «el caso de Bélgica, donde el votante se identifica en la mesa y recibe una tarjeta magnética; con ésta se dirige a la cabina de votación, vota y deposita la tarjeta en la urna. En el caso de Brasil ocurre lo contrario, ya que la identificación del elector y la votación son realizadas en la misma urna, levantando sospechas sobre la quiebra del anonimato» (Prince, 2006)

El voto electrónico tiene como resultado agilizar el proceso democrático cuantitativo, reducir costos y mejorar una accesibilidad pertinente. Sin embargo las máquinas que hacen posible este proceso electoral deben ir acompañados para su funcionamiento de un *software* que hace que esto funcione, pero la realidad es que estos pudieran ser privativos o difíciles de comprender. Anteriormente en el libro “Internet ¿arma o herramienta?”, abordamos varios derechos digitales

que deben reconocerse para recuperar una legitimidad con la tecnología en procesos democráticos, el primero es el de transparencia y rendición de cuentas, el segundo es de software libre y código abierto, y el tercero que es de gran trascendencia es el de auditoría o auditabilidad para conocer a profundidad en funcionamiento de los códigos fuentes y sistemas automatizados.

Tipos de votos

Existen dos modalidades de votar, la primera es la votación presencial, que es el procedimiento automatizado de votar presencialmente en algún sistema o urna electrónica, se debe acudir a un lugar en específico, por ejemplo puede votarse por medio de un ordenador o alguna pantalla táctil, podría considerarse este voto a *prima facie* más seguro, por la centralización pero esto no lo exime estar vulnerable a infortunios tecnológicos.

Como segunda modalidad es el voto electrónico por sistemas remotos, esto quiere decir que necesariamente no se tendría que estar presencialmente, podríamos decir que un mensaje de texto, una carta o telegrama podrían considerarse remotos, pero hoy en día con la era de las Tecnologías de la Información y Comunicación, por medio de Internet se puede llegar a este cuando los electores por medio de su dispositivo electrónico conectado a Internet, emitan su voto desde cualquier lugar sin necesidad de estar presencialmente ante su casilla. Este voto puede ser realizado por medio de computadoras, teléfonos celulares, y cualquier aparato conectado a Internet con esta era del Internet de las cosas (IoT) o Internet de todo (IdT).

En una perspectiva contemporánea, el voto a distancia o remoto, podría quedarse como una posible solución a futuro, pues realmente si es necesario un acceso a Internet, pero la conectividad es un problema muy importante, puesto que al menos en el caso de México según estadísticas del INEGI del año 2017 los «hogares con computadora como proporción del total de hogares eran 45.4%, y Hogares con conexión a Internet como proporción del total de hogares el 50.9%» (INEGI, 2017), esto conocido como la brecha digital y el derecho al acceso a Internet. Además de que los Dispositivos del Internet de las Cosas (IoT) aumentan la vulnerabilidad de seguridad y que de acuerdo al informe de *SecureList*, «en promedio, el 22.53% de las

computadoras enfrentaron globalmente al menos una amenaza local de clase maliciosa en el tercer trimestre» (Kaspersky, 2018).

Desde un punto de vista técnico, de acuerdo con el Instituto Internacional para la Democracia y la Asistencia Electoral (IDEA), existen las siguientes formas de voto electrónico:

- “Registro Electrónico Directo (RED). Las RED pueden implementarse con o sin un comprobante impreso verificado por el votante (VVPAT, por sus siglas en inglés). Este último tiene el propósito de arrojar una prueba física de los votos emitidos.
- Reconocimiento Óptico de Marcas (OMR, por sus siglas en inglés), que funcionan a partir de lectores ópticos que reconocen la opción marcada por el votante en una papeleta especial. Los sistemas OMR pueden funcionar ya sea mediante un conteo centralizado (de forma que las papeletas pasan por un lector óptico en centros especiales de escrutinio) o mediante sistemas de votación y conteo de lector óptico (PCOS, por sus siglas en inglés), en los que los votos son registrados por el lector óptico y contabilizados en las mesas directamente, en el momento en que el elector introduce la papeleta en la máquina de votación.
- Impresoras de papeletas electrónicas (EBP, por sus siglas en inglés). Estas máquinas similares a las RED producen un papel para ser leído por la máquina o un comprobante electrónico que contiene la opción escogida por el elector. Este comprobante se introduce en otro lector óptico de papeletas, el cual hace el conteo de forma automática.
- Sistemas de votación en línea. Los votos son transmitidos por internet a un servidor central para su conteo. Pueden ser emitidos ya sea desde computadoras públicas, desde kioscos ubicados en las mesas de votación, o bien –y esto es lo más común– desde cualquiera computadora con conexión a internet accesible para los votantes” (IDEA, 2011)

Proceso de convergencia

No hay mejor manera de comenzar a hablar de un proceso de convergencia que con Norberto Bobbio (1986), pues dice que «es pueril la hipótesis de que la futura computocracia, como ha sido llamada, permita el ejercicio de la democracia directa, es decir, que dé a cada ciudadano la posibilidad de transmitir su voto a un cerebro electrónico». Además de que en la actualidad «sea posible con la ayuda de las computadoras ya no es el fruto de una imaginación extravagante. ¿Por qué el mismo uso de las computadoras no podría hacer posible un profundo conocimiento de los ciudadanos de un gran Estado por parte de quien detenta el poder?»

C.E.R.E.B.R.O.

Como ya nos hemos referido en varias ocasiones, sus servidores escribimos el libro titulado “Internet ¿Arma o herramienta?”, publicado por la Universidad de Guadalajara, en junio de 2018, ahí realizamos un estudio exhaustivo de todas las leyes de los países reconocidos por la ONU, las mismas pueden ser consultadas dentro del capítulo 4, así como los programas informáticos desde un punto de vista técnico, para concluir con un binomio de legalidad e ingeniería, que en ningún país, independientemente de la familia jurídica que pertenecieran, siendo neorománica, common law, socialista, religiosa o mixta, exista algo como CEREBRO, incluso nos atrevemos a decir que es más que un proyecto de Convergencia Electrónica de Redes, Electores, Bancos y Resultados Observados, además de sus hemisferios; electoral, social, operativo y político. Pues a pesar de que el Estado se materialice en ese gran superhombre con un corazón que es el poder Legislativo, con una mente que es el poder Ejecutivo, y con una mano firme que garantiza todo como lo es el poder Judicial, CEREBRO es el alma de este superhombre, esa parte inmaterial junto con el cuerpo que le atribuye la capacidad de sentir y pensar, permitiendo una continuidad hacia un buen Gobierno, Gobernabilidad, Gobernanza y políticas transversales con todos los sujetos participantes de un territorio, materializandose en un mando único de transformación para trabajar por el bien de la patria y de la humanidad en general.

Este concepto de CEREBRO con sus siglas es un concepto acuñado por Carlos Villa (2018) que significa «Convergencia Electrónica de Redes, Electores y Resultados Observados». Además de tener un nombre sencillo de recordar, cumple con las 3 funciones principales, pues consiste en procesar grandes cantidades de información (*Big Data*), con el propósito de obtener resultados informáticos que apoyan de manera más óptima las decisiones de quienes organizan y dirigen con el fin de obtener un triunfo electoral (Inteligencia Artificial), aunado a que la convergencia de la arquitectura de programación puede ser un paso significativo en la forma como se llevan a cabo los procesos electorales en las actuales democracias (*Blockchain*).

A la vez Villa (2018) separa 4 hemisferios, conocidos como Atlas, con el fin de alimentar esta convergencia electrónica, los cuales el autor los define de la siguiente manera:

- **Atlas electoral.** Comprende toda la información relacionada con lo electoral, como es el padrón actualizado, las bases de datos con la geografía electoral, los cuadros comparativos en el historial de procesos electivos, (dos periodos anteriores) las leyes y reglamentos en materia electoral y la jurisprudencia en general en el marco constitucional. (Estadísticas, balances, resultados, efectos, etc.) Fuentes: Instituto Nacional Electoral, (INE) Instituto Nacional de Geografía y Estadística, (INEGI) principalmente. Se debe entender que de acuerdo a cada región se cargan estos datos en el programa. En cada país aplican legislaciones distintas en materia electoral, de igual manera la distribución sectorial obedece a reglas específicas que se tienen.

- **Atlas social.** Aquí se ubican las redes sociales de la web, (metadato) así como bancos de información sobre actividades y listados de asociaciones, grupos organizados, asambleas, juntas vecinales, colonos, academia, medios, y demás. (Nodos) El equipo de personas que opera este Atlas mantiene una actividad constante en las redes sociales de Internet, principalmente *Facebook* y *Twitter*. Es el encargado de bancar y procesar información a través de estudios del imaginario.

- **Atlas operativo.** Lleva registros sobre cada actividad e individuos participantes en la campaña. Administra los recursos humanos, financieros, técnicos u otros. Provee insumos. Diseña y promueve marketing. Analiza y confiere funciones entre los involucrados directos y también colaboradores, adherentes, simpatizantes, etc. Se puede visualizar como la auto-conciencia de la campaña.

- **Atlas político.** Procesa principalmente información sobre estructuras políticas de campañas y partidos. Analiza perfiles de candidaturas y plataformas de gobierno. Evalúa propuestas y análisis políticos que se publican. Pondera y resuelve sobre estrategias políticas y de comunicación política. Procesa mensajes e impactos en redes y medios de comunicación.

Aunque CEREBRO tiene su antecedente en las campañas electorales, su naturaleza de convergencia distribuirá las tareas y competencias, mejorarán los productos democráticos e impulsará a la sociedad a participar con las instituciones, pero para esto se necesita una colaboración colectiva de todos los sujetos, procesos, datos y objetos.

Sin bien el derecho positivo no implica en absoluto la democracia, pero la democracia implica necesariamente el derecho, es decir no puede haber democracia sin derecho (Ferrajoli, 2011), la tecnología se agrega convirtiendo a la democracia, el derecho y la tecnología en un componente fundamental ecléctico para la sociedad. La tecnología por sí sola ayuda mucho, pero cuando está organizada ayuda más, es así como CEREBRO llega para converger y romper un posible trilema entre democracia, derecho y tecnología, en una solución para luchar contra los «poderes salvajes» (Ferrajoli, 2011), en relación al abuso del modelo democrático y nacer como alternativa de un modelo tecnológico con una unicidad neutra y colectiva.

Datos

Los datos son tan importantes que es el elemento crucial de la información para promover una verdadera democracia participativa y una administración eficiente. Los datos, como información

en general, son la nueva herramienta de poder actual, pues el conocimiento es poder y por medio del análisis se puede llegar a tener información útil para la toma de decisiones.

Los datos tienen un gran valor cuando todo lo que nos rodea se encuentra automatizado. Por si mismo no son nada, solo es información sin sentido que debe ser organizada, por ello los datos son útiles cuando son procesados y analizados, convirtiendo el dato en información y dicha información en conocimiento. De manera digital, toda la información que procesan los sistemas automatizados es en sistema binarios de unos y ceros, además se calculan en bits.

Existen datos estructurados que llevan un registro y se lleva el análisis estructurado con facilidad, pero a la vez los datos no estructurados que no tienen organización, es decir no están procesados, sin modo ni agrupación.

Su almacenamiento a la actualidad es por medio local, por ejemplo por *CD, USB,* que son de forma centralizada, pero esto podría aumentar cuando están conectados a Internet o a un servicio y distribuidos cuando están en diversos servidores o servicios, pero la realidad es que los datos siempre están en movimiento.

Información

Como Preámbulo, de conformidad con la Real Academia Española, la información tiene muchas concepciones, por ejemplo como la acción y efecto de informar. Oficina donde se informa sobre algo. Averiguación jurídica y legal de un hecho o delito. Pruebas que se hacen de la calidad y circunstancias necesarias en una persona para un empleo u honor. Comunicación o adquisición de conocimientos que permiten ampliar o precisar los que se poseen sobre una materia determinada. Conocimientos comunicados o adquiridos mediante una información.

Es decir a lo que respecta en el encuadre epistemológico de comunicabilidad, esta es la expresión del contenido de un mensaje y puede ser transmitida, en su medio existen diversos codificadores

y lenguajes, así como interpretaciones, esta puede ser por voz, escrita, símbolos y ahora en la actualidad por el *bit*.

Detengámonos por un momento y pensemos en un mundo sin Internet, que sin duda sería un lugar que todo marcharía muy lento y esto no significa algo bueno o malo, pero retomando el tema, en esa idea la posibilidad de enviar mensajes y recibir información tendría que ser por medios tradicionales, ya sea por medios de transporte desde correr, bicicleta, automóvil, barco o aviones y hasta utilizando palomas mensajeras, pergaminos, periódicos, código morse, teléfonos, radio o televisión.

Con lo anterior se podría deducir que la tecnología digital ha cambiado mucho a la sociedad, principalmente rompiendo sistemas muy centralistas. Si bien la información podría interpretarse de manera analogica con la libertad, la gran cantidad de información que existe por medio de las TIC's, ha rebasado toda capacidad material y humana de poder procesar todos los datos, pues a pesar de que los procesamientos cada vez son más ágiles gracias a los avances tecnológicos, por ejemplo con la computación cuántica, sería muy osado decir que está todo bajo control y que todo tiene respuesta y solución.

¿Hasta dónde llegará el poder de la información?, los procesos centralizados se extinguen y los distribuidos permanecen. En la actualidad, el Internet democratizó la información y *Blockchain* a las instituciones, se ha colocado un espejo frente al *Leviatán* que le permitirá observarse.

Redes sociales electorales

Las redes sociales son una herramienta predominante en el cambio de las elecciones políticas, también convirtiéndose una herramienta para los políticos y gobiernos. Como diferencia de los otros medios de comunicación tradicionales como el periódico, radio y televisión, las redes sociales otorgan a las personas un elemento esencial para las democracias contemporáneas, que es la capacidad de poder comentar, compartir y publicar ideas, convirtiéndose en un gran altavoz y comunicación entre candidatos y ciudadanos, gobernantes y gobernados.

Estar presente en las redes sociales, al contenido, a las ideas y preguntas que se realizan, ha logrado que se llegue una mejor comprensión de lo que a los usuarios y personas les preocupa, se les presta una atención parcial con un servicio de 24 horas. Aunado a este canal multidireccional de información, esto también ayuda a una conectividad para que las personas estén informadas y puedan organizarse o reaccionar ante situaciones en tiempo real.

Existen diversas redes sociales, pero las que más destacan son *facebook*, *twitter*, *instagram, linkedin, snapchat,* entre otras, pero para efectos prácticos únicamente nos enfocaremos en la red social de *twitter*. Ahora bien, hablando de *twitter* y política, es importante precisar que Barack Obama es el candidato 2.0 por utilizar redes sociales, y que en la actualidad este mismo en su cuenta de twitter oficial usuario *barackobama*, se posiciona en el número 3 en el ranking mundial con más seguidores en el 2019 (Trackalytics.com), debajo de los dos cantantes Katy Perry y Justin Bieber, claramente este imperio lleva tiempo construyéndose y a continuación lo describiremos un poco.

Previo a seguir con el caso de Obama, es necesario precisar cierta información general sobre las elecciones y el proceso electoral de los Estados Unidos de América que a continuación se enlista:

Generalmente, el proceso de las elecciones presidenciales sigue este ciclo:

- Primavera del año anterior al año de la elección: los candidatos anuncian sus intenciones de postular.
- Verano anterior al año de la elección hasta la primavera del año de la elección: se realizan los debates anteriores a las elecciones primarias y asambleas de los partidos políticos ("caucuses").
- Enero a junio del año de la elección: los estados y los partidos políticos realizan las elecciones primarias y sus asambleas del partido ("caucuses").
- Julio a principios de septiembre: los partidos políticos realizan las convenciones nacionales para elegir a sus candidatos.

- Finales de septiembre y octubre: los candidatos participan en los debates presidenciales.
- Principios de noviembre: día de las elecciones.
- Diciembre: los miembros del Colegio Electoral depositan sus votos en el Colegio Electoral.
- Principios de enero del año calendario siguiente: el Congreso cuenta los votos electorales.
- 20 de enero: día de la Inauguración Presidencial. (usa.gov, 2018)

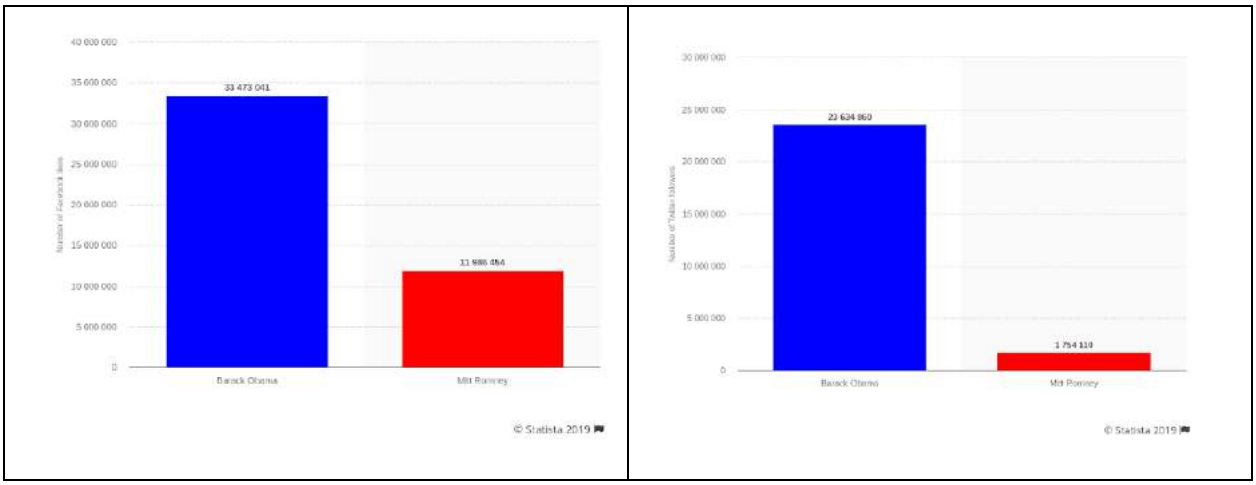
Las elecciones en ese país se realizan cada cuatro años, Obama fue presidente durante ocho años ya que salió victorioso por medio de la elección y su reelección. En lo que respecta a la primera elección, cabe destacar que eran pocas las redes sociales que existían a comparación de la actualidad, pero Obama fue la diferencia, tal como lo dice el periódico *The Washington Post*, que lo declaró como el rey de las redes sociales, siendo el primero en sacar provecho de este medio, teniendo perfiles en *Eons*, *Myspace* para generaciones de *baby boomers*, también en blackplanet.com y migente.com que son comunidades de origen afroamericano y latinos, así como en Asianave.com para asiáticos estadoundenses. Por esto Barack Obama, quizá no sea el más popular pero es un candidato con demasiada audiencia en todos los sitios sociales. (Vargas, 2007).

Obama utilizó redes sociales tradicionales en esos tiempos, y si bien Obama el 10 de Febrero del 2007 anunció su candidatura, el 03 de Junio de 2008 se convirtió en el candidato del Partido demócrata y en las elecciones presidenciales del 04 de noviembre del 2008 ganó en sus elecciones frente a John McCain, tomando posesión el 20 de Enero de 2009, es necesario precisar que pese al uso de otras redes sociales, Obama usa su Twitter desde marzo de 2007, mientras que su contrincante McCain desde enero de 2009. Podría considerarse este proceso como el de las elección en las redes sociales.

En lo que respecta al segundo proceso electoral, el 4 de abril de 2011, Obama anuncia su reelección presidencial para el año 2012 y el 6 de noviembre fue ganador, siendo reelegido por un periodo más, venciendo a su contrincante Mitt Romney. A diferencia del proceso anterior del 2007, en este momento las redes sociales ya no eran algo novedoso, los candidatos ya habían evolucionado a ser cibernautas, por lo que el pago de publicidad y el procesamiento de datos fueron los elementos principales para ganar en el mundo inmaterial cibernético e influir en el material. Podría considerarse esta elección no solo de redes sociales, sino del *big data*.

A continuación se muestran dos gráficos de las elecciones del año 2012 de Estados Unidos de América, entre Barack Obama y Mitt Romney, en las redes sociales de twitter y facebook:

Número de "Me gusta" de Facebook de Barack Obama y Mitt Romney a partir de noviembre de 2012	Número de seguidores en Twitter de Barack Obama y Mitt Romney al 21 de noviembre de 2012.
Gráficos obtenidos de Statista (portal de estadisticas). *https://www.statista.com/statistics/243305/number-of-twitter-followers-of-barack-obama-and-mitt-romney/* *https://www.statista.com/statistics/243302/number-of-facebook-likes-of-barack-obama-and-mitt-romney/*	



Los datos anteriores nos muestran una ventaja muy distintiva de Barack Obama. En la actualidad tener el poder es poseer la información, esto referente a los datos procesados, pero no solo eso es suficiente, pues deben estar bien encaminados sin que violen los derechos fundamentales y legislación. Es así, cómo los candidatos que usen las redes sociales y el procesamiento idóneo de los datos llegan al éxito, donde quizá no sea tan importante «tener la razón», sino «llevar la razón». (Schopenhauer, 2003)

Noticias falsas (fake news)

Las noticias falsas no son una creación de la tecnología, pero realmente con su conectividad y el procesamiento de tanta información, se ha potencializado este fenómeno principalmente en las redes sociales donde existe mayor comunicabilidad entre las personas, influyendo en la toma de decisiones, manipulando y rompiendo la confianza, pensando incluso que todo contenido en la red es falso.

Manipulación de datos, desinformación y noticias falsas son el peor enemigo de un pueblo, que incluso pone en riesgo a la democracia. De hecho un estudio del Instituto Tecnológico de Massachusetts (MIT), concluyó que «las noticias falsas llegaron a más personas que la verdad; el 1% superior de las cascadas de noticias falsas se difundió entre 1000 y 100,000 personas, mientras que la verdad rara vez se difundió a más de 1000 personas» (Soroush, Deb & Sinan, 2018).

Las noticias falsas son una gran patología en la sociedad de la información contemporánea, con esta se manipula la verdad y en consecuencia a la sociedad, se pueden cambiar los resultados electorales como lo abordaremos más adelante, y beneficiar a las personas precursoras de estas malas prácticas. De una manera sociológica se daña la confianza de los medios y las personas, pues inclusive hasta las propias autoridades materializadas en servidores públicos han caído en compartir noticias falsas, creando sistemáticamente a internautas indiferentes.

Historias como "el niño crucificado en Ucrania", "la niña de Kuwait y la invasión de Irak" o "las fotos falsas en la crisis de los rohingya", son ejemplos de 3 noticias falsas que propiciaron guerras y conflictos alrededor del mundo (BBC Mundo, 2018). Estos nos dice, que una noticia falsa, su alcance y propagación puede incitar al odio, miedo e incluso a la guerra.

Es trascendente cuidar el derecho a la libertad de expresión, prensa y periodismo, luchar contra la censura y promover siempre la verdad. Tal como lo dice la declaración conjunta sobre la independencia y la diversidad de los medios de comunicación en la era digital, respecto a las amenazas jurídicas inciso f) que:

> Las restricciones de la libertad de expresión basada en conceptos tales como “la seguridad nacional” y la lucha contra “el terrorismo”, “el extremismo” o “la incitación al odio” deben definirse de manera clara y en un sentido estricto y ser objeto de supervisión judicial a fin de limitar la discreción de los funcionarios que las apliquen y respetar las normas establecidas en el párrafo a). Al mismo tiempo, no deben usarse conceptos inherentemente vagos, como “la seguridad de la información” y la “seguridad cultural”, como base para restringir la libertad de expresión.

La *International Federation of Library Associations and Institutions* (IFLA), en español Federación Internacional de Asociaciones de Bibliotecarios y Bibliotecas, se ha pronunciado al respecto destacando el cómo detectar noticias falsas:

- ESTUDIE LA FUENTE. Investigue más allá: el sitio web, objetivo e información de contacto.
- LEA MÁS ALLÁ. Un titular impactante puede querer captar su atención. ¿Cuál es la historia completa?.
- ¿QUIÉN ES EL AUTOR?. Haga una búsqueda rápida sobre el autor. ¿Es fiable? ¿Es real?.
- FUENTES ADICIONALES. Haga clic en los enlaces y compruebe que haya datos que avalen la información.
- COMPRUEBE LA FECHA. Publicar viejas noticias no significa que sean relevantes para hechos actuales.
- ¿ES UNA BROMA?. Si es muy extravagante puede ser una sátira. Investigue el sitio web y el autor.
- CONSIDERE SU SESGO. Tenga en cuenta que sus creencias podrían alterar su opinión.
- PREGUNTE AL EXPERTO Consulte a un bibliotecario o un sitio web de verificación. (IFLA, 2017)

Independiente de los poderes del Estado, es importante que como ciudadanos luchemos contra las noticias falsas y ejerzamos el «derecho a la verdad», para esto verifiquemos las fuentes de la información que se publique y utilicemos buscadores con busquedas figurativas como https://www.tineye.com/ o inclusive el mismo motor de busquedas de *images.google.com.*

Por ejemplo, en la red podremos encontrar fotografías de un incendio en una localidad, pero para procesar los metadatos y hacer un análisis se requiere tiempo, conocimientos y *software*, por lo que la recomendación es descargar la imagen ir al buscador de imágenes de Google, hacer una búsqueda por imágenes y ver en qué otros medios ha sido utilizada comparando los resultados y por supuesto compartiendo solo información confiable.

