Sociedad Descentralizada: Encontrando el Alma de la Web3[1]

E. Glen Weyl,[2] Puja Ohlhaver,[3] Vitalik Buterin[4]
Traducido al español y editado por: Sofía Cossar, Paula Berman, Daniel Knobelsdorf

Mayo del 2022

"El Dao es el corazón y el hogar
de las diez mil cosas.
Las almas buenas lo atesoran,
las almas perdidas encuentran refugio en él."
— Laozi, #62

Abstract

Actualmente, la Web3 se centra en expresar activos transferibles y financiables, en lugar de codificar relaciones sociales de confianza. Sin embargo, muchas actividades económicas centrales, como los préstamos sin garantía y la creación de marcas personales, se basan en relaciones persistentes e intransferibles. En este documento, ilustramos cómo los tokens no transferibles "vinculados al alma" (Soulbound Tokens, o SBTs, por sus siglas en inglés) que representan los compromisos, las credenciales y las afiliaciones de las "Almas" pueden codificar las redes de confianza de la economía real para establecer procedencia y reputación. Más importante aún, los SBTs permiten otras aplicaciones ambiciosas, como la recuperación comunitaria de billeteras, la gobernanza resistente a los ataques Sybil, mecanismos para la descentralización y mercados novedosos con derechos compartidos y descomponibles. Llamamos a este ecosistema más rico y pluralista "Sociedad Descentralizada" (DeSoc), una sociabilidad codeterminada, donde las Almas y las comunidades se unen de abajo hacia arriba, como propiedades emergentes entre sí para cocrear inteligencias y bienes de redes plurales, en un rango de escalas. La clave de esta sociabilidad son derechos de propiedad descomponibles y mejores mecanismos de gobernanza, como el financiamiento cuadrático descontado por puntajes de correlación, que recompensan la confianza y la cooperación mientras que protegen las redes de la captura, la extracción y la dominación. Con una sociabilidad tan aumentada, la Web3 puede evitar la hiperfinanciación de hoy en favor de un futuro más transformador y pluralista de rendimientos crecientes a través de la distancia social.

[1] Agradecemos a Audrey Tang, Phil Daian, Danielle Allen, Leon Erichsen, Matthew Prewitt, Divya Siddarth, Jaron Lanier y Robert Miller por sus valiosos comentarios y sugerencias. Todos los errores y puntos de vista son nuestros.
[2] Microsoft Corporation & RadicalxChange Foundation, glen@radicalxchange.org. Glen vincula este documento a su Alma.
[3] Flashbots Ltd., puja@flashbots.net. Puja dedica este artículo a su abuela, Satya, cuyo amor y luz siempre van a brillar en muchas Almas.
[4] Ethereum Foundation, vitalik.buterin@ethereum.org.

§1. INTRODUCCIÓN

La Web3 ha asombrado al mundo al forjar un sistema paralelo de finanzas con una flexibilidad y creatividad sin precedentes en menos de una década. Primitivas criptográficas y económicas como la criptografía de clave pública, los contratos inteligentes, Proof of Work y Proof of Stake han dado lugar a un ecosistema abierto y sofisticado para expresar transacciones financieras.

Sin embargo, son los seres humanos y sus relaciones quienes generan el valor económico que se intercambia en las finanzas. Debido a que la Web3 carece de primitivas para representar esta identidad social, se ha vuelto fundamentalmente dependiente de la misma estructuras centralizadas que la Web2 que pretende trascender, replicando sus limitaciones.

Ejemplos de estas dependencias incluyen:

1. La mayoría de los artistas de NFTs confían en plataformas centralizadas como OpenSea y Twitter para comprometerse con la escasez y una **procedencia** inicial.

2. Las DAOs que intentan ir más allá de la simple votación con monedas a menudo se basan en la infraestructura de la Web2, como los perfiles de las redes sociales, para la **resistencia Sybil**.

3. Muchos participantes de la Web3 confían en billeteras de custodia administradas por entidades centralizadas como Coinbase o Binance. Los sistemas de **gestión de claves** descentralizados no son fáciles de usar salvo para los usuarios más sofisticados

Además, la falta de una identidad nativa de la Web3 hace que el ecosistema DeFi actual no pueda apoyar actividades ubicuas en la economía real, tales como **préstamos subcolateralizados** o contratos simples, como un **arrendamiento de apartamento**. En este artículo, ilustramos cómo incluso pasos pequeños e incrementales hacia la representación de la identidad social con tokens "vinculados al alma" podría superar estas limitaciones y acercar el ecosistema mucho más a mercados regenerativos con sus relaciones humanas subyacentes en un contexto nativo de la Web3.

Aún más prometedor, destacamos cómo la identidad social nativa de la Web3, con *componibilidad* social rica, puede ayudar a solucionar problemas más amplios en la Web3 en torno a la concentración de la riqueza y vulnerabilidad de la gobernabilidad a los ataques financieros, al tiempo que estimula una explosión cámbrica de innovación política, aplicaciones económicas y sociales. Estos casos de uso y el ecosistema pluralista que éstos posibilitan es a lo que nos referimos con **"Sociedad Descentralizada" (DeSoc, por su versión en inglés, "Decentralized Society").**

§2 NOCIONES GENERALES

Comenzaremos explicando las primitivas de DeSoc, centradas en las cuentas (o billeteras) con **tokens no transferibles (inicialmente públicos) "vinculados al alma" (SBTs)** que representan compromisos, credenciales y afiliaciones. Dichos tokens equivalen a una especie de currículum extendido, emitido por otras billeteras que atestiguan estas relaciones sociales.

Luego describiremos una "escalera" de aplicaciones cada vez más ambiciosas que estas primitivas pueden facilitar, incluyendo:

- el establecimiento de la procedencia
- el desbloqueo de mercados de préstamos subcolateralizados a través de la reputación
- la habilitación de la administración descentralizada de claves
- el obstruimiento y compensación del comportamiento estratégico coordinado
- la medición de la descentralización
- la creación de mercados novedosos con derechos y permisos compartidos y descomponibles

Esta descripción culmina con una visión de DeSoc, una sociabilidad co-determinada, donde las Almas y las comunidades se unen de abajo hacia arriba, como propiedades emergentes de cada una para co-crear una red de bienes plurales, incluidas las inteligencias plurales, en una variedad de escalas sociales.

Finalmente, responderemos potenciales inquietudes y objeciones y haremos comparaciones con otros paradigmas de identidad familiares en el espacio de la Web3, reconociendo cómo nuestra visión es sólo un primer paso pero, así mismo, un avance considerable en términos de privacidad y comunicación programable. Luego, consideraremos caminos técnicos para poner en marcha la visión que imaginamos. Sobre la base de éstos, examinaremos, más filosóficamente, el potencial de DeSoc para redirigir la Web3 a un camino más profundo, legítimo y transformador.

§3 ALMAS

Nuestra primitiva clave son cuentas, o billeteras, **que contienen tokens *públicamente visibles*, intransferibles (pero posiblemente *revocables* por el emisor).**[5] Nos referimos a las cuentas como "Almas" y a los tokens en poder de estas cuentas como **"Tokens vinculados al alma" (SBTs)**. A pesar de nuestro profundo interés en la privacidad, inicialmente optamos por la publicidad porque es técnicamente más simple de validar como prueba de concepto, incluso si está limitada por el

[5] Hemos elegido este conjunto de propiedades no porque sean claramente el conjunto de características más deseable, sino porque son fáciles de implementar en el entorno actual y permiten una funcionalidad significativa. Exploramos SBT privados programables en la Sección 5.3.

subconjunto de tokens que la gente está dispuesta a compartir públicamente. Más adelante en el documento, presentaremos el concepto de "privacidad programada" para casos de uso más ricos.

Imagine un mundo donde la mayoría de los participantes tienen Almas que almacenan SBTs correspondientes a una serie de afiliaciones, membresías y credenciales. Por ejemplo, una persona puede tener un Alma que almacena SBTs que representan credenciales educativas, historial de empleo o hashes de sus escritos u obras de arte. En su forma más simple, estos SBTs pueden ser "autocertificados", de manera similar a cómo compartimos información sobre nosotros mismos en nuestros CVs. Pero el verdadero poder de este mecanismo emerge cuando un SBT en poder de un Alma es emitido o atestiguado por otras Almas, que son contrapartes de estas relaciones. Estas Almas en contraparte podrían ser personas, empresas o instituciones. Por ejemplo, la Fundación Ethereum podría ser un Alma que emita SBTs para Almas que asistan a una conferencia de desarrolladores de software. Una universidad podría ser un Alma que emite SBTs a los graduados. Un estadio podría ser un Alma que emite SBTs a quienes han sido fanáticos de los Dodgers desde hace mucho tiempo.

Es importante destacar que no es necesario que un Alma esté vinculada a un nombre legal o que haya cualquier intento a nivel de protocolo para asegurar "un Alma por humano". Un Alma podría ser un seudónimo persistente con una gama de SBTs que no se pueden vincular fácilmente[6]. Tampoco asumimos la intransferibilidad de las Almas entre humanos. En su lugar, tratamos de ilustrar cómo estas propiedades, donde sea necesario, pueden surgir naturalmente del diseño en sí mismo.

§4 ESCALERA A DESOC

4.1 Arte y Alma

Las Almas son una forma natural para que los artistas “comprometan” (“stake”)su reputación en sus obras. Al emitir un NFT comercializable, un artista podría emitir el NFT desde su Alma. Cuantos más SBTs posea el Alma del artista, más fácil será que los compradores identifiquen al Alma como perteneciente a ese artista y, por lo tanto, también confirmen la legitimidad del NFT. Los artistas podrían ir un paso más allá y emitir un SBT vinculado, almacenado en su Alma, que certifique que el NFT pertenece a una “colección” y que avale cualquier límite de escasez que el artista desee establecer. Las Almas crearían una forma confiable dentro de la blockchain (“*on-chain”)* de construir reputación sobre la procedencia y la escasez de un objeto.

Las aplicaciones se extienden más allá del arte hacia servicios, alquileres y cualquier mercado basado en la escasez, la reputación o la autenticidad. Un ejemplo de este último caso es la verificación

[6] Tenga en cuenta, sin embargo, que, en principio, los nombres legales podrían representarse como un SBT: un apellido sería un SBT de membresía a un grupo familiar y un nombre de pila podría ser un SBT de regalo, otorgado de padres a su hijos. De hecho, nociones de nombres más complejas serían fáciles de representar si, por ejemplo, otras líneas familiares o relaciones pudieran otorgar un SBT de membresía a un nuevo niño.

de la autenticidad de supuestas grabaciones de hechos, como fotografías y videos. Con los avances en la tecnología "deepfake", será cada vez más difícil para los humanos y los algoritmos detectar la veracidad de estas grabaciones por medio de la inspección directa. **Si bien la inclusión de la tecnología blockchain nos permite rastrear el momento en que un trabajo en particular ha sido realizado, los SBTs nos permitirían rastrear la *procedencia social* de los mismos**, otorgando un contexto social rico sobre el Alma que emite el trabajo—su constelación de membresías, afiliaciones, credenciales y su distancia social del sujeto. Los deepfake podrían identificarse fácilmente como artefactos originados fuera del tiempo y contexto social, mientras que los artefactos confiables (como fotografías) surgirían de la certificación de fotógrafos de renombre. Mientras que la tecnología actual descontextualiza los productos culturales (como imágenes) y los abre a ataques virales que carecen de contexto social, los SBTs pueden recontextualizar tales objetos y empoderar a las Almas para aprovechar las relaciones de confianza ya presentes dentro de las comunidades como un respaldo significativo para proteger la reputación.

