# Cuando la gobernanza de los algoritmos falla: el caso The DAO

## When the governance of algorithms fails: The DAO case

Javier Sandoval Archila*

* Ph. D. Docente-Investigador, Observatorio de Economía y Operaciones Numéricas (ODEON), Universidad Externado de Colombia, Bogotá (Colombia). [javier.sandoval@uexternado.edu.co], [ORCID ID: 0000-0001-9862-9613].
Artículo recibido: 8 de mayo de 2023
Aceptado: 26 de junio de 2023

Para citar este artículo:
Sandoval Archila, J. (2023). Cuando la gobernanza de los algoritmos falla: el caso The DAO. *Odeon*, 24, 55-70.
DOI: https://doi.org/10.18601/17941113.n24.04

## Resumen

Este artículo explora los desafíos de la gobernanza algorítmica utilizando el estudio de caso de The DAO, una efímera tentativa de crear una organización autónoma descentralizada en la plataforma de *blockchain* Ethereum. A pesar de su breve existencia y la significativa pérdida de inversión debido a una explotación de seguridad, The DAO ofrece ideas críticas sobre las formas emergentes de autoridad algorítmica, la gobernanza práctica de sistemas autónomos y descentralizados, y las posibles fallas en el diseño de incentivos y la modelización de acciones. El artículo también profundiza en el problema de agencia en economía y la gobernanza corporativa, ilustrando cómo estos conceptos se entrelazan con la gobernanza algorítmica.



**Palabras clave:** gobernanza algorítmica; Etherium; DAO.

**Clasificación JEL:** D23, D74, O33.



## Abstract

This article explores the challenges of algorithmic governance using the case study of "The DAO", an ephemeral attempt to create a decentralized autonomous organization on the Ethereum blockchain platform. Despite its brief lifespan and significant loss of investment due to a security exploit, The DAO offers critical insights into emerging forms of algorithmic authority, the practical governance of autonomous and decentralized systems, and the potential failures in designing incentives and modeling actions. The article also delves into the agency problem in economics and corporate governance, illuminating how these concepts intertwine with algorithmic governance.



**Key words**: Algorithmic governance; Etherium; DAO.

**JEL classification:** D23, D74, O33**.**


## Introducción

En la intersección de la economía, la tecnología y el derecho surge la gobernanza algorítmica, un paradigma que explora cómo se toman y aplican las decisiones dentro de sistemas automatizados. Los desafíos asociados a este nuevo modelo de gobierno son múltiples y complejos, particularmente en cuanto al problema de agencia, un concepto central en economía y teoría organizacional.

Este artículo se centra en el estudio de caso de The DAO, una efímera tentativa de crear una organización autónoma descentralizada en la plataforma de *blockchain* Ethereum. Lanzado en junio de 2016, The DAO consiguió una

inversión sin precedentes de 250 millones de dólares. Sin embargo, pocos días después de su lanzamiento, The DAO fue explotado y drenado en casi 3,7 millones de tokens de Ethereum.

A pesar de su fracaso, The DAO representa un artefacto importante para entender las formas emergentes de autoridad algorítmica y la gobernanza práctica de sistemas autónomos y descentralizados. Durante años, los defensores idealistas de la tecnología *blockchain* han sostenido que el "código es ley". Esta idea de "autoridad algorítmica", identificada por Frank Pasquale (2011) (como "autoridad automatizada"), postula que los sistemas de toma de decisiones basados en algoritmos podrían ser suficientes para gobernar.

La existencia de armas autónomas, coches autoconducidos y, por supuesto, The DAO, pone de relieve el desafío de integrar socialmente estas tecnologías. Para ello se requieren formas de gestión del riesgo, diseño y desarrollo internos, soluciones de mercado, autorregulación de la industria y regulación estatal. The DAO introdujo una tecnología innovadora para experimentar con cuestiones de gobernanza y nuevos modelos de sociedad, especialmente en aplicaciones dirigidas a empresas.

Las entidades corporativas dependen de la conexión entre los accionistas y los administradores, así como de la eficacia de estas relaciones de agencia para funcionar eficientemente. Sin embargo, la desconexión entre la dirección que toma decisiones y los intereses de los propietarios puede causar conflicto debido a los intereses divergentes entre sus roles. Por lo tanto, las corporaciones enfrentan costos adicionales para gobernar de manera efectiva producto de las divergencias que surgen de la estructura de las relaciones de agencia. En este sentido, la creación de The DAO estuvo motivada por el incentivo de eliminar los costos de agencia que se generan a través de las relaciones de agencia.