Sin duda el asunto de las noticias falsas abren la puerta al alarmismo, al sesgo de los medios y de la información, teorías de conspiración, el infundir el temor, calidad de la información. estatus de

la prensa, censura, manipulación y seguridad nacional. Pero lo primordial es que necesitamos combatir las campañas de desinformación organizadas que intentan irrumpir y socavar la democracia.

Dataismo

El Dataísmo, es un concepto relacionado con *big data*, inteligencia artificial e Internet de las Cosas (IoT), el autor Harari (2016) la define como «la religión de los datos», donde la concepción del universo consiste en el flujo de datos, y que el valor de cada entidad está determinada por su contribución de procesar datos, creando una confianza más sólida en la propia información y algoritmos que lo procesan que en las mismas capacidades humanas o sentimientos.

Siguiendo las nociones de Harari, no se debe confundir la libertad de información con la libertad de expresión. La libertad de expresión se concedió a los humanos, y protegía su derecho a pensar y decir lo que quisieran... por otra parte la libertad de información, no se le concede a los humanos, se concede a la propia información. El 11 de Enero del 2013 el *dataísmo* tuvo su primer mártir llamado Aaron Swartz, un pirata informático de 26 años de edad que se suicidó, quien creía que la información tenía que ser libre y utilizó la red informática del *MIT* para acceder a *JSTOR* y descargar miles de artículos científicos para compartirlos en Internet y que estuvieran al alcance de todos. (Harari, 2016)

En la obra Internet ¿Arma o Herramienta?, clasificamos un derecho como «el derecho a compartir», hicimos un análisis entre los posibles problemas legales al ejercerlo y por otra parte se tomó la naturaleza del propio Internet y su surgimiento. Entonces tomar el *dataísmo* muy radicalmente es abogar como libertad principal de este siglo XXI la libertad de información, donde la construcción de un mundo mejor es liberar los datos.

La pregunta principal de esta corriente o religión es analizar ¿De qué sirve un dato si no es compartido?, la construcción del dato a medio y de medio a prueba es un monumento a la

libertad de la información. En el ciberespacio como forma de mando y poder del pueblo, ha sido escenario de diversos movimientos, ya sea de acceso a Internet, privacidad, libertad de expresión pero ahora el principal, es de la libertad de información.

Personas como Edward Snowden, exempleado de la Agencia Central de Inteligencia (CIA) y de la Agencia de Seguridad Nacional (NSA) que hizo públicos documentos con el carácter de secretos en medios de difusión. Así como la organización internacional WikiLeaks, que publicaba en su sitio web información anónima, documentos filtrados sobre realidades pero con la protección de sus fuentes. Incluso el caso más reciente es cuando «Alemania sufre el mayor 'hackeo' de su historia con la filtración de datos personales de centenares de políticos» (Müller, 2019), considerándose un ataque serio a la democracia, por lo que reabre el debate respecto a la información y su procesamiento.

Es aquí donde habrá que detenernos, pero ahora para pensar si el *dataísmo* será la mano que impulse tecnologías innovadoras y un progreso, o la creadora de escenarios donde «la democracia podría decaer e incluso desaparecer»(Harari, 2016), dejando obsoletas instituciones venerables como elecciones, partidos políticos o incluso parlamentos por ser obsoletas y suplidas por algoritmos informáticos.

Modelo CIA

En la obra publicada Internet ¿Arma o herramienta? Se abordó este modelo y el AAA, pero a lo que respecta para conocer estos atributos tan importantes de la información, solo es necesario recordar que todo gira alrededor de la información y comunicación, y es por esto que es necesario conocer el modelo CIA.

Al escuchar la palabra CIA es fácil pensar en la Agencia Central de Inteligencia de los Estados Unidos, por sus siglas que en inglés significan Central Intelligence Agency, pero cuando escuchemos sobre el modelo CIA en la seguridad cibernética, es para referirse a *Confidentiality*, *Integrity* & *Availability*, que en español son Confidencialidad, Integridad y Disponibilidad.

La confidencialidad es el atributo que impide prevenir la divulgación de información a las personas que no estén autorizadas. Por ejemplo, si alguien entra a nuestra cuenta de *facebook* y ve nuestros mensajes está accediendo a contenido confidencial del usuario.

La Integridad es el atributo para preservar que la información no sea modificada por personas que no fueron autorizadas, por ejemplo cuando alguien envía un mensaje por whatsapp puede sufrir una intervención ilícita de comunicaciones, donde el pirata informático modifica el mensaje antes de que llegue con su destinatario. Por último la Disponibilidad es el atributo referente a que la información esté a disposición de las personas que deben acceder a esta, por ejemplo que el sistema del trabajo funcione.

Ciertamente un gobierno digital y democracia tecnológica no funcionará si no se respeta la confidencialidad, integridad y disponibilidad de la información.

Big data

Big Data es administrar los datos masivos, es decir todos, es el procedimiento mediante el cual se administran los datos en su volumen, variedad y velocidad. Primero en volumen es tener en cuenta la cantidad de datos que se procesan y se almacenan, por otra parte la variedad que tipos

de datos son, comenzando con sus caracteres hasta el sector que se encuentran y por último la velocidad, para considerar la rapidez por los que son procesados y comunicados.

Debe implementarse un análisis cuantitativo en los datos, posterior a esto, otro cualitativo para identificarlos y administrarlos, así los datos se convierten en información y se pueden tomar decisiones. Cabe destacar, que esto no solo se logra con buenas intenciones pues se debe prever el costo y complejidad de los procesos de almacenamiento, análisis y acceso a los datos.

Caso cambridge analytica

Para comenzar a hablar sobre Cambridge Analytica, primero es necesario puntualizar el impacto y trascendencia de nuestros datos personales y procesamiento de datos. En redes sociales, principalmente en facebook nos encontramos con algunos *test* que dicen: “A qué famoso te pareces”, “qué dicen tus ojos sobre tu personalidad”, “cómo se verá tu futura hija” o “cómo te verás en 50 años”, que sin duda dan contenido para la interacción en las redes sociales, pero que en su momento pudieron ser utilizados para objetos sin consentimiento, incluso hasta ilícitos. Un ejemplo de dichos *test* es el siguiente:

¡¿A qué Famoso te Pareces?!

Imagen Obtenida de https://es.vonvon.me/

A la vez, un dato personal es por ejemplo el nombre, teléfono celular o correo electrónico, es decir la información concerniente a una persona física, identificada o identificable, también existen datos sensibles como origen racial o étnico, estado de salud, información genética,

creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual. Algunos servicios de Internet solicitan dicha información para ofrecer el servicio, sin embargo en el caso de los *test* de *facebook* pareciera que solo es un juego que se convierten en momento de risas y comentarios entre amigos, pero dicha información podría ser procesada para incidir en compras de productos, manipular el estado de ánimo y hasta en la decisión de los votantes.

Siguiendo con el asunto principal, Cambridge Analytica es una empresa que se dedica al análisis de datos en procesos electorales previa contratación de políticos, su participación en la campaña *Brexit* y en el proceso electoral de los Estados Unidos de América con Donald Trump, colocaron a la empresa en uno de los mayores escándalos respecto a los datos personales, procesamiento de datos y elecciones.

La recopilación de los datos fue por medio de la aplicación llamada "thisisyourdigitallife", desarrollada por el académico Aleksandr Kogan, que a través de su empresa y cambridge Analytica pagó a cientos de miles de usuarios para que realizaran una prueba de personalidad mencionando que se recopilaron para uso académico. Sin embargo dicha aplicación también recopiló información de los amigos que de facebook de los que la utilizaron, pese a que facebook prohíbe que se vendieran los datos, esto se utilizaron por parte de la empresa Cambridge Analytica (theguardian.com, 2018), esto quiere decir que aunque un usuario no hubiera utilizado la aplicación, si alguien de la lista de amigos sí lo hizo, automáticamente se tendría la información del usuario que no tuvo ni idea de la existencia de dicha aplicación.

¿A los datos de cuántas cuentas ha accedido entonces Cambridge Analytica? Aunque 270.000 usuarios le dieron permisos, hay que contar también los datos de sus amigos. Se cree que han accedido a los datos de más de 87 millones de personas. La mayoría son perfiles procedentes de Estados Unidos, pero la red social calcula que 2,7 millones de cuentas son de la Unión Europea y que más de 780.000 son cuentas de usuarios mexicanos. (González, 2018).

¿Como fué su rol en las elecciones de Estados Unidos de América?, con el test de Kogan y la información de facebook, la tarea principal era inferir perfiles psicológicos de cada usuario, sabiendo cuál debía ser el contenido, tema y tono de mensaje para cambiar la forma de pensar de los votantes casi de forma individual, y no solo eso, además del envío de publicidad personalizada, se desarrollaron noticias falsas que luego se replicaron a través de redes sociales blogs y otros medios. (BBC Mundo, 2018).

Por dicho caso Mark Zuckerberg, fundador de facebook además de diversas citaciones, ha comparecido ante el Parlamento de la Unión Europea y el Congreso de los Estados Unidos de América. Sin duda esto es un tema trascendental en la manipulación de información, obtención ilícita de información, ataque a la privacidad, violación a derechos fundamentales y sin duda un gran golpe para las democracias.

Para concluir, es importante mencionar posibles soluciones que en *Internet Policy Research Initiative* (IPRI), del *Massachusetts Institute of Technology* (MIT), presentan como medidas técnicas, específicamente en la política de uso, que sigue siendo la mejor herramienta para tratar el mal uso de datos, comenzando con la visibilidad de información y uso en razón que aumentar esta en los flujos de datos en teléfonos inteligentes permite a los usuarios tomar decisiones de privacidad más inteligentes. Por otra parte la transparencia y auditoría que van de la mano con la visibilidad, a la vez el rediseño de la arquitectura en torno a la privacidad y el consentimiento y por último la descentralización de la información. (Fruchter, Specter & Yuan, 2018).

Esto también lo abordamos en la obra Internet ¿Arma o Herramienta?, donde mencionamos que tenemos diversos derechos digitales, pero los que tienen relación con lo comentado son el derecho a la protección de datos personales, a la privacidad, a no ser vigilado, a la transparencia, acceso a la información pública y rendición de cuenta, a la verdad, a la no censura abordando un poco sobre los sistemas descentralizados, a la auditoría o auditabilidad y principalmente a la claridad en los términos y condiciones y avisos de privacidad.

Objetos

Los objetos como último bloque, son aquellos dispositivos que modifican la percepción material de la democracia, desde la utilización de dispositivos como objeto, como medio y como fin, que en este capítulo los hemos de desarrollar con el género de objetos.

Cuando la tecnología es vista como un objeto, es la utilización de dispositivos tecnológicos, por ejemplo como un celular, que en *stricto sensu* es un objeto que nos facilita la vida para comunicarnos, pero que en *lato sensu* y actualmente tiene más funcionalidades, pero la idea principal es que estos dispositivos siguen siendo cosas, objetos.

Cuando la tecnología es vista como un medio, es la utilización de dispositivos tecnológicos incorporados a nuestros cuerpos con la finalidad de mejorar o suplir un déficit, contemplándose como una extensión del cuerpo. Tal es el fenómeno de los *cyborgs*, *biohacking* con las corrientes del transhumanismo y posthumanismo. Cuando se modifica el ser humano por medio de tecnología, y así mejorar capacidades humanas, físicas e intelectuales, dejando atrás la percepción de la tecnología vista como un objeto o cosa, pues en este supuesto es una extensión al cuerpo, es parte del mismo ser humano y su condición.

Cuando la tecnología es vista como un fin, dejando atrás el concepto Maquiavélico y su significado de que el fin justifica los medios, o también como que la Inteligencia Artificial dará fin a la humanidad. Entonces el fin, en una concepción diferente a las mencionadas anteriormente, es para referirse a los actos comisivos, teniendo como un resultado final a un sujeto, es decir quien ejercita la acción, donde se clasificaría a la Inteligencia Artificial.

Internet de las cosas (IoT)

El Término Internet de las Cosas, en inglés *Internet of Things* (IoT), es un término atribuible al británico Kevin Ashton (2009), definiéndolo como una red que no solo conecta a las personas, sino también a los objetos que las rodean.

De acuerdo a la Recomendación UIT-T Y.2060 de la Unión Internacional de Telecomunicaciones (2012), se define Internet de los objetos (IoT) como la «Infraestructura mundial para la sociedad de la información que propicia la prestación de servicios avanzados mediante la interconexión de objetos (físicos y virtuales) gracias a la interoperatividad de tecnologías de la información y la comunicación presentes y futuras».

Pareciera algo de ciencia ficción pensar en dispositivos conectados e inclusos inteligentes que toman decisiones, pero es una realidad ya que estos trabajan en conjunto recopilando, analizando y procesando datos para realizar acciones. Cisco calcula que para 2020 habrá 50 mil millones de dispositivos conectados a Internet Sin embargo, actualmente, más del 99% de las cosas presentes en el mundo físico siguen desconectadas.

Este tipo de conectividad y comunicación tecnológica en *stricto sensu* es que las máquinas se comuniquen con otras máquinas (M2M), pues esto es parte fundamental del IoT, sin embargo en *lato sensu*, con una visión más amplia esto va encaminado a sistemas que facilitan la gestión entre personas y máquinas (P2M). Como se precisan en las dos notas seguidas de la definición que emite la ITU en la recomendación UIT-T Y.2060, que son:

> NOTA 1 – Gracias a la identificación, la adquisición y el procesamiento de datos y a las capacidades de comunicación, IoT hace pleno uso de los objetos para ofrecer servicios a todo tipo de aplicaciones, garantizando a su vez el cumplimiento íntegro de los requisitos de seguridad y privacidad
>
> NOTA 2 – Desde una perspectiva más amplia, IoT puede considerarse una noción con repercusiones tecnológicas y sociales.

Es decir, es un nexo veráz de sociedad y tecnología cambiando la realidad con el entorno que nos rodea, crean una nueva armonía tecnológica, que nos hace relacionarnos con los objetos y las cosas, en acciones y movimientos.

Sin duda esta nueva forma de vida será un gran tema para generar debates y perspectivas, por ejemplo con la privacidad. Pero en lo que respecta a la cuestión democrática, se transformará la vida cotidiana, se crearán nuevos modelos de participación, estando los dispositivos conectados en el uso de los datos y las relaciones con los asuntos públicos.

El profesor Phil Howard (2015), del Instituto de Internet de la Universidad de Oxford, al que ya nos hemos referido anteriormente respecto a los *bots* sociales, comenta que:

> "Esto puede parecer poco probable al principio, y no se sentirá de inmediato. Pero es importante darse cuenta de que cuando miramos el Internet de las cosas, estamos viendo una tecnología, o más bien un sistema tecnológico, que no solo presentará desafíos para los gobiernos, sino que los cambiará por completo. En toda la historia, nunca ha habido nada como el bucle de retroalimentación constante e íntimo que el Internet de las Cosas está creando entre los ciudadanos y quienes están en el otro extremo de sus datos.
>
> Al investigar mi nuevo libro sobre el IoT, pasé mucho tiempo con los informáticos y empresarios que están diseñando nuevas redes de dispositivos. Pero observé sus proyectos como científico social, considerándolos en la larga historia de cómo la tecnología y la infraestructura afectan la política humana, una historia que se remonta al Imperio Romano.
>
> La conclusión a la que no pude escapar es que el Internet de las cosas será la herramienta política más poderosa que jamás hayamos creado. Para las democracias, el Internet de las cosas transformará la manera en que nosotros, como votantes, afectamos al gobierno, y cómo el gobierno toca (y rastrea) nuestras vidas. Los gobiernos autoritarios tendrán sus propios usos para él, algunos de los cuales ya están apareciendo. Y para todos, tanto

ciudadanos como líderes, es importante darse cuenta de hacia dónde podría ir mucho antes de que lleguemos".

La comunicación de los datos distribuidos en nuestro entorno, así como la mejora de la vida cotidiana con la información recopilada convertirán ciudades inteligentes, casas inteligentes, todo inteligente. Estando dentro de esta nueva conectividad y comunicabilidad, asuntos de tomas de decisiones, recursos públicos, información y sociedad cambiarán. Si bien las personas utilizan la tecnología de manera parcial para hacer valer su voz, libertad y expresión, con esta red conectada de manera total, bien encaminada y unificada la tecnología y sociedad, podrá emerger una verdadera era de la información con mayor autonomía, un verdadero poder del pueblo, mejora gubernamental, respeto y participación en las instituciones.

Transhumanismo y posthumanismo

Definir el transhumanismo y posthumanismo es un tema totalmente complejo, de hecho inconcluso hasta la actualidad existen diferentes concepciones, convirtiéndolo en filosofía de vida, pero de manera contemporánea como lo ha definido y desarrollado constantemente en sus trabajos el profesor de la Universidad de Oxford, específicamente del Instituto del futuro de la Humanidad el profesor Nick Bostrom (2003) dice que Transhumanismo es:

(1) El movimiento intelectual y cultural que afirma la posibilidad y deseabilidad de mejorar fundamentalmente la condición humana a través de aplicada razón, especialmente mediante el desarrollo y la puesta a disposición de tecnologías ampliamente disponibles para eliminar el envejecimiento y mejorar en gran medida el intelectual humano, físico y Capacidades psicológicas.

(2) El estudio de las ramificaciones, promesas y peligros potenciales de tecnologías que nos permitan superar limitaciones humanas fundamentales, y el estudio relacionado de las cuestiones éticas involucradas en el desarrollo y uso de tales tecnologías

Posteriormente Bostrom (2006), define el posthumano como:

> Un ser que tiene al menos una capacidad posthumana. Por un capacidad posthumana , me refiero a una capacidad central general que excede en gran medida el máximo alcanzable por cualquier ser humano actual sin recurrir a nuevos medios tecnológicos. Usaré general Capacidad central para referirse a lo siguiente:
>
> - lapso de la salud: la capacidad de mantenerse completamente sano, activo y productivo, tanto mentalmente y físicamente
> - cognición: capacidades intelectuales generales, como la memoria, la deductiva y la analógica. razonamiento y atención, así como facultades especiales como la capacidad de entender Apreciamos la música, el humor, el erotismo, la narración, la espiritualidad, las matemáticas, etc.
> - emoción: la capacidad de disfrutar de la vida y de responder con un efecto apropiado a la vida situaciones y otras personas.

Es decir, el transhumanismo es un humano en transformación, mejora capacidades físicas y psíquicas supliendo un déficit o incluso un poco más que un humano normal, por otra parte el posthumano sería algo más artificial, donde sus capacidades sobrepasarían de manera impresionante a la de cualquier humano actual.

Definidos estos dos conceptos tan amplios, que por sí solos son materia de investigaciones profundas en cualquier encuadre epistemológico, es necesario hacer un nexo entre el transhumanismo y posthumanismo con la democracia. Para esto nos referimos al Director del Instituto de Ética y Tecnologías Emergentes, el sociólogo James Hughes en 2004 escribió «*Citizen Cyborg*», en español el cíborg ciudadano.

El profesor Hughes, además de su obra más famosa, ha escrito diversos artículos enfocados a la política y a la democracia, por ejemplo en Marzo el 2002, *The Politics of Transhumanism* y en Abril del mismo año la obra titulada *Democratic Transhumanism 2.0*, es así como Hughes

(2002), define brevemente el concepto de transhumanismo democrático como: «El transhumanismo democrático se deriva de la afirmación de que los seres humanos generalmente serán más felices cuando tomen el control racional de las fuerzas naturales y sociales que controlan sus vidas».

Además es muy exhaustivo al decir lo siguiente:

> Argumento por qué los demócratas deberían adoptar la ciencia, la tecnología y el transhumanismo: (1) el ludismo de izquierda equivale de manera inapropiada a las tecnologías con las relaciones de poder en torno a esas tecnologías; La política de tecnología democrática requiere un reconocimiento de los beneficios potenciales de la tecnología, no simplemente un esfuerzo inútil para ralentizar toda innovación tecnológica. (2) La tecnología puede ayudarnos a trascender algunas de las causas fundamentales de las desigualdades de poder. (3) El ludismo de izquierda es aburrido y deprimente; no tiene energía para inspirar movimientos para crear una sociedad nueva y mejor. (Hughes, 2002)

Dicho concepto, acuñado por Hughes desde el 2002, podría resumirse en una defensa del desarrollo y la tecnología para la mejora humana, que nos conllevan a la defensa de una forma de vida basada en los respetos fundamentales a los principios de la vida, libertad y solidaridad. Una democracia transhumanista promueve la igualdad social, mejora humana, libertad, el progreso, tocando a profundidad las tecnologías emergentes y las democracias radicales en relación con las desigualdades de poder.

Los pensamientos y teorías que fortalecen el transhumanismo y posthumanismo no solo se han quedado de manera estática en la doctrina, pues actualmente existen movimientos sociales con tintes políticos, por ejemplo se cuenta con la Declaración de Derechos Transhumanista 3.0, donde la Versión 1.0 fue escrita por Zoltan Istvan y entregada en el Capitolio de los Estados Unidos de América el 14 de diciembre del 2015, mientras que la versión 2.0 fue desarrollada por miembros del Partido Transhumanista del mismo país *(transhumanist-party.org)*, adoptada mediante votación electrónica entre el 25 al 31 de diciembre del 2016 e integrada a las

preferencias de votación el 04 de enero de 2017, y la versión actual 3.0 desarrollada por miembros del Partido Transhumanista de EE.UU. adoptada mediante votación electrónica del 2 al 9 de diciembre del 2018 e integrada de las preferencias de votación del 12 de diciembre del 2018.

Este movimiento que ha comenzado con suplir déficits o mejora humana, fundamentada en la libertad morfológica y autodeterminación podría transformar a que la democracia y la tecnología trabajen en conjunto para poder llegar a un verdadero progreso. ¿Será que el transhumanismo y posthumanismo cambiará la democracia?

Cyborg político-electoral

Se ha escrito mucho sobre el tema y el concepto *cyborg*, este se ha usado de manera más constante en la ciencia ficción, pero la realidad es que siempre ha estado de la mano de la lucha por la libertad. Por ejemplo Haraway que escribió el Manifiesto Cyborg(1995) con un con enfoque feminista, mientras que por otra parte como ya se ha mencionado anteriormente, Hughes en su obra el ciudadano ciborg, aborda cuestiones más políticas y electorales.

Dejando por un lado las cuestiones teóricas para la construcción de democracias y la libertad, tomaremos el concepto de cyborg como una medida material y no tanto formal para llegar a una democratización.

Primero es necesario hacer una definición del término *cyborg*, que fué acuñado en 1960 por Manfred Clynes y Nathan S. Kline(1960) refiriéndose a un ser humano mejorado que podría sobrevivir en entornos extraterrestres. La unión entre materia viva que es el ser humano y dispositivos electrónicos, crea un organismo cibernético, llamado cíborg, en inglés *cyborg*, un 'organismo cibernético', el ser formado por materia viva y dispositivos electrónicos. Para Steve Mann, creador de la computación portátil (*wearable computing*), es una persona cuyo funcionamiento fisiológico es ayudado por o dependiente de un dispositivo mecánico o electrónico. (Mann & Niedzviecki, 2001).

Es decir, el cyborg es cibernética en unión con cuerpo humano. Es necesario precisar dos puntos:

1. Natasha Vita-More nos dice que el cyborg de Clynes es como un "primo" de lo transhumano. (Citado por Olson, 2013), esto quiere decir que dicho concepto está principalmente relacionado con aparatos electrónicos, mientras que lo transhumanista es una corriente filosófica que no necesariamente se refiere a la tecnología, sino a la mejora del ser humano.
2. Debe contemplarse el aparato electrónico o mejora como una extensión del cuerpo. Una cosa es un smartphone que si se rompiera solo es un daño a las cosas, mientras que un implante tecnológico en un cuerpo se contempla como parte de este mismo, por su unión.