4.2 Préstamo entre Almas

Quizás el valor financiero más grande que se basa directamente en la reputación es el crédito y los préstamos sin garantía. Actualmente, el ecosistema de la Web3 no puede replicar formas simples de préstamos sin garantía porque todos los activos son transferibles y vendibles y, por lo tanto, son simplemente formas de garantía. El ecosistema financiero "tradicional" admite muchas formas de préstamos sin garantía, pero se basa en puntajes de crédito para medir la solvencia de los prestatarios, quienes tienen pocos incentivos para compartir información sobre su historial crediticio. Pero tales puntuaciones tienen muchos defectos. En el mejor de los casos, de forma poco transparente, dan más o menos peso a factores considerados relevantes para la solvencia y poseen un sesgo frente a quienes no han acumulado suficientes datos, principalmente las minorías y las personas viviendo en la pobreza. En el peor de los casos, pueden llevar a sistemas de "crédito social" poco transparentes como en la serie *Black Mirror* que diseñan resultados sociales y refuerzan las discriminaciones.

Un ecosistema de SBTs podría posibilitar una alternativa de abajo hacia arriba y resistente a la censura a los sistemas de crédito comerciales y "sociales". Los SBTs que representan credenciales educativas, historial laboral y contratos de alquiler podrían servir como un registro persistente del historial crediticio relevante, lo que permitiría que las Almas "comprometan" ("stake") una reputación significativa para evitar los requisitos de garantía y asegurar un préstamo. Los préstamos y líneas de crédito podrían ser representados como SBTs no transferibles pero revocables, por lo que estarían anidados con los otros SBTs de un Alma, como una especie de garantía de reputación no embargable, hasta que se reembolsen y posteriormente se quemen, o mejor aún, sean reemplazados por el comprobante de pago. Los SBTs ofrecen propiedades de seguridad útiles: la intransferibilidad impide transferir u ocultar préstamos pendientes, mientras que un ecosistema de SBTs garantiza que los prestatarios que intenten evitar pagar sus préstamos (por

ejemplo, haciendo un Alma nueva) carezcan de SBTs para comprometer significativamente su reputación.

La facilidad de calcular los pasivos públicos con los SBTs abriría mercados de préstamos de código abierto. Surgirían nuevas correlaciones entre los SBTs y el riesgo de reembolso, dando lugar a mejores algoritmos de préstamo para predecir la solvencia y, por lo tanto, reduciendo el papel de la infraestructura centralizada y poco transparente de calificación crediticia. Mejor aún, los préstamos probablemente ocurrirían *dentro* de nuestras conexiones sociales. En particular, los SBTs ofrecerían un sustrato para prácticas de préstamos comunitarios similares a las iniciadas por Muhammad Yunus y el Grameen Bank, donde los miembros de una red social acuerdan apoyar las responsabilidades de los demás en esta. Porque la constelación de SBTs de un Alma representa membresías a través de grupos sociales, los participantes podrían descubrir fácilmente otras Almas que serían copartícipes valiosas en un proyecto de préstamos grupales. Mientras que los préstamos comerciales son un modelo de pago "préstalo y olvídalo" hasta el momento del pago, los préstamos comunitarios podrían tomar un enfoque "préstalo y ayúdalo" —combinando capital de trabajo con capital humano con mayores tasas de retorno.

¿Cómo se ponen en marcha los préstamos comunitarios sin garantía? Inicialmente, esperamos que las Almas sólo porten SBTs que reflejen información con la que se sientan cómodas de compartir públicamente, como la información que aparece en un CV. Si bien tiene un alcance limitado, podría ser un nivel de resolución suficiente para llevar a cabo experimentos de préstamos intracomunitarios, especialmente si los SBTs son emitidos por instituciones acreditadas. Por ejemplo, una constelación de SBTs que muestran ciertas credenciales de programación, participación en varias conferencias y el historial de trabajo puede ser suficiente para que un Alma tome un préstamo (o recaude capital inicial) para su empresa. De hecho, las credenciales y las relaciones sociales ya desempeñan un papel importante pero poco transparente en la distribución del capital de riesgo.

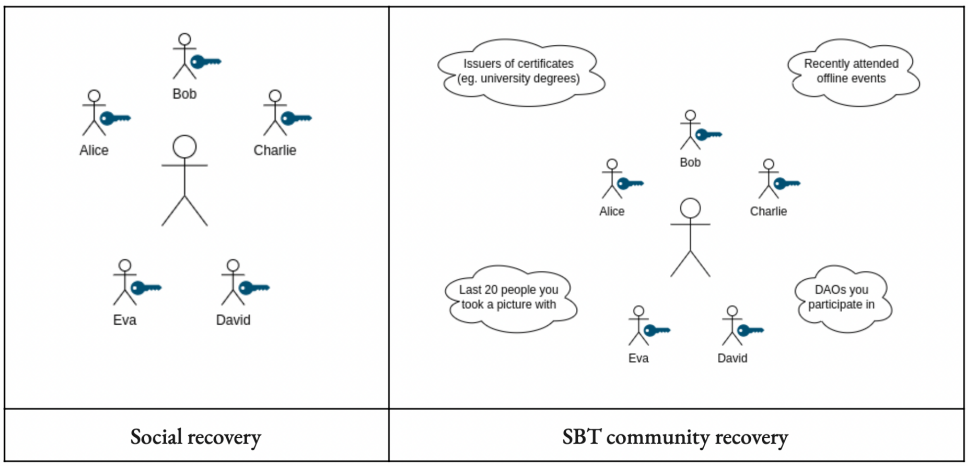
4.3 No perder el Alma

La intransferibilidad de los SBTs clave, como las credenciales educativas emitidas una sola vez, plantea una pregunta importante: ¿cómo no perder el Alma? Los métodos de recuperación actuales, como mnemónicos o la recuperación muti-sig, implican ciertas concesiones a nivel de sobrecarga mental, facilidad de transacción y seguridad. La recuperación social es una alternativa emergente que se basa en las relaciones de confianza de una persona. Los SBTs permiten un enfoque similar, pero más amplio: recuperación comunitaria, **donde el Alma es el voto interseccional de su red social.**

La recuperación social es un buen punto de partida para la seguridad, pero tiene varios inconvenientes en materia de seguridad y usabilidad. Un usuario selecciona un conjunto de "guardianes" y les otorga el poder, por mayoría, de cambiar las claves de su billetera. Estos guardianes

pueden ser una mezcla de individuos, instituciones, u otras billeteras. El problema es que un usuario debe equilibrar el deseo de un número razonablemente alto de guardianes contra la precaución de que los guardianes sean de círculos sociales discretos para evitar colusión. Además, los guardianes pueden fallecer, las relaciones arruinarse o las personas pueden simplemente perder el contacto, lo que requiere actualizaciones frecuentes y exigentes. Si bien la recuperación social evita un único punto de falla, la recuperación exitosa depende, no obstante, de curar y mantener relaciones de confianza con la mayoría de los guardianes.

Una solución más robusta es vincular la recuperación del Alma a las membresías de esta Alma en diferentes comunidades, sin hacer una curación, sino basándose en un conjunto máximamente amplio de relaciones en tiempo real por seguridad. Recuerde que los SBTs representan membresías en diferentes comunidades. Algunas de estas comunidades, como los empleadores, clubes, colegios o iglesias, podrían ser más de naturaleza off-chain, mientras otras, como la participación en el protocolo de gobernanza de una DAO, podría ser más de naturaleza on-chain. En un modelo de recuperación comunitaria, recuperar las claves privadas de una Alma requerirían el consentimiento de un miembro de una mayoría calificada de (un subconjunto aleatorio de) comunidades a las cuales pertenece un Alma.



Social recovery	SBT community recovery

Bob, Alice, Charlie, Eva, David	Bob y Alice: emisores de certificados (por ejemplo, diplomas universitarios). Charlie: participación reciente en eventos offline. Eva: las últimas 20 personas con quienes te has sacado una foto. David: las DAOs en las que participas.
Recuperación Social	**Recuperación comunitaria por SBTs**

Al igual que la recuperación social, asumimos que el Alma tiene acceso a canales de comunicación seguros fuera de la blockchain ("*off-chain*") donde la "autenticación" puede ocurrir ya

sea a través de una conversación, una reunión en persona o la confirmación de un secreto. Dichos canales de comunicación requerirían un mayor ancho de banda (técnicamente, la capacidad para transportar una "entropía de información" más rica) que, por ejemplo, los bots on-chain o la computación sobre los mismos SBTs. De hecho, podemos pensar que los SBTs se tratan fundamentalmente de representar la participación o acceso a dichos canales de comunicación auténticos, es decir, de gran ancho de banda.

Los detalles precisos para realizar este trabajo requerirán experimentación. Cómo se eligen los guardianes y de cuántos guardianes se requiere el consentimiento, por ejemplo, son parámetros de seguridad clave para futuras investigaciones. Con una base de información tan rica, sin embargo, la recuperación comunitaria debería ser computacionalmente posible, con la seguridad aumentando a medida que un Alma se une a más comunidades distintas y forma relaciones más significativas.

La recuperación comunitaria, como mecanismo de seguridad, encarna la teoría de la identidad propuesta por Georg Simmel, sociólogo de principios del siglo XX, fundador de la teoría de las redes sociales, en el que la individualidad emerge de la intersección de los grupos sociales, así como los grupos sociales emergen de la intersección de individuos. Mantener y recuperar la posesión criptográfica de un Alma requiere el consentimiento de la red de esta Alma. **Al integrar la seguridad en la sociabilidad**, un Alma siempre puede regenerar sus claves a través de la comunidad, lo que disuade el robo (o venta) del Alma: porque un vendedor necesitaría probar que vende las relaciones de recuperación, cualquier intento de vender un Alma carece de credibilidad.

4.4 Souldrops

Hasta ahora hemos explicado cómo las Almas pueden llegar a representar a los individuos y reflejar sus rasgos únicos y solidaridades a medida que adquieren SBTs que reflejan sus afiliaciones, membresías y credenciales. Tal individuación ayuda a las Almas a construir reputaciones, establecer procedencia, acceder a mercados de préstamos sin garantía y proteger la reputación y la identidad. Pero lo contrario también es cierto; **los SBTs también permiten que las *comunidades* sean convocadas en intersecciones únicas de Almas.** Hasta ahora, la Web3 se ha basado en gran medida en las ventas de tokens o “airdrops” para convocar nuevas comunidades, pero poseen poca exactitud o precisión. Los airdrops, en los se otorgan tokens algorítmicamente de forma gratuita a un conjunto de billeteras, recaen en su mayoría en alguna combinación de poseedores existentes de tokens y billeteras y son fácilmente vulnerables a ataques Sybil, fomentando el comportamiento estratégico y el efecto Mateo. Los SBTs ofrecen una mejora radical a la que llamamos "souldrops”.

Los “souldrops” son airdrops basados en cálculos sobre SBTs y otros tokens dentro de un Alma. Por ejemplo, una DAO que quiera convocar a una comunidad dentro de un protocolo particular de capa 1 podría hacer un souldrop para desarrolladores que tienen 3 de los 5 últimos SBTs de asistencia a la conferencia u otros tokens que reflejen la asistencia como los Proof of Attendance

Protocols (POAPs) o protocolos de prueba de asistencia. Los protocolos también podrían ponderar mediante programación los "token drops" a través de una combinación de SBTs. Nosotros podemos imaginar una organización sin fines de lucro cuya misión es plantar árboles llevando a cabo "drops" de tokens de gobernanza a las Almas que tengan un combinación de SBTs de acción ambiental, SBTs de jardinería y tokens de secuestro de carbono, tal vez asignando más tokens a los poseedores de tokens de secuestro de carbono.

Los souldrops también podrían introducir incentivos novedosos para fomentar la participación de la comunidad. Los "dropped" SBTs podrían diseñarse para estar vinculados al Alma por un período, pero eventualmente se "convertirán" en tokens transferibles a lo largo del tiempo. O lo contrario podría suceder. Los tokens transferibles retenidos durante un período podrían desbloquear el derecho a los SBTs que confieren más derechos de gobernanza sobre un protocolo. Los SBTs abren un rico espacio de posibilidades para experimentar con mecanismos que maximizan la participación de la comunidad y otros objetivos, como la descentralización, que analizamos más abajo.

4.5 La DAO de las Almas

Las organizaciones autónomas descentralizadas (DAOs) son comunidades virtuales que se unen en torno a un propósito común, coordinando a través de votos en smart contracts en una blockchain pública. Mientras que las DAOs ofrecen un gran potencial para la coordinación de comunidades globales, son vulnerable a los ataques Sybil donde un solo usuario puede tener múltiples billeteras para acumular poder de voto, o en estilos de gobernanza menos sofisticados como un-token-un-voto, simplemente puede acumular tokens para poseer el 51% del poder de voto y desposeer el otro 49%.