A partir de lo anterior, este artículo se propone examinar cómo The DAO sirve como un caso de estudio para entender las formas emergentes de autoridad algorítmica, explorar los modos prácticos de gobernanza para sistemas autónomos y descentralizados, y entender cómo pueden fallar los diseños de incentivos y modelos de acción.

Primero se presentarán las generalidades de la red Etherium. Posteriormente, se hablará de contratos inteligentes y los DAO como un caso particular. Después, se desarrollará el auge y la caída de The DAO. Por último, el artículo expone algunas conclusiones.

## 1. Generalidades de la red Etherium

Blockchain es una tecnología de registro inmutable y distribuido que se utiliza para diversos fines. A pesar de ser conocida principalmente por su uso en transacciones criptográficas, su alcance va más allá de las criptomonedas. La información registrada en un *blockchain* es transparente y puede ser vista por todos, lo que promueve la integridad y la confiabilidad de los datos.

Ethereum y Bitcoin son dos de las plataformas de *blockchain* más reconocidas, pero sirven a propósitos distintos y tienen características intrínsecas diferentes. Bitcoin fue la primera criptomoneda y su *blockchain* se desarrolló para facilitar un sistema de efectivo digital de igual a igual, que permite a los participantes realizar transacciones en línea.

Por otro lado, Ethereum es una plataforma de *blockchain* que ofrece herramientas para que los desarrolladores construyan aplicaciones descentralizadas. A diferencia de Bitcoin, estas aplicaciones pueden utilizarse para diversos fines, extendiendo el alcance de lo que se puede lograr con la tecnología *blockchain*.

Una diferencia clave entre estas dos plataformas radica en sus mecanismos de consenso. El consenso es esencial para mantener la integridad y la seguridad de un *blockchain*, ya que asegura que todas las transacciones y bloques sean verificados y acordados por todos los participantes de la red.

Bitcoin y Ethereum, originalmente, utilizaban un mecanismo de consenso conocido como Prueba de Trabajo (Proof of Work, PoW). En este sistema, los "mineros" compiten para resolver problemas matemáticos difíciles utilizando grandes cantidades de potencia computacional. Los mineros que resuelven el problema son recompensados con criptomonedas. Sin embargo, este enfoque consume grandes cantidades de electricidad y presenta desafíos para escalar la red, ya que la congestión de la red puede aumentar las tarifas y reducir las tasas de procesamiento.

En contraposición, Ethereum recientemente migró hacia un mecanismo de consenso llamado prueba de participación (Proof of Stake, PoS). En este sistema, los "validadores" hacen un aporte tipo garantía, es decir, depositan tokens para tener la oportunidad de ser seleccionados para validar transacciones y obtener recompensas. Cuanto más grande el aporte de un validador, mayores son sus posibilidades de ganar la recompensa. Esto hace que el sistema sea más eficiente en términos de consumo de energía y permite un potencial de escalabilidad mayor que el proporcionado por la Prueba de Trabajo. Todos los tokens invertidos en la Prueba de Participación generan intereses, lo que hace

que participar sea parecido a comprar acciones o bonos, pero sin la necesidad de consumir grandes cantidades de energía computacional (Ackermann, 2022).

Adicionalmente, la gobernanza de Ethereum es otro aspecto crucial que diferencia esta plataforma de otras como Bitcoin. Mientras que Bitcoin sigue una filosofía de inmutabilidad donde las reglas se establecen desde el principio y no se cambian, Ethereum adopta un enfoque más flexible y adaptable. En Ethereum, las decisiones sobre cambios en la plataforma son tomadas por una comunidad diversa de participantes que incluye desarrolladores, mineros, inversores y usuarios. Este modelo de gobernanza comunitaria y descentralizada busca equilibrar los intereses de todos los participantes, lo que permite que Ethereum se adapte y evolucione con el tiempo en respuesta a las necesidades y los desafíos emergentes. Sin embargo, este enfoque también presenta desafíos en términos de coordinación y consenso, ya que no siempre es fácil lograr un acuerdo entre un grupo tan amplio y diverso de partes interesadas.