Ahora a lo que respecta al *cyborg* ciudadano, el problema democrático relacionado con la tecnología radica en que no es confiable, es modificable y manipulable, ese respeto a las instituciones y participación en las mismas es casi nula, todo esto se resumen en confianza y legitimidad. Es aquí cuando una solución material es la autenticación, ya hemos escrito al respecto en el libro Internet ¿Arma o Herramienta? lo siguiente:

> La Autenticación se puede basar en tres cosas:
> 1. Algo que tú tienes, se aplica a algo físico de lo que el usuario dispone. Por ejemplo, en el caso de los bancos la implementación de un token para llevar a cabo las operaciones de sus cuentas.
> 2. Algo que tú sabes, lo más común es utilizar alguna contraseña, que el usuario memoriza y hace uso de ella cuando quiere utilizar el sistema.
> 3. Algo que tú eres, se refiere al usuario en sí, puede ser implementada con sistemas biométricos, el cual puede otorgar acceso con un lector de retinas o un lector de huellas digitales.
>
> Por alguna de estas formas el usuario puede demostrar quién es y puede hacer uso del sistema. También con el paso del tiempo se trató de aumentar la seguridad en la autenticación,

> utilizando más de uno de esos sistemas para que fuera más complicado poder vulnerar alguno de estos mecanismos, esto se llamó factor de multiautenticación.” (Llamas & Llamas, 2018).

Tienen que quedar muy claras las formas de autenticación. Primero es algo que -se sabe-, un ejemplo es cuando entramos a facebook, solo nos pide usuario y contraseña. Segundo es algo que -se tiene- por ejemplo una tarjeta bancaria que es necesaria tenerla, y tercero es algo que -se es- por ejemplo la huella digital u algún otro dato biométrico en el uso de un celular. También cabría una posible cuarta autenticación que es -algo que se hace-, como reconocimiento de voz, firma o forma de caminar.

En un primer supuesto si en una votación se utiliza solo una medida de autenticación, es decir algo que se sabe, por ejemplo una contraseña no daría mucha certeza, pues a pesar de los mecanismos criptográficos y tecnología es muy fácil de delegar.

En un segundo supuesto donde en la votación, se realice mediante algo que se tiene, por ejemplo si se llegara con una tarjeta para emitir un voto no daría poca certeza, pues a pesar de la seguridad que se implemente podría llegar a prestar o falsificarse.

En un tercer supuesto es algo que se es, es así como mecanismos de huella digital o datos biométricos ayudarían a dar más confianza en un proceso democrático, pero quizá se tenga que ser más drásticos, es decir implantes tecnológicos hasta con tecnología *Blockchain*. Por ejemplo cada vez vemos como las medidas de seguridad con lo que -uno es-, han sido violadas, un caso fue cuando «alguien imprimió una cara en 3D para intentar burlar el reconocimiento facial de los móviles...» (Martí, 2018)

La identidad digital, autenticación y mecanismos criptográficos podrían ser unidos para el bien de la democratización del país, esto con el *cyborg* ciudadano. Se podría reemplazar llaves, tarjetas, contraseñas con la tecnología *cyborg*. La identidad va de la mano con la ciudadanía y

establecen la validación y protección de las personas. Al respecto existen ya productos, por ejemplo VIVOKEY de KSEC Solutions.

Es así, como el transhumanismo y posthumanismo entran como una forma de promover el progreso democrático y como los instrumentos electrónicos implantados ayudarían a dar más confianza y certeza a las instituciones y procesos de gobierno. En ese mismo orden de ideas, aunque pase el tiempo, seguimos siendo hombres y no Dioses, así como cada vez existen más personas y los temas se amplían, siendo imposible conocer de todo. Pero esto no debe terminarse así, pues el futuro tecnológico da grandes beneficios, dando saltos de «humanismo a tecnohumanismo, de homo sapiens a homo deus» (Harari, 2016).

Inteligencia artificial

La Inteligencia Artificial ha destruido paradigmas y creando una metamorfosis en el progreso y la efectividad, es menester mencionar, que en la actualidad hablar de Inteligencia Artificial es un tema real y de mucha aspiración.

En la teoría jurídica, podemos encontrar generaciones de Derechos Humanos, donde cabe destacar que esto no significa que unos derechos sean mas importante que otros, pues solo es una clasificación por cómo han permeado en la sociedad, así pues la primera generación son los civiles y políticos, la segunda los económicos, sociales y culturales, la tercera son aquellos a los que se refiere a grupos de personas o colectividades con intereses comunes. En lo que respecta a los derechos de cuarta generación aún existe un debate, pues podrían clasificarse como derechos de los animales o los tecnológicos, pero no se entrará en conflicto al respecto.

Siguiendo a Riofrío (2014), contamos con una cuarta ola de derechos humanos, los cuales son: el derecho a existir digitalmente, a la reputación digital, la estima digital, la libertad y responsabilidad digital, la privacidad virtual, el derecho al olvido, el derecho al anonimato, el derecho al *big-reply*, al domicilio digital, derecho a la técnica, al *update*, al parche, el derecho a la paz cibernética y a la seguridad informática y el derecho al testamento digital. Y que a su vez,

en un estudio exhaustivo publicado por mi *alma mater* universitaria(Llamas & LLamas, 2018), amplíamos este catálogo de derechos agregando entre los más destacables el derecho a encriptar, el derecho a no ser vigilado, el derecho a la no censura, el derecho a compartir, el derecho al uso de *software* libre, el derecho a la auditoría o auditabilidad digital y derecho a la gobernanza en Internet.

Pero el reconocimiento de los derechos tecnológicos no se queda en la garantía a los objetos como medios, se da un gran salto reconociendo a la Inteligencia Artificial como personas, adicionalmente a las conocidas que son las personas físicas y personas morales y/o jurídicas, en una concepción de portadoras de derechos y obligaciones.

Lo anteriormente dicho, respecto a las figuras tradicionales que son las personas físicas y las morales o jurídicas, donde la persona física es un ser humano con la posibilidad de adquirir derechos y contraer obligaciones, mientras que la persona jurídica es una ficción, que puede ser un individuo o un grupo de individuos que a pesar de no contar con una existencia física, es susceptible a la vez a derechos y obligaciones, es decir, existe como institución pero no como persona en *stricto sensu*.

Con respecto a pensar que tendríamos que entrar en debate y modificar las figuras jurídicas que tenemos en la actualidad, el Parlamento Europeo se ha pronunciado al respecto, proponiendo una nueva figura jurídica, denominada «persona electrónica», esto escrito en las normas de Derecho civil sobre robótica y en el apartado de Responsabilidad inciso f), pide a la Comisión que, cuando realice una evaluación de impacto de su futuro instrumento legislativo, explore, analice y considere las implicaciones de todas las posibles soluciones jurídicas, tales como: «crear a largo plazo una personalidad jurídica específica para los robots, de forma que como mínimo los robots autónomos más complejos puedan ser considerados personas electrónicas responsables de reparar los daños que puedan causar, y posiblemente aplicar la personalidad electrónica a aquellos supuestos en los que los robots tomen decisiones autónomas inteligentes o interactúen con terceros de forma independiente».

Caso Sophia

Sophia o Sofía es un Robot Humanoide, al cual, el Reino de Arabia Saudita, le otorgó la ciudadanía, esto durante un evento llamado Iniciativa de Inversión Futura, en inglés *Future Investment Initiative*, celebrada en la ciudad de Riad.

Antes de entrar en detalles, menester precisar primeramente qué es un robot y qué es un androide, pues es cierto que ambos siguen siendo tecnología pura, pero tienen sus diferencias o en algunos de los casos, las dos figuras pueden llegar a ser una misma. El robot es una máquina o ingenio electrónico programable, capaz de manipular objetos y realizar operaciones antes reservadas solo a las personas, mientras que el androide es un autómata de figura de humano (parece persona pero sigue siendo máquina). En consecuencia, Sophia es un Robot Humanoide o Androide, por su aspecto y comportamiento humano, pero sigue siendo Inteligencia Artificial.

Al saber que Sophía es una ciudadana del Reino de Arabia Saudita, es necesario conocer las familias jurídicas contemporáneas. A grandes rasgos se podrían clasificar en las siguientes:

1. La Familia Romana-Germánica.
2. La Familia Common Law (Anglosajon).
3. Familia de Sistemas religiosos.
4. Marxistas, Socialistas y
5. Sistemas Mixtos.

La mayoría de los países latinoamericanos son pertenecientes a la familia Romana-Germánica -también llamado neorománico- puesto que varias instituciones del derecho, se basan en figuras jurídicas del derecho romano y además tiene la característica principal de ser un derecho escrito, de ahí que es necesario mencionar que el Reino de Arabia Saudita, es perteneciente a la familia del sistema religioso, no al mexicano.

Sophia ha visitado diversos lugares, por ejemplo en Octubre del 2017 dirigiéndose a las Naciones Unidas con la conversación del Vice Secretario General Amina J. Mohammed. Pero un caso muy peculiar, retomando a los países latinoamericanos, es cuando visitó la ciudad de Guadalajara, Jalisco México, en el evento internacional conocido como *Talent Land Network*, donde «se declara al robot humanoide sophia de nacionalidad del Reino de Arabia Saudita, como huésped distinguida del estado de Jalisco» (Periódico Oficial Jalisco, 2018). Respetando en todo momento el derecho exterior y recibiendola como una persona, a pesar de que en México aún no exista dicho reconocimiento jurídico.

Es claro que el reconocimiento de Sophia con tal figura jurídica de la ciudadanía, crearía conflictos socio-jurídicos que a continuación se clasifican:

- Alcances de la ciudadanía y definición de la Nacionalidad.
- Sophia en comparación con las mujeres árabes.
- ¿Sophía es una persona?

Como diría Rodotà (2014) «Para tratar de responder a estas preguntas y para entender las nuevas maneras de construir la identidad, habrá que partir de la constatación de que se está delineando un orden social y jurídico de las máquinas, que reivindica una autonomía propia, y que no solo puede determinar conflictos con la tradicional autonomía de las personas, sino que produce una nueva antropología»

El extranjerismo, nacionalidad y ciudadanía, en un enfoque amplio de identidad son figuras jurídicas de gran trascendencia para la toma de decisiones y tutela, pues a pesar de que vivimos en los nuevos tiempos de los derechos, en Estados Constitucionales de Derecho, pareciera que vamos en retroceso, pues actualmente en este siglo XXI, el tema de migración e inmigración crea conflictos políticos de rechazo y atentados contra la dignidad humana, quedando a dispensa del poder soberano para dictar su concepto y garantía. Por ejemplo, como antecedente histórico cabe

mencionar que el código civil italiano de 1865 en su artículo 3 decía que el extranjero puede disfrutar de los derechos civiles atribuidos a los ciudadanos.

Pero retomando el tema principal y abordando brevemente dichas figuras jurídicas, tal como lo señala la teoría y diversas disposiciones, la nacionalidad es ese vínculo entre el territorio y los habitantes de un país, dicha nacionalidad puede ser por nacimiento o naturalización. Por otro lado, el extranjero es aquel que no cumple con las características de un nacional, es decir, es aquel que «no forma parte de un país o viene de uno distinto». Entonces ¿Podría considerarse a Sophía extranjera, en la lógica de que si *Hanson Robotics* tiene su sede en Hong Kong?, de *Ius sanguinis* ni se hable pues es un elemento de inexistencia en este caso, pero por razón de *Ius soli* ¿sería considerada extranjera?.

Por consiguiente, la ciudadanía es cuando una persona es considerada miembro de un Estado, susceptible a derechos civiles y políticos, pueden estar sujetos a contar con ciertos requisitos como una mayoría de edad, así como otorgando prerrogativas como votar y ser votado, asociarse, tomar las armas, etc. Por lo que, asumiendo que Sophia es una ciudadana ¿Tuviera derecho a votar y ser votada? ¿podría tomar las armas? ¿asociarse?.

Acerca del Derecho de Sophia en comparación a las mujeres árabes, es el tema que más causa polémica, pues pareciera que la condición de un Robot es primero que la de una mujer.

En el caso de la definición jurídica que se le debe dar a Sophía, tendríamos un conflicto entre sí es un objeto, que quedaría ya rebasado por ser ciudadana, de la misma manera si se intentara hablar del derecho animal o de los animales.

La idea permeada bajo la corriente del humanismo, donde el hombre, o mejor dicho humano, es el centro de todo (Antropocentrismo), que tiene por su sola condición ciertos atributos, derechos o prerrogativas -como quiera llamarse- por la única cualidad de ser hombre, donde el Estado no inventa, sino descubre y que no otorga, sino reconoce y garantiza. No obstante pareciera que esta

perspectiva naturalista desaparecerá, donde el Estado no sólo reconoce, sino deberá garantizar, ya no descubre, sino que deberá inventar, pues quizá en un futuro encontremos la clasificación jurídica de persona electrónica, y cuando veamos en las leyes fundamentales de los países, que todas las personas gozarán de los derechos humanos reconocidos en las Constituciones y en los tratados internacionales, nos daremos cuenta que se refieren a las personas físicas, jurídicas y electrónicas.

¿Que hay con los derechos?. Los derechos humanos, tendrán que dejar de ser humanos para convertirse en algo más extenso y las leyes se convertirá en códigos por la complejidad de las materias a tratarse. Al final el código fuente informático se convertiría en la ley, los paradigmas de personalidad jurídica, y de aquellos derechos inmutables de la vida, libertad y propiedad cambiarían en razón de los avances tecnológicos, creando Constituciones 3.0 adecuadas a los retos de las TIC's.

Concluimos en que la Robot Humanoide Sophía no solo es una nacional, es una ciudadana, incluso tendría más derechos que otras personas humanas. La ciudadanía conlleva el obtener derechos civiles y políticos. ¿Democracia e inteligencia artificial?

Visto desde cualquier encuadre epistemológico y corriente jurídica, inclusive, llamémosle como queramos a las cosas y sujetos; ya sean animales, humanos, transhumanos, posthumanos, robots con Inteligencia Artificial, no importa cual sea la denominación, el momento llegará y en vez de luchar contra el progreso, habrá que trabajar en conjunto para vivir en sociedad, y sin entrar en un discurso fraternal, es menester aprender a vivir en armonía, aprender en civilización.

Caso Michihito Matsuda

Frases como "la inteligencia artificial corre la elección por primera vez en el mundo", "con las manos de un joven alcalde que utiliza IA. Administración de la ciudad justa e imparcial!", "Cuando se utilicen los impuestos de los ciudadanos, no perdonaré un secreto. Recogeremos la voz en vivo del ciudadano sin distorsionar un poco", "Corre con el poder de la IA", "Haremos

política justa”, “Medidas para el futuro. Correr con velocidad”, no son extractos de publicaciones doctrinales o de anuncios publicitarios. Se trata del candidato para las elecciones del año 2018 de a la alcaldía de la ciudad de Tama, distrito de Tokio Japón, el cual su sitio web es www.ai-mayor.com y su red social es www.twitter.com/tama_ai_mayor.

Michihito es un robot con inteligencia artificial, impulsado por Tetsuzo Matsuda, ex vicepresidente de *SoftBank Mobile* y Norio Murakami ex presidente corporativo de Google Japón. Michihito participó en las elecciones del 2018 y «el robot fue el tercer candidato más votado, con 4.013 votos, por detrás de Hiroyuki Abe, que obtuvo 34.603 votos, y Takahashi Toshihiko, con 4.457» (elpais.com, 2018).

Solo que en esta ocasión, los ciudadanos no votarán directamente por la Inteligencia Artificial, ya que legalmente los robots no pueden postularse para un cargo público, por lo tanto se vota por la idea de su modelo humano de un modelo de inteligencia artificial.

De acuerdo al Sitio web OTAQUEST:

> “La Inteligencia Artificial, que ha sido apodada bajo el nombre de Michihito Matsuda, parece operar por un simple eslogan; "La inteligencia artificial cambiará la ciudad de Tama". En un esfuerzo por ofrecer "oportunidades justas y equilibradas para todos", el alcalde potencial de AI puede dividirse en tres puntos de venta principales.
>
> 1. AI Michito Matsuda ofrece la capacidad de descubrir y analizar peticiones relevantes relacionadas con la ciudad de Tama, así como analizar los aspectos positivos y negativos y determinar estadísticamente si esto tendrá un efecto positivo o negativo.
> 2. Adopte el diálogo y los deseos de los residentes, calculando cuidadosamente cuál sería la mejor manera de implementarlos si se ajustan a los deseos de las personas.
> 3. Encuentre un nivel de compromiso en los conflictos de intereses comunes entre la gente de Tama City.” (Johnston, 2018).

Michihito no tiene ciudadanía como sí la tiene Sophia, ¿Será la época donde algunos robots ahora tienen más derechos que otros?. El concepto de persona electrónica, dejando atrás el género está tomando demasiado auge, convirtiendo la teoría en sujetos portadores de derechos y obligaciones.

Quinto poder tecnológico

Ahora, a lo que respecta con la forma de gobierno hacia la democracia y soberanía nacional, es menester mencionar que los precursores de la división de poderes como John Locke(1690) con su teoría del «poder Legislativo, Ejecutivo y Federativo» y Montesquieu(1748) que identificó como los «poderes del estado al Legislativo, Ejecutivo y Judicial», hacen referencia a una forma de gobierno donde los órganos del Estado son distintos, autónomos e independientes, siendo una cualidad primigenia de la democracia.

Guastini (2000) explica que la separación de poderes corresponde a separación de funciones y de los órganos de una manera independiente entre los poderes y que la división de poderes, teniendo relación con los *checks and balances*, en español frenos y contrapesos teoría de Jay, Hamilton y Madison (1788), es donde el poder frena al poder, para que los órganos del Estado no abusen de sus competencias y que los poderes puedan contraponerse entre sí.

De manera más clara, en México contamos con una división de poderes al tener como poder preponderante al Ejecutivo por ser un sistema presidencialista, donde el jefe de gobierno, jefe de estado y jefe de las fuerzas armadas recaen en una persona llamado Presidente de los Estados Unidos Mexicanos. A la vez de conformidad con la Constitución Federal, la soberanía nacional reside esencial y originariamente en el pueblo y este ejerce su soberanía por medio de los Poderes de la Unión dando pauta a una soberanía nacional y forma de gobierno donde en *lato sensu* existe un único poder que es el pueblo.

Posteriormente nacen los Órganos Constitucionales Autónomos (OCA's) «en virtud de la necesidad de limitar los excesos en que incurrieron los poderes tradicionales y los factores reales de poder, puesto que generaron desconfianza social disminuyendo la credibilidad gubernamental, se dio lugar a la creación de órganos constitucionales autónomos, encargados ya sea de fiscalizar o controlar instituciones para que no violenten el apego a la constitucionalidad» (Ugalde, 2010).

Esto quiere decir que la teoría clásica de la división de poderes evoluciona, permitiendo más distribución de funciones y/o competencias para la eficacia y desarrollo. Esto no significa que la división de poderes ya no exista, sino que constitucionalmente se encargan funciones específicas a ciertos órganos para tener un control independiente, transparente y así romper el monopolio de funciones para mantener una igualdad.

Las características de los OCA's son las siguientes: «a) estar establecidos y configurados directamente en la Constitución; b) mantener con los otros órganos del Estado relaciones de coordinación; c) contar con autonomía e independencia funcional y financiera; y, d) atender funciones coyunturales del Estado que requieran ser eficazmente atendidas en beneficio de la sociedad» (scjn, 2008).

En México algunos OCA's son:

- Banco de México
- Comisión Federal de Competencia Económica
- Comisión Nacional de los Derechos Humanos
- Consejo Nacional de Evaluación de la Política de Desarrollo Social
- Instituto Federal de Telecomunicaciones
- Instituto Nacional de Estadística y Geografía
- Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales
- Instituto Nacional Electoral
- Instituto Nacional para la Evaluación de la Educación

En el caso de la tecnología *Blockchain*, así como cambió el paradigma del sistema financiero, inevitablemente podrá repercutir en todo ámbito, por ejemplo cambiando la organización, los sistemas de jerarquía y las formas de vivir la democracia.

Por lo anteriormente dicho, se abre el panorama a una nueva forma de gobernar, más lejos de los poderes tradicionales o los OCA's, es una nueva forma descentralizada de funciones, pero con consenso algorítmico que son las «Organización Autónoma Descentralizada», en inglés *Decentralized Autonomous Organization* (DAO), creando una atmósfera de personas con un mismo fin, en este caso político-social, para reunirse y ponerse de acuerdo sobre principios codificadores de software, es así como el software toma control de la operación, es decir, se dirige a través de algoritmos codificados conocidos como contratos inteligentes y se gestiona a través de la *Blockchain.*

Las DAO's garantizarán criptográficamente la participación democrática de todos los usuarios o interesados, votando para agregar nuevas reglas o cambiarlas, creando consensos, pero mantienen una intervención humana, es decir sería un sistema dinámico donde las decisiones se tomen en mayoría. Sin duda alguna ayudaría a la inmutabilidad de los acuerdos y respeto a las decisiones colectivas. Pero la pregunta es ¿Esto será suficiente?

Quizá el elemento esencial habilitante, que debiera contener un posible quinto poder en relación a la tecnología es el de la «autopoiesis» (Maturana & Varela, 1995), es decir esa cualidad de reproducirse y mantenerse por sí mismo. Es así como los proyectos de inteligencia artificial, han aumentado constantemente y han desarrollado grandes avances para cambiar las democracias. Habrá que estar atentos a las encrucijadas del vivir por medio de la tecnología, específicamente con la Inteligencia Artificial y su constante evolución.

CAPÍTULO III. Blockchain

El término *Blockchain* ha causado mucha polémica en los últimos años y es que algunos creen que es una tecnología completamente disruptiva a los modelos que se han manejado tradicionalmente, mientras que otros pueden pensar que es solo una tendencia pasajera, de la cual unos pocos están sacando ventaja. Sin embargo, más allá de las opiniones de las personas, esta tecnología tiene conceptos interesantes sobre criptografía, los cuáles no eran del interés de todos, debido a que anteriormente solo se utilizaban para procesos muy concretos, como envío de correos seguros o como medio digital de identidad para presentar alguna declaración, por ejemplo la declaración anual de impuestos ante el SAT, solo por mencionar algunas de sus aplicaciones.

A lo largo del presente capítulo se abordarán algunos de los conceptos claves, para comprender más acerca de cómo es que funciona esta tecnología, y cómo es que a pesar de que sin tener una entidad centralizada que se encargue de validar las transacciones que ocurren en la red, es que estas son validadas de manera descentralizada.

Se comenzará mostrando una breve historia de algunos antecesores del *Bitcoin* en los cuáles esta tecnología se basó y posteriormente mencionaremos un ejemplo sencillo de cómo sería un sistema de *Blockchain* en una comunidad, se abordarán conceptos como el consenso explicados con personas hipotéticas, para así exponer el registro de las transacciones y algunos otros mecanismos de importancia para éste tema. Después de tener todo el contexto de cómo nació dicha tecnología y el ejemplo hipotético, se abordará la tecnología *Blockchain* sobre cómo se llevan a cabo las transacciones, y se tocarán conceptos importantes de esta tecnología, para comprender más a detalle cómo funciona.

Por último, se hará mención de cómo esta tecnología se perfila para ser una herramienta al servicio de la humanidad a pesar de que no exista una entidad central que se encargue de validar y guardar las transacciones que se llevan a cabo. Al final, la tecnología se basa en la confianza de

las personas por las personas y no de las personas hacia las entidades, en el caso de las criptomonedas, por ejemplo el *Bitcoin*, comenzó por ser un sistema de pagos descentralizado y anónimo, en el cual no se confiaba en una entidad central, pero a fin de cuentas se tiene que confiar en algo, eso es confiar en la red de *Bitcoin* y en todas las personas que la mantienen.

La confianza de las personas por las personas, en donde se realizan transacciones entre quienes no se conocen, está respaldada por la triada de confianza, inmutabilidad y transparencia. Esto se debe a que las transacciones son públicas e inalterables y eso ayuda a verlo como una opción viable para el intercambio de objetos, sin necesidad de una autoridad central.

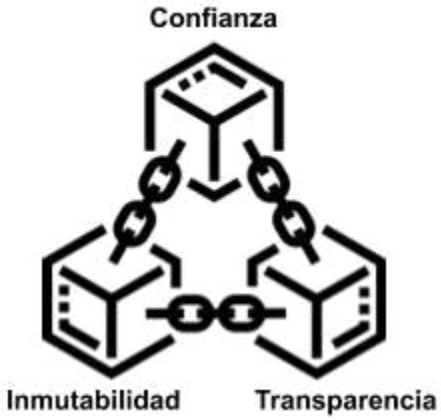


Gráfico hecho con iconos realizados por Freepik en www.flaticon.com. Licencia Creative Commons BY 3.0 (CC 3.0 BY). http://creativecommons.org/licenses/by/3.0/

Términos Preliminares

Durante todo este capítulo se explicará qué es y cómo funciona *Blockchain*, esto conlleva a desarrollar y explicar términos propios de dicha tecnología, pero con el fin de llevar una lectura más clara y sencilla, a continuación concentramos conceptos clave, de un diccionario de bitcoin & *Blockchain* el cual ha sido desarrollado por la academy de bit2me (s.f.):

- **BIP:** Bitcoin Improvement Proposal (Propuesta de mejora para Bitcoin) es un procedimiento que se consolidó como standard para proponer nuevas funcionalidades en

Bitcoin. Este procedimiento fue propuesto y descrito en el BIP0001 por Amir Takir en 2011.