Las DAOs podrían mitigar los ataques Sybil utilizando SBTs de varias maneras:

- calcular sobre la constelación de SBTs de un Alma para **diferenciar entre Almas únicas y probables bots**, negando *cualquier* poder de voto a un Alma que parece ser un Sybil.

- **otorgar más poder de voto a las Almas** que tienen SBTs de mayor reputación, como credenciales de trabajo o educativas, licencias o certificaciones.

- **emitir SBTs especializados bajo "proof of personhood" (POP) o pruebas de personalidad**, que podrían ayudar a otras DAOs a desarrollar resistencia a los ataques Sybil.

- **verificar las *correlaciones* entre los SBTs** de las Almas que apoyan un voto en particular y aplicar un peso de voto más bajo a los votantes que están altamente correlacionados.

La última idea de verificación de correlación es particularmente prometedora y novedosa. Un voto apoyado por muchas Almas que comparten el/los mismo(s) SBT(s) tiene más probabilidad que sea un ataque Sybil e, incluso si no es un ataque Sybil, tal voto es más probable que sea de u*n grupo de Almas que están cometiendo el mismo error de juicio o que comparten el mismo sesgo*, por lo que debería ponderarse razonablemente menos que un voto con el mismo nivel numérico de apoyo pero de una una base más diversa de participantes.[7]

Exploramos la última idea matemáticamente con mayor detalle en el contexto de la financiación cuadrática en el Apéndice, donde presentamos una nueva primitiva, llamada **"puntuación de correlación"**. Este concepto de descuento de correlación podría extenderse para estructurar conversaciones deliberativas. Por ejemplo, las DAOs susceptibles a la captura mayoritaria podrían computar sobre la base de SBTs para reunir a los miembros más diversos en una conversación y garantizar que se escuchen las voces de las minorías.

Las DAOs también podrían confiar en los SBTs para disuadir formas de comportamiento estratégico como el "ataque vampiro" (vampire attacks). En tales ataques, una DAO (generalmente asociada con un protocolo DeFi de valor económico) “free-rides” o se beneficia sin pagar costos de la investigación y el desarrollo de otra DAO copiando su código abierto y, posteriormente, atrayendo la liquidez de los usuarios con un token. Las DAOs podrían disuadir a los oportunistas creando una norma en torno al souldropping, quizás primero confiriendo SBTs a Almas con probabilidad de ser resistentes a los ataques Sybil que hayan entregado liquidez y luego negando el souldropping a las Almas que hayan modificado su liquidez en un ataque vampiro. El mismo mecanismo no funcionaría con airdrops a billeteras sin SBTs porque un titular puede distribuir la liquidez en muchas billeteras para ofuscar su rastro de liquidez.

Las DAOs también podrían usar los SBTs para hacer que el liderazgo y la gobernanza respondan programáticamente a sus comunidades. Los roles de liderazgo podrían cambiar dinámicamente a medida que cambia la composición de la comunidad, como es reflejado en la distribución cambiante de SBTs entre las Almas miembros. Se podría elevar un subconjunto de miembros a roles potencialmente oficiales, basados en su interseccionalidad y cobertura a través de múltiples comunidades dentro de la DAO. Los protocolos que valoran la cohesión de la comunidad podrían usar SBTs para mantener las Almas interseccionales en el centro. Alternativamente, las DAOs pueden optar por una gobernanza que eleve ciertas combinaciones de rasgos más que otras, como la diversidad de códigos postales o la participación entre un subconjunto de DAOs de pasatiempos especiales.

[7] Consulte https://twitter.com/VitalikButerin/status/1264948490834247681 y https://twitter.com/VitalikButerin/status/1265252184813420544 para evidencia de encuesta informal de Twitter que sugiere que la gente encuentra intuitiva la idea de tener en cuenta la diversidad en mecanismos de toma de decisiones.

4.6 Medición de la Descentralización a través del Pluralismo

Al analizar ecosistemas del mundo real, es deseable medir cuán descentralizado el ecosistema es en realidad. ¿En qué medida es el ecosistema realmente descentralizado y en qué medida es la descentralización "falsa" y el ecosistema *de facto* dominado por una o un pequeño conjunto de entidades coordinadoras?

Dos métricas de descentralización populares son el coeficiente de Nakamoto propuesto por Balaji Srinivasan, que mide cuántas entidades distintas deben combinarse para reunir el 51% de algún recurso y el Índice de Herfindahl–Hirschman utilizado para medir la concentración del mercado con fines antimonopolio, el cual se calcula sumando los cuadrados de las cuotas de mercado de los participantes del mercado. Estos enfoques, sin embargo, dejan abiertas preguntas clave sobre cuáles son los recursos correctos para medir, cómo lidiar con la coordinación parcial y las áreas grises en lo que constituye una “entidad distinta” (distinct entity).

Por ejemplo, las empresas nominalmente independientes pueden tener muchos accionistas principales en común, tener directores que son amigos entre sí, o ser regulados por el mismo gobierno. En el contexto de protocolos de tokens, medir la descentralización de las tenencias de tokens enfocándose en las billeteras on-chain es tremendamente incorrecto porque muchas personas tienen múltiples billeteras y algunas billeteras (por ejemplo, las billeteras de casas de intercambios) representan a muchas personas. Además, *incluso* si las billeteras pudieran rastrearse a individuos únicos, esos individuos podrían ser grupos socialmente correlacionados, propensos a la coordinación accidental (en el mejor de los casos) o colusión intencional (en el peor de los casos). **Una mejor forma de medir la descentralización sería captar las dependencias sociales, las alianzas tenues y las solidaridades fuertes.**

Mineros y operadores de grupos de minería, que juntos representan 90% del poder de hash de Bitcoin, sentados en el panel de una conferencia sobre Bitcoin.

Los SBTs apoyan una forma diferente de medir el nivel de descentralización (o pluralismo) en una DAO, protocolo o red.

- Como primer paso, el protocolo podría limitar la votación vía tokens a Almas razonablemente resistentes a Sybil (o ricas en SBTs).

- Como segundo paso, un protocolo podría examinar las correlaciones entre los SBTs mantenidos por diferentes Almas y descontar votos por Almas si comparten un gran número de SBTs (agrupándolas como sólo parcialmente separadas). Exploraremos la última idea matemáticamente con mayor detalle en el contexto de la financiación cuadrática en el Apéndice A, donde presentamos una nueva primitiva, llamada la "puntuación de correlación".

- Como tercer paso, para alejarse y tener una idea más vasta de la descentralización en toda la red, uno podría medir las correlaciones entre los SBTs mantenidos por las Almas entre y a través de diferentes capas de la red: midiendo las correlaciones en votaciones, propiedad de tokens, comunicaciones relacionadas con la gobernanza e incluso el control sobre recursos computacionales.

Los SBTs nos permiten comenzar a medir la descentralización de ecosistemas interoperables y en capas, algo muy difícil de medir hoy en día. Todavía existe una gran pregunta abierta sobre qué fórmulas serían mejores para capturar lo que queremos medir y ser menos vulnerables a la manipulación. También hay muchas preguntas sobre cómo examinar las relaciones de los SBTs: ponderar algunos SBTs más que otros, descontar SBTs anidados, o tener en cuenta también la composición de tokens transferibles dentro de las Almas. Sin embargo, con un rico ecosistema de Almas y SBTs, una cantidad mucho mayor de datos estaría disponible para hacer estos cálculos y avanzar hacia una descentralización significativa.

4.7 Propiedad Plural

Las DAOs a menudo poseen o se organizan en torno a la propiedad de activos, tanto en el mundo virtual como en el físico. Hasta ahora, el alcance de la Web3 se ha limitado en gran medida a una clase estrecha de propiedad cuyo paquete de derechos son *totalmente transferibles*: tokens, NFTs, obras de arte, primeras ediciones o manuscritos poco comunes como la Constitución de los EE. UU. Pero el énfasis en la transferibilidad ha ido en detrimento de la Web3, haciéndola incapaz de representar y dar apoyo a algunos de los contratos de propiedad más simples y omnipresentes en la actualidad, como los arrendamientos de apartamentos. Los derechos de propiedad se definen en la

tradición jurídica romana como conjuntos de derechos de uso (“usus”), consumo o destrucción (“abusus”) y lucro (“fructus”). Rara vez todos estos derechos pertenecen conjuntamente al mismo propietario. Los arrendamientos de apartamentos, por ejemplo, confieren derechos limitados de uso ("usus") al arrendador, pero no derechos ilimitados a destruir el piso (“abusus”), venderlo (“fructus”), o incluso ceder su uso (subarriendo). Los derechos de las propiedades reales (tierra) suelen estar gravados por una serie de restricciones sobre el uso privado, la concesión de derechos públicos de acceso, límites a los derechos de venta, e incluso derechos de compra por expropiación. También son típicamente gravados con hipotecas que transfieren algún valor financiero a los prestamistas.

Es poco probable que el futuro de la innovación de la propiedad se base en la propiedad privada totalmente transferible, como hasta ahora se imagina en la Web3. Más bien, **la innovación dependerá de la capacidad de descomponer los derechos de propiedad para que coincidan con las características de los regímenes de propiedad existentes y codifiquen elaboraciones aún más ricas.** Las corporaciones y otras formas organizacionales evolucionaron precisamente para reconfigurar los derechos de propiedad de formas aún más creativas; por ejemplo, otorgando a los empleados acceso a instalaciones propias ("usus"), pero reservar para los gerentes los derechos de cambiar o dañar activos (“abusus”), mientras se paga a los accionistas el mayor beneficio económico (“fructus”). Los SBTs tienen la flexibilidad de representar y proliferar tales derechos de propiedad de activos físicos y virtuales, mientras que posibilitan nuevos experimentos. Estos son sólo algunos casos de uso:

- **Permitir el acceso** a recursos controlados pública o privadamente (por ejemplo, casas, automóviles, museos, parques y equivalentes virtuales). Los NFTs transferibles no logran capturar este caso de uso pues muchas veces los derechos de acceso son condicionales e intransferibles: si confío en ti para entrar mi patio trasero y usarlo como espacio recreativo, eso no implica que confíe en ti para sublicenciar ese permiso a otra persona.

- **Cooperativas de datos** donde los SBTs otorguen a investigadores acceso a los datos, al tiempo que instancien derechos a sus miembros para otorgar acceso (quizás por voto cuadrático) y negociar derechos económicos a los descubrimientos y la propiedad intelectual nacidos de la investigación. Exploramos esto más a fondo en la Sección 4, sobre Creación de Sentido Plural.

- **Experimentos con monedas locales**, con reglas que las hagan más valiosas para ser mantenidas y gastadas por las Almas que vivan en una región en particular, o sean parte de una comunidad en particular.

- **Experimentos de participación** en los que los SBTs creen una base de actividades continua para que Almas menos contextualizadas (p. ej., inmigrantes, adolescentes) puedan ganar influencia dentro de redes novedosas y más amplias. Tales Almas comenzarían con SBTs

estrechos que las agruparán con sus familias o comunidades locales. A medida que sus alianzas se diversifiquen gradualmente, obtendrían SBTs más amplios con derechos de voto para influir en redes más amplias, siguiendo la idea de polipolitanismo de Danielle Allen, un proceso que actualmente está mediado por límites arbitrarios de edad y residencia.

- **Experimentos en el diseño de mercados,** como la tributación Harberger y Self-Assessed Licenses Sold at Auction (SALSA) o Licencias Autoevaluadas y Cendidas en Subasta (LACS), donde los titulares de un activo publican un precio autoevaluado al que cualquier otra persona puede comprarles el activo y deben pagar periódicamente un impuesto proporcional a el precio autoevaluado para mantener el control del activo. Los SBTs podrían usarse para crear versiones más matizadas de SALSA—por ejemplo, donde los derechos de participación son aprobados por la comunidad para minimizar el comportamiento estratégico desde dentro o fuera de la comunidad.