Otro elemento fundamental de la red de Etherium es su máquina virtual (EVM). Esta es un componente clave en la arquitectura de la plataforma. En esencia, el protocolo de Ethereum se diseñó para garantizar la operación ininterrumpida e inmutable de esta particular máquina de estado. La EVM actúa como un entorno que aloja toda la información de la red. En cada bloque de la cadena, Ethereum tiene un estado "canónico" único y la EVM se encarga de definir las reglas para calcular un nuevo estado válido de un bloque a otro.

Por esta razón, a diferencia de otras *blockchains* que se describen comúnmente como "libros de contabilidad distribuidos", Ethereum se comporta más como una "máquina de estado distribuida". Su estado es una extensa estructura de datos que no solo mantiene todas las cuentas y los saldos, sino también el estado de la máquina. Este estado puede cambiar de un bloque a otro siguiendo un conjunto de reglas predefinidas que ejecutan un código de máquina arbitrario que se presenta como transacciones, instrucciones firmadas criptográficamente que provienen de las cuentas. Existen dos tipos de transacciones: las que se derivan de llamadas de mensajes y las que se originan en la creación de contratos. La creación de contratos da lugar a una nueva cuenta que contiene el *bytecode* compilado del contrato inteligente. En el siguiente apartado se desarrolla el concepto de contrato inteligente.

Una forma especial de entender la EVM es como una función matemática: dada una entrada, produce una salida determinista. De esta manera, Ethereum puede describirse como una función de transición de estado: dado un estado válido previo (S) y un nuevo conjunto de transacciones válidas (T), la función

de transición de estado de Ethereum, Y(S, T), produce un nuevo estado de salida válido, S'.

La EVM funciona como una máquina de pila con una profundidad de 1024 ítems. Cada ítem es una palabra de 256 bits, seleccionada para trabajar de manera eficiente con la criptografía de 256 bits. Durante la ejecución, la EVM mantiene una memoria temporal que no se conserva entre transacciones (Etherium, 2022).

Ahora bien, como toda red de cadena de bloques, Etherium cuenta con su propia criptomoneda nativa, el ether, crucial para el funcionamiento de la plataforma. Los ethers se utilizan para pagar las transacciones y los servicios computacionales en la red Ethereum. Además de ser una criptomoneda, el ether es también el combustible que impulsa la plataforma Ethereum, lo que proporciona el incentivo necesario para que los nodos de la red verifiquen las transacciones y mantengan la integridad de la *blockchain*.

## 2. Contratos inteligentes

La gran novedad presentada por la red Etherium es el concepto de contratos inteligentes. Estos artefactos tecnológicos son programas que residen dentro de las *blockchains* descentralizadas y se ejecutan conforme a instrucciones solicitadas. Estos contratos funcionan de una manera similar a como lo haría un contrato convencional entre dos o más partes. Las partes no necesitan confiar en abogados o bancos para establecer un acuerdo entre ellas; en su lugar, el contrato inteligente se ejecuta automáticamente para emitir, por ejemplo, un pago una vez que se cumplen ciertas condiciones (Sayeed *et al*., 2020).

Una característica clave de los contratos inteligentes es su inmutabilidad. Una vez que un contrato inteligente se implementa en la *blockchain*, no se puede modificar ni actualizar para aplicar parches de seguridad. Esto debería incentivar a los desarrolladores a poner en marcha estrategias de seguridad sólidas antes de la implementación para evitar una posible explotación en un momento posterior.

Las condiciones o cláusulas dentro de un contrato inteligente están incorporadas criptográficamente, lo que significa que ninguna parte puede alterar el contenido del contrato, lo que proporciona una garantía de seguridad y confiabilidad en el cumplimiento de las condiciones de este. Al ser de código abierto, el código del contrato permite a las partes involucradas determinar qué hace el contrato y cómo se inicia (DeMatteo, 2023).

Las aplicaciones descentralizadas que hacen uso de contratos inteligentes se corren exactamente según las condiciones del código, sin correr el riesgo de censura, engaño o tiempo de inactividad. Esto proporciona un nivel de confianza y seguridad en el cumplimiento de los términos del contrato que va más allá de lo que es posible con los contratos tradicionales.