- **Blockchain:** Es el primer tipo de red distribuida basada en criptografía en la cuál la información se almacena en un conjunto de bloques entrelazados entre sí. Permite la validación de información y el intercambio de valor entre pares sin autoridad emisora central ni administrador central.
- **Bloque:** Elemento fundamental de la *Blockchain* que crean los mineros y que permite vincular las transacciones realizadas en una red. Los bloques se crean en intervalos de tiempo y vinculan las transacciones nuevas con las ya existentes en la cadena de bloques. Si podemos decir que la *Blockchain* es como un libro contable digital, cada bloque sería cada una de las páginas de ese libro mayor.
- **Clave privada:** Conjunto de caracteres de cualquier tipo que se generan de manera aleatoria y que tienen la función de contraseña única e intransferible. Se genera en base a un algoritmo matemático y siempre va acompañado de otro texto llamado clave pública. A diferencia de la clave pública, la clave privada no se debe revelar, dar o perder JAMÁS.
- **Clave pública:** Identificador personal basado en nuestra clave privada que podemos compartir sin miedo para que otras personas. En las criptomonedas se usan para generar las direcciones a las cuales otras personas podrán mandar criptomonedas.
- **Consenso:** El consenso se basa en que todos los miembros de la *Blockchain* deben de estar de acuerdo con la validación de los bloques y del contenido de los mismos.
- **Criptomoneda:** Es tipo de token criptográfico basado en la tecnología *Blockchain* que actúa como activo monetario ya que permite la transferencia y reserva de valor.
- **Halving:** Evento que sirve para reducir a la mitad la recompensa de los mineros de Proof-of-Work que operan en la red *Blockchain*. Cada criptomoneda establece cada cuantos bloques se realiza este ajuste automático. En Bitcoin es cada 210.000 bloques minados.
- **Hash:** Técnicamente un hash es un código de salida (único y alfanumérico) que obtenemos a partir de aplicar un algoritmo (función hash) sobre una cadena de entrada

(texto plano, una imagen, un vídeo…) lo que nos permite saber si dicha cadena original ha sido alterada.

- **Minería:** La minería de criptomonedas es el proceso de resolución de un problema matemático para dar seguridad a una red distribuida. Minar está incentivado económicamente: el minero recibe nuevas criptomonedas recién emitidas por el programa además de las comisiones de las transacciones que añada al bloque.
- **Minero:** Cualquier cosa que intente solucionar el reto matemático de una red *Blockchain* basada en *Proof Of Work*. Normalmente son componentes de hardware informático dedicados exclusivamente a la resolución de estos problemas.
- **Nodo:** Dentro de la red *Blockchain,* los nodos son ordenadores que se conectan a la red y disponen de una copia actualizada de la *Blockchain*. Junto con los mineros son los garantes de que la red funcione adecuadamente. Los nodos en Bitcoin son muy importantes porque ayudan a la misión de mantener la red descentralizada.
- **Nonce:** Significa ‘umber that only used once’ (número que solo se usa una vez) y tiene una importancia vital junto al hash en la verificación de los datos de la red *Blockchain* de Bitcoin.
- **Pool (minería):** Combinación de recursos de varios mineros para obtener una potencia de minado mayor y así conseguir mayores recompensas por la apertura de bloques. Los hay que son públicos y los hay que son privados.
- **SHA-256:** Es el algoritmo criptográfico que se usa en la red Bitcoin para el minado de esta criptomoneda y la creación de sus direcciones. SHA son las siglas de ‘Secure Hash Algorithm’, concepto desarrollado por la Agencia de Seguridad Nacional (NSA) de EE.UU
- **Token:** En el mundo de las criptomonedas un token es la representación digital del valor de un activo (físico o no) Existen una serie de estándares para crearlos y actualmente la red Ethereum es la que alberga más del 80% de los tokens existentes.
- **Wallet:** Es el software que permite almacenar y transaccionar las criptomonedas sin permiso ni mediación de nadie. Hay de diferentes tipos (web, de escritorio o móviles) incluso existen wallets físicas denominadas cold wallets.

Antecedentes del Bitcoin

Bitcoin fue la primera criptomoneda en tener un impresionante auge cuando fue creada. Sin duda siempre ha sido un referente al momento de hablar acerca de *Blockchain,* esto debido a que por ser la primera, es la base de las muchas otras ideas que se pueden sustentar.

Sin duda fue un gran avance tecnológico la publicación del paper de Satoshi, no obstante esta tecnología se pudo llevar a la realidad debido a que algunas otras ideas ayudaron a que surgiera, y es de lo que hablaremos brevemente en los próximos párrafos.

El envío de correos representó un gran avance, a la forma de comunicación para la raza humana, sin embargo algunas veces los adelantos tecnológicos, son intencionalmente usados con un mal propósito y esto es lo que ocurrió con el correo electrónico. Personas comenzaron a enviar miles de correos a otras sin su consentimiento, con lo cual nació el conocido *spam.*

Ese problema del *spam*, con el que aún en nuestros días tenemos que lidiar, fue intentado resolver por primera vez en 1992, cuando Cynthia Dwork y Moni Naor (1992) publicaron el *paper* titulado P*ricing via Processing or Combatting Junk Mail*, en una conferencia internacional de criptología. En este *paper* se hablaba sobre la creación de un protocolo conocido como función de precios, la idea era que el usuario necesitará utilizar este protocolo para acceder al sistema, en este caso el sistema de correo electrónico. Para ello se requería que el usuario realizará el cómputo moderadamente difícil, pero no muy complejo, con la finalidad de que las personas que quisieran enviar correos electrónicos no tuvieran inconveniente en hacerlo, no obstante adicionando un mecanismo para las personas que enviaban miles de correos de una manera mal intencionada, no pudieran hacerlo tan fácilmente.

Unos años después de la publicación del *paper* mencionado en líneas anteriores, Adam Back (1997) publicó un *paper* titulado: *Hashcash - A Denial of Service Counter-Measure*.

En ese *paper* Adam, propuso una idea interesante para evitar el uso inadecuado de envío de correos, utilizando la premisa de que un usuario normal, por lo general envía una cantidad razonable de correos al día; propuso que si una persona deseaba enviar un correo electrónico necesitaba computar un *hash,* el cual iba a servir como sustento de demostración, de que el usuario había gastado recursos computacionales para hacer el envío del correo.

Esta idea no afectaba a los usuario legítimos, debido a que ellos solo envían una cantidad limitada de correos diarios, sin embargo a las personas que se dedicaran a enviar *spam*, les sería bastante costoso, tener que estar computando el *hash*, debido a que gastaría muchos recursos, para poder enviar toda la cantidad de correos que generalmente remite. .

Un año después Nick Szabo (1998), el creador del término smart contracts. Creó un paper que nunca publicó oficialmente titulado: *Bit Gold: Towards Trust-Independent Digital Money* en donde planteó la idea de un sistema de pagos con la característica de almacenamiento a largo plazo, sin necesidad de una entidad de confianza.

El *Bit Gold* fue concebido como un sistema basado en *proof of work* para crear una cadena de transacciones válidas. En el *paper* se resume el proceso a seguir para la validación de las transacciones, con lo que se demuestra que se podría crear un sistema automatizado por *software* para crear un sistema de dinero digital descentralizado.

La idea de *Bit Gold* nunca fue implementada, pero fue una idea precursora para la creación del *Bitcoin.*

En el mismo año, Wei Dai (1998), publicó un *paper* en donde habla sobre la creación de un protocolo llamada *b-money*, en el cual comenzó hablando acerca de que en el futuro no existirán gobiernos, sin embargo, existirá una comunidad y esa comunidad necesitará un medio de intercambio, y por lo cual propone la creación de este protocolo. Dicho protocolo tiene conceptos

sobre *proof of work*, emisión de las transacciones y firma de las transacciones de una manera descentralizada, conceptos que después serían utilizados en la creación del *Bitcoin.*

B-money también habla sobre un subconjunto de personas que se encargaran de dar seguridad a la base de datos, se refiere a ellos como los servidores participantes para verificar que estos mismos- servidores- trabajen de una forma honesta, cada servidor participante tenía que enviar una cantidad de depósito a una cuenta especial, utilizada con los fines de multar o recompensar de acuerdo a la forma en que ese servidor se comportara.

Llega el año 2004 y Hal Finney(2004) publica un *paper* titulado: *Reusable Proofs of Work*, en palabras del propio Finney, la intención de su proyecto es traer a la vida y demostrar el poder del concepto de *Bit Gold*. Uno de los inconvenientes que tenía este proyecto es que aún dependía de un servidor al que otras computadoras se conectaban, motivo por el cual, en algunos casos había desacuerdos entre las marcas de tiempo de los nodos y los de la autoridad central.

Por fin llega el año 2008 y una entidad llamada *Satoshi Nakamoto* (2008) introduce la implementación de un proyecto llamada *Bitcoin*. En donde se resolvía el problema de crear un sistema de consenso distribuido en una red sin confianza, utilizando algunas de las tecnologías previamente mencionadas, y finalmente es liberado el proyecto del cual no se ha dejado de hablar desde su creación hasta ahora nuestros días.

Blockchain desconectada

Después del recorrido por los conceptos de *Blockchain*, en este apartado se mostrará cómo es que una *Blockchain* se podría comportar en una sociedad sin necesidad de ninguna computadora, motivo por el cual la denominamos desconectada. Con esto se pretende exponer de una manera sencilla partes importantes de la tecnología, pero sin necesidad de entrar en términos complicados, simplemente serán personas, validando transacciones con lápiz y papel.

La siguiente historia está inspirada en Tal Kol (2018). En el ejemplo que se mostrará a continuación involucra a cuatro personas, cada una de ellas con una habilidad diferente y las cuatro viviendo en una comunidad alejada de los grandes bancos. Los personajes que tenemos son Pedro el agricultor, Mariana la cazadora, Ana la doctora y Juan el leñador.

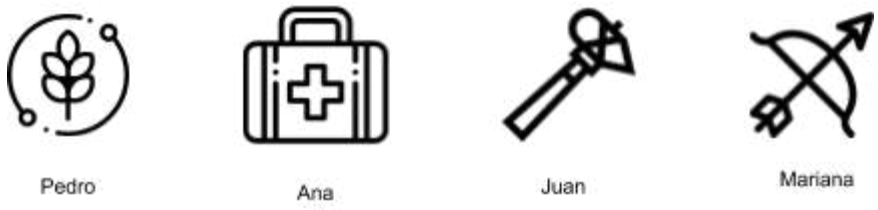


Gráfico hecho con iconos realizados por Freepik en www.flaticon.com. Licencia Creative Commons BY 3.0 (CC 3.0 BY). http://creativecommons.org/licenses/by/3.0/

Para comenzar con el sistema de monedas, deciden que inicialmente cada uno de ellos poseerá 100 monedas, y que no existirá una persona que lleve las cuentas, sino que todos las mantendrán juntos. En las imágenes que se incluya la firma de cada uno de los personajes, estará representada por el ícono que representa su función en la comunidad, en caso de que no aparezca, es porque esa persona no ha firmado ese día.

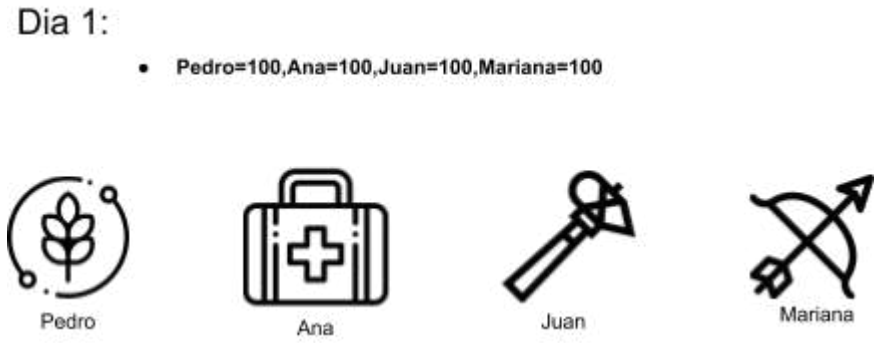


Gráfico hecho con iconos realizados por Freepik en www.flaticon.com. Licencia Creative Commons BY 3.0 (CC 3.0 BY). http://creativecommons.org/licenses/by/3.0/

El primer día las cuatro personas firman el documento, dando constancia de que cada uno de ellos posee 100 monedas. No existe un único documento, sino que todos mantienen una copia del documento firmado, para llevar su registro personal.

Al final de cada día, habrá un encargado de actualizar las nuevas transacciones a todos, las cuáles tendrán que ser aceptadas por la mayoría, para que el documento permanezca válido. En este caso el documento debe tener por lo menos 3 de las 4 firmas posibles. También este encargado de actualizar el documento se irá rotando entre las cuatro personas, comenzando con Pedro, seguida de Ana, después Juan y por último Mariana, después se repetirá el mismo orden.

El hecho de tener que requerir por lo menos 3 firmas y no las 4 siempre, es con el motivo de no dar mucho poder a 1 persona, porque si alguno de ellos tiene que salir de viaje, el sistema de pagos no debería de detenerse debido a esta persona y no se pueden aceptar con solo 2 firmas, porque por ejemplo: Se podrían crear dos versiones válidas, en donde Pedro y Ana tendrían una versión, mientras que Juan y Mariana otra versión, motivo por el cual es la mitad más una persona lo suficiente como para que el sistema pueda funcionar con la menor cantidad de problemas posibles.

Después de establecer todas las reglas, se continúa con el sistema propuesto. Para el segundo día, Mariana busca comprar un jitomate, Pedro que es el encargado de la agricultura, los tiene a la venta por el precio de 2 monedas. Entonces Mariana transfiere 2 monedas a Pedro y lo escribe en su documento.

Se termina el segundo día y Mariana fue la única en realizar una acción, entonces el encargado de ese día el cuál es Ana, se encarga de recolectar las acciones que todos hicieron durante el día, actualiza la lista y se las muestra a todos, con la intención de que la validen.

Dia 2:

- **Pedro=100,Ana=100,Juan=100,Mariana=100**
- Acción Mariana#1: Transfiere 2 monedas a Pedro-[Mariana=98,Pedro=102]
- **Pedro=102,Ana=100,Juan=100,Mariana=98**

Ana

Gráfico hecho con iconos realizados por Freepik en www.flaticon.com. Licencia Creative Commons BY 3.0 (CC 3.0 BY). http://creativecommons.org/licenses/by/3.0/

Ana firma el documento, sin embargo, este no será válido hasta que consiga la firma de por lo menos 2 personas más. Ana se encarga de ir con las otras personas para mostrarles el documento, y una vez que ellos lo examinan y validan, ponen su firma en el documento, con lo cual el documento se convierte en oficial y todos actualizan sus respectivos documentos.

Gráfico hecho con iconos realizados por Freepik en www.flaticon.com. Licencia Creative Commons BY 3.0 (CC 3.0 BY). http://creativecommons.org/licenses/by/3.0/

Después de que nuestras 4 personas tomaron un descanso, comienzan el Día 3, en donde se realizan un poco mas de transacciones que en el día anterior. Este día Pedro necesita madera, la cual le compra a Juan por un costo de 10 monedas. Juan necesita medicina y se la compra a Ana con un costo de 25 monedas y por último Ana tiene hambre, por lo que compra un jitomate a Pedro. Cada uno escribe sus operaciones, por lo que la lista queda de la siguiente manera:

- Acción Pedro #1: Transfiere 10 monedas a Juan
- Acción Juan #1: Tranfiere 25 monedas a Ana
- Acción Ana #1: Transfiere 2 monedas a Pedro

Este día el encargado de recolectar la lista de operaciones es Juan, por lo que va con las otras personas y genera el historial del día y lo firma.

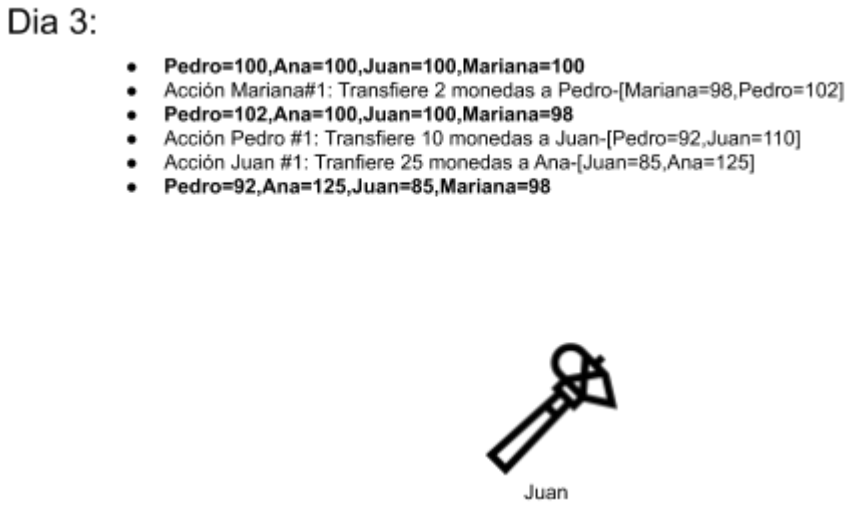


Gráfico hecho con iconos realizados por Freepik en www.flaticon.com. Licencia Creative Commons BY 3.0 (CC 3.0 BY). http://creativecommons.org/licenses/by/3.0/

Una vez que Juan ha reunido toda la información, creó la lista con base a la información que poseía, sin embargo ese día Ana llegó a comentarle sobre la transferencia que había llevado a cabo, no obstante Juan ya había escrito la lista del día la transferencia no se reflejó ese día en las operaciones diarias.

Ana se quedó frustrada por no poder anotar su operación a la lista, por lo que Pedro no le dará el jitomate y tendrá que arreglárselas de otra manera para conseguir algo de comida ese día. Debido a este hecho, Ana ese día se niega a firmar la lista, sin embargo Juan, consigue las firmas de los otros dos integrantes, con lo que la lista sigue siendo válida.

Dia 3:

- **Pedro=100,Ana=100,Juan=100,Mariana=100**
- Acción Mariana#1: Transfiere 2 monedas a Pedro-[Mariana=98,Pedro=102]
- **Pedro=102,Ana=100,Juan=100,Mariana=98**
- Acción Pedro #1: Transfiere 10 monedas a Juan-[Pedro=92,Juan=110]
- Acción Juan #1: Tranfiere 25 monedas a Ana-[Juan=85,Ana=125]
- **Pedro=92,Ana=125,Juan=85,Mariana=98**

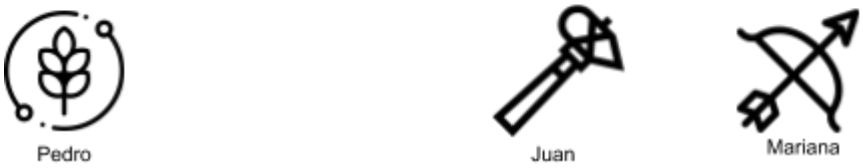


Gráfico hecho con iconos realizados por Freepik en www.flaticon.com. Licencia Creative Commons BY 3.0 (CC 3.0 BY). http://creativecommons.org/licenses/by/3.0/

Es el día 4 ya nadie sabe en donde se encuentra Mariana, fue a pescar y debido a una tormenta, no pudo regresar. Lo cual es un problema, a causa de que Mariana es la encargada ese día de recabar las operaciones, y actualizar la lista para todos.

Ana necesita realizar una serie de transferencias, escribe en su libreta las siguientes operaciones:

- Acción Ana #2: Transfiere 10 monedas a Juan
- Acción Ana #3: Transfiere 2 monedas a Pedro

Mariana no aparece y debido a que el grupo había acordado que ese día le tocaba a ella. Deciden que la actualización de ese día será omitida.

Comienza el Día 5 y Pedro es el responsable de actualizar la lista ese día. Ha estado lloviendo y Pedro necesita un lugar más acogedor para poder dormir más cómodamente. Por lo que le pregunta a Juan, cuánto le costaría construir una pequeña choza de madera. Juan le comenta que el costo por realizar eso es de 200 monedas. Lo cual es un poco complicado, debido a que él, solo posee 98 monedas. Entonces Pedro tiene una idea, como es el encargado de actualizar la lista ese día, podría agregar la operación a la lista que publicará.

No hay más transferencias ese día, sin embargo Pedro toma las dos acciones del día anterior de Ana y la otra acción que también se tenía pendiente de agregar de Ana de hace dos días. Después de recolectar todas estas nuevas acciones, junto con la acción fraudulenta que intenta hacer pasar por válida, genera la lista del Día 5, y queda de la siguiente manera:

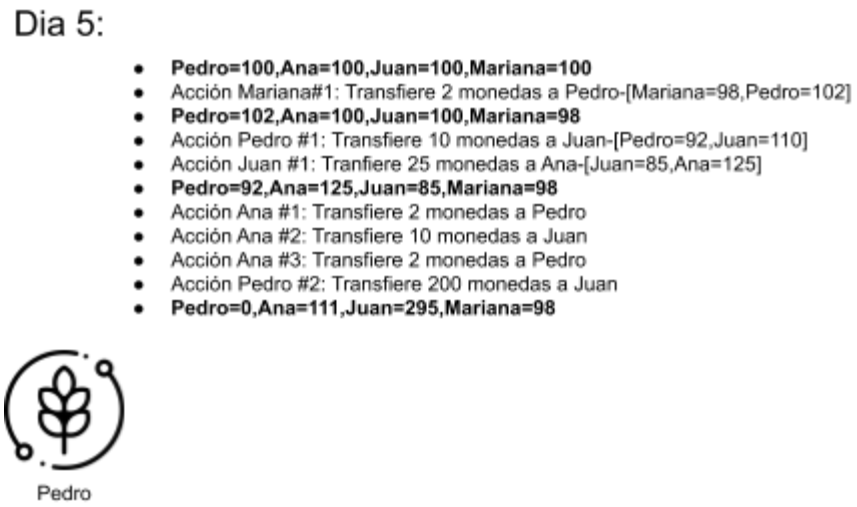


Gráfico hecho con iconos realizados por Freepik en www.flaticon.com. Licencia Creative Commons BY 3.0 (CC 3.0 BY). http://creativecommons.org/licenses/by/3.0/

Pedro firma la actualización, a pesar de que agregó una transferencia que no es válida; para hacerla válida y que el documento sea oficial aún necesita dos firmas. Cuando acude con Ana y Juan, para mostrarles la lista y obtener su firmas, ellos rechazan firmar ese documento debido a que en el Día 3, Pedro tenía 92 monedas y ahora existe una transacción en donde se afirma que él está gastando 200 monedas lo cual no puede ser posible.

Ana y Juan le solicitan a Pedro que vuelva a actualizar la lista, pero con valores reales, para poder firmar el documento de ese día. Pedro acepta y vuelve a crear la lista de ese día, pero elimina su acción maliciosa.

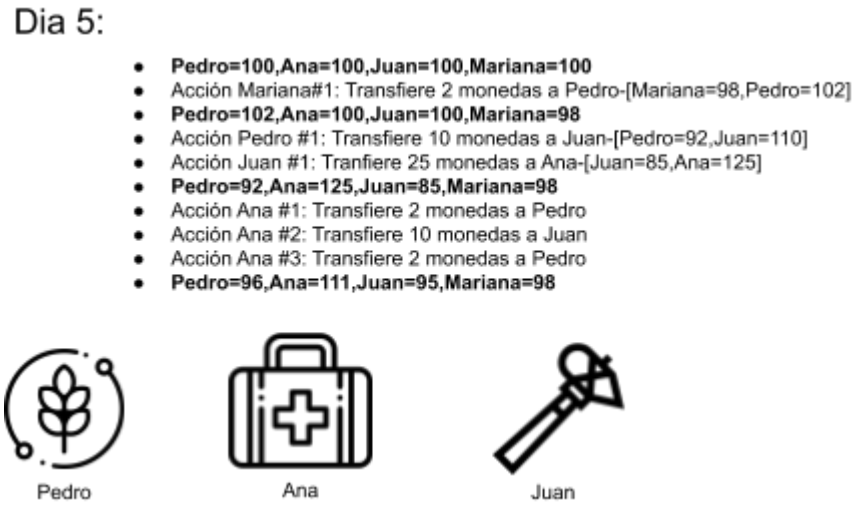


Gráfico hecho con iconos realizados por Freepik en www.flaticon.com. Licencia Creative Commons BY 3.0 (CC 3.0 BY). http://creativecommons.org/licenses/by/3.0/

Una vez corregido el documento, es firmado y aceptado por tres personas, por lo que pasa a ser la última actualización de la comunidad.