- **Experimentos en el diseño de mecanismos democráticos** como la votación cuadrática. Los titulares de SBTs que representen la pertenencia a una comunidad pueden votar cuadráticamente sobre parámetros tales como incentivos y las tasas de impuestos. En última instancia, los "mercados" y la "política" no son espacios de diseño separados; los SBTs pueden ser una parte importante de una pila tecnológica que permita que todo el espacio *entre* estas dos categorías sea explorado. La provisión de bienes públicos a través de la financiación cuadrática es otra intersección de este tipo.

Por supuesto, hay escenarios distópicos a considerar. Los sistemas de inmigración podrían ser autorizados con SBTs migratorios. La captura regulatoria podría codificarse en tokens comunitarios anidados, donde los propietarios de viviendas tengan un poder de voto desproporcionado y estanquen la construcción de viviendas. Los SBTs podrían automatizar el “redlining”, o las prácticas discriminatorias que ponen ciertos servicios (financieros y de otro tipo) fuera del alcance de los residentes de ciertas áreas en función de la raza o el origen étnico. Como discutiremos más adelante, estos escenarios deben ser considerados dentro del contexto actual de permisos poco transparentes impuestos de arriba hacia abajo y discriminaciones. Los SBTs hacen que la discriminación sea más transparente y, por lo tanto, potencialmente contestable.

4.8 De Bienes Privados y Públicos a Bienes de Red Plural

De manera más general, los SBTs podrían permitirnos representar y administrar de manera efectiva activos y bienes que están en cualquier lugar del **espectro entre lo totalmente privado y lo totalmente público.** En realidad, casi todo está dentro de este espectro: los bienes para consumo personal tienen efectos indirectos positivos, como hacer que el consumidor sea más capaz de contribuir a su familia o comunidad, y aún los bienes públicos más disponibles a nivel mundial (por ejemplo, el clima) son inevitablemente más útiles para algunas personas que para otras (por ejemplo,

Seychelles comparado a Siberia). De manera similar, la *motivación humana* rara vez es completamente egoísta o completamente altruista; hay muchos patrones preexistentes de cooperación y algunos más presentes entre ciertas comunidades que en otras.

Sin embargo, el diseño de mecanismos hoy en día asume agentes atomizados y egoístas sin una cooperación *preexistente*, a menudo haciendo que los mecanismos sean vulnerables, en el mejor de los casos, a una sobrecoordinación inocente[8] y, en el peor de los casos, a la colusión intencional por grupos que *ya son* cooperativos. Así, incluso los mejores modelos de financiación pública, como el financiamiento cuadrático (quadratic funding o QF, por sus siglas en inglés), no se pueden escalar. QF fomenta la coordinación al ofrecer recompensas decrecientes a acción concentrada de unos pocos, pero recompensas crecientes para la acción colectiva de muchos. Por ejemplo, un total de $1 aportado por igual por 10 personas es compensado con $99 para generar $100 en total, mientras que $10 aportados por una sola persona no recibe ningún fondo compensatorio. Matemáticamente, esto se logra con fondos de emparejamiento proporcionales a la suma de las raíces cuadradas de las contribuciones individuales (como elaboraremos más a fondo en el Apéndice). Pero incluso la *cooperación débil* (por ejemplo, donar $1 a una causa) entre grupos grandes (por ejemplo, la mayoría de los ciudadanos de China) dominaría el sistema y absorbería todos los fondos de emparejamiento por el *premium* que QF pone en el número de contribuyentes únicos. Tal como está, el QF no descarta la coordinación entre intereses especiales y correlacionados que puedan inundar una ronda de QF, más bien *la recompensa*.

Pero en lugar de tratar la cooperación preexistente como un "error en el sistema que debemos corregir", la clave es reconocerla como reflejo de una cooperación parcial que debemos aprovechar y compensar. Al fin y al cabo, estamos en el negocio de fomentar la cooperación. El truco consiste en hacer que los mecanismos cuadráticos funcionen junto con redes de cooperación preexistentes, corrigiendo sus sesgos y tendencias a la sobrecoordinación. Los SBTs ofrecen una forma natural al permitirnos inclinar la balanza a favor de la cooperación *a través de las diferencias*. Como destacó la laureada con el premio Nobel Elinor Ostrom, el problema no es tanto coordinar los bienes públicos *per se*, sino más bien ayudar a las comunidades formadas por individuos imperfectamente cooperativos pero socialmente conectados a *superar* sus diferencias sociales para coordinarse a escala en redes más amplias.

Si los SBTs representan membresías comunitarias que reflejan las parcialidades de un Alma, **favorecer la cooperación a través de las diferencias simplemente significa descontar las recompensas cooperativas a Almas afiliaciones similares o correlacionadas —** similitud **medida por sus SBTs compartidos**. La suposición es que el consenso *entre* los que tienen afiliaciones

[8] Decimos "inocente", porque los grupos altamente cooperativos naturalmente buscarán promover sus intereses, lo que puede muy bien ser para su beneficio colectivo.

diferentes señala mejor los bienes plurales a través de redes más amplias, mientras que el consenso entre los que tienen afiliaciones *similares* señala sobrecoordinación (o colusión) que sirve a intereses más limitados.

Al revelar membresías compartidas a través de las Almas, los SBTs nos permiten *descontar* la cooperación preexistente y escalar cuadráticamente bienes plurales que confieren beneficios ampliamente a través de redes emergentes **acordadas por los miembros más diversos,** en lugar de bienes más limitados inocentemente sobrecoordinados (o coludidos intencionalmente) por intereses especiales. La fórmula precisa para el descuento por correlación "óptimo" depende de las características del modelo y aún no se ha estudiado, pero proporcionamos un primer paso para experimentar y llevar a cabo investigación adicional en el Apéndice.

§5 CREACIÓN DE SENTIDO PLURAL

Un ejemplo de bienes de red plurales que se destacan cada vez más en en un mundo digital son los modelos predictivos construidos con datos de usuarios. Tanto la inteligencia artificial (IA) como los mercados de predicción buscan predecir el futuro basados en datos obtenidos principalmente de personas. Pero ambos paradigmas están limitados en maneras diferentes y casi opuestas. El paradigma dominante en IA evita los incentivos. En su lugar, aspira datos (públicos o privados) para sintetizarlos en predicciones a través de modelos propietarios no lineales a gran escala, aprovechando el monopolio predeterminado de la Web2 sobre "usus" sin ningún "fructus" que fluya hacia los trabajadores de datos. Los mercados de predicción adoptan el enfoque opuesto, donde las personas apuestan por un resultado con la esperanza de obtener ganancias financieras, apoyándose completamente en los incentivos económicos de la especulación financiera ("fructus") sin sintetizar las creencias de los apostadores para producir modelos componibles. Al mismo tiempo, ambos paradigmas arrojan conclusiones que se caracterizan como verdades "objetivas". Mientras que los modelos de IA se describen como "universales" o "generalmente inteligentes", los mercados de predicción se representan como un resumen de todas las creencias de los participantes del mercado en un número único: un precio de equilibrio.

Un paradigma más productivo es evitar estos extremos y, en cambio, aprovechar las virtudes de ambos, compensando sus debilidades y enriqueciendo su amplitud. Proponemos combinar cuidadosamente la complejidad de los modelos de IA no lineal con los incentivos de mercado de los mercados de predicción para transformar a los trabajadores de datos pasivos en creadores de datos activos. Con información tan rica de procedencia arraigada en la sociabilidad de los creadores de datos, ilustramos como DeSoc puede desbloquear una inteligencia de/en red plural más poderosa que cualquiera de estos enfoques.

5.1 De Mercados de Predicción a la Pluralidad de Predicción

Los mercados de predicción apuntan a agregar creencias basadas en la riqueza y las preferencias de riesgo de aquellos que están dispuestos a apostar: el dinero habla. Pero esta "supervivencia del más apto" no es una forma deseable de agregar creencias. Un juego de suma cero donde la ganancia de un vendedor es la pérdida de otro supone una habilidad generalizada para predecir de "los inteligentes" y no de "los tontos". Si bien la riqueza puede ser un indicador de algunas formas de habilidad y experiencia, las predicciones que dan cuenta de otras formas de pericia relativa pueden ser más confiables. Participantes que han perdido apuestas en un dominio particular, pueden tener creencias más precisas en otro dominio. Pero los mercados de predicción tienen el desafortunado efecto de suscitar creencias de aquellos propensos al juego, lo que enriquece a los que ganan apuestas, empobrece al resto y desalienta la participación general de aquellos aversos al riesgo.

Hay mejores formas de obtener creencias. Una investigación reciente sugiere que mientras los mercados de predicción generalmente superan el sondeo simple, estos no superan el *sondeo de predicción sofisticado en equipo*, donde las personas tienen incentivos para compartir y discutir información. Bajo los modelos de deliberación en equipo, los miembros pueden ser ponderados basado en factores como el desempeño pasado y la evaluación de pares y el equipo participa en discusiones semi-estructuradas para agrupar información que no se puede encapsular simplemente en un contrato de compra o venta. Tales modelos de deliberación en equipo se pueden mejorar aún más con **reglas cuadráticas para obtener estimaciones de probabilidad exactas de todos los participantes** (en comparación con los mercados de predicción, que sólo obtienen opiniones de arriba hacia abajo sobre el actual precio de equilibrio)[9]. Se ha demostrado que la cantidad de contratos que las personas tienen un incentivo para comprar refleja su evaluación subjetiva de probabilidad.[10] Dichos mercados también distribuyen las ganancias de participación mucho más equitativamente, premiando la precisión sin arruinar al resto y manteniendo así a todos como participantes para futuras rondas.

Los SBTs podrían desbloquear una nueva clase de modelos y experimentos ricos en poder predictivo y pericia relativa. Mientras que los mercados de predicción proveen un número (el precio de un contrato) las encuestas cuadráticas proveen la creencia exacta de cada participante sobre la probabilidad de un evento. Los SBTs permiten un **cálculo adicional sobre esas creencias en el *contexto social*** de las credenciales educativas, membresías y sociabilidad general de un participante a desarrollar modelos predictivos mejor ponderados (o sintetizados no linealmente), probablemente posibilitando que emerjan predictores expertos en intersecciones novedosas e imprevistas. Por lo tanto, incluso si una encuesta no agrega bien las creencias, las encuestas podrían estudiarse

[9] Bajo una regla cuadrática, los miembros del equipo pueden comprar un contrato que paga $X condicionalmente a que ocurra un evento, pero cuesta $(X^2)/2. Por ejemplo, una persona que establece X=0,5 recibirá $0,5 si ocurre el evento (pagado por el encuestador) y pagará $0,125 independientemente.

[10] Si un individuo evalúa la probabilidad p, su pago esperado es pX y el costo es X^2/2. Tomando la derivada con respecto a X, la condición de optimización es p=X, suponiendo neutralidad al riesgo, lo cual es razonable para apuestas pequeñas (tanto el pago como el costo pueden reducirse o aumentarse arbitrariamente y se mantiene el mismo argumento).

retroactivamente para descubrir las características de los participantes "más correctos" y convocar “expertos” mejor adaptados en futuras encuestas, tal vez en un contexto de equipo deliberativo. Estos mecanismos están estrechamente relacionados con aquellos que proponemos a lo largo de este documento. De la misma manera que los mecanismos cuadráticos descontados por puntajes de correlación pueden transformar bienes públicos de arriba hacia abajo mal coordinados en poderosos bienes de red plurales de abajo hacia arriba, también pueden transformar sistemas de gobernanza basados en mercados de predicción de suma cero que incentiven a los participantes a ocultar su información (p. ej., futarquía) en sistemas de suma positiva y creación de sentido plural que puedan fomentar la revelación y síntesis de información nueva y mejor.