Algunos contratos inteligentes famosos para finanzas son: Uniswap, el cual incorpora un protocolo de intercambio de tokens descentralizado; MakerDAO, un contrato que permite a los usuarios tomar prestado su *stablecoin* DAI contra otros activos de criptomoneda. En este caso, el sistema utiliza los contratos inteligentes para garantizar que los préstamos estén siempre sobrecolateralizados y que el valor de DAI sea estable. En esta familia de aplicaciones también estaría Compound, un protocolo de finanzas descentralizado (DeFi) en Ethereum que permite a los usuarios prestar y tomar prestados diferentes criptomonedas. Los intereses y las tasas son manejados automáticamente por contratos inteligentes, eliminando la necesidad de intermediarios financieros. Cada uno de estos ejemplos muestra cómo los contratos inteligentes pueden crear interacciones digitales seguras que trascienden las capacidades de los sistemas tradicionales.

### 2.1. Los DAO como contratos inteligentes

Las organizaciones autónomas descentralizadas (DAO – Decentralized Autonomous Corporation) tienen como objetivo codificar las políticas de una organización limitando la necesidad de actividades centralizadas mediante el uso de un enfoque descentralizado. En otras palabras, una DAO es una entidad que vive en la *blockchain* y es gobernada por un conjunto de reglas preestablecidas y ejecutadas por contratos inteligentes. Estas reglas se acuerdan y se establecen durante la creación de la DAO y, una vez implementadas, no se pueden cambiar a menos que la mayoría de los participantes (según se defina en el contrato inteligente) estén de acuerdo en hacerlo.

De esta forma los DAO, como contratos autónomos, son esencialmente códigos de *software* que automatizan la gestión de una organización. Pueden recibir, almacenar y distribuir fondos de manera eficiente y transparente sin la necesidad de intermediarios. Esta transparencia, junto con la capacidad de los participantes para retener el control directo sobre la dirección y los fondos de la organización, es uno de los principales atractivos de las DAO (Siegel, 2016).

Los fundadores de una DAO generalmente emiten tokens que dan derecho a voto a quienes los poseen. Estos tokens pueden ser comprados durante una oferta inicial o ganados por contribuir a la organización, y su propiedad puede

ser transferida de una persona a otra. Cada token da derecho a un voto y los cambios en la DAO deben ser aprobados por una mayoría de los votos de los tokens.

La descentralización que brindan las DAO puede facilitar la cooperación entre individuos a una escala global. Por ejemplo, una DAO puede ser configurada para apoyar un proyecto de código abierto, donde cualquier persona en cualquier parte del mundo puede contribuir y recibir una compensación justa y transparente. Las decisiones sobre la dirección del proyecto pueden ser tomadas por todos los contribuyentes, y no solo por un pequeño grupo de personas.

Cabe destacar que, aunque las DAO prometen una nueva forma de organizar la actividad humana, también plantean desafíos significativos, especialmente en lo que respecta a la gobernanza y la resolución de conflictos. Al eliminar los intermediarios, también se eliminan las entidades centralizadas que tradicionalmente han tomado decisiones y han resuelto disputas. Esto significa que se necesita un enfoque completamente nuevo para resolver conflictos y garantizar la equidad. Sin embargo, a pesar de estos desafíos, las DAO ofrecen una visión emocionante y radicalmente nueva de lo que podría ser el futuro de las organizaciones.

La siguiente es una guía de cómo funciona una DAO (Del Castillo, 2016; Siegel, 2016): primero, un grupo de programadores escribe contratos inteligentes (programas) que guiarán y administrarán la organización. Posteriormente, se lleva a cabo un periodo de financiamiento inicial, en el que las personas agregan fondos a The DAO comprando tokens que representan la propiedad a fin de proporcionarle los recursos que necesita. Después del financiamiento, la organización comienza a operar. Las personas, entonces, pueden hacer propuestas sobre cómo gastar el dinero, y los miembros que han comprado pueden votar para aprobar estas propuestas. Una vez que las propuestas son aceptadas, los contratos inteligentes guían los términos del proyecto y lo ejecutan en consecuencia. Este mismo mecanismo fue el que siguió The DAO, el primer y más famoso DAO de la historia.

El siguiente apartado presenta el primer DAO desplegado en la red Etherium, famoso no solamente por ser el mayor proyecto de fondeo colaborativo a la fecha, sino por haber vivido unos pocos días solo para verse clausurado debido a las nefastas consecuencias de un uso no autorizado de su lógica programática.