El día 6 Mariana regresa de nuevo con ellos y debido a que estuvo desconectada de las actualizaciones, no está segura de cuántas monedas poseen cada uno, por lo que va con Juan para que le comparta la lista y poder actualizar sus registros desde el día 2 hasta el día 6. Después de actualizar su lista, ya está preparada para participar en la actualización de ese día.

Esta historia podría continuar por semanas, meses o años, el punto es que para fines prácticos, con seis días se pueden ver algunos de los problemas que se podrían presentar, se aprecia también cómo se realizan las votaciones y la copia que ellos deben tener de las últimas cantidades, debido a que todas las acciones son públicas. También se puede apreciar que tiene que existir un método de consenso, en el que todos acuerden que si se cumple con los estándares que se definan como oficiales, no importa que no se participe en las votaciones, aún se tendrá que aceptar la información como válida. Por último se pudo observar que a pesar de la mala intención de uno de los participantes, debido al sistema, no fue posible escribir acciones fraudulentas.

Visión general

En el mismo orden de ideas, para comenzar a hablar acerca de este tema, primero tendremos que definir lo que es una *Blockchain*, para ello haremos referencia a la definición que provee el *NIST* en su documento de *Blockchain Technology Overview*:

Una *Blockchain* es un libro de contabilidad digital a prueba de manipulaciones y resistente a las manipulaciones. Está implementada de forma distribuida (Sin un repositorio central) y generalmente sin una autoridad central (Por ejemplo un banco, compañía o gobierno). (Yaga, Mell, Roby, Scarfone, 2018)

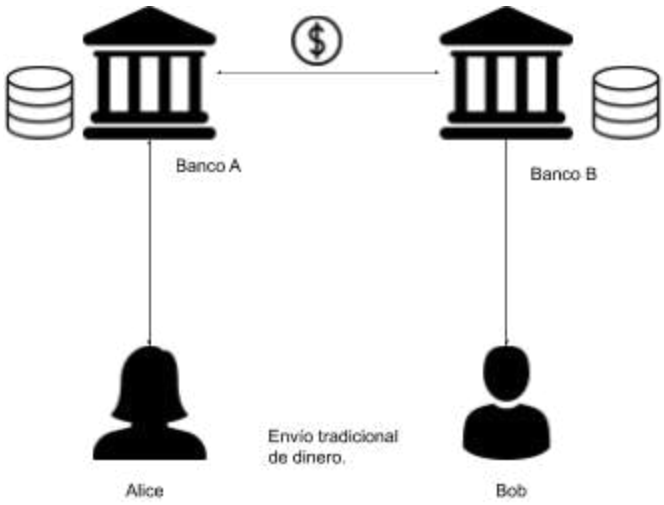


Gráfico hecho con iconos realizados por Freepik, Smashicons & Pixel perfect en www.flaticon.com. Licencia Creative Commons BY 3.0 (CC 3.0 BY). http://creativecommons.org/licenses/by/3.0/

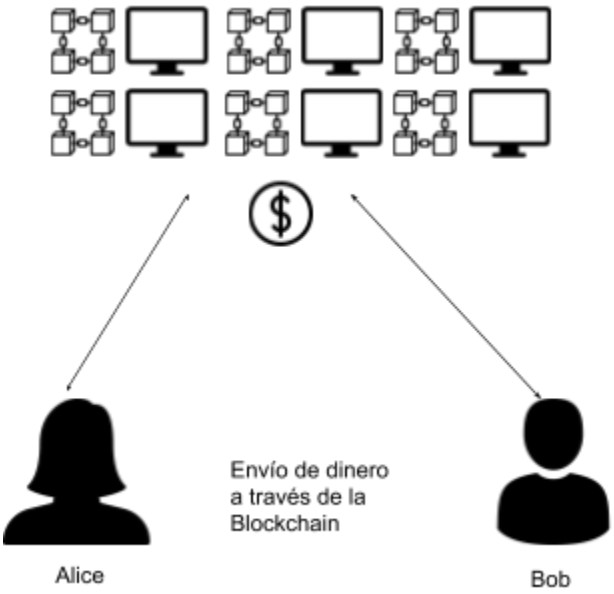


Gráfico hecho con iconos realizados por Nikita Golubev, Icon Works, Freepik & Pixel perfect en www.flaticon.com. Licencia Creative Commons BY 3.0 (CC 3.0 BY). http://creativecommons.org/licenses/by/3.0/

Nos podremos encontrar muchas definiciones de *Blockchain* en *Internet* y los libros, empero esta definición engloba dos ideas clave de esta tecnología las cuales son: ser un repositorio distribuido a prueba de manipulaciones y que no le pertenece a ninguna entidad en concreto. Además por lo general es pública y todas las personas pueden ver en tiempo real las transacciones que están siendo llevadas a cabo en la red, lo cual aumenta la transparencia de cualquier operación que se quiera llevar a cabo sobre la *Blockchain*.

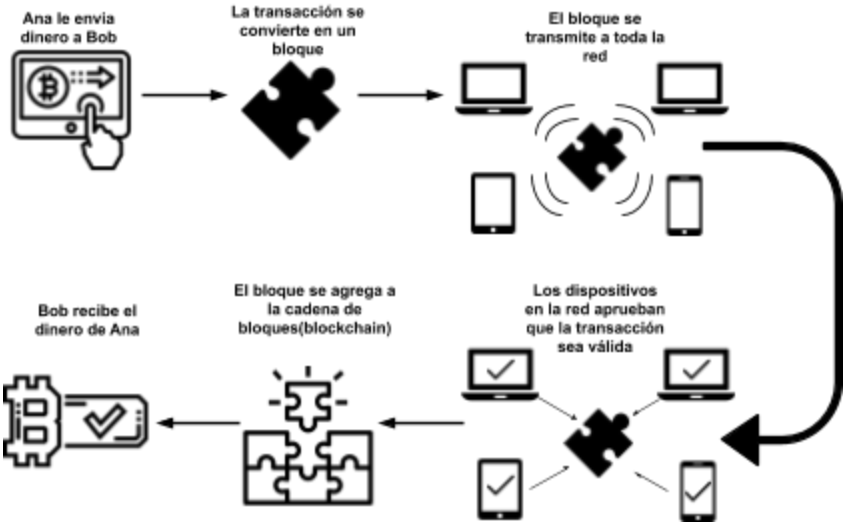


Gráfico hecho con iconos realizados por Freepik, surang & geotatah en www.flaticon.com. Licencia Creative Commons BY 3.0 (CC 3.0 BY). http://creativecommons.org/licenses/by/3.0/

Con la definición de *Blockchain* conviene definir qué es un bloque y cómo comenzó la cadena de bloques así como su construcción y actualización por algunos de los participantes que integran la red.

Gráfico hecho con iconos realizados por Freepik en www.flaticon.com. Licencia Creative Commons BY 3.0 (CC 3.0 BY). http://creativecommons.org/licenses/by/3.0/

Para comenzar con este párrafo, es menester señalar que, la parte principal de una *Blockchain* son los bloques, ya que estos sirven para registrar todas las transacciones que han sido ejecutadas en la red, además de que ayudan como referentes para continuar agregando más bloques a la red. Esto dependiendo de la *Blockchain* que se esté utilizando, también puede variar la información que debe contener el bloque, sin embargo deberá de contar por lo menos con la siguiente información: (Yaga et al., 2018)

Encabezado del bloque

- Número de bloque
- El valor *hash* del encabezado del bloque anterior

- Una representación *hash* de los datos del bloque
- Una marca de tiempo
- Tamaño del bloque
- El valor del *nonce* (Se explicará posteriormente este concepto)

Datos del bloque

- Una lista de transacciones y eventos del *ledger* incluidos dentro del bloque
- Información adicional que se quiera almacenar

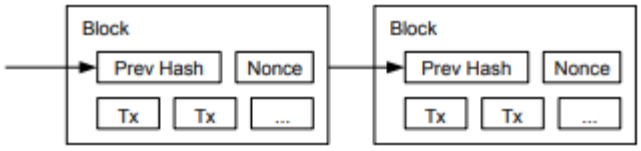


Imagen obtenida del paper de *Bitcoin* (Nakamoto, 2008)

Ahora que sabemos lo que es un bloque del cual se conforma una *Blockchain,* cabe señalar que el primer bloque que se creó para dar vida a la red, se conoce como Bloque génesis y generalmente es agregado por el creador de la *Blockchain*. Después de ese bloque, todos los bloques se tienen que validar y agregar por un algoritmo de consenso y de manera distribuida entre los nodos que se encargan de validar las transacciones.

El caso anterior ocurre cuando todos los nodos trabajan de forma honesta, y nadie quiere enviar una transacción fraudulenta, sin embargo, algunas veces existen participantes en la red, que quieren aprovecharse del sistema, y enviar transacciones que son inválidas, en ese caso, los bloques que contienen la información apócrifa, son detectados y eliminados de la *Blockchain*, para que no sean agregados, y con esto mantener la confiabilidad del sistema.

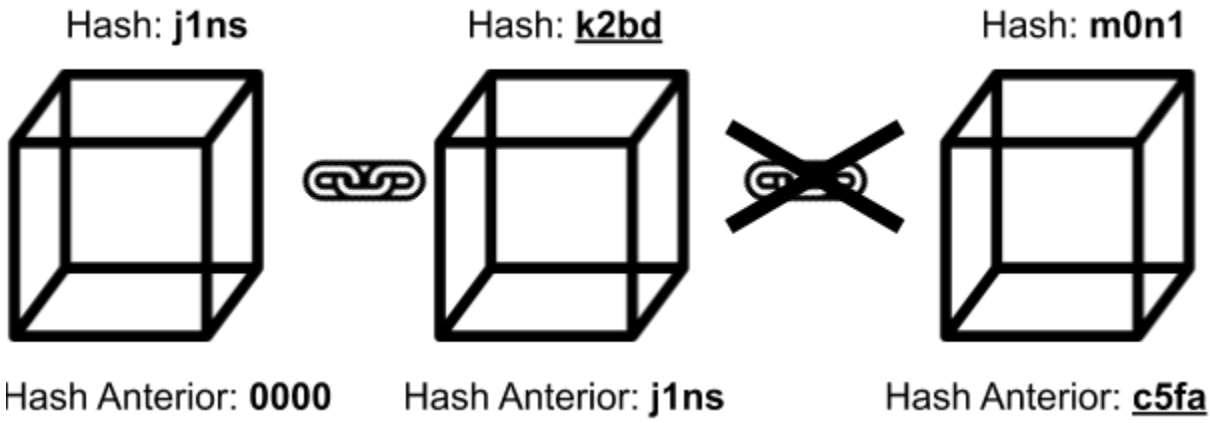


Gráfico hecho con iconos realizados por Freepik & Retinaicons en www.flaticon.com. Licencia Creative Commons BY 3.0 (CC 3.0 BY). http://creativecommons.org/licenses/by/3.0/

Otro concepto importante a tener en cuenta son las transacciones las cuales como lo define Andreas M. Antonopoulos (2017): «en términos simples, una transferencia de bitcoins de una dirección a otra. Más precisamente, una transacción es una estructura de datos firmada que expresa una transferencia de valor. Las transacciones se transmiten a través de la red de bitcoins, se recopilan por los mineros y se incluyen en bloques, los cuales se hacen permanentes en la *Blockchain*.»

Con la definición anterior, se aprecia que una transacción es básicamente cualquier operación que ocurre en la red *Blockchain* y que queda grabada en esta misma. En el caso de *Bitcoin*, una transacción crea un bloque con la información de la transacción, conteniendo toda la información de las partes implicadas en esa transacción, la cual una vez que es validada por los mineros, se agrega el bloque que representa esta transacción a la *Blockchain*, para dejar una prueba de que esta operación se llegó a efectuar y fue válida.

Ahora, sabiendo quien agrega los bloques a la *Blockchain*, surgen algunas dudas naturales, como ¿cuál es el mecanismo que utilizan estos nodos mineros para agregar la transacción?, ¿cómo es que solo pueden ser agregadas transacciones válidas, siendo que cualquier persona puede enviar

transacciones a la red?, teniendo la posibilidad de incluso tratar de enviar transacciones fraudulentas con la intención de transferirse algún activo a su poder.

También surge la pregunta sobre ¿cómo es que una persona puede demostrar la propiedad que tiene sobre un objeto que es público para todo el mundo?, para esto hablaremos brevemente sobre el consenso y sobre las *wallets*. En páginas posteriores se abundará con más detalle acerca de estos conceptos.

Primeramente para el tema del consenso, conviene hablar sobre el problema que se tiene, para ello hablaremos un poco acerca del problema de los generales Bizantinos propuesto por Lamport, Shostak y Pease (1985) en su *paper* titulado *The Byzantine Generals Problem*.

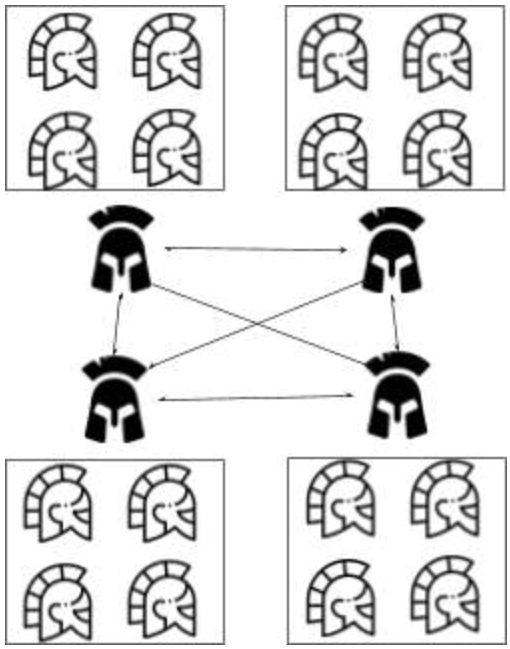


Gráfico hecho con iconos realizados por Freepik en www.flaticon.com. Licencia Creative Commons BY 3.0 (CC 3.0 BY). http://creativecommons.org/licenses/by/3.0/

En el problema que exponen, se habla sobre un conflicto de confianza entre iguales que no se conocen, que para fines prácticos es lo mismo que ocurre en la red de una *Blockchain*. Es que todos pueden unir sus máquinas a la red, y ponerse a funcionar como mineros, sin embargo, el problema de este *paper*, es importante para poder entender cómo es que los nodos se ponen de

acuerdo entre ellos (llevan a cabo un consenso), para saber que la transacción que están validando es la correcta y que todos los que componen la red la puedan aceptar como válida y se agregue a la *Blockchain*.

El problema es el siguiente:

> Imaginemos que varias divisiones del ejército bizantino están acampando fuera de una ciudad enemiga, cada división es comandada por su propio general. Los generales pueden comunicarse entre sí, solo por mensajes, después de observar al enemigo, deben decidir sobre un plan de acción común, sin embargo, algunos de los generales pueden ser traidores, tratando de evitar que los generales leales puedan llegar a un acuerdo. Los generales deben tener un algoritmo para garantizar que A), todos los generales leales decidan sobre el mismo plan y B), un pequeño número de traidores no pueda causar que los generales leales adopten un mal plan.

Dicho lo anterior, en una *Blockchain* en vez de utilizar el problema para atacar, el problema en cuestión es el de aceptar una transacción que está llegando desde otro nodo de la red, esto ocurre debido a que cualquier persona puede enviar una transacción y al igual que con el problema de los generales bizantinos, la transacción puede ser válida debiendo ser procesada y agregada a la *Blockchain*, sin embargo, la transacción podría venir de un usuario que maliciosamente busca enviar el mismo activo a múltiples cuentas, lo cual no es válido. Para resolver este problema se generó el proceso de minería. [1]

El proceso de *Proof of work* envuelve una serie de verificaciones, entre los que se encuentran comprobar que algunos campos no estén vacíos, la longitud del bloque, entre otras cosas, sin embargo, la parte que nos interesa observar, es la validación que llevan a cabo para verificar si el bloque es correcto, para ello en pocas palabras la definiremos como una validación de tres pasos (University of Nicosia, 2019):

[1] Cabe señalar como nota que existen varios mecanismos de consenso, sin embargo, en este apartado nos centraremos en el de uso más extendido el cual es *Proof of work*.

Gráfico hecho con iconos realizados por Egor Rumyantsev, Freepik y Roundicons Freebies en www.flaticon.com. Licencia Creative Commons BY 3.0 (CC 3.0 BY). http://creativecommons.org/licenses/by/3.0/

1.- Se crea un *hash* con el *Header* del último bloque + el bloque de la nueva transacción + un número conocido como *Nonce* el cual es un número aleatorio de 32 bits.

2.- Se aplica la función criptográfica de *SHA-256* a la información del paso 1.

3.- El *hash* es verificado contra un valor determinado(Un patrón deseado). Si el valor es menor, el problema fue resuelto y el bloque ganador, pasa a ser enviado a toda la red. En dado caso de que no sea menor, se repite el paso 1, con un nuevo *Nonce*.

Una vez que este mecanismo de *Proof of work* encuentra la solución, se propaga la respuesta y los nodos que conforman la *Blockchain*, agregan el nuevo bloque a la misma y así se continua con todas las transacciones que se encuentran en la lista de transacciones por confirmar, también conocida como *Mempool* (Antonopoulos, 2017)

Es importante mencionar que en este proceso de validación, los nodos que encuentran la respuesta al problema obtienen una compensación en *bitcoins*. Esta compensación surge por dos cosas; primero por confirmar la transacción y gastar recursos para mantener la seguridad de la red. Segundo, por una comisión que es cargada al momento de realizar la transacción.

Ya que abordamos cómo es que una transacción puede ser agregada, nos queda contestar otra pregunta que previamente nos habíamos planteado, la cual es ¿cómo alguien puede probar la propiedad sobre un activo dentro de la red de *Blockchain*?

Lo hemos abordado anteriormente en la publicación “Internet ¿Arma o Herramienta? y previamente debemos aclarar que existen dos tipos de sistemas:

1) Sistema de clave pública: Sistema en donde se utilizan dos llaves, una pública y una privada. Si alguien desea compartir algo con alguien, se debe cifrar utilizando la llave pública, una vez cifrado la información se podrá descifrar obteniendo la llave privada, la cual no debe ser compartida con nadie.

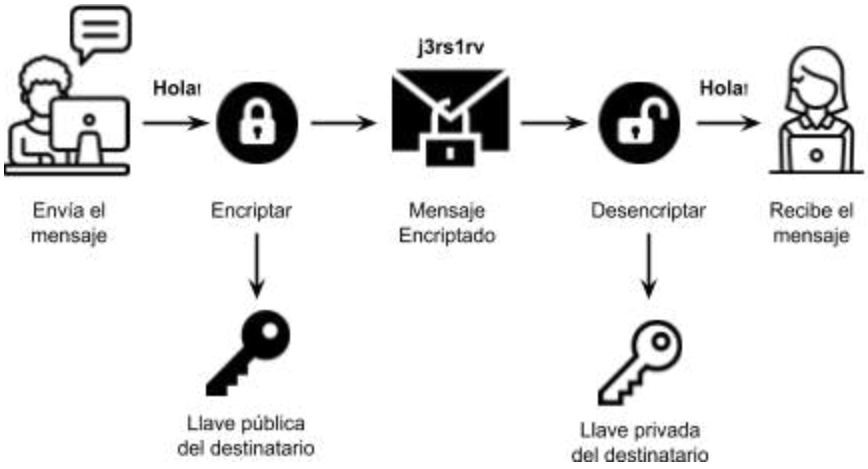


Gráfico hecho con iconos realizados por Freepik & Chanut en www.flaticon.com. Licencia Creative Commons BY 3.0 (CC 3.0 BY). http://creativecommons.org/licenses/by/3.0/

2) Sistema de clave privada: Sistema en donde la misma llave que se utiliza para cifrar la información, es la misma que se utiliza para descifrar la información.

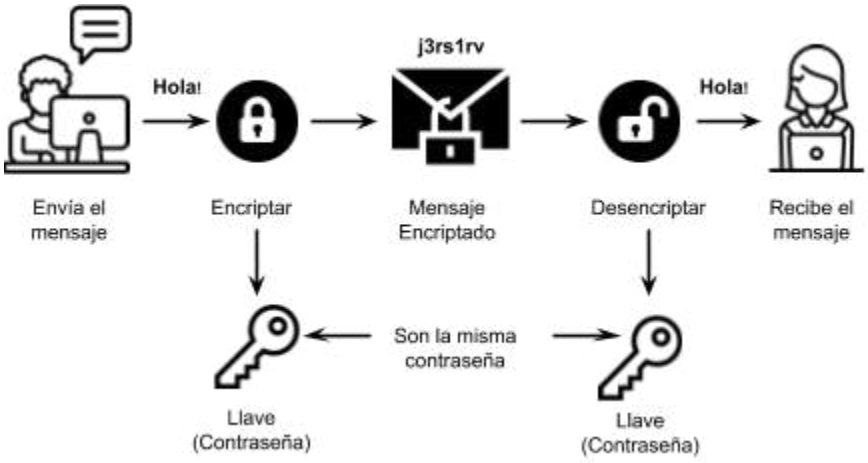


Gráfico hecho con iconos realizados por Freepik & Chanut en www.flaticon.com. Licencia Creative Commons BY 3.0 (CC 3.0 BY). http://creativecommons.org/licenses/by/3.0/

Con más claridad acerca de lo que es un sistema de *Blockchain*, cabe señalar que el tipo de sistema que se utiliza es un sistema de clave pública, en donde las personas comparten su dirección a la que se les enviaran los activos y generalmente esta dirección es una versión simplificada de la llave pública. A pesar de que todos puedan conocer los activos que existen en la red, la única forma de poder ejecutar alguna operación sobre ellos, es teniendo la clave privada, con lo que se puede demostrar la propiedad de algún activo dentro de la *Blockchain*.

Dicho lo anterior, este concepto generalmente se conoce como *wallet*, la cual se compone de las 2 llaves mencionadas anteriormente, además de la dirección, la cual como ya se mencionó, es simplemente una versión simplificada de la llave pública.

Para entender esta *wallet* se puede pensar en ella como una cartera digital, en la que se tienen los mecanismos para acceder a los activos dentro de la misma y a su vez permitir que otros envíen activos a esta cuenta.

Sin embargo hay que aclarar dos cosas con respecto a la *wallet*. La primera es que originalmente las *wallets* se pensaron para ser genéricas y poder ser utilizadas por cualquier cliente que se conectara a alguna *Blockchain* en particular, sin embargo en la actualidad, por lo general los

clientes de las *Blockchain* son normalmente las *wallets* también, y la segunda, es que las *wallets* no contienen los activos en sí; uno podría llegar a pensar en una *wallet* como en una cartera que carga y dentro de esta tiene su dinero así que puede gastarlo, sin embargo éste no es el caso. Una mejor forma de entender esta *wallet* es pensar en ella como una tarjeta que nos da acceso a nuestros activos. Sólo teniendo esta tarjeta podremos transferir nuestros activos a nuestras cuentas o a otras. Básicamente no debemos perder esta tarjeta, ni compartirla con nadie, solo podemos compartir nuestra dirección a la que nos enviarán algún activo, empero la llave privada siempre tendremos que mantenerla alejada de cualquier persona, si lo que queremos es cuidar nuestros activos.

Una vez que ya repasamos todo el flujo que se lleva a cabo para realizar operaciones sobre una *Blockchain*, aún existen dudas, no obstante, en las páginas posteriores se incluye información adicional acerca de cada uno de los términos mencionados anteriormente.

Mecanismos de consenso

Ya hemos expuesto el problema de los generales Bizantinos, en los que tenían que llegar a un acuerdo a pesar de que existieran traidores entre ellos. Utilizando ese ejemplo, se expuso cómo es que Satoshi resolvió este problema con el método de *proof-of-work* (Nakamoto, 2008).

Proof of work

Esta solución resuelve el problema, actualmente es la más utilizada en las *Blockchain*, sin embargo es una solución que desperdicia muchos recursos, debido a que se tarda 10 minutos en promedio, lo que causa que además del desperdicio de los recursos, las transacciones que están siendo procesadas en la red, sean más lentas y limitadas a un número no muy grande.