5.2 Inteligencia artificial a inteligencia plural

Los modelos de "redes neuronales" no lineales a gran escala (como BERT y GPT-3) también podrían ser transformados por los SBTs. Dichos modelos succionan (“data hoovering”) grandes cantidades de fuentes de datos vigilados pública o privadamente para producir modelos y predicciones ricas, como el código basado en mensajes de lenguaje natural. La mayoría de los creadores de datos vigilados no son conscientes de su papel en la creación de estos modelos, no retienen derechos residuales y son vistos como "incidentales" en lugar de como participantes clave. Además, esta succión de datos separa a los modelos de su contexto social, lo que enmascara sus prejuicios y limitaciones y socava nuestra capacidad para compensarlos. Estas tensiones se destacan cada vez más con la creciente demanda de disponibilidad de datos, nuevas iniciativas como "hojas de datos para conjuntos de datos” que documentan la procedencia de los datos, y enfoques de preservación de la privacidad para el aprendizaje automático. Estos enfoques requieren otorgar importantes intereses económicos y de gobernanza a quienes generan los datos, incentivándolos a cooperar en la producción de modelos más poderosos que los que podrían construir solos.

Los SBTs ofrecen una forma natural de programar **incentivos económicos para datos ricos en procedencia mientras empoderan a los creadores de datos con derechos residuales de gobernanza sobre sus datos**. En particular, los SBTs proveen incentivos para los datos (y la calidad de estos) dirigidos cuidadosa y proporcionalmente a individuos y comunidades en base a sus características. Al mismo tiempo, los modelistas pueden rastrear las características de los datos recolectados y su contexto social, tal como lo reflejan los SBTs, y encontrar contribuyentes que eliminen los sesgos y compensen por límites. Los SBTs también pueden programar derechos de gobernanza personalizados para los creadores de datos, lo que les permite formar cooperativas que agrupen datos y negocien usos. Esta capacidad de programación de abajo hacia arriba por parte de los creadores de datos permite una futuro de inteligencias plurales, donde los creadores de modelos pueden competir para negociar usos sobre los mismos datos para construir diferentes modelos. Así, nos alejamos de un paradigma de una “inteligencia artificial” monolítica separada o libre de orígenes humanos succionando datos vigilados sin procedencia y, en su lugar, nos acercamos a una **explosión**

cámbrica de inteligencias plurales construidas cooperativamente enraizadas en la procedencia social y gobernadas por Almas.

Con el tiempo, al igual que los SBTs individualizan un Alma, también llegan a individualizar modelos insertando datos de procedencia, gobernanza y derechos económicos directamente en el código del modelo. Así, las inteligencias plurales, como los humanos, construyen un Alma incrustada en la sociabilidad humana. Según cómo se mire, los humanos evolucionan con el tiempo incrustados en inteligencias plurales, cada una con un Alma única, complementando y cooperando con otras Almas. Y, en esto, vemos la convergencia del mercado de predicción y los paradigmas de IA hacia el sentido plural, combinando incentivos ampliamente distribuidos y un seguimiento cuidadoso del contexto social para crear un diversidad de modelos que combinan lo mejor de ambos enfoques en un paradigma tecnológico más potente que cualquiera.

5.3 Privacidad Plural Programable

Las inteligencias plurales plantean preguntas importantes sobre la privacidad de los datos. Después de todo, para construir tales inteligencias poderosas, se requiere agrupar datos de individuos en base a grandes conjuntos de datos (por ejemplo, datos de salud) o capturar datos que no son interpersonales sino compartidos (por ejemplo, un gráfico social). Los defensores de la "identidad auto-soberana" tienden a tratar los datos como propiedad privada: los datos sobre esta interacción son *míos*, por lo que debería poder elegir cuándo y a quién para revelarlo. Sin embargo, aún más que en la economía física, la economía de datos es mal interpretada en términos de simple propiedad privada. En relaciones bidireccionales simples, como un asunto ilícito, el derecho a revelar la información suele ser simétrico y, a menudo, requiere permiso y consentimiento mutuos. Como destacó la erudita Helen Nissenbaum, la preocupación no es la "privacidad" como tal, sino la falta de integridad en el contexto al compartir información. El escándalo de Cambridge Analytica fue, en gran parte, sobre personas revelando propiedades de sus gráficos sociales e información sobre sus amigos sin su consentimiento.

En lugar de la privacidad como derecho de propiedad transferible, un enfoque más prometedor es tratar **la privacidad como un conjunto de derechos programables y débilmente acoplados para *permitir el acceso, alterar o beneficiarse de información*.** Bajo tal paradigma, cada SBT, como un SBT que representa una credencial o acceso a un almacén de datos, idealmente también tendría un derecho de propiedad programable implícito que *especificara el acceso* a la información subyacente constituyendo el SBT: los titulares, los acuerdos entre ellos, la propiedad compartida (por ejemplo, ciertos datos) y obligaciones con terceros. Por ejemplo, algunos emisores elegirían que los SBTs sean totalmente públicos. Algunos SBTs, como un pasaporte o un registro de salud, serían privados en el sentido de auto-soberanía, con derechos unilaterales de divulgación por parte de las Almas que portan el SBT. Otros, como los SBTs que reflejan la membresía de una cooperativa de

datos, tendrían múltiples firmas o permisos de voto comunitario más sofisticados, donde todos o una mayoría cualificada de los titulares de SBTs deben dar su consentimiento para la divulgación.

Si bien actualmente existen preguntas técnicas como si se pueden programar los SBTs de esta manera y preguntas importantes sobre la compatibilidad de incentivos exploradas más a fondo en la Sección 7, pensamos que la privacidad plural programable justifica una mayor investigación y ofrece ventajas clave sobre los paradigmas alternativos. Bajo nuestro enfoque, los SBTs tienen el potencial de habilitar la privacidad como un derecho programable y componible que puede mapear el conjunto complejo de expectativas y acuerdos que tenemos hoy. Además, tal programabilidad podría ayudarnos a reimaginar nuevas configuraciones, ya que hay un **número *infinito* de formas en que la privacidad —como un derecho al permiso de acceso a la información— podría estar compuesta por "usus", "abusus" y "fructus"** para crear una constelación matizada de derechos de acceso. Por ejemplo, los SBTs podrían autorizar cálculos sobre almacenes de datos, tal vez siendo propiedad y gobernados por una pluralidad de Almas, utilizando un técnica de preservación de la privacidad específica. Algunos SBTs pueden incluso permitir el acceso a los datos de una manera en la que se pueden hacer ciertos cálculos, pero los resultados no se pueden *revelar* a terceros. Un ejemplo simple es una votación: el mecanismo de votación necesita contar los votos de cada Alma, pero los votos no deben ser revelados a nadie más para evitar la compra de votos.

La comunicación es quizás la forma más canónica de datos compartidos. Sin embargo, los canales de comunicación actuales carecen tanto de control como de gobierno del usuario ("usus" y "abusus") y, al mismo tiempo, subastan la atención del usuario ("fructus") al mejor postor, incluso si se trata de un bot. Los SBTs posibilitan la administración más saludable de la "economía de la atención" que permite a las Almas filtrar correo no deseado entrante de posibles bots fuera de su gráfico social, al tiempo que eleva la comunicación de las comunidades reales y las intersecciones deseadas. Los oyentes podrían volverse más conscientes de a quién están escuchando y ser más capaces de asignar crédito a trabajos que estimulen ideas. En lugar de optimizar para lograr el máximo compromiso, tal economía podría optimizarse para colaboraciones de suma positiva y co-creaciones valiosas. Dichos canales de comunicación también son importantes para la seguridad: como se señaló anteriormente, los canales de comunicación de "gran ancho de banda" son fundamentales para construir los cimientos de seguridad de la recuperación comunitaria.

§6 SOCIEDAD DESCENTRALIZADA

La Web3 aspira a transformar las sociedades en general, en lugar de simplemente los sistemas financieros. Sin embargo, el tejido social actual —familias, iglesias, equipos, empresas, sociedad civil, celebridades, democracia—no tienen sentido en mundos virtuales (a menudo llamado el "metaverso") sin primitivas que representen Almas humanas y las relaciones más amplias que sostienen. Si la Web3 evita las identidades persistentes, sus patrones de confianza y cooperación, y sus derechos y permisos

componibles, vemos, respectivamente, ataques Sybil, colusión y un ámbito económico limitado de propiedad privada totalmente transferible, todo lo cual tiende hacia la hiper-financiarización.

Para eludir la hiper-financiarización, pero aún desbloquear un crecimiento exponencial, proponemos *aumentar y unir* nuestra sociabilidad a través de realidades virtuales y físicas, empoderando a Almas y comunidades para codificar relaciones sociales y económicas ricas. Pero simplemente construir sobre la base de la confianza y la cooperación no es suficiente. La corrección de sesgos y tendencias a la sobrecoordinación (o colusión) entre las redes de confianza es esencial para alentar relaciones más intrincadas y diversas que abarquen mayores distancias sociales que antes. Llamamos a esto **"Sociedad Descentralizada (DeSoc, por sus siglas en inglés)": una sociabilidad co-determinada, donde se reúnen Almas y Comunidades de abajo hacia arriba, como propiedades emergentes de cada una para producir *bienes de redes plurales* a través de diferentes escalas.**

Hacemos hincapié en los bienes de redes plurales como una característica de DeSoc, porque las redes son el motor de crecimiento económico más poderoso, pero el más susceptible a la captura distópica por parte de actores privados (por ejemplo, la Web2) y gobiernos poderosos (por ejemplo, el Partido Comunista Chino). El crecimiento económico más significativo resulta de *rendimientos crecientes de la red*, donde cada unidad adicional de insumos produce cada vez *más* rendimientos. Los ejemplos de redes físicas simples incluyen carreteras, redes eléctricas, ciudades y otras formas de infraestructura construidos con mano de obra y otros insumos de capital. Ejemplos de poderosas redes digitales incluyen mercados, modelos predictivos e inteligencias plurales construidas a partir de datos. En ambos casos, la economía de redes se aparta de la economía neoclásica, que enseña rendimientos *decrecientes,* donde cada unidad adicional de insumo produce incrementalmente menos rendimiento y donde la propiedad privada produce los resultados más eficientes. La propiedad privada aplicada a un contexto de rendimientos crecientes tiene el efecto opuesto: estrangula el crecimiento de la red por medio de la extracción de renta. Un camino entre dos ciudades puede desbloquear rendimientos crecientes de las ganancias del comercio, pero la misma carretera como propiedad privada puede estrangular el crecimiento si los propietarios optan por extraer renta hasta el valor comercial entre las dos ciudades. La propiedad pública de una red también tiene sus propios peligros, ya que es susceptible de captura regulatoria o falta de fondos.

Las redes con rendimientos crecientes son más eficientes cuando no se las trata como bienes puramente públicos ni puramente privados, sino como *bienes compartidos parciales y plurales*. DeSoc proporciona el sustrato social para desagregar y reconfigurar derechos: derechos de uso ("usus"), derechos de consumir o destruir ("abusus") y derechos de ganancia ("fructus"), y permitir mecanismos de gobernanza eficientes a través de estos derechos que aumentan la confianza y la cooperación al mismo tiempo que se verifica la colusión y la captura. Hemos explorado varios mecanismos a lo largo de este documento, como SALSA basado en la comunidad y el financiamiento

(y votación) cuadrático descontado por puntajes de correlación. Esta tercera vía de propiedad parcial y plural evita la Caribdis de la extracción de la renta privada y la Scylla de la captura regulatoria pública.

En muchos sentidos, **DeFi hoy es un paradigma de propiedad privada de rendimientos decrecientes reacondicionado sobre redes de rendimientos crecientes**. Construido sobre la premisa de la *falta de confianza* ("trustlessness"), DeFi está inherentemente limitado al ámbito de la propiedad privada totalmente transferible (por ejemplo, tokens transferibles) que en su mayoría agrupan "usus", "abusus" y "fructus". En el mejor de los casos, DeFi corre el riesgo de estrangular el crecimiento de la red mediante la extracción de rentas y, en el peor, corre el riesgo de introducir monopolios de vigilancia distópicos dominados por "ballenas" que recolectan y succionan datos de forma similar a la Web2.