## 3. The DAO

Parecía que las organizaciones autónomas descentralizadas finalmente verían la luz en 2016, cuando surgió el diseño, construido en la plataforma Ethereum, de una pequeña empresa de *blockchain* llamada Slock.it. Anteriormente, en junio de 2015, Slock.it había comenzado el desarrollo de un marco de organización autónoma descentralizada, aceptando contribuciones de la comunidad de *software* de código abierto (Dupont, 2017). Para mayo de 2016, y después de casi un año de trabajo, unos pocos participantes de la sociedad Ethereum inauguraron The DAO[1], un contrato inteligente de código abierto que permitía a cualquier persona intercambiar tokens DAO por ethers. Utilizando ese método de intercambio, los creadores de The DAO permitieron al contrato inteligente recaudar alrededor de $150 millones de dólares (Falkon, 2018).

La misión de The DAO era funcionar como un fondo de capital de riesgo autodirigido, con los contribuyentes votando directamente sobre los proyectos propuestos para asignar el capital aportado según los resultados de las votaciones. Y no era para menos, The DAO recaudó fondos a través de la campaña de *crowdfunding* más exitosa hasta ese momento en la historia. Con solo 900 líneas de código fuente de *software*, The DAO se había propuesto permitir que los "inversores" de criptomonedas financiaran y gestionaran directamente nuevas empresas, todas ellas operadas en la *blockchain* de Ethereum.

De manera novedosa, The DAO introdujo y exploró una tecnología interesante para experimentar con problemas de gobernanza y nuevos modelos de sociedad. Se podría decir que The DAO fue un intento de construir una plataforma de financiamiento, similar a Kickstarter, pero que utilizaba específicamente tecnologías de organización autónoma descentralizada (*blockchain*) para su operación (Falkon, 2018).

Se estima que entre 10.000 y 20.000 personas invirtieron en The DAO, aportando 11'994.260,98 tokens Ethereum (conocidos como ether, o ETH), que representaban alrededor del 14 % del suministro total de ETH. The DAO confiaba en esta multitud participativa para su toma de decisiones de inversión,

1 The DAO hace referencia al primer DAO de la historia, de ahí su nombre. Posteriormente, el término DAO se ha usado de forma genérica para referirse a todos los proyectos de administración autónoma que han salido tanto en la red de Etherium como en otras redes descentralizadas.

requiriendo votos positivos del 20 % de los tokens emitidos para que una propuesta fuera considerada aceptada. Los participantes con tokens DAO podían emitir su voto sobre las propuestas y recibir recompensas siempre que resultaran en beneficios.

La primera etapa de The DAO fue un periodo de financiamiento o "fase de creación" de 28 días (comenzando el 30 de abril y concluyendo el 28 de mayo de 2016), durante el cual cualquiera podía intercambiar criptomonedas ETH a cambio de tokens DAO. Durante el periodo de financiamiento inicial, el precio de los tokens DAO aumentó programáticamente (desde un valor inicial de 1:100).

Cualquier persona con un depósito mínimo (reembolsable) podía crear una propuesta para que fuera votada por los titulares de tokens. Los inversores votaban asignando tokens DAO para propuestas específicas.

The DAO era innovador en sí ya que la lógica programada se enfocó especialmente en abordar las reglas de interacción especialmente con los propietarios minoritarios. Las disposiciones en la gobernanza corporativa y la ley estatutaria habían, sin éxito hasta ese momento, intentado abordar este problema, sin embargo, muchas de las soluciones anteriormente planteadas no habían sido exitosas porque los propietarios minoritarios carecían de derechos de voto e influencia para recuperar su capital en caso de diferir de las decisiones de la mayoría. The DAO abordó este problema distribuyendo la autoridad de manera equitativa a los tenedores de tokens. Para prevenir que un usuario con mayoría, es decir, con más del 51 % de los tokens, se transfiriera los fondos a sí mismo o ejecutara otras acciones de abuso de poder, The DAO podía dividirse de tal manera que los usuarios minoritarios que no estuvieran de acuerdo con una propuesta podían recibir su porción de ether en un vehículo de inversión paralelo al DAO original. Así, los usuarios que estaban de acuerdo con la propuesta presentada podían gastar sus ethers en ella y los que no estaban de acuerdo tenían una opción para no participar (BlockChannel, 2017). De esta manera se resolvía la falta de autoridad y control de los propietarios minoritarios. The DAO abordó este problema distribuyendo de manera creativa la autoridad entre los poseedores de tokens. Irónicamente, fueron estas reglas generadas para proteger a los pequeños inversionistas las que fueron utilizadas de manera maliciosa.