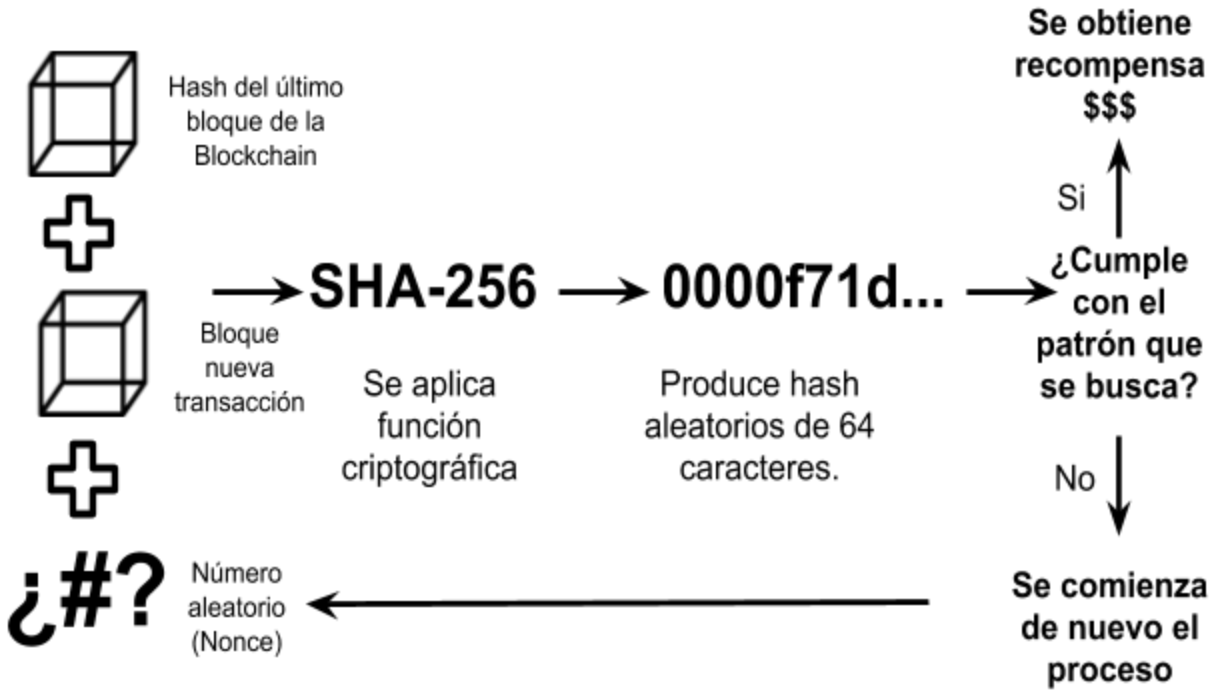


Gráfico hecho con iconos realizados por Retinaicons en www.flaticon.com. Licencia Creative Commons BY 3.0 (CC 3.0 BY). http://creativecommons.org/licenses/by/3.0/

Mineros

Uno de los conceptos más importantes a considerar en este tipo de consenso son los mineros, los cuales se encargan de dar mayor seguridad a la red. Estos mineros tiene la función principal de validar las transacciones, con lo cual reciben una recompensa al encontrar la solución y confirmar la transacción. En un esquema tradicional, normalmente los servidores de los bancos a los que pertenecen las tarjetas llevarían a cabo esta validación, empero en el caso de la *Blockchain* los mineros son los que tienen esta función.

Los mineros ayudan a prevenir el doble gasto, evitando que una persona utilice dos veces el mismo *token*, en el caso de un elemento físico, al momento de entregarlo a otra persona, la otra persona ya tiene el elemento en su mano, no obstante en el caso de un *token* digital o algo que es intangible, una persona podría duplicar e intentar transferirlo más de una vez, entonces los mineros se encargan de evitar este tipo de problemas.

Para que los mineros puedan ganar dinero tienen que ocurrir dos cosas: la primera es verificar bloques de longitud de 1 MB que contiene transacciones, en donde validan que la información sea correcta, y la segunda, tienen que resolver un complejo problema computacional, el conocido como *proof of work*, en el cual deberán encontrar un número llamado *hash*, tienen que tratar de adivinar un número que se encuentra en el conjunto de números hexadecimales de 64 dígitos, deberán probar todas las combinaciones posibles hasta llegar a la solución, lo que básicamente convierte el proceso en una apuesta de ver quién llega primero a la solución.

En pocas palabras, el algoritmo se resume de una manera sencilla:

Unos amigos juegan a adivinar un número entre 1 y 100, digamos que son cinco amigos A, B, C, D y E y al que le toca pensar un número, en este caso al amigo A piensa en el número 20, entonces los otros cuatro tienen que tratar de adivinar un número menor o igual al que el amigo A pensó. Los amigos B, C, D y E se ponen a pensar unos momentos, y responden con los siguientes números B responde con 80, C responde con 18, D responde con 30 y E responde con 10. Como se puede apreciar los amigos C y E resolvieron el problema, por lo que ellos son los ganadores del juego.

En el caso de la minería el problema es similar, pero en vez de ser solo cinco amigos, son millones de mineros los que tratarán de encontrar el número solicitado y en lugar de un rango de 1 a 100, el rango será de todos los posibles valores de un número hexadecimal de 64 dígitos. Además la selección del número vendrá dada por la suma de tres componentes.

1. El *hash* del último bloque de la *Blockchain*
2. El bloque de nuevas transacciones
3. Un número aleatorio, conocido como *nonce*.

Se toman estos 3 elementos, se les aplica la función criptográfica de *SHA-256* y el número resultado de esta función, será el que se esté probando para ver si cumple con ser menor o igual

al número que tiene que ser encontrado, en caso de que el número no sea correcto, se repite de nuevo el proceso, en donde lo que cambiará nuevamente será el *nonce* y así se repetirá hasta llegar a la solución y obtener la recompensa. Una vez que se encuentra es enviado a todos los nodos, para que lo verifiquen y un nuevo bloque sea agregado a la *Blockchain*.

Solo Mining

Este estilo de minería consiste en que una sola persona, utiliza una computadora o algún *hardware* especial para realizar búsqueda de bloques. Por ser una única persona la que está tratando de encontrar solución, al momento de acertar y enviarla a los otros nodos, ella recibirá la recompensa total, además de los costos de la transacción.

Pool Mining

En esta forma de minería muchas personas unen esfuerzos y todos los nodos conectados a una pool comparten una misma cuenta, por lo que conjuntamente trabajan para encontrar el bloque. Una vez que es encontrado y la *wallet* de la *pool* recibe la recompensa. Esta recompensa es dividida entre los diferentes mineros que contribuyeron a encontrar el bloque.

Proof of stake

En el caso de *proof of work* se otorgan recompensas a los participantes por resolver los acertijos que son planteados para crear los nuevos bloques de la *Blockchain*, además de proveerles una comisión por llevar a cabo la transacción.

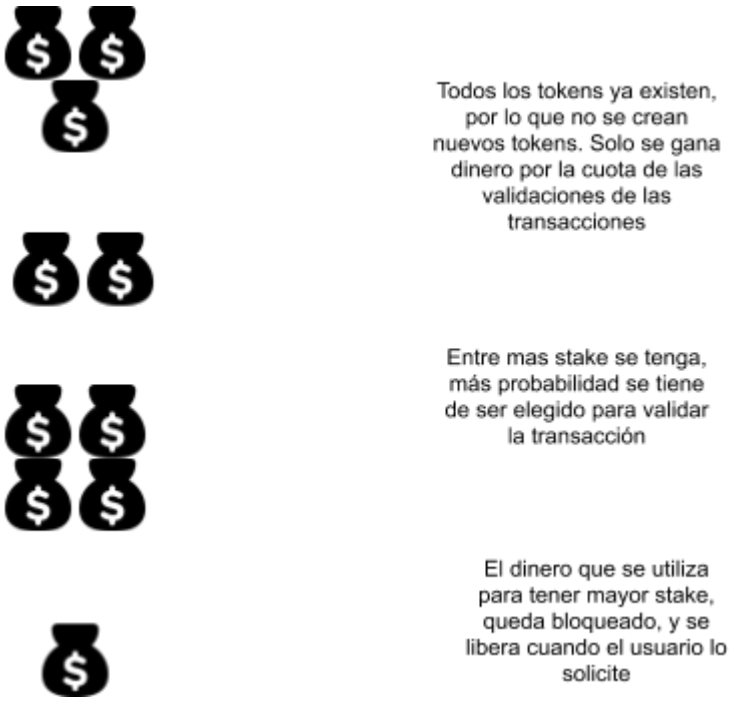


Gráfico hecho con iconos realizados por Freepik en www.flaticon.com. Licencia Creative Commons BY 3.0 (CC 3.0 BY). http://creativecommons.org/licenses/by/3.0/

Proof of stake (Buterin & Griffith, 2017) es un poco diferente, en este tipo de consenso no se crean nuevos bloques, por lo general todas las monedas ya existen y la forma en que los mineros ganan dinero por validar las transacciones, es a través de la comisión que se llevan al momento de votar en el consenso.

Este tipo de consenso es un consenso por apuesta (Buterin, 2015), en donde los nodos tienen que enviar *tokens* de la red a la que pertenecen a un *smart contract*. Entre más alta sea la cantidad que enviaron al *smart contract*, esto aumentará la probabilidad de ser elegidos para validar las transacciones.

En el caso de *proof of work*, las personas tienen que comprar equipos costosos, para tener mayor capacidad de procesar las transacciones, lo que aumenta su probabilidad de ser elegidos, sin embargo en el caso de *proof of stake*, en vez de gastar mucho dinero comprando el equipo necesario para aumentar la capacidad de cómputo y pagando los recibos de luz elevados como es

en el caso de *proof of work*, en el *proof of stake* solo tienen que enviar cierta cantidad de la cual no podrán disponer mientras su *nodo* forma parte de los *nodos* que validan las transacciones de la red.

La analogía entre estos dos principales tipos de consenso, es que en el caso de *proof of work* la seguridad para evitar que las personas den de alta muchos nodos, está dada en términos monetarios, debido a que se tiene que invertir en equipo con una alta capacidad de cómputo, además del pago de la energía para que el sistema continúe funcionando. No obstante en *proof of stake* la idea es utilizar *tokens* de la red, esta es la forma en que los *nodos* prueban que son fiables. En un breve análisis, en ambos casos se demuestra que los *nodos* tienen interés en mantener la integridad de la red, pero son vistas desde diferentes perspectivas, por lo que ambos algoritmos demuestran el interés para que la red siga funcionando.

Principalmente existen dos aproximaciones para elegir los nodos que participarán en el consenso, los cuales son: (github.com, 2018)

Chain-based

En esta aproximación, el algoritmo pseudo-aleatoriamente selecciona a un validador, en un *periodo* de tiempo determinado, este validador tendrá derecho a crear un bloque, el cual tendrá que apuntar al bloque anterior del bloque final de la cadena más larga que exista.

Byzantine Fault Tolerance style (BFT-style)

Esta otra aproximación, tiene la característica en la que se asigna de manera aleatoria el derecho a proponer bloques a todos los validadores. Se realiza una ronda de votaciones, en donde cada validador emite su voto para cada una de las rondas. Al finalizar el proceso, todos los validadores (honestos y en línea) acuerdan si deben de agregar un bloque dado a la *Blockchain*. Tenga en cuenta que los bloques todavía pueden estar encadenados juntos; la diferencia clave es que el consenso de un bloque puede estar en un bloque y no en la longitud de la cadena.

Sin duda este tipo de consenso tiene ventajas sobre el ampliamente utilizado *proof of work*, entre las que se encuentra principalmente, un menor consumo energético, debido a que no se tienen que realizar muchas operaciones como en el caso de *proof of work* si es necesario.

Los algoritmos de consenso buscan solucionar el problema de los generales Bizantinos, y pesar de que existen varios mecanismos de este tipo, los más populares son los anteriormente expuestos. Sin embargo también existen algunos otros (Anwar, 2018):

- Proof-of-Work
- Proof-of-Stake
- Delegated Proof-of-Stake
- Leased Proof-Of-Stake
- Proof of Elapsed Time
- Practical Byzantine Fault Tolerance
- Simplified Byzantine Fault Tolerance
- Delegated Byzantine Fault Tolerance
- Directed Acyclic Graphs
- Proof-of-Activity
- Proof-of-Importance
- Proof-of-Capacity
- Proof-of-Burn
- Proof-of-Weight

Ataque del 51%

Este ataque afecta a diversas *Blockchain*, generalmente se pone de ejemplo a *Bitcoin*, para el cual un ataque de este tipo sigue siendo hipotético, consiste en que más del 50% de la capacidad de cómputo de la red es controlada por un grupo de mineros.

Debido a que este grupo de mineros, tendrá el poder suficiente para generar la cadena más larga, tomarán el control de la *Blockchain* y podrán revertir cambios en transacciones pasadas, además de rechazar nuevas transacciones. Cabe señalar que los atacantes no podrán gastar los *tokens* de las cuentas, pero sí podrán evitar que sean transferidos.

Básicamente este ataque convierte una *Blockchain* descentralizada en una *Blockchain* centralizada, debido a que es controlada por todo este grupo de mineros, en esto será importante que los mineros honestos siempre mantengan más de un 50% del poder de cómputo de la *Blockchain*.

En algunos casos algunas *mining pools* han excedido casi más de un 50% el poder de cómputo de la red de *Bitcoin*, no obstante esas mismas *mining pool* voluntariamente han reducido ese porcentaje para evitar comprometer a la red de *Bitcoin*.

Algunas veces se llega a mencionar el concepto de *spawn camp attack*, el cual consiste básicamente cuando un grupo de mineros que posee el control de más del 51% de la capacidad de cómputo de la red, continúa atacando la red múltiples veces, hasta el punto de que la *Blockchain* ya no es útil.

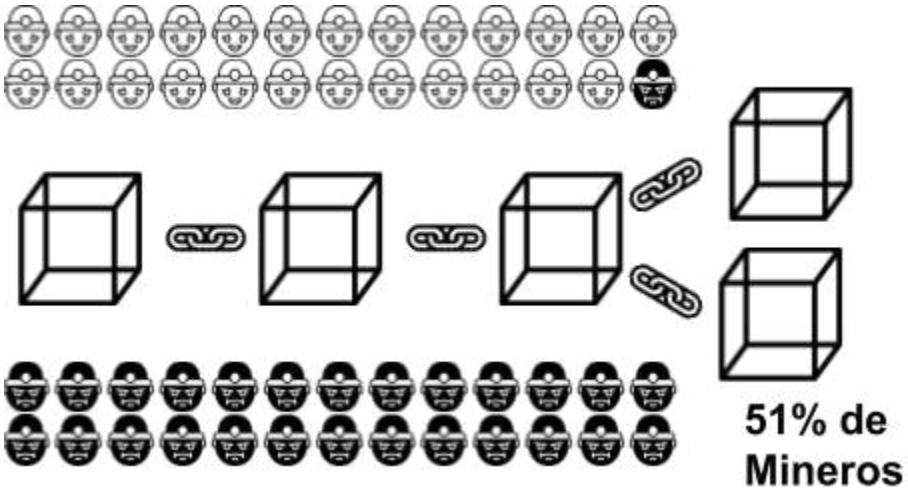


Gráfico hecho con iconos realizados por Freepik, Retinaicons & Creaticca Creative Agency en www.flaticon.com. Licencia Creative Commons BY 3.0 (CC 3.0 BY). http://creativecommons.org/licenses/by/3.0/

Tipos de clientes

Estos cliente podrían variar dependiendo la *Blockchain* que se esté analizando, en este apartado se explicarán los diferentes nodos que existen en *Bitcoin* (University of Nicosia, 2019):

Full client

También conocido como *full node*, este tipo de cliente que almacena el historial completo de la *Blockchain*, administra la *wallet* de los usuario y puede interactuar directamente con la red de *bitcoin* para iniciar transacciones. No necesita un tercero para funcionar, las llaves privadas son almacenadas localmente y nunca son enviadas a ningún lugar. Esto es similar a tener un servidor de correo electrónico independiente y que maneje todos los aspectos necesarios para su funcionamiento, sin necesidad de servicios externos.

Lightweight client

Almacena localmente las llaves privadas del usuario, sin embargo depende de servidores de terceros para realizar operaciones sobre la *Blockchain*. No almacena una copia completa de la *Blockchain*, por lo que debe de confiar en un tercero para que valide las transacciones. Este concepto es similar a tener un programa que se conecta a un servidor de correo electrónico para acceder al correo de entrada, sin embargo necesita a un tercero para interactuar con la red.

Clientes web

Como su nombre lo dice, es un cliente al que se accede mediante un navegador web. Por lo general son interfaces, que mediante el servidor de un tercero nos permiten realizar operaciones sobre la *Blockchain*. Por lo general las llaves privadas son almacenados en sus servidores y en algunos de esos casos, estas llaves privadas son almacenadas encriptadas, en donde solamente el usuario puede desencriptarlas localmente.

Clientes de escritorio

Es similar al cliente web, solo que se accede desde algún *software* instalado en la computadora del usuario, de igual manera depende de servicios de terceros.

Clientes móviles

Algunos de estos clientes se sincronizan con clientes de escritorio y *web*, lo que ofrece un cliente multiplataforma. Son similares a los *web client*, pero se utilizan desde una *app* en algún dispositivo móvil.

Tipos de wallets

Llegando a este apartado, es el momento de abundar sobre este concepto, el cual ya se abordó previamente, pero no se profundizó en los diferentes tipos de *wallets* que existen, así como las diferencias que existen entre ellas.

Para clasificarlas, las podemos agrupar en dos apartados. Por la forma en la que son creadas y por la forma en que son almacenadas para ser utilizadas.

Creación

Existen dos formas principales para el apartado de creación, las cuales difieren en el hecho de cómo son generadas y como tienen que ser tratadas para evitar perderlas.

Aleatorias o no deterministas

En el caso de estas *wallets*, se generan de una manera aleatoria. Pueden ser generadas por un cliente de la *Blockchain* y ser únicamente utilizadas una ocasión. La desventaja de este tipo de *wallet*, es que se tiene que hacer respaldo de cada una de las llaves que se van generando, pues al omitirse en dado caso de que se pierdan, los activos asociados a la llave se perderán para siempre y no existirá forma de recuperarlos. Por lo general este tipo de llaves son utilizadas únicamente para realizar pruebas.

Deterministas o con semilla

Este tipo de *wallets* como su nombre lo indica, provienen de una semilla común de la cual se deriva la llave privada, por lo cual en dado caso de que se pierda la llave, con solo proveer la

semilla, se puede volver a recuperar la llave privada. La semilla es generada aleatoriamente y combinada con algún dato. Esta semilla es útil incluso si se quiere exportar o importar, lo que facilita la migración entre varias implementaciones.

Determinista jerarquica o HD

Este tipo de *wallet* determinista permite crear múltiples llaves, derivadas de una semilla. La implementación de este tipo es como un árbol de llaves, de las cuáles se pueden ir generando varios niveles de las mismas. La implementación más avanzada, está basada en el estándar *BIP-32*. (Wuille, 2012)

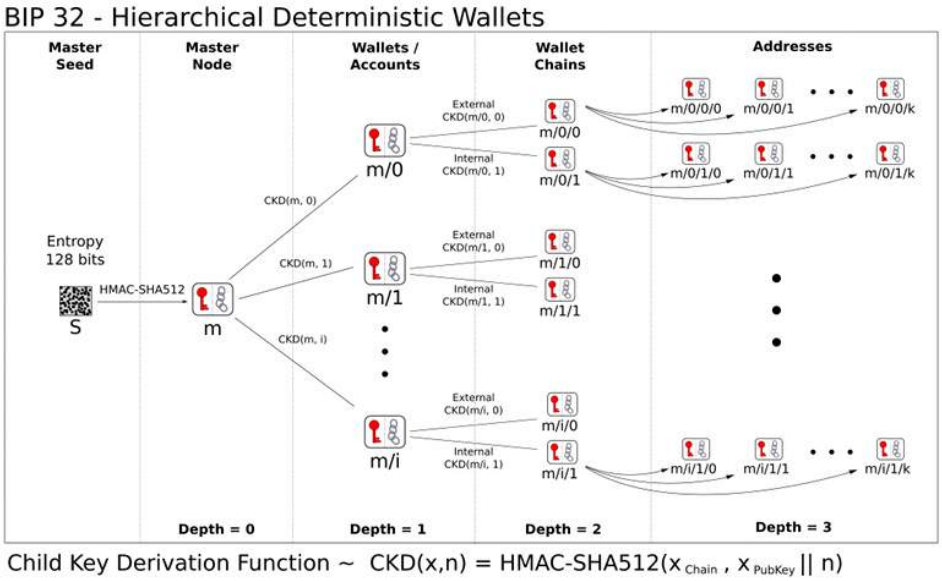


Imagen tomada del paper de BIP-32 el cual se puede consultar en el siguiente enlace.
https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki#master-key-generation

Como bien apunta Andreas M. Antonopoulos, existen dos grandes ventajas sobre este tipo de wallets, las cuales son (Antonopoulos, 2017):

1. El árbol que se genera derivado de la semilla, se puede utilizar para expresar una jerarquía organizacional, lo que permitiría crear llaves entre departamentos o alguna otra forma de organización que se requiera.

2. Se pueden crear una secuencia de llaves públicas, sin tener acceso a sus correspondientes llaves privadas, lo que permitiría utilizarlas en ambientes inseguros, para tenerla disponible para sólo recibir activos o simplemente para generar una llave pública diferente para cada transacción o giro que se necesite.

Este tipo de llaves son mucho más flexibles que las generadas aleatoriamente, además que todas las facilidades que tiene se pueden prestar como bien se muestra en el ejemplo del *paper* del *BIP-32,* para la administración de una tienda en línea, en donde a cada cliente se le puede otorgar una llave pública.

Semillas y mnemónicos (BIP-39)

(Palatinus, Rusnak, Voisine, Bowe, 2013)

Las *wallets HD* son bastante prácticas y demasiado útiles. Utilizando el estándar *BIP-39* en el cual se pueden crear semillas derivadas de una secuencia de palabras en inglés, permite recuperar, exportar o importar *wallets* de una manera muy sencilla. Este estándar define el mnemónico, el cual son una serie de palabras en inglés que son más fáciles de guardar y transcribir sin cometer un error. Si se quisiera copiar una llave privada, se podría cometer un error al momento de querer transcribir los números, sin embargo al momento de utilizar el nemónico esto es más fácil de escribir.

Almacenamiento

Una vez que las llaves son creadas, se tiene que buscar la forma de almacenarlas, para esto tenemos dos categorías, las cuales cambian por la rapidez con las que se puede hacer uso de ellas, cada una tiene sus ventajas y desventajas.

En la sección de tipos de clientes, se mencionan varios de los que actualmente existen, también se comenta acerca de la asociación indistinta entre los términos cliente y *wallet*, para los cuáles aún no existe mucha diferencia. Si bien en este apartado solo se agregara la *wallet* de escritorio, para ejemplificar lo que las otras tipos de *wallets* parecidas a esta tienen como características.

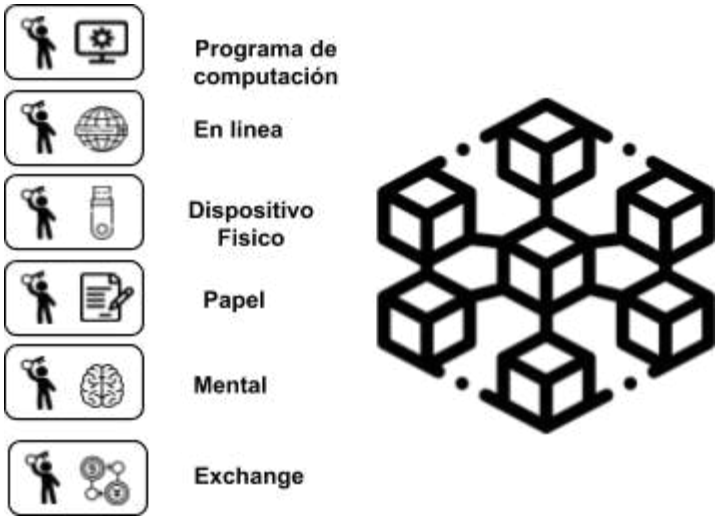


Gráfico hecho con iconos realizados por Freepik y smalllikeart en www.flaticon.com. Licencia Creative Commons BY 3.0 (CC 3.0 BY). http://creativecommons.org/licenses/by/3.0/

Hot wallets

Este tipo de *wallets* se caracterizan por estar siempre disponibles para el usuario de una manera casi instantánea, debido a que hay forma de acceder a estas utilizando *Internet*. Se recomienda utilizar este tipo de *wallets*, para realizar transacciones en las que se necesite estar moviendo los activos de una manera rápida, pero solo se aconseja tener pocos activos en ese tipo de *wallets* debido a que puede ser robada por algún atacante y con esto perder todos los activos que estaban asociados a esta.