DeSoc transforma la carrera de DeFi para controlar y especular sobre el valor de las redes en una coordinación de abajo hacia arriba para construirlas, participar en ellas y gobernarlas. Como mínimo, el sustrato social de DeSoc puede hacer que DeFi sea resistente a los ataques Sybil (permitiendo el gobierno de la comunidad), resistente a los ataques vampiro (internalizando las externalidades positivas para construir una red de código abierto) y resistente a la colusión (preservando la descentralización de una red). Con las correcciones estructurales de DeSoc, DeFi puede apoyar y expandir redes plurales que confieren beneficios en términos generales, según lo acordado por los miembros más diversos, en lugar de afianzar aún más las redes capturadas por intereses estrechos.

Sin embargo, la **mayor fortaleza de DeSoc es la *componibilidad de su red***. Rendimientos crecientes sostenidos y el crecimiento de la red no es simplemente evitar los peligros de la extracción de rentas, sino también fomentar la proliferación e intersección de redes anidadas. Una carretera puede formar una red entre dos ciudades. Pero sin una cooperación más amplia, dos ciudades cooperantes finalmente alcanzarán un techo de disminución de retornos financieros, ya sea por *congestión* (carreteras y viviendas) o por a*gotamiento* (llegar al límite de las personas a las que pueden servir). Sólo a través de la innovación tecnológica y una cooperación cada vez más amplia, si bien más laxa, con las redes vecinas en pro de nuevas fuentes de rendimientos crecientes pueden continuar creciendo exponencialmente. Algunos tipos de cooperación serán físicos, ampliando progresivamente el comercio físico a través del espacio. Pero muchas más conexiones serán informativas y digitales. Con el tiempo, veremos nuevas matrices de cooperación entre redes físicas y digitales, que dependen y amplían las interconexiones sociales sobre las que se construyen. Aquello que permite DeSoc es precisamente esta estructura creciente de cooperación interseccional y parcialmente anidada a través del mundo digital y físico.

A través de la composición de redes y la coordinación, DeSoc emerge en la intersección de la política y los mercados, aumentando a ambos con la sociabilidad. DeSoc potencia la visión de JCR Licklider, fundador de ARPANET que creó Internet, de "simbiosis hombre-computadora" en una "red de computadora intergaláctica" con un dinamismo social dramáticamente aumentado *basado en la confianza*. En lugar de construir la premisa de DeFi de "sin confianza", DeSoc codifica las redes de confianza que sustentan la economía real actual y nos permite aprovecharlas para generar bienes plurales en red resistentes a la captura, extracción o dominación. Con tal sociabilidad aumentada, la Web3 puede evitar la hiper-financiarización al corto plazo en favor de un futuro ilimitado de rendimientos crecientes a través de la distancia social.

6.1 Las almas pueden ir al cielo... o al infierno

Si bien hemos resaltado selectivamente el potencial de DeSoc que consideramos prometedor, es importante recordar que casi cualquier tecnología con tal potencial transformador tendrá un potencial efecto similar de transformación destructiva: el fuego quema; la rueda arrolla; la televisión lava el cerebro; los coches contaminan; las tarjetas de crédito atrapan en deudas, y así sucesivamente. Aquí, los mismos SBTs que podrían usarse para compensar dinámicas internas de grupo y lograr la cooperación a través de las diferencias también podría usarse para automatizar la segregación injusta y discriminatoria de grupos sociales desfavorecidos o fomentar ataques cibernéticos o físicos a los mismos, imponer políticas de migración restrictivas o dar préstamos depredadores. Muchos de estos escenarios no son destacados en el ecosistema de la Web3 actual porque, dado el sustrato actual, no son conceptos significativos. Explorar las ventajas de DeSoc también incrementa las chances de que se produzcan estos daños. Así como la desventaja de tener un corazón es que a uno le pueden romper el corazón, la desventaja de tener un Alma es que puede irse al infierno y la desventaja de tener una sociedad es que las sociedades a menudo están animadas por el odio, prejuicios, violencia y miedo. A menudo, la humanidad es un gran y trágico experimento.

Mientras meditamos sobre las posibles distopías de DeSoc, también debemos contextualizar estas posibilidades dentro de otras distopías tecnológicamente habilitadas. La Web2 es una arquitectura autoritaria y poco transparente para la vigilancia y el control social. Mientras que la Web2 a menudo se basa en burocracias artificiales de arriba hacia abajo para conferir identidad (una "licencia de conducir"), DeSoc se basa en certificaciones sociales horizontales ("peer-to-peer"). Mientras que DeSoc empodera a Almas para codificar sus propias relaciones y co-crear propiedad plural, la Web2 intermedia conexiones sociales o las monetiza con algoritmos opacos que pueden polarizar, dividir y desinformar. DeSoc elude sistemas de crédito social opacos y de arriba hacia abajo. La Web2 forma la base de ellos. DeSoc trata a las Almas como agentes, mientras que la Web2 trata a las Almas como objetos.

El riesgo de control social con DeFi, sin ningún sustrato de identidad, es menor, al menos en el corto plazo. Pero DeFi tiene su propia distopía. **Si bien DeFi supera las formas *explícitas* de centralización, donde los actores específicos tienen un nivel de poder formal descomunal dentro de un sistema, no tiene una forma integrada de superar la centralización *implícita* a través de la colusión y el poder de mercado.** Los monopolios no siempre aparecen como las Standard Oils del pasado. La colusión puede ocurrir incluso en niveles más altos y remotos de un ecosistema. Hoy vemos esto con el surgimiento de una clase de administradores de activos institucionales (por ejemplo, Vanguard, BlackRock, State Street, Fidelity, etc.) que son los principales accionistas de todos los bancos, aerolíneas, compañías automotrices y otras industrias importantes. Debido a que tales administradores de activos tienen una participación en todos los rivales dentro de una industria (es decir, una participación en cada una de las principales aerolíneas), su incentivo es hacer que las empresas que controlan *parezcan* una industria competidora pero *actúen* como un monopolio que maximiza las ganancias de toda la industria y el afianzamiento a expensas del consumidor y del público en general[11].

En DeFi, las mismas "ballenas" y VCs acumulan mayores acciones en cada nivel de la pila y entre competidores dentro de una misma pila tecnológica, sea votando en el gobierno de tokens o delegando a la misma clase de delegados, que también están correlacionados de manera similar en toda la red. Sin ningún sustrato social para la resistencia a los ataque Sybil y descuentos de correlación para la descentralización fuerza-función, también deberíamos esperar ver más monopolios financiados por ballenas, a medida que los monopolios se convierten cada vez más en el mayor grupo capital de inversión disponible. A medida que divergen “la clase de dinero” y los usuarios, deberíamos esperar ver (y ya estamos viendo) mayores y mayores niveles de desalineación de incentivos y extracción de rentas. Si surgen aplicaciones de DeFi que manejen datos privados, es posible que veamos dinámicas similares, como que las aplicaciones fomenten guerras de ofertas entre múltiples personas que "poseen" datos que en realidad son interpersonales (por ejemplo, su gráfico social) para construir IA privadas monolíticas que compitan contra los humanos, evitando un futuro de IA plurales competidoras que aumenten a los humanos.

Por lo tanto, DeSoc no necesita ser perfecta para pasar la prueba de ser aceptablemente no distópica: para ser un paradigma que vale la pena explorar, simplemente necesita ser mejor que las alternativas disponibles. Mientras que DeSoc puede llevar a *posibles* escenarios distópicos contra los que protegerse, la Web2 y DeFi existentes están cayendo en patrones que son *inevitablemente* distópicos, concentrando el poder en una élite que decide los resultados sociales o posee la mayor parte de la riqueza. La dirección de la Web2 es determinísticamente autoritaria, acelerando la capacidad de vigilancia y la manipulación del comportamiento de arriba hacia abajo. Hoy por hoy, la

[11] Ver Posner, E. & Weyl, E. G., “Dismembering the Octopus,” *Radical Markets: Uprooting Capitalism and Democracy for a Just Society,* Princeton University Press, 2018.

dirección de DeFi es nominalmente anarcocapitalista, pero está cayendo en el efecto de red y las presiones de monopolio que, de la misma manera, ponen en riesgo convertir su camino en uno autoritario en el mediano plazo.

DeSoc, por el contrario, es **pluralismo social estocástico**: una red de individuos y comunidades que se juntan, como propiedades emergentes unas de otras, co-determinando su propio futuro. Observando la Web2, la consecuencia de DeSoc se puede comparar con el surgimiento de gobiernos participativos populares a partir de siglos de monarquía. Los gobiernos participativos no dieron lugar *inevitablemente* a la democracia; también condujeron al surgimiento del comunismo y del fascismo. De manera similar, los SBTs no hacen que la infraestructura digital sea *inherentemente* democrática, pero son democrático-compatible dependiendo de lo que las Almas y las comunidades co-determinan. Abrir este espacio de posibilidad es una mejora notable sobre el autoritarismo de la Web2 y el anarcocapitalismo de DeFi.

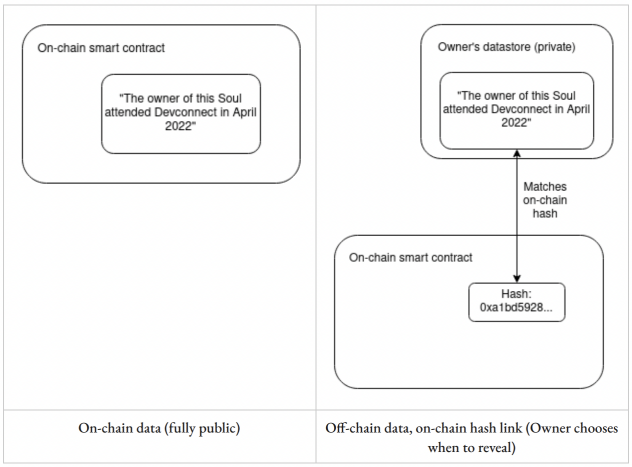
§7 DESAFÍOS DE IMPLEMENTACIÓN

La privacidad presenta un desafío clave para DeSoc. Por un lado, demasiados SBTs públicos pueden revelar mucha información sobre un Alma, haciéndolas vulnerables al control social. Por otro lado, demasiados SBTs puramente privados también pueden conducir a canales de comunicación privados que evitan el descuento de correlación para la gobernanza y la coordinación social, lo que presenta importantes preguntas sobre compatibilidad de incentivos. Cercanamente relacionado con el tema de la privacidad está el tema del engaño: las Almas pueden tergiversar sus solidaridades sociales, mientras que coordinan a través de canales privados o secundarios. No podemos aspirar a conocer todas las posibilidades y respuestas pero, en su lugar, explorar la naturaleza del desafío y esbozar algunos caminos prometedores para futuras investigaciones.

7.1 Almas privadas

Los sistemas basados en blockchain son públicos por defecto. Cualquier relación que se registra on-chain es inmediatamente visible no solo para los participantes, sino también para cualquier persona en todo el mundo. Un poco de privacidad puede ser retenida teniendo múltiples seudónimos: un Alma familiar, un Alma médica, un Alma profesional, un Alma política cada una con diferentes SBTs. Pero si se hace de manera ingenua, podría ser muy fácil correlacionar estas Almas entre sí. Las consecuencias de esta falta de privacidad son graves. De hecho, **sin medidas explícitas adoptadas para proteger la privacidad, la visión "ingenua" de simplemente poner todos los SBTs on-chain puede generar demasiada información pública para muchas aplicaciones.**

Para hacer frente a la publicidad excesiva, hay una serie de soluciones con diferentes niveles de complejidad técnica y funcionalidad. El enfoque más simple es que un SBT podría almacenar datos off-chain, dejando solo el hash de los datos on-chain.