### 3.1 La caída de The DAO

El 5 de junio de 2016 se reveló al público que los contratos inteligentes de The DAO tenían vulnerabilidades significativas. El fallo residía en un *bug* programático que permitía vaciar los saldos de los usuarios a través de un ataque. Este

hecho fue descubierto casualmente por un usuario de GitHub, una plataforma de desarrollo de *software* basada en la web. El usuario, Chriseth, notificó a los desarrolladores clave que trabajaban con Ethereum y al fundador de la Fundación Blockchain, Peter Vessenes. Peter publicó un artículo detallando la vulnerabilidad de The DAO (Cuofano, 2022). En pocas palabras, el fallo en el código podría permitir a un atacante retirar repetidamente su saldo almacenado en The DAO antes de que este se ajustara.

Sin embargo, los fundadores de The DAO, Slock.it, desestimaron esta amenaza. El 12 de junio de 2016, en un artículo web, el fundador de Slock.it reconoció que había una vulnerabilidad que se introdujo accidentalmente en los contratos inteligentes de Ethereum debido a fallas de diseño inherentes al lenguaje de programación de contratos inteligentes Solidity, que se utilizó en la creación de The DAO (Tual, 2016). También declaró que ya se había creado una solución para la vulnerabilidad en el marco de The DAO y que los fondos de The DAO ya no corrían riesgo por este error. Cinco días después, el 17 de junio de 2016, The DAO fue atacado.

El atacante simplemente usó el código de The DAO tal como estaba escrito para un propósito no previsto. El atacante pudo drenar The DAO utilizando la función de división (*split*). Normalmente, la función de división permitía a los contribuyentes que tenían ethers en The DAO retirar sus contribuciones si no estaban de acuerdo con la manera como se estaban utilizando los fondos. La naturaleza misma de The DAO daba a los contribuyentes esta libertad de retirar sus fondos, tanto sus contribuciones iniciales como los tokens de recompensa acumulados por participar.

Lamentablemente, a la hora de entregar los recursos, el contrato inteligente solo verificaba el saldo del usuario una vez, al inicio de la solicitud de división o *splitting*. Al solicitar divisiones repetidamente antes de que se ajustara el saldo del atacante, este último pudo engañar a The DAO para que entregara más fondos de los que tenía originalmente. El código se usó de tal manera que una solicitud desencadenaba inmediatamente otra antes de que los saldos se ajustaran y el proceso se repetía hasta 20 veces.

Esto era posible porque la estructura de la función de retiro, llamada por la función *split*, estaba construida según la figura 1. Al solicitar retirar los recursos, la función de retiro primero consultaba el balance del usuario, posteriormente enviaba los recursos a la nueva cuenta y, por último, actualizaba el nuevo balance del usuario en el DAO original a cero. Lamentablemente, como la función de envío de recursos primitiva de Etherium necesitaba confirmación de

terminación desde la cuenta receptora de los recursos, el retiro podía detenerse después de efectuado, pero antes de la actualización del saldo. En resumen, la infortunada ubicación de la línea de código que actualizaba el saldo a cero después de un retiro total fue la causa de la vulnerabilidad.

Figura 1: Función de cobro de recursos y recompensas llamada por la función *split* de The DAO

```
function revoke() remote{
   uint256 value = balances[msg.sender];
   require(msg.sender.call.value(value)());
   balances[msg.sender] = 0;
}
```

Los ethers fueron colocados en un duplicado de The DAO, esencialmente un Child DAO. Tal cual como estaba pensado en las reglas originales programadas, la restricción con respecto a este nuevo DAO hijo era que los recursos retirados expresados en ether no podían ser controlados y, por ende, retirados hasta que transcurriera el ya mencionado periodo inicial de financiación de 28 días.

Durante 36 horas, la comunidad simplemente observó cómo se drenaba The DAO a razón de 228.500 ethers por hora. Fue tal la impotencia al no poder desconectar o parar el ataque, que la única forma de reaccionar fue realizar la misma acción del atacante. Otro grupo de individuos, los llamados "*hackers* de sombrero blanco", comenzaron su propio drenaje de The DAO para mover los ethers restantes a un lugar aparentemente seguro; otro DAO hijo. La idea era drenar ether más rápido que el atacante, para el 22 de junio, todo el ether accesible en The DAO había sido vaciado por el atacante original y por los *hackers* de sombrero blanco.