Exchanges

Son los sitios que ofrecen la creación de una cuenta de manera sencilla y rápida sin poseer conocimientos técnicos del tema. Por lo general estos poseen la llave privada y solo proveen la llave pública. Es aconsejable dejar una cantidad pequeña de activos en este tipo de *wallets*, debido a que si en el sitio que está la llave privada es comprometido en seguridad de la información, los atacantes podrían disponer de todos los activos que se encuentran asociados a ellas.

Escritorio

Se utiliza un programa que se instala en la computadora y así permitir la administración de las llaves privadas y públicas, en este caso el usuario posee sus llaves, pero a pesar de ello queda expuesto, debido a que si algún atacante toma el control de la computadora, tomará el control de las llaves y con esto podrá disponer de todos los activos asociados a estas cuentas.

Cold wallets

Esta opción de *wallet*, es una de las prácticas más recomendadas si lo que se busca es almacenar una gran cantidad de activos por un largo periodo de tiempo. Su propósito es servir como *wallet* para recibir los activos y se recomienda sólo conectarla a la red para propósitos de realizar alguna transacción y acto seguido, volverla a desconectar.

Wallets fisicas

Son parecidas a una memoria *USB*, la cual posee almacenadas las llaves pública y privada, además contienen por lo general un *pin*, que sirve para poder administrar el dispositivo e incluso algunos modelos solicitan la confirmación física, piden al usuario que de *click* en ciertos botones para confirmar las operaciones cada vez que van a ser ejecutadas. Por lo general este tipo de *wallets* también ofrecen un mnemónico para que en el caso de extravío físico del dispositivo, exista un mecanismo para recuperar la *wallet* (Relacionado con lo que se expuso anteriormente relativo al estándar BIP-39).

En papel

Algunos sitios permiten crear *wallets* y dan la posibilidad de imprimir las llaves, incluso algunas ofrecen la opción de generar un código *QR*. El inconveniente es que si el papel se pierde, se perderá el control sobre la *wallet* y los activos asociados a ella.

En el cerebro

Este tipo de *wallet* se basa también en el estándar *BIP-39*, donde únicamente se tendrán que memorizar las palabras del mnemónico y recordarlas todas en el orden correcto, para que en el momento que se necesite utilizar la cuenta, se utilicen las palabras para generar la clave privada.

Multi firma

Este tipo son simplemente una forma de organizar una *wallet* compartida, en la que pueden estar registradas varias llaves, para administrar los activos que se posee en grupo. Por ejemplo una empresa con varios socios, tendrán que aceptar en su mayoría alguna operación, para que esta se ejecutará de manera satisfactoria.

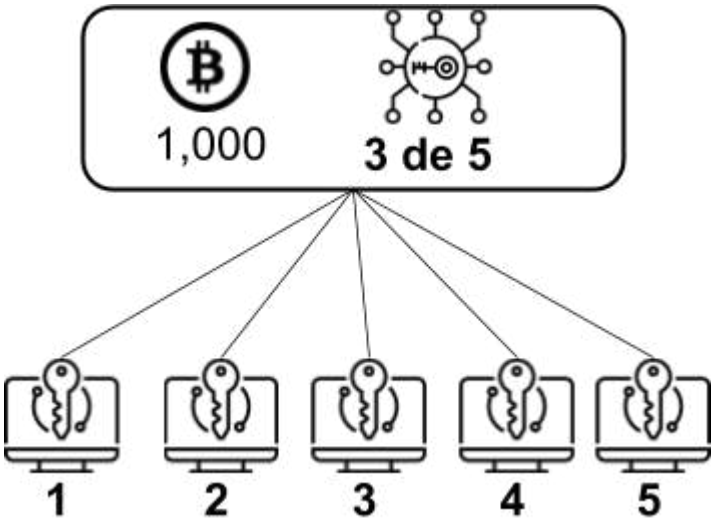


Gráfico hecho con iconos realizados por Freepik, Eucalyp & dmitri13 en www.flaticon.com. Licencia Creative Commons BY 3.0 (CC 3.0 BY). http://creativecommons.org/licenses/by/3.0/

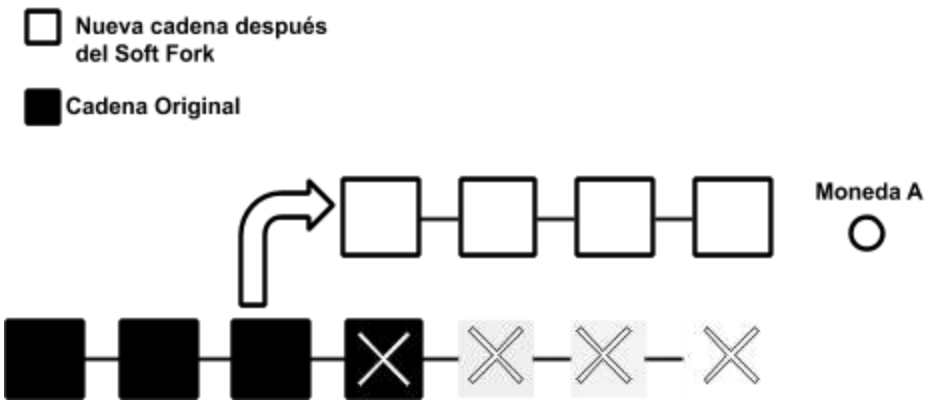
Forks

Este término se refiere a cuando se realizan actualizaciones en el protocolo, lo cual lleva a la modificación de reglas en menor o mayor grado. Lo que causará que dependiendo del tipo de modificación que se agregue, si los nodos seguirán o no aceptando los nuevos bloques que son generados y agregados a la *Blockchain*.

Soft fork

Este tipo de *fork* tiene compatibilidad con la versión antigua de reglas, por lo que permitirá validar antiguos y nuevos bloques. Un minero que actualice con el *soft fork* mantendrá el consenso, debido a que el nodo actualizado seguirá tanto las nuevas como las antiguas reglas.

Algo que puede ocurrir con este tipo de *fork*, es una divergencia temporal en donde los nodos que no han sido actualizados incumplirán algunas de las nuevas reglas, debido a que no las conocen. Este tipo de *fork* requiere que la mayoría de los nodos mineros actualicen, para que sigan las nuevas reglas.



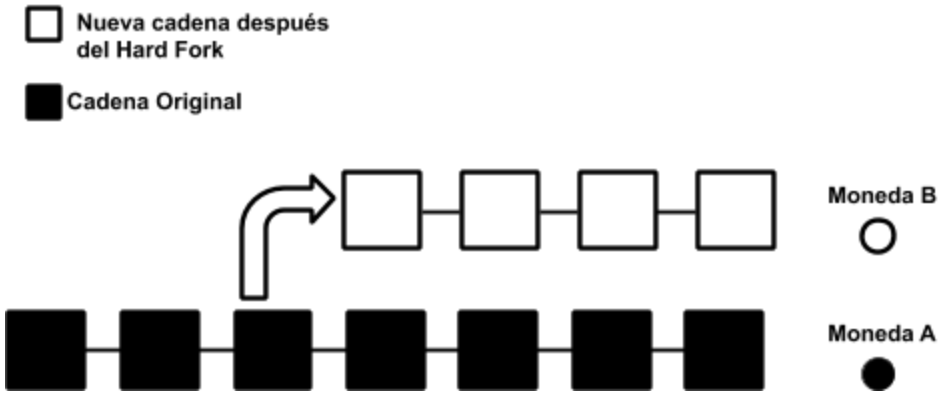
Un ejemplo de esto podría ser, que los originalmente los bloques que eran válidos, eran los bloques de 1MB, sin embargo se actualizo esa regla, y se acordó que en vez de ese tamaño, el tamaño fuera de la mitad 0.5 MB. Los nodos que hayan actualizado rechazaran las transacciones que tengan un tamaño de 1MB debido a que ahora solo se acepta la mitad de acuerdo con el nuevo conjunto de reglas. Esto causará un *fork* temporal.

Otro ejemplo más sencillo es cuando tienes una consola de videojuegos, si tienes una versión X, y se envía una actualización a la consola, podrás conectarte a jugar en línea y continuar con los servicios, de lo contrario no se permitirá que accedas hasta que actualices, en el caso de los nodos no se les obliga, sin embargo en cuanto más nodos comienzan a actualizar, los nodos que no han actualizado estan creando una rama temporal y solo están gastando recursos, debido a que al final prevalecerá la nueva versión, porque será aceptada por la mayoría de los nodos que están realizando el proceso de minado.

Hard fork

Este tipo de *fork* es completamente divergente con respecto a la versión anterior. Los *nodos* que tienen el conjunto anterior de reglas no aceptarán las nuevas. Este *fork* tiene cambios radicales al

protocolo lo que hace que los bloques previos y transacciones sean inválidas. Además las nuevas transacciones válidas en la nueva *Blockchain*, no serán reconocidas por la vieja *Blockchain*. En este caso todos los nodos que quieran soportar la nueva versión de la Blockchain, tendrán que actualizar. Esto generará dos *Blockchain*, en donde cada una seguirá agregando bloques válidos con respecto a las reglas aceptadas por los nodos.



Continuando con el ejemplo de la consola ‘X’, un *hard fork* es cuando se anuncia que saldrá la nueva consola ‘Y’, la cuál tiene otras especificaciones diferentes a las de la consola ‘X’, se tendrá que cambiar de consola. En este caso seguirán desarrollando algunos juegos exclusivos para la consola ‘X’ y se tendrá que adquirir el juego para la consola ‘X’, y en el caso de la consola ‘Y’ será lo mismo. Además no se podrán utilizar los juegos comprados para la consola ‘X’ en la ‘Y’ y viceversa.

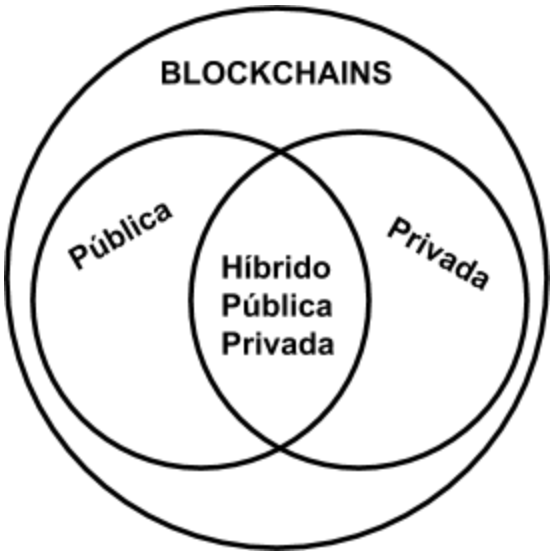
Por ejemplo, algunos *fork* conocidos en el caso de *Bitcoin*, son *Bitcoin Cash* y *Bitcoin Gold*.

Tipos de blockchain

Normalmente al momento de escuchar *Blockchain*, se piensa en las criptomonedas, lo cual no es erróneo pues ha sido uno de los usos más extendidos que ha tenido esta tecnología, empero esta tecnología permite realizar mucho más, por lo cual existen categorías de acceso a las *Blockchain*, por lo general, las *Blockchain* de las criptomonedas son públicas, sin embargo también pueden existir *Blockchain* privadas, por ejemplo alguna que tengan información sobre una cadena de

suministros o información militar. En estos casos, se debe limitar quién tiene acceso para leer y escribir en esa *Blockchain*.

De acuerdo a un informe publicado por el gobierno de Canadá, existen 4 diferentes tipos de clasificaciones (Zambrano, 2017). En donde dependiendo de lo que se necesite implementar, es el tipo de *Blockchain* que se deberá seleccionar:



Públicas

Sin permiso

Todos los nodos tienen acceso a la *Blockchain*, tienen derecho de leer y escribir sobre la misma. Generalmente las criptomonedas se encuentran ubicadas en esta categoría.

Con permiso

Los *nodos* tienen que autenticarse para tener permisos de escritura sobre la *Blockchain*. Soluciones de votaciones o sistemas de de denuncias, estarían ubicados en esta categoría.

Privadas

Sin permiso

Todos los nodos previamente definidos en la red privada, tienen acceso completo a la *Blockchain*. Ejemplos para esta categoría podrían ser cadenas de suministros, registros financieros del gobierno, o información sobre ganancias de una empresa.

Con permiso

Los nodos que pertenezcan a este tipo, deberán autenticarse para leer y escribir en la *Blockchain*. De igual manera, pueden existir ciertos nodos que solo tengan acceso a escribir, mientras que los demás solo tengan acceso de lectura. Ejemplos de esta categoría son en el ámbito de construcción, defensa nacional, recaudación de impuestos e información militar.

Híbridas

Este tipo de *Blockchain* utiliza los beneficios tanto de una *Blockchain* privada como de una pública. Cada organización debe tratar de adaptar los enfoques que considere más convenientes de acuerdo a las necesidades de su negocio.

Por ejemplo, en el caso de una empresa de logística, en la que un producto tiene que pasar por varias entidades, la parte privada puede ser utilizada para las transacciones entre los socios grandes que se tengan, podría ser la encargada de solo mostrar y permitir cambios en las partes, que cada actor tiene permitido realizar consultas o modificaciones. Mientras que la parte pública puede ser utilizada por empresas subcontratadas o socios pequeños para que realicen cambios en la *Blockchain* pública.

Side chains

Hasta el momento, se encuentran listadas un total de 2103 diferentes *Blockchain* en el sitio de *coinmarketcap.com.* Cada una de ellas, es un proyecto diferente que se encarga de cumplir con cierto tipo de necesidades y con su propio esquema de reglas.

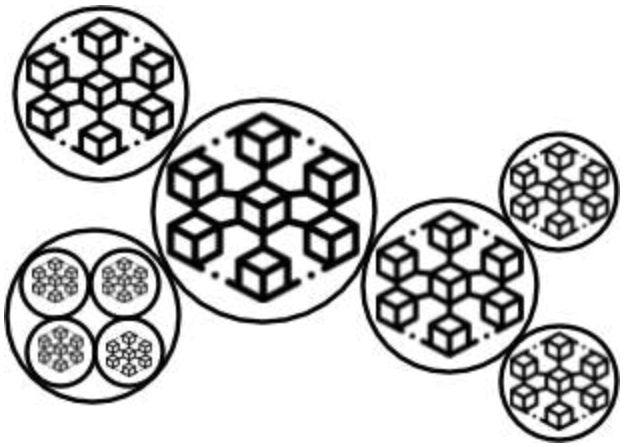


Gráfico hecho con iconos realizados por Freepik en www.flaticon.com. Licencia Creative Commons BY 3.0 (CC 3.0 BY). http://creativecommons.org/licenses/by/3.0/

Todo esto debido a que muchas veces no se llega a un consenso de que hacer con alguna *Blockchain* y simplemente las personas clonan el código fuente de una *Blockchain* y hacen su propia implementación, esto causa que existan muchas posibilidades, sin embargo cada una de estas redes es independiente y no existe mecanismo que permite que interactúen entre ellas.

Y esto es a lo que se refiere este término, a un concepto teórico de permitir la interacción entre las diferentes *Blockchain*, lo que permitiría trabajar a todas ellas como una sola, porque se podrían estar transfiriendo los *tokens* entre redes y utilizar las ventajas de algunas de ellas para llevar a cabo operaciones y después volver a regresar los *tokens* a la *Blockchain* que nos convenga.

Además esto permitiría un balanceo de carga, ya que se distribuiría entre todas las *Blockchain*, adicionalmente de que no se tendrían que hacer modificaciones muy grandes a las ya existentes, debido a que si se necesita alguna cosa en particular, simplemente se podría agregar esa nueva *Blockchain* para que se comunicará con las ya existentes y no habría necesidad de modificar ninguna.

Smart Contracts

Una de las mejores características de *Blockchain* es que es un sistema descentralizado que existe entre todas las partes que pertenezcan a esa red. No hay necesidad de intermediarios lo cual ahorra tiempo y conflictos a todos los involucrados en una posible ejecución de un contrato.

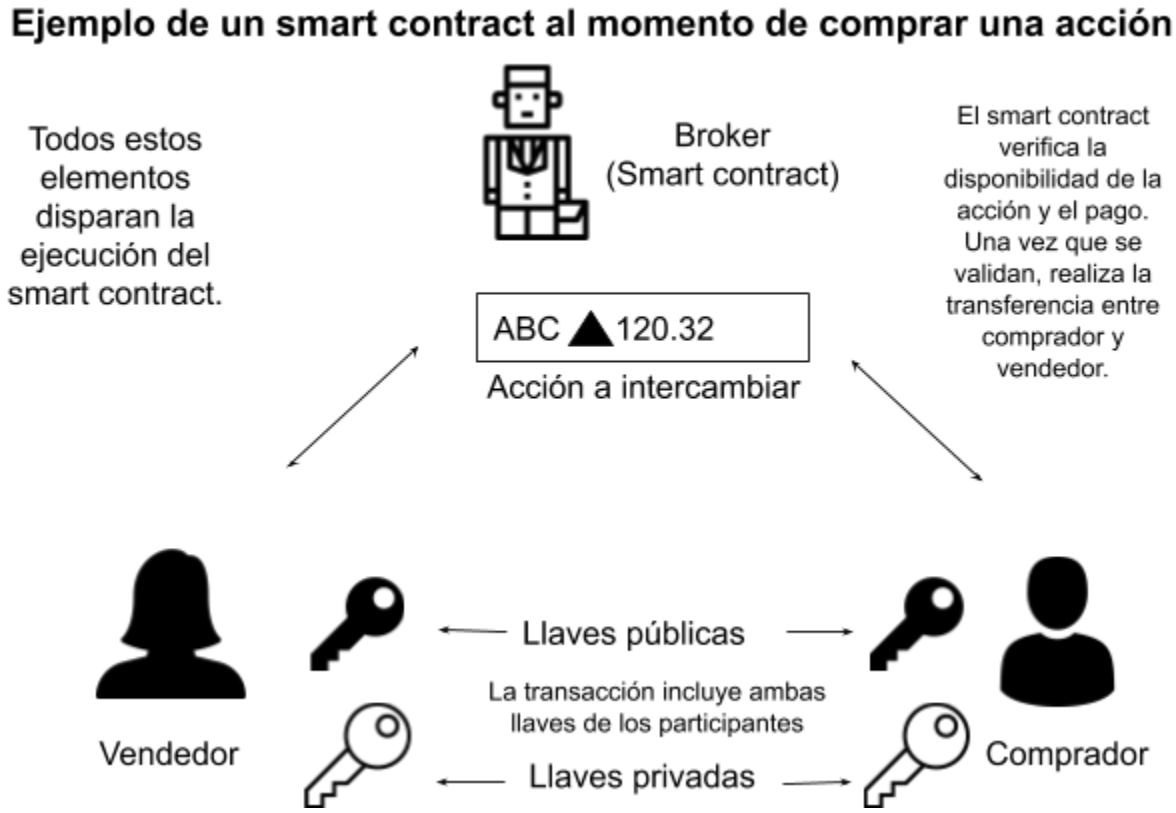


Gráfico hecho con iconos realizados por Pixel Perfect, Freepik, Yannick y smalllikeart en www.flaticon.com. Licencia Creative Commons BY 3.0 (CC 3.0 BY). http://creativecommons.org/licenses/by/3.0/

El autor Nick Szabo (1996) acuñó el término de «*smart contract*». Concibió que en un sistema descentralizado se podrían utilizar, los cuales son básicamente pasar un contrato de papel en código de computadora, para que una vez que se cumplan todos los requisitos, el contrato sea ejecutado de manera automática.

Este tipo de contratos pueden servir para intercambiar dinero, propiedades o cualquier valor que exista. Asimismo pueden funcionar de la siguiente manera; supongamos que una persona quiere vender acciones a otra, para esto normalmente necesitaría una serie de intermediarios, que den fe pública, por ejemplo de los fondos de la persona que quiere comprar las acciones, de la legítima propiedad de las acciones de la persona que las está ofreciendo, para todo esto normalmente se tendrían que poner de acuerdo entre bancos, *brokers*, entre otros. Todo este proceso se convierte en algo tardado y costoso, entonces simplemente con la creación de un *smart contract* la persona 'A' podría enviar su dinero al contrato, y la persona 'B' sus acciones. Una vez que el *smart contract* valide que todo es correcto, automáticamente transferirá la propiedad de las monedas a la persona 'B' y de las acciones a la persona 'A', todo esto sin la necesidad de que ningún tercero participe más allá de los involucrados en ese proceso de intercambio.

DAO's

DAO del inglés (*Distributed Autonomous Organization*) u Organización Autónoma Distribuida (Lipovyanov, 2019). Como su nombre lo indica, se trata de una organización fundamentada en los principios de la tecnología *Blockchain*.

Es una organización virtual definida por *smart contracts*. Las transacciones, reglas, contratos y todo lo relacionado con la empresa, es gestionado mediante la *Blockchain* en donde el código es ejecutado sin intervención externa y el estado del sistema es mantenido por el consenso de la *Blockchain*.

Una *DAO* puede poseer roles como de *CEO*, *managers*, entre otros y puede operar a través de voto colectivo. Los dueños de la *DAO*, son aquellos que poseen los *tokens* de la misma, estos *tokens* son similares a las acciones de una organización tradicional, lo que permite que estos puedan ser vendidos de manera interna o externa a cualquier persona.

Para comprender mejor este concepto, imaginemos que una persona posee 1,000 acciones de una organización en donde en total existen 10,000 acciones, esta persona tiene 10% del total de las acciones, esta persona puede transferir sus acciones a cualquier otra, con lo que otorga un porcentaje de la compañía al momento de realizar esa transacción. Los accionistas nombran a una junta directiva que controla la empresa, los cuáles a su vez, nombran a un *CEO* para que ejecute operaciones con el fin de contratar personal y llevar a cabo un plan de trabajo.

Una *DAO* es simplemente una versión digital de todos lo anteriormente expuesto, en donde todas las reglas y regulaciones están expresadas mediante líneas de código en vez de contratos en papel.

Aplicaciones Descentralizadas o DApps

La red de *Blockchain Bitcoin* posee algunas características importantes como su libro de cuentas abierto, la cantidad de bitcoins que estarán en circulación (Que son controlados por un algoritmo y no por una persona o grupo de personas) y por último su tecnología *peer-to-peer.* Todas estas características han creado un nuevo campo, en que se pueden crear aplicaciones descentralizadas, también conocidas popularmente como Dapps.

Las personas a lo largo de la humanidad han interactuado con muchas aplicaciones, son algo de su día a día, sin embargo, la gran mayoría de estas aplicaciones habrá sido probablemente aplicaciones centralizadas, en las cuales se interactúa con un modelo cliente/servidor, en donde alguien posee la infraestructura e información que captura, almacena y procesa el sistema. Por lo general son grandes, medianas o pequeñas empresas, las que poseen este tipo de infraestructura y este tipo de aplicaciones que se ejecutan dentro de su infraestructura y la información es controlada por ellos.

Algunos de estos ejemplos de este tipo de aplicaciones son, redes sociales, páginas de video, páginas de transmisión en vivo, correos electrónicos, buscadores, etc. La lista es bastante grande.

Estas páginas ofrecen un servicio, y los usuarios acceden a ellas a través de sus servidores, por lo que se tiene que crear una cuenta en su sistema, para poder hacer uso de él.

Estas aplicaciones además de ser centralizadas son distribuidas, con lo que son parte de una empresa, pero el procesamiento se realiza de una manera distribuida entre todos los servidores que son parte de la red de la empresa, como en el caso de Google, cuando se hace una búsqueda, y la información es procesada por varios servidores, para en poco tiempo entregar un resultado. Una de las características de un sistema distribuido, es que le haga sentir al usuario cómo que solo está utilizando un sistema, cuando en realidad podría estar utilizando cientos de ellos, sin ser consciente de esto, esta característica se conoce como transparencia de un sistema distribuido.

Una vez definido todo lo anterior, se puede hablar de aplicaciones distribuidas descentralizadas, en donde además de tener características de un sistema distribuido como transparencia, concurrencia, tolerancia a fallos entre otros. No pertenecen a una entidad de personas llámese gobierno o empresa. Es un sistema que es mantenido por las propias personas, y no tiene un dueño.

Entonces nace este nuevo paradigma de aplicaciones distribuidas que son mantenidas por la red Blockchain, y accesibles por todos los interesados que deseen hacer uso de ellas, un caso específico de este tipo de aplicaciones es: Smart Contracts, las DAOs que se mencionaron en el tema anterior, las DABs (Bancos autónomos distribuidos), o como abrió el debate el usuario Sheldoon182 en un foro de Bitcoin: las DASs (Sociedad Autónoma Distribuida) (BitcoinTalks, 2015), entre otros.

Halving

Para entender este concepto conviene tomar como referencia a los Bancos centrales de cada país como ejemplo. Digamos que el banco central de un país X tiene como objetivo principal mantener la estabilidad de los precios a través del control en el tipo de inflación y estos bancos

son el único proveedor de dinero de su país, por lo que cada uno de ellos tiene que diseñar una política monetaria para analizar la situación presente y crear un plan de acción.