Smart contract on-chain "El dueño de esta Alma participó en Devconnect en abril del 2022"	Base de datos del dueño (privada) "El dueño de esta Alma participó en Devconnect en abril del 2022" Coincide con el hash on-chain Smart contract on-chain: Hash: 0xa1bd5928
Data on-chain (totalmente pública)	Data off-chain, link al hash on-chain (el dueño elige cuando revelarla)

La elección de cómo almacenar los datos off-chain se deja en manos de la persona. Las posibles soluciones incluyen (i) su propios dispositivos, (ii) un servicio en la nube en el que confíen, o (iii) redes descentralizadas como Interplanetary File System (IPFS). El almacenamiento de datos off-chain nos permite seguir teniendo smart contracts que permitan el derecho a *escribir* datos SBTs, pero al mismo tiempo tener permisos separados para *leer* esos datos. Bob puede elegir revelar el contenido de cualquiera de sus SBTs (o los almacenes de datos que estos autorizan) sólo cuando lo desee. Esto ya supone una mejora y tiene el beneficio adicional de mejorar la escalabilidad técnica porque la mayoría de los datos sólo necesita ser manejado por un número muy pequeño de partes. Pero para alcanzar completamente propiedades como la privacidad plural, así como formas de divulgación más detalladas, debemos ir más allá. Afortunadamente, muchas tecnologías criptográficas nos permiten hacer esto.

Un poderoso conjunto de bloques de construcción que permite nuevas formas de revelar parcialmente los datos es una rama de la criptografía denominada "pruebas de conocimiento cero". Si

bien las pruebas de conocimiento cero se usan con mayor frecuencia en la actualidad para permitir transferencias de activos que preservan la privacidad, también pueden permitir que las personas prueben declaraciones arbitrarias sin desvelar más información más allá del propio comunicado. Por ejemplo, en un mundo donde documentos del gobierno y otras atestaciones son comprobables criptográficamente, alguien podría probar una declaración como "Soy un ciudadano de Canadá, con más de 18 años y con un título universitario en economía y más de 50.000 seguidores en Twitter, y aún no he reclamado una cuenta en este sistema".

Las **pruebas de conocimiento cero** se pueden calcular sobre SBTs para probar características sobre un Alma (por ejemplo, que tiene ciertas membresías). Esta técnica se puede ampliar aún más mediante la introducción de técnicas de **cómputo multipartidista** como circuitos ilegibles, que podrían hacer que tales pruebas sean *doblemente privadas*: el "probador" no revela quién es al "verificador" y el "verificador" no revela su mecanismo de verificación a el "probador". En cambio, ambas partes hacen el cálculo juntas y sólo se enteran del resultado.

Otra técnica poderosa son las ***pruebas de verificador designado***. En general, los "datos" son resbaladizos: si yo te envío una película, no puedo evitar tecnológicamente que la grabes y la envíes a un tercero. Las soluciones alternativas como la gestión de derechos digitales (DRM) tienen, en el mejor de los casos, una eficacia limitada y, a menudo, grandes costos para los usuarios. Las pruebas, sin embargo, no son resbaladizas de la misma manera. Si Amma quiere probar una propiedad X sobre sus SBTs a Bob, puede hacer una prueba de conocimiento cero de la declaración "Tengo SBTs que satisfacen la propiedad X, *o* Tengo la clave de acceso al Alma de Bob". A Bob le parecería convincente esta afirmación: él sabe que él no hizo la prueba, por lo que Amma debe tener SBTs que satisfagan la propiedad X. Pero si Bob pasa la prueba a Cuifen, Cuifen no estaría convencido: hasta donde él sabe, Bob podría haber hecho la prueba con su propia llave. Esto se puede reforzar aún más con ***funciones de retardo verificables (VDFs, por sus siglas en inglés)***: Amma puede hacer y presentar una prueba que sólo se puede hacer con los SBTs requeridos en este momento, pero cualquiera otra persona podrá hacerlo en *cinco minutos a partir de ahora*. **Esto significa que es posible representar permisos sofisticados de acceso a *pruebas fehacientes sobre los datos* a pesar de la imposibilidad de realizar los mismos tipos de permisos selectivos a los datos sin procesar en sí, que simplemente se pueden copiar y pegar.** No obstante, esto puede llevarnos bastante lejos. Así como las blockchains ofrecen trazabilidad en transacciones que impiden que alguien haga clic con el botón derecho y copie y pegue un NFT valioso (lanzando un ataque Sybil al propietario original), de manera similar los SBTs puede ofrecer trazabilidad en la prevención social, que como mínimo puede reducir el valor de los datos copiados y pegados con orígenes no verificados.

Estos datos off-chain y técnicas de conocimiento cero son compatibles con la **reputación *negativa***: los SBTs que se hacen visibles incluso si el titular no *quiere* que sean visibles. Ejemplos importantes de reputación negativa incluyen el historial crediticio, datos sobre préstamos no pagados,

críticas negativas y quejas de socios comerciales, y los SBTs que acrediten conexiones sociales relevantes para la coordinación. Las blockchains junto con la misma criptografía podrían ofrecer una solución: las Almas podrían ser forzadas por lógica de smart contract para incorporar SBTs negativos en una estructura de datos como un árbol Merkle que se almacena on-chain, y cualquier prueba de conocimiento cero o cálculo de circuito distorsionado requeriría que introduzcan esa información, porque de lo contrario habría un "agujero" visible en los datos proporcionados que el verificador reconocería. El protocolo Unirep es un ejemplo de cómo se podría implementar esto.

El objetivo de estos ejemplos no es mostrar exactamente cómo se puede utilizar la tecnología criptográfica para resolver todos los problemas de privacidad y permisos de datos con SBTs. Más bien, se trata de esbozar algunos ejemplos para mostrar el poder de tales tecnologías. Una dirección de investigación futura importante es el alcance de los límites exactos de diferentes tipos de permisos de datos y las combinaciones específicas de técnicas que funcionan mejor para alcanzar el nivel deseado de permisos. Otra cuestión es qué tipos de regímenes de propiedad plural son deseables para gobernar los datos y cómo desglosar adecuadamente el acceso ("usus"), la edición ("abusus") y los derechos de flujo de caja (“fructus”).

7.2 Almas engañosas

Si los SBTs son el sustrato social sobre el que la propiedad plural, los bienes en red y las inteligencias son coordinadas, uno podría preocuparse de que las Almas intenten engañar a las comunidades para ganar acceso a la gobernanza o los derechos de propiedad que imaginamos que los SBTs otorgan. Por ejemplo, si muchas aplicaciones dependen de los SBTs que representan la asistencia a conferencias, las conferencias sin escrúpulos podrían ofrecer tales SBTs a cambio de sobornos. Con suficientes sobornos, los humanos (y los bots) podrían generar un gráfico social falso que hace que la cuenta parezca un Alma humana auténtica, ricamente diferenciada por (falsos) SBTs. Así como las DAOs pueden ser sobornadas, también lo pueden ser las Almas y los mecanismos de votación on-chain que utilizan. Por el contrario, si los SBTs se utilizan para descontar coordinación, las Almas pueden evitar los SBTs para maximizar su influencia. ¿Por qué debemos creer que los SBTs que un Alma posee reflejan con precisión sus verdaderos compromisos sociales en lugar de simplemente mostrar cómo eligen jugar este juego?

Un argumento es que los diversos incentivos para hacer trampa pueden “equilibrarse”. Las Almas pueden ordenar e identificarse a sí mismas en las redes que son importantes para ellas en la escala correcta, al igual que los impuestos Harberger equilibran el incentivo para sobrevaluar y subvaluar los activos para obtener valoraciones de mercado aproximadamente precisas. Las Almas querrán tener más SBTs para ganar influencia dentro de sus comunidades, pero por otro lado evitarán los SBTs de las comunidades que menos les importa para obtener una puntuación más baja en las métricas de correlación y aumentar su influencia en la gobernanza sobre redes más amplias.

Pero sería ingenioso suponer que estos dos incentivos (ganar acceso y maximizar influencia) siempre se cancelan uniformemente, o incluso se acercan a cancelarse, como por arte de magia. Pueden haber muchas comunidades que utilizan sistemas distintos a los SBTs para el acceso y la gobernanza. Las comunidades pueden, en contra de nuestra suposición principal sobre la publicidad, distribuir SBTs privados para reflejar derechos de gobernanza pero inducir a los miembros de la comunidad a mantener estos SBTs en secreto en decisiones más amplias

El problema de los "juegos" no debe subestimarse. Es un tema significativo y resolverlo es uno de los focos más importantes para futuras investigaciones. De hecho, es una de las principales razones por las que el código abierto de muchos algoritmos existentes que priorizan o filtran usuarios humanos es un gran desafío. Para mitigar y disuadir los juegos sobre SBTs, sugerimos varias normas y direcciones criptográficas:

1. El ecosistema de SBTs podría **iniciarse en canales comunitarios "gruesos"**, donde los SBTs señalan membresía comunitaria off-chain con fuertes lazos sociales e interacciones repetidas. Esto facilitaría a que las comunidades filtren y revoquen los SBTs de imitadores y bots. Tales canales gruesos, que a menudo encontramos en iglesias, lugares de trabajo, escuelas, grupos de reunión y organizaciones de la sociedad civil— proporcionarían un sustrato social más resistente a los ataques Sybil para controlar estos juegos (por ejemplo, a través de bots, sobornos, suplantación de identidad) en canales sociales más "delgados".

2. **Las comunidades anidadas podrían requerir SBTs para forzar el contexto sobre posibles vectores de colusión "solo por debajo" de ellos**. Por ejemplo, si un Estado estuviera realizando una ronda de financiación o votación, el Estado podría requerir que cada ciudadano participante también tenga un SBT de un condado y municipio definido.

3. La apertura y la demostrabilidad criptográfica del ecosistema SBT podrían usarse para **detectar activamente patrones colusorios y penalizar el comportamiento no auténtico**, tal vez descartando el poder de voto de las Almas colusorias u obligando a las Almas a aceptar SBTs que representen atestaciones negativas. Por ejemplo, si un Alma da fe de la humanidad de otra Alma que resulta ser un bot, el caso puede escalarse y verificarse públicamente, lo que lleva a que esa Alma tenga una gran cantidad de atestaciones negativas. Esto ya sucede hasta cierto punto dentro del ecosistema de financiación cuadrática de GitCoin, donde se utiliza una variedad de señales para detectar "grupos colusorios".

4. La tecnología de conocimiento cero (p. ej., MACI) podría **impedir criptográficamente que algunas atestaciones realizadas por un Alma sean demostrables**. Esto haría que los intentos de vender ciertos tipos de certificaciones no fueran creíbles, porque el sobornador no tendría forma de saber si el receptor del soborno cumplió o no con su parte del trato. Ha habido una gran cantidad de investigaciones sobre el uso de tales técnicas para votar, pero en

última instancia, cualquier mecanismo social no financiable puede terminar beneficiándose de ideas similares.

5. Podríamos **alentar a los denunciantes** como una forma de hacer que la colusión de tamaño significativo sea inestable. En lugar de detectar y sancionar comportamientos incorrectos o abusivos, detectamos y sancionamos *patrones abusivos de colusión*. Esta técnica es arriesgada de usar en exceso debido a la posibilidad de sobornos falsos, pero, sin embargo, es parte del conjunto de herramientas.

6. Podríamos usar **mecanismos de la teoría de la predicción entre pares** para fomentar que los informes sean honestos en todos los casos, excepto cuando la colusión sea extremadamente alta. En lugar de que la conferencia dé fe de la asistencia de los asistentes, los asistentes podrían dar fe de la asistencia *de los demás*, por lo que la cantidad de participantes que tendrían que ser sobornados para dar fe de un reclamo falso se vuelve muy grande. Las recompensas no necesitan ser financieras, pero podrían ser SBTs, lo que hace que las recompensas sean más útiles para los miembros genuinos de la comunidad que para los atacantes.

7. Si un grupo de Almas comparte un interés común, podríamos usar puntajes de correlación que se **centren en las correlaciones donde existe un gran incentivo para ser honesto**. Por ejemplo, la técnica de puntuación de correlación utilizada en la financiación cuadrática acotada por pares utiliza donaciones de financiación cuadráticas para determinar qué tan correlacionados están dos participantes y, por lo tanto, cuánto descontar su intersección. Si dos participantes comparten muchos intereses comunes, sus incentivos para expresar este hecho al mecanismo de financiación cuadrática ciertamente disminuye con el descuento de correlación, pero nunca llega a ser *cero* o *negativo*.

§8 COMPARACIONES Y LIMITACIONES

Si bien la gama de marcos de identidad propuestos es casi ilimitada, hay cuatro paradigmas adyacentes particularmente prominentes y ampliamente discutidos en el espacio de la Web3 que merecen una comparación: el ecosistema de identidad "heredado" dominante, la economía de seudónimos, proof of personhood o la prueba de personalidad y las credenciales verificables. Cada paradigma destaca contribuciones y desafíos importantes para el desarrollo futuro del paradigma de identidad social que defendemos, y utilizamos tales limitaciones como trampolín para explorar direcciones futuras. Considerando eso, también explicamos por qué creemos que nuestras primitivas de identidades sociales de Almas y tokens vinculados al Alma son un camino más prometedor para los regímenes de privacidad.

8.1 Legado

Los sistemas de identidad heredados se basan en documentos o tarjetas de identidad emitidos y mediados por un tercero (un gobierno, universidad, empleador, etc.). La procedencia se establece llamando al tercero para una confirmación. Si bien el sistema heredado tiene un conjunto interesante de propiedades que debemos entender más profundamente, tales sistemas son tremendamente ineficientes y no se prestan a la componibilidad o computación para una coordinación rápida y eficiente. Además, estos sistemas carecen de contexto social y hacen que las Almas dependan de un tercero centralizado para confirmar la pertenencia a una comunidad, en lugar de la comunidad integradora. Por ejemplo, la mayoría de las identificaciones emitidas por el gobierno finalmente se remontan a un certificado de nacimiento emitido con la autoridad de un médico y miembros de la familia, que son la fuente última de la verdad y dejan de lado muchas conexiones sociales igualmente significativas que, en conjunto, ofrecen una validación mucho más sólida. De hecho, cuando los centros de poder concentrado buscan una fuerte identificación (por ejemplo, obtener una autorización de seguridad de un gobierno importante), rara vez confían en dichos documentos, sino que recurren a entrevistas en las redes sociales. **Por lo tanto, tales sistemas de identidad heredados tienden a concentrar el poder en el emisor y en aquellos que pueden emprender la debida diligencia para obtener una verificación más sólida, quienes a su vez se convierten en burocracias calcáreas y poco confiables.** Un objetivo de diseño crucial de DeSoc es garantizar que los requisitos de seguridad de las identificaciones gubernamentales puedan cumplirse y superarse, lo que permite que las redes horizontales ofrezcan una mayor seguridad a todos los usuarios y a través de una variedad de sustratos sociales.

8.2 Economía de seudónimos

La visión de una sociedad basada en la combinación de sistemas de reputación con mecanismos de prueba de conocimiento cero para preservar la privacidad ha sido promovida ampliamente por Balaji Srinivasan, quien acuñó y popularizó la frase “economía de seudónimos”. Su primera versión enfatiza el uso de seudónimos para evitar la discriminación y evadir la “cultura de cancelación” por parte de grupos sociales que buscan dañar la reputación de una persona y romper sus lazos sociales. Prevé que las personas acumulen certificaciones *transferibles* de conocimiento cero (ZK) en sus billeteras y evadan los ataques a la reputación transfiriendo un subconjunto de certificaciones a nuevas billeteras, o dividiendo las certificaciones entre varias billeteras, presumiblemente sin trazabilidad. Al reducir las certificaciones que porta, una persona elige el nivel de seudónimo deseado en la nueva cuenta, sopesando un intercambio entre más anonimato (portar menos certificaciones) o más distribución a su red social (portar más atestaciones).

La diferencia práctica entre las típicas propuestas de la económica de seudónimos y DeSoc es que le quitamos énfasis a la separación de identidad como una forma principal de proteger a los participantes de los abusos y cancelar la cultura. Cierto nivel de separación (por ejemplo, diferentes Almas entre la familia, el trabajo, la política, etc.) puede ser saludable, pero en general existen grandes

desventajas al confiar en la capacidad de generar nuevas identidades como ayuda principal contra los ataques. Hace que la reputación de los préstamos y la procedencia sea más difícil, y se integra mal con los mecanismos de gobernanza que intentan corregir las correlaciones o Sybils.

En lugar de proteger a las víctimas permitiéndoles resurgir de los ataques con una identidad nueva, aunque disminuida, DeSoc permitiría otros enfoques, como **contextualizar al atacante**. La "cancelación" a menudo surge precisamente porque las declaraciones y las acciones se *sacan de contexto* y las señales virales viajan a través de redes no contextualizadas, cuando una persona o un bot tiene poca conexión social o contexto con una víctima. De la misma manera que los SBTs brindan procedencia para protegerse contra las falsificaciones profundas ("deep fakes"), un mapa de SBTs representa socialmente, de forma gráfica, el origen de una "pieza de difamación". Estas son esencialmente artefactos que surgen fuera de las comunidades de la víctima (como lo reflejan las membresías compartidas de SBTs), o que carecen de certificaciones de SBTs de las comunidades de la víctima, lo que debería generar dudas sobre la veracidad de la pieza. Los SBTs también empoderan a las víctimas para que lancen una respuesta defensiva para contrarrestar el golpe, seleccionado y propagado desde *su* red de confianza (representada aquí por los patrones de tenencia conjunta de los SBTs). Al mantener referencia el contexto social, las personas pueden mantener la confianza, incluso si están bajo amenaza de cancelación, y responsabilizar a los atacantes. Mejorar la procedencia mejora la base social de la verdad.

8.3 Proof of Personhood (PoP) o Prueba de Personalidad

Los Protocolos de Prueba de Personalidad o Proof of Personhood (PoP) tienen como objetivo proporcionar tokens de singularidad individual, para evitar ataques Sybil y permitir aplicaciones no financiadas. Para hacerlo, se basan en enfoques como el análisis global de gráficos sociales, la biometría, reuniones globales simultáneas de actores claves o alguna combinación de los mismos. Sin embargo, debido a que los protocolos PoP buscan representar identidades *individuales*, enfocadas en lograr la *singularidad global*, en lugar de *identidades sociales* mapeando relaciones y solidaridades, **los protocolos PoP se limitan a aplicaciones que tratan a todos los humanos por igual**. La mayoría de las aplicaciones que nos interesan, como comprometer la reputación de uno, son relacionales y pasan de ser un ser humano único a ser un ser humano *diferenciado*.

Además, los protocolos PoP no son inmunes a los ataques Sybil. En casi todas las aplicaciones previsibles a corto plazo, los sistemas PoP están efectivamente abiertos a los ataques Sybil, sólo que a un costo ligeramente mayor. A menos que la mayoría de las personas en el planeta estén registradas en un servicio PoP y participen en un ejercicio de validación particular, un atacante siempre puede reclutar humanos desinteresados que aún no participan para actuar como Sybils. Si bien estos mercenarios no son exactamente bots, la diferencia es superficial y supone apenas un pequeño gasto adicional.

Muchos protocolos PoP tienen como objetivo construir un sustrato para la renta básica universal o la democracia global. Si bien no compartimos la misma ambición, dichos protocolos nos han incitado a considerar cómo construir gradualmente hacia la coordinación de bienes de red plurales. En contraste con la naturaleza binaria, individualista y global de PoP, nuestro enfoque tiene como objetivo construir un sustrato rico, contextual y en capas para la reputación, la propiedad y la gobernanza de abajo hacia arriba que permita la participación en una variedad de comunidades y redes, pequeñas y grandes.

8.4 Credenciales verificables

Las credenciales verificables (VCs, por su siglas en inglés) son un estándar del World Wide Web Consortium (W3C) donde las credenciales o atestaciones se pueden compartir bajo pruebas de conocimiento cero a discreción del titular. Las VCs resaltan las principales limitaciones de nuestro paradigma de privacidad básico y motivan nuestra discusión sobre las extensiones de privacidad anteriores. Hasta que los SBTs tengan extensiones de privacidad que limitan la publicidad, las VCs y los SBTs pueden verse como complementos naturales: en particular, los SBTs son inicialmente públicos, lo que los vuelve inapropiados para información confidencial como la identificación emitida por el gobierno, mientras que las implementaciones de VCs tienen dificultades de implementar un paradigma de recuperación que podría ser abordado por la recuperación de la comunidad. Los dos enfoques combinados pueden, a corto plazo, ser más fuertes que cualquiera de ellos por separado. Pero las VCs también tienen una limitación clave: al menos en su forma estandarizada, las VCs no son compatibles con la mayoría de las aplicaciones que hemos enumerado debido a su privacidad *unilateral.*

El compartir unilateralmente por medio de pruebas de conocimiento cero no es compatible a nivel de incentivos en nuestros casos de uso, ni refleja nuestras normas sobre privacidad. La mayoría de nuestras aplicaciones dependen de un cierto nivel de publicidad. Pero bajo las pruebas de conocimiento cero, las Almas no pueden saber que otras Almas poseen un SBT a menos que se les comparta, lo que hace que comprometer la reputación, los compromisos creíbles, la gobernanza resistente a Sybil y los contratos de alquiler simples (por ejemplo, el arrendamiento de un apartamento) sean imposibles de obtener ya que otros compromisos y gravámenes no son necesariamente visibles. Más profundamente, somos escépticos en tanto que la compartibilidad unilateral sea generalmente el paradigma de privacidad correcto. Rara vez una de las partes en una relación de múltiples partes tiene derechos unilaterales de revelar la relación sin el consentimiento de la otra parte. Así como la propiedad privada transferible unilateralmente no es un régimen de propiedad rico, la compartibilidad unilateral simplista no es un régimen de privacidad muy rico. Si dos partes son copropietarias de un activo y eligen representar su relación a través de una VC, dicha credencial no permite el consentimiento mutuo y los permisos mutuos. Este problema aplica a casos

más complejos de propiedad plural y formas organizacionales y permisos complejos, que son una característica de DeSoc.

§9 NACIMIENTO DEL ALMA

El camino desde el ecosistema de la Web3 actual hasta la sociabilidad aumentada mediada por los SBTs enfrenta un clásico desafío de "arranque en frío". Por un lado, los SBTs no son transferibles. Por otro lado, la combinación actual de billeteras puede no ser el "hogar final" de los SBTs porque carecen de mecanismos de recuperación comunitarios. Pero para que las billeteras de recuperación comunitaria funcionen, necesitan una gran variedad de SBTs en comunidades discretas para estar seguras. **¿Qué viene primero: los SBTs o la recuperación comunitaria?** ¿Quiénes son las comunidades de adopción temprana? ¿Cómo interoperan los SBTs en diferentes cadenas? No podemos aspirar a conocer todas las posibilidades y respuestas, sino a esbozar algunos caminos prometedores para que el lector explore más dentro de la arquitectura de la Web3 e incluso la Web2 actual.

9.1 Proto SBTs

Aunque el sello distintivo de los SBTs es la no transferibilidad, los SBT también pueden tener otra propiedad que puede resultar más útil en el arranque: la *revocabilidad.* Es posible que los SBTs primero se gesten como tokens revocables y transferibles, antes de convertirse en intransferibles. Un token es revocable si un emisor puede quemar el token y volver a emitirlo en una nueva billetera. Quemar y volver a emitir tendría sentido cuando, por ejemplo, las claves se pierden o se comprometen, y el emisor tiene interés en garantizar que los tokens no se financien y se vendan a una parte; en otras palabras, cuando el token indica una membresía auténtica de la comunidad. Los empleadores, las iglesias, los grupos de reunión, los clubes con interacciones repetidas off-chain están bien posicionados para quemar y volver a emitir tokens porque tienen una relación con una persona y pueden verificar fácilmente la suplantación por llamada telefónica, videoconferencia o simple encuentro en persona. Las interacciones individuales, como la asistencia a un concierto o una conferencia, no son adecuadas porque los lazos comunitarios son más débiles.

Los tokens revocables y transferibles son una especie de proto SBTs, que cumplen funciones placentarias de apoyo antes del nacimiento del Alma. Estos tokens ganan tiempo tanto para que las billeteras gesten mecanismos seguros de recuperación comunitaria como para que una persona acumule suficientes proto SBTs que eventualmente pueden quemarse y volver a emitirse en SBTs no transferibles. Bajo este enfoque, la pregunta no es "¿qué sucede primero: los SBTs o la recuperación comunitaria?" Más bien, los SBTs y la recuperación comunitaria se instancian