Dado el periodo de pausa extenso que existía, el atacante no podía tomar posesión de los recursos obtenidos inmediatamente. De esta forma, la comunidad de Etherium tuvo un periodo de tiempo considerable para pensar en todas las posibles acciones y las consecuencias de las diferentes decisiones que se podían tomar.

### 3.2 Cómo se resolvió el ataque y cuáles fueron las consecuencias para la red Etherium

En el mes posterior al ataque surgieron diversas propuestas para resolver el problema. Entre ellas, destacaron tres alternativas principales: la primera, no hacer

nada y permitir que después del periodo de retención de 28 días, el atacante se quedara con los 50 millones en ethers robados. La segunda opción consistía en realizar un *soft fork* (bifurcación suave). Y, por último, la tercera opción consistía en deshacer completamente el *hackeo* devolviendo todos los ethers desviados a The DAO y reembolsando a los inversores (una propuesta de bifurcación dura).

La primera alternativa era consistente con la doctrina de que "el código es la ley" y que el atacante ahora tenía derecho a los ethers ya que simplemente usó el código de The DAO tal como estaba escrito. La segunda alternativa, conocida como una bifurcación suave, habría resultado en la pérdida de los ethers aportados por los inversores. Sin embargo, habría evitado que el atacante se beneficiara aún más del ataque. La tercera opción, apoyada por los fundadores de The DAO y Ethereum, implicaba rebobinar los contratos inteligentes a través de un consenso especial de los mineros y devolver todos los ethers robados a un DAO original modificado, que solo permitiría la retirada de los fondos originales. Desde allí, los ethers serían restaurados a los inversores y The DAO sería cerrado.

A pesar de los diversos debates y discusiones, finalmente la comunidad de Ethereum acordó implementar la solución de la bifurcación dura. Una versión "bifurcada" del *software* de Ethereum se desarrolló y se liberó a los mineros. Esta bifurcación creó un contrato especial "solo de retiro" en la *blockchain* de Ethereum y movió todos los tokens hacia este. La mayoría de los mineros implementaron este *software*, y el libro de contabilidad de la *blockchain* se actualizó para borrar efectivamente The DAO.

El atacante, considerándose con el derecho de mantener y disponer de los ether adquiridos de forma irregular, envió una carta abierta a la comunidad de Etherium recordándole que él realmente no hackeó ni cambió ningún contrato inteligente o sistema. Que él solamente, y de manera inteligente y "legal", aprovechó lo que estaba escrito originalmente en el contrato de The DAO. También le recordó a la comunidad en general que cualquier esfuerzo por bloquear sus recursos sería moralmente equivocado e iría en contra del espíritu de las entidades descentralizadas (The Attacker, 2016).

No todos los mineros de la red de Etherium estaban obligados a implementar el cambio que implicaba la bifurcación dura acordada. Siguiendo la línea argumentativa del atacante, la minoría de los mineros que se negaron a actualizar su *software* de Ethereum, rechazando la bifurcación dura, se separaron de la *blockchain* principal. Esta nueva *blockchain*, todavía susceptible de ataques al estilo de The DAO, fue apodada "Ethereum Classic" y ganó un seguimiento algo

significativo, incluso su token nativo se negoció activamente en los *exchanges* más grandes del mercado cripto.

Para el 22 de junio, la bifurcación dura fue implementada con éxito y la comunidad principal de Ethereum suspiró aliviada. Y horas después, los que disentían reanudaron la minería de la cadena original, de donde nació Ethereum Classic (ETC), la cual mantenía todos los componentes y mecanismos estructurales del *blockchain* de Etherium original. A la fecha, a pesar de que para ser exactos Etherium Classic es más similar a la red de Etherium antes del ataque, la cadena bifurcada sigue siendo considerada la red principal de Ethereum.

En total, alrededor de 90 días vivió la experiencia más ambiciosa de gobernanza algorítmica que representaba The DAO. Su auge, y especialmente su caída, por poco causan la destrucción de la misma red descentralizada que lo vio nacer.

## 4. Conclusiones

The DAO representa un importante punto de inflexión en la historia de la gobernanza algorítmica y de la *blockchain*. Concebido como un experimento ambicioso para descentralizar la toma de decisiones y las operaciones financieras, terminó ilustrando las limitaciones y los riesgos de confiar completamente en el código como ley.