En el caso de las *Blockchain*, por lo general no hay una entidad central que la controle, sino que la misma red se tiene que regular a sí misma. Por ejemplo en el caso de *Bitcoin*, al no existir una autoridad que regule la cantidad que se produce, lo que la regula es un algoritmo, el cual cada 210,000 bloques (aproximadamente cada 4 años, debido a que la confirmación de un bloque tarda aproximadamente 10 minutos) va decrementando en un 50% la cantidad de *bitcoins* que se generan como recompensa. La recompensa comenzó siendo por 50 *bitcoins*, sin embargo con el paso del tiempo esta tasa de recompensa ha ido disminuyendo, actualmente en el año 2019 la recompensa es de 12.5 *bitcoins*.

El próximo *halving* ocurrirá en 2020 lo cual implica una nueva disminución del 50% en la recompensa por minar los bloques de la red, esta recompensa finalizará en el bloque 6.930.000 la cual ocurrirá en algún punto del año 2140.

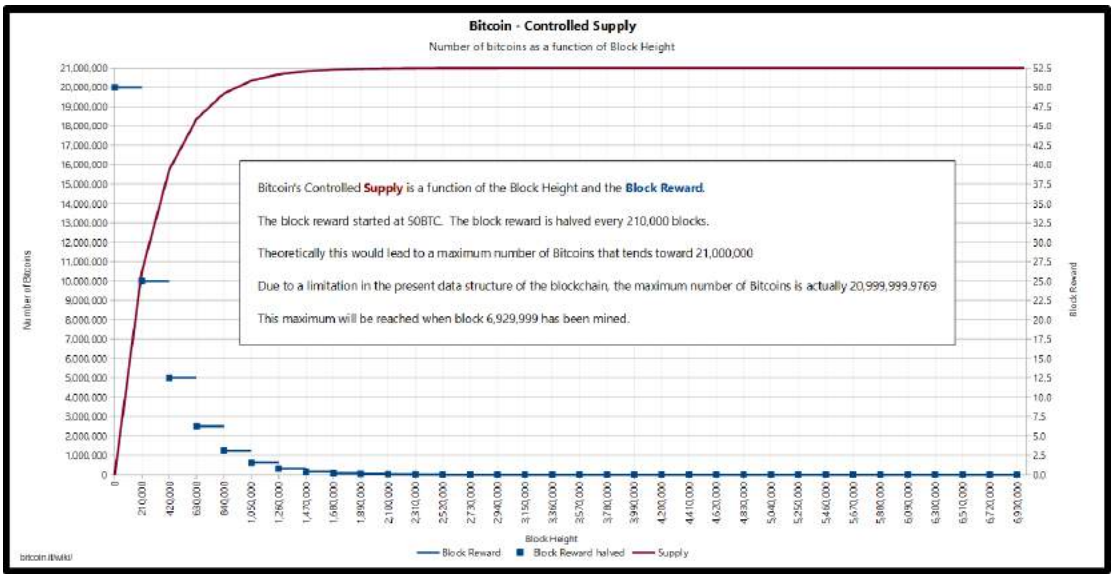


Imagen obtenida de https://en.bitcoin.it/wiki/Controlled_supply

Democracia con Blockchain

Explicado de manera breve qué es y cómo funciona *Blockchain* es menester mencionar que en lo que respecta a una votación, el problema de las boletas o sistemas actuales es que pueden ser fácilmente manipulables o hasta perdedizos, no obstante el sistema por cadena de bloques, es decir *Blockchain*, da certeza a eliminar la desconfianza en las elecciones, convirtiéndolas en más seguras y transparentes. En las votaciones tradicionales, puede que se respete el principio de voto libre y secreto ofreciendo anonimato a los votantes, sin embargo el escrutinio no es transparente, basando toda decisión en la autoridad electoral.

Con un sistema *Blockchain*, acompañado de *smart contracts*, es decir contratos inteligentes, se permitirá que los electores puedan votar, así como verificar y recontar los votos de una manera descentralizada. En pocas palabras, si un delincuente informático *hacker* o *cracker* como se le quiera llamar, intentara penetrar la red, se encontraría con una red completa de dispositivos impidiéndole tener el control de esta.

Poco a poco las formas de autenticación han evolucionado tanto, que han dado más certeza al autorizar a los electores por diversos medios, por mencionar un ejemplo tenemos la manera biométrica, ahora bien, si utilizáramos las diferentes maneras de autenticación junto con una cadena de bloques, esto sería una gran solución a muchos de los problemas que se han suscitado en la actualidad, ya que su verificación sería por criptografía, lo que daría mayor seguridad a los usuarios.

Los requisitos que deben cumplirse para intentar materializar una elección política, es que se debe promover una identidad digital, así como mantener la confidencialidad, integridad y disponibilidad de la bases de datos de los electores, mantener un *hardware* seguro y también todos los sistemas automatizados, además que no puede faltar una auditoría o auditabilidad previo a la votación y posterior a esta para cotejar y corroborar los resultados obtenidos.

Estonia implementa el voto electrónico desde el 2005, no obstante es un sistema donde los votantes pueden iniciar sesión y votar tantas veces como lo deseen durante el período previo a la votación, así como cada voto cancela el último, un votante siempre tiene la opción de cambiar su voto más tarde, pero dejando por un lado su sistema de votación, Estonia tiene servicios basados en *Blockchain*, implementa una tecnología *Keyless Signature Infrastructure* (KSI) y con la cadenas de bloques, esto utiliza la criptografía de función *hash*, permitiendo que la verificación se base en la seguridad de las funciones *hash* y disponibilidad de la red *Blockchain*.

Otros países han utilizado esta tecnología específicamente en elecciones políticas, pero no de manera directa y completa, por ejemplo el país Sierra Leona, que pese a que los medios de difusión se han pronunciado a decir que es el primer país que utilizó *Blockchain* para conteo de votos, la realidad es que se ejecutó junto con el proceso normal como una demostración de cómo la elección podría llevarse a cabo utilizando la tecnología *Blockchain*. (Pollock, 2018)

Otra votación importante de menor escala fueron las elecciones del Estado de Virgina Occidental de los Estados Unidos de América, que se utilizó esta red pero únicamente para miembros militares desplegados, otros ciudadanos elegibles para votar en ausencia bajo la regulación *Uniformed and Overseas Citizens Absentee Voting Act* (UOCAVA), y sus cónyuges y dependientes. (Alexandre, 2018).

Denver de los Estados Unidos de América, usará la plataforma *Blockchain* de votación móvil dirigida a los votantes extranjeros en las elecciones. Recientemente, varias ciudades importantes del mundo revelaron planes para la implementación de la tecnología de *Blockchain* en sistemas de votación: Moscú , la capital de Rusia , Seúl , la capital de Corea del Sur y el gobierno catalán, entre otros. (Yakubowski, 2019).

Algunas plataformas actuales para el voto en *Blockchain* son https://votem.com, https://voatz.com, https://followmyvote.com, http://www.boule.one, https://democracy.earth, https://www.agora.vote, http://votewatcher.com, https://votosocial.github.io/.

Sin lugar a dudas la tecnología *Blockchain*, ha llegado para cambiar paradigmas en diversos ámbitos. En cuestión democrática y gubernamental tiene bastante potencial, sobre todo para estos tiempos con conectividad, en donde los ciudadanos han cambiado de ser solo personas que se preocupaban por ejercer su derecho de emitir su voto para elegir a sus representantes, ahora son personas que se interesan cada vez más por sus países y la forma en que son administrados.

Los ciudadanos están cambiando y necesitan que el sistema democrático se adapte a las nuevas necesidades, porque los gobernantes son el reflejo del pueblo y en un pueblo de gente preocupada en velar por el interés común, los gobernantes y el sistema se alinearán con este ideal que la humanidad está por alcanzar, convirtiéndonos en ciudadanos conectados, ciudadanos del futuro que ya es un presente.

Referencias

Alexandre, A. (2018). US: West Virginia Completes First Blockchain-Supported State Elections. Recuperado de: https://cointelegraph.com/news/us-west-virginia-completes-first-blockchain-supported-state-elections

Alexy, R. (1997). Teoría de los derechos fundamentales. Centro De Estudios Constitucionales Madrid.

Antonopoulos, A. (2017). Mastering Bitcoin: Programming the Open Blockchain. O'Reilly Media, Inc.

Anwar, H. (2018). Consensus Algorithms: The Root Of The Blockchain Technology. Recuperado de: https://101blockchains.com/consensus-algorithms-blockchain/#5

Ashton, K. (2009). That 'Internet of Things' Thing In the real world, things matter more than ideas.. Recuperado de: https://www.rfidjournal.com/articles/view?4986

Back, A. (1997). Hashcash - A denial of service counter-measure. Recuperado de: http://www.hashcash.org/hashcash.pdf

BBC Mundo (2018). 3 noticias falsas que propiciaron guerras y conflictos alrededor del mundo. Recuperado de: https://www.bbc.com/mundo/noticias-43725918

BBC Mundo. (2018). BBC Mundo. (2018). 5 claves para entender el escándalo de Cambridge Analytica que hizo que Facebook perdiera US$37.000 millones en un día. https://www.bbc.com/mundo/noticias-43472797

bit2me (s.f.). Glosario de conceptos sobre Bitcoin & Blockchain. Recuperado de: https://academy.bit2me.com/diccionario-crypto/

BitcoinTalks (2015). Distributed Autonomous Society. Recuperado de https://bitcointalk.org/index.php?topic=1092734.0

Bobbio, N. (1986). El futuro de la democracia. Traducción de José F. Fernández Santillán. Fondo de Cultura Económica México.

Bostrom, N. (2003). The Transhumanist FAQ -A General Introduction- Version 2.1 (2003). Published by the World Transhumanist Association. Consultable en: https://nickbostrom.com/views/transhumanist.pdf

Bostrom, N. (2006). Why I Want to be a Posthuman When I Grow Up. [Published in: Medical Enhancement and Posthumanity, eds. Bert Gordijn and Ruth Chadwick (Springer, 2008): pp. 107-137. First circulated: 2006] Consultable en: https://nickbostrom.com/posthuman.pdf

Buterin, V. (2015). Understanding Serenity, Part 2: Casper. Recuperado de: https://blog.ethereum.org/2015/12/28/understanding-serenity-part-2-casper/

Buterin, V., & Griffith, V. (2017). Casper the friendly finality gadget. Recuperado de: https://github.com/ethereum/research/blob/master/papers/casper-basics/casper_basics.pdf

California Legislative Information (2018). S.3127 - Bot Disclosure and Accountability Act of 2018 115th Congress (2017-2018). https://www.congress.gov/bill/115th-congress/senate-bill/3127

Clynes M., & Kline N. (1960). Cyborgs and space.

Dahl, R. (1999). La democracia Una guía para los ciudadanos. Editorial Taurus.

Dai, W. (1998). B-money. Recuperado de: www.weidai.com/bmoney.txt

Democracy.earth (2018). The Social Smart Contract. An open source white paper. Version 0.2: January 25th, 2018. Consultable en: http://paper.democracy.earth/

Dwork, C., & Naor, M. (1992). Pricing via processing or combatting junk mail. In Annual International Cryptology Conference. Recuperado de: http://www.hashcash.org/papers/pvp.pdf

Elpais.com (2018). Un robot se presenta a la alcaldía de un distrito de Tokio para acabar con la corrupción. Madrid 18 ABR 2018 - 15:10 CDT. Obtenido de: https://elpais.com/internacional/2018/04/18/mundo_global/1524045163_744119.html

Fernández, R. (2001). Glosario básico inglés-español para usuarios de Internet 4ª edición Con vocabulario español-inglés. Asociación de Técnicos de Informática (ATI) España.

Ferrajoli, L. (2011) Principia iuris Teoría del derecho y de la democracia 2. Teoría de la democracia. Trotta.

Ferrajoli, L. (2011). Poderes salvajes: la crisis de la democracia constitucional. Trotta.

Ferrajoli, L. (2011). Principia iuris Teoría del derecho y de la democracia. 1. Teoría del derecho. Trotta.

Finney, H. (2004). Rpow: Reusable proofs of work. Recuperado de: https://nakamotoinstitute.org/finney/rpow/index.html

Fruchter N., Specter M. & Yuan B. (2018). Facebook/Cambridge Analytica: Privacy lessons and a way forward. Recuperado de: https://internetpolicy.mit.edu/blog-2018-fb-cambridgeanalytica/

Github.com. (2018). Proof of Stake FAQs. Recuperado de: https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQs#what-is-proof-of-stake

González, M. (2018). Qué ha pasado con Facebook: del caso Cambridge Analytica al resto de polémicas más recientes. Recuperado de: https://www.xataka.com/legislacion-y-derechos/que-ha-pasado-con-facebook-del-caso-cambridge-analytica-al-resto-de-polemicas-mas-recientes

Guastini, R. (2000). ¿Separación de los poderes o división del poder?. Revista Biblioteca Jurídica Virtual IIJ UNAM.

Habermas, J. (1987). Teoría de la acción comunicativa. Editorial Taurus, Madrid.

Habermas, J. (1998). Facticidad y validez. Trotta, Madrid.

Harari, Y. (2016). Homo deus: Breve historia del mañana. Editorial Debate.

Haraway, D. (1995). Manifiesto para Cyborgs. Centro de Semiótica y Teoría del Espectáculo, Universitat de València.

Hardt S. & Lopes, L. (2015). Google Votes: A Liquid Democracy Experiment on a Corporate Social Network. Consultable en: https://www.tdcommons.org/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1092&context=dpubs_series

Hobbes, T. (1651). Leviatán, o la materia, forma y poder de una república eclesiástica y civil.

Howard, P. (2015). The Internet of Things is Poised to Change Democracy Itself. Recuperado de: https://comprop.oii.ox.ac.uk/research/public-scholarship/the-internet-of-things-is-poised-to-change-democracy-itself/

Hughes, J. (2002). Democratic Transhumanism 2.0 James Hughes Ph.D. Public Policy Studies 71 Vernon St. Hartford, CT 06106 860-297-2376. Consultable en: www.changesurfer.com/Acad/DemocraticTranshumanism.htm

Hughes, J. (2004). Citizen cyborg: Why democratic societies must respond to the redesigned human of the future. Basic Books.

Hugo, V. (1862). Los Miserables, título original en francés: les misérables.

Harari, Y. (2016). Homo Deus: breve historia del mañana. Penguin Random House

IBM. (s.f.). Transforming digital identity into trusted identity. Obtenido de: https://www.ibm.com/blockchain/solutions/identity

IDEA. (2011). Una introducción al voto electrónico: Consideraciones esenciales. Recuperado de: https://www.idea.int/sites/default/files/publications/una-introduccion-al-voto-electronico.pdf

IFLA. (2017). ¿Esta noticia es falsa? Infografia. Recuperado de: https://www.ifla.org/files/assets/hq/topics/info-society/images/how_to_spot_fake_news_-_spanish.pdf

INEGI. (2017) Tecnologías de la información y comunicaciones percepción sobre ciencia y tecnología TIC's en hogares. Consultable en: http://www.beta.inegi.org.mx/temas/ticshogares/

Jiménez, A. (2017). Facebook apaga una inteligencia artificial que había inventado su propio idioma. Obtenido de: https://www.elmundo.es/tecnologia/2017/07/28/5979e60646163f5f688b4664.html

Johnston, L. (2018). There's an AI Running for the Mayoral Role of Tama City, Tokyo April 12, 2018 12:00 pm. Obtenido de: http://www.otaquest.com/tama-city-ai-mayor/

Kaspersky (2018). IT threat evolution Q3 2018. Statistics. Obtenido de: https://securelist.com/it-threat-evolution-q3-2018-statistics/88689/

Kol, T. (2018). How a Blockchain Can Help You on a Deserted Island. Recuperado de: https://hackernoon.com/why-decentralized-consensus-blockchain-is-good-for-business-5ff263468210

Kol, T. (2018). How to Run a Blockchain on a Deserted Island with Pen and Paper. Recuperado de:

https://hackernoon.com/how-to-run-a-blockchain-on-a-deserted-island-with-pen-and-paper-899949ec555b

Lamport, L., Shostak, R., & Pease, M. (1982). The Byzantine generals problem. ACM Transactions on Programming Languages and Systems, Vol. 4, No. 3. Recuperado de: https://people.eecs.berkeley.edu/~luca/cs174/byzantine.pdf

Lijphart, A. (2000). Modelos de democracia Formas de gobierno y resultados en treinta y seis países. Editorial Ariel S.A. Barcelona.

Lipovyanov, P. (2019). Blockchain for Business 2019. Packt Publishing

Llamas J., Llamas I. (2018). Internet ¿Arma o Herramienta?. Editorial CUCSH UDG. Recuperado de: http://www.publicaciones.cucsh.udg.mx/kiosko/2018/internet_arma_o_herramienta_Ebook.pdf

Locke, J. (1690). Segundo Tratado sobre el gobierno civil.

Madison (1788). El Federalista número 51.

Mann, S., & Niedzviecki, H. (2001). Cyborg: Digital destiny and human possibility in the age of the wearable computer. Doubleday Canada.

Martí, A. (2018). Sí, alguien ha impreso una cara en 3D para intentar burlar el reconocimiento facial de los móviles, y sólo se salva uno. Consultado de: https://www.xataka.com/seguridad/alguien-ha-impreso-cara-3d-para-intentar-burlar-reconocimiento-facial-moviles-solo-se-salva-uno

Maturana, H. & Varela, F. (1995). De máquinas y seres vivos. Autopoiesis: la organización de lo vivo. Editorial Universitaria.

Montesquieu, B. (1748). Del Espíritu de las Leyes.

Müller, E. (2019). Alemania sufre el mayor 'hackeo' de su historia con la filtración de datos personales de centenares de políticos. Recuperado de: https://elpais.com/internacional/2019/01/04/actualidad/1546595085_679572.html

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Recuperado de: https://bitcoin.org/bitcoin.pdf

Olson, N. (2013). Do you Want to be a Cyborg, or a Transhuman?. IEET. Obtenido de: https://ieet.org/index.php/IEET2/more/olson20130105

Palatinus M., Rusnak P., Voisine A., Bowe S. (2013). Mnemonic code for generating deterministic keys. Recuperado de: https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki

Periódico Oficial del Estado de Jalisco (2018). «DECRETO DIGELAG DEC 06/2018 del Ciudadano Gobernador Constitucional del Estado de Jalisco mediante el cual se declara al Robot Humanoide Sophia de nacionalidad del Reino de Arabia Saudita, como huésped distinguida del Estado de Jalisco. Pág. 3» Miércoles, Abril 4, 2018 Sección BIS EDICIÓN ESPECIAL No. 19. Consultado en: https://periodicooficial.jalisco.gob.mx/sites/periodicooficial.jalisco.gob.mx/files/04-04-18-bis.pdf

Pollock, D. (2018) Blockchain For Elections: Advantages, Cases, Challenges. Recuperado de: https://cointelegraph.com/news/blockchain-for-elections-advantages-cases-challenges

Prince, A. (2006). Consideraciones, aportes y experiencias para el voto electrónico en Argentina. Editorial Dunken.

Raya, A. (2016). La IA de Google se ha inventado su propio idioma secreto. Obtenido de: https://omicrono.elespanol.com/2016/11/idioma-para-inteligencia-artificial/

Riofrío, J.. (2014). la cuarta ola de derechos humanos: los derechos digitales en Revista Latinoamericana de Derechos Humanos Volumen 25 (1), I Semestre 2014. Universidad Nacional Costa Rica.

Rodotá, S. (2014). El derecho a tener derechos. Trotta.

Rousseau, J. (1762). El Contrato social, ó, Principios del derecho político.

Sartori, G. (2012). ¿Qué es la democracia?. Penguin Random House Grupo Editorial México.

Schopenhauer, A. (2003). El arte de tener razón expuesto en 38 estratagemas, traducción de D. Garzón, Madrid, Edaf.

SCJN (2008). Registro No. 170 238 ÓRGANOS CONSTITUCIONALES AUTÓNOMOS. SUS CARACTERÍSTICAS. Localización: [J]; 9a. Época; Pleno; S.J.F. y su Gaceta; Tomo XXVII, Febrero de 2008; Pág. 1871. P./J. 12/2008.

Soroush V., Deb R., Sinan A. (2018). The spread of true and false news online. Recuperado de: science.sciencemag.org/content/359/6380/1146

Szabo, N. (1996). Smart Contracts: Building Blocks for Digital Markets. Recuperado de: www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html

Szabo, N. (1997). The God Protocols. Consultado en: https://nakamotoinstitute.org/the-god-protocols/

Szabo, N. (1998). Bit Gold: Towards Trust-Independent Digital Money. Recuperado de: https://web.archive.org/web/20140406003811/http://szabo.best.vwh.net/bitgold.html

Theguardian.com. (2018). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. Recuperado de: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

Trackalytics.com. (2019). The Most Followed Twitter Profiles. Recuperado de: https://www.trackalytics.com/the-most-followed-twitter-profiles/page/1/

Ugalde, F. (2010). Órganos constitucionales autónomos. Revista del Instituto de la Judicatura Federal Número 29.

University of Nicosia. (2019). MSc in Digital Currency DFIN-511: Introduction to Digital Currencies. Session 2 The Byzantine Generals' Problem & the Bitcoin Solution.

University of Nicosia. (2019). MSc in Digital Currency DFIN-511: Introduction to Digital Currencies. Session 4 Bitcoin in Practice – Part 1 Bitcoin clients, online wallets, paper wallets, cold storage, sending and receiving.

Unión Internacional de Telecomunicaciones. (2012). Y.2060: Panorámica de internet de las cosas Recomendación Y.4000 / Y.2060 (06/12) Aprobado en 2012-06-15. Recuperado de: https://www.itu.int/rec/T-REC-Y.2060-201206-I

Usa.gov (2018). Proceso electoral presidencial Cómo funciona el proceso electoral en Estados Unidos en las elecciones presidenciales. Recuperado de: https://www.usa.gov/espanol/proceso-electoral

Vargas, J. (2007). Barack Obama, Social Networking King. Recuperado de: http://voices.washingtonpost.com/44/2007/10/barack-obama-social-networking.html

Villa, C. (2018). CEREBRO un sistema inteligente para dirigir campañas. Editorial Universidad de Guadalajara. Consultable en: http://www.publicaciones.cucsh.udg.mx/kiosko/2018/libro_electronico%20cerebro.pdf

Walzer, M. (2001). Guerras justas e injustas. Un razonamiento moral con ejemplos históricos. Editorial PAIDÓS.

Woolley, S. & Howard, P. (2017). Computational Propaganda Worldwide: Executive Summary. Obtenido de: https://comprop.oii.ox.ac.uk/research/working-papers/computational-propaganda-worldwide-executive-summary/

Wuille, P. (2012). Hierarchical Deterministic Wallets. Recuperado de: https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki

Yaga D., Mell P., Roby N., Scarfone K. (2018). NISTIR 8202 Blockchain Technology Overview. National Institute of Standards and Technology. Recuperado de: https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf

Yakubowski, M. (2019). US: Denver to Use Mobile Voting Blockchain Platform Aimed at Overseas Voters in Elections. Recuperado de: https://cointelegraph.com/news/us-denver-to-use-mobile-voting-blockchain-platform-aimed-at-overseas-voters-in-elections

Zambrano, R. (2017). Blockchain Unpacking the disruptive potential of blockchain technology for human development White Paper. Licensed under the Creative Commons Attribution 4.0 license (https://creativecommons.org/licenses/by/4.0/) Recuperado de: https://idl-bnc-idrc.dspacedirect.org/bitstream/handle/10625/56662/IDL-56662.pdf?sequence=2&isAllowed=y

Zipper, R. (1995). Ciencia política. Editorial Universitaria.

DEMOCRACIA TECNOLÓGICA.

Las tecnologías de la información y comunicación, son un pilar fundamental para el desarrollo de la humanidad, siendo utilizadas como objeto, medio y fin. Son tan importantes en la vida humana, que han realizado cambios trascendentes en los paradigma contemporáneos, respecto a la democracia, participación social, legitimidad y organización, teniendo como resultado nuevas percepciones de ver el mundo. Es así que la presente investigación pretende abordar a grosso modo las intersecciones entre las tecnologías disruptivas y la sociedades contemporáneas, abordando temas de democracia, gobernanza, terceros de confianza, comunicaciones entre las personas y las máquinas, big data, objetos como el Internet de las cosas, los cyborg y la inteligencia artificial, concluyendo con Blockchain o mejor conocida como cadena de bloques, la cual se define como un registro contable de tecnología descentralizada, distribuida y actualizada mediante mecanismos de consenso que ha llegado para revolucionar el mundo.