El ataque a The DAO dejó en claro que, a pesar de las promesas de autonomía y descentralización, la tecnología de contratos inteligentes todavía estaba en su infancia y era susceptible de vulnerabilidades inesperadas. El código, aunque se propone ser imparcial e incuestionable, no es infalible y puede ser manipulado de maneras no intencionadas, como lo demostró el atacante que drenó una importante cantidad de ethers de The DAO.

La solución al ataque, en lugar de ser puramente tecnológica o algorítmica, requirió la intervención humana y la toma de decisiones colectiva. A pesar de la retórica de "el código es la ley", la comunidad de Ethereum tuvo que llegar a un consenso entre humanos y tomar la difícil decisión de implementar una bifurcación dura, alterando efectivamente el "inmutable" libro de contabilidad de la *blockchain*.

Además, la bifurcación dura y la subsiguiente creación de Ethereum Classic evidenciaron que, en la práctica, la gobernanza de la *blockchain* todavía depende en gran medida de la acción humana y la negociación comunitaria. Estos hechos refutan la idea de que la *blockchain* y los contratos inteligentes

pueden existir y operar completamente fuera del alcance de la intervención y la gobernanza humana.

En conclusión, The DAO sirve como un valioso recordatorio de que, aunque la tecnología *blockchain* y los contratos inteligentes ofrecen posibilidades emocionantes para la descentralización y la autonomía, la intervención humana, la gobernanza y el consenso siguen siendo cruciales en la resolución de conflictos y en la toma de decisiones importantes. El experimento de The DAO no fue un fracaso total; más bien, proporcionó lecciones valiosas sobre los desafíos y las limitaciones de la gobernanza algorítmica y la necesidad de equilibrios y controles humanos.

## Referencias

Ackermann, R. (2022, septiembre 19). Ethereum abandona la criptominería y adopta la prueba de participación. *MIT Technology Review*. https://www.technologyreview.es//s/14589/ethereum-abandona-la-criptomineria-y-adopta-la-prueba-de-participacion. https://papers.ssrn.com/abstract=1762766

BlockChannel (2017, mayo 22). What is a "DAO"? How do they benefit consumers? *BlockChannel*. https://medium.com/blockchannel/what-is-a-dao-how-do-they-benefit-consumers-f7a0a862f3dc

Cuofano, G. (2022). *The history of ethereum and the Web3 Business Playbook*. https://www.linkedin.com/pulse/history-ethereum-web3-business-playbook-gennaro-cuofano

Del Castillo, M. (2016). The DAO attacked: Code issue leads to $60 million ether theft. *CoinDesk*. https://www.coindesk.com/markets/2016/06/17/the-dao-attacked-code-issue-leads-to-60-million-ether-theft/

DeMatteo, M. (2023). Are dapps the future of the creator economy? *CoinDesk*. https://www.coindesk.com/learn/are-dapps-the-future-of-the-creator-economy/

Dupont, Q. (2017). *Experiments in Algorithmic Governance: A history and ethnography of "The DAO". A failed Decentralized Autonomous Organization*. Libro, Bitcoin and Beyond: Cryptocurrencies, Blockchains and Global Governance. Routledge.

Etherium, F. (2022). *Máquina virtual de Ethereum (EVM)*. ethereum.org. https://ethereum.org

Falkon, S. (2018, agosto 12). The Story of the DAO — Its History and Consequences. *The Startup*. https://medium.com/swlh/the-story-of-the-dao-its-history-and-consequences-71e6a8a551ee

Pasquale, F. A. (2011). Restoring Transparency to Automated Authority. *SSRN Scholarly Paper*, 1762766. https://papers.ssrn.com/abstract=1762766

Sayeed, S., Marco-Gisbert, H. y Caira, T. (2020). Smart Contract: Attacks and Protections. *IEEE Access*, 8, 24416-24427. https://doi.org/10.1109/ACCESS.2020.2970495

Siegel, D. (2016). The DAO attack: Understanding what happened. *CoinDesk*. https://www.coindesk.com/learn/understanding-the-dao-attack/

The Attacker (2016). An Open Letter (The DAO Attacker). *Hacker News*. https://news.ycombinator.com/item?id=11927891

Tual, S. (2016). No DAO funds at risk following the Ethereum smart contract 'recursive call' bug discovery. Slock.it Blog. https://archive.vn/402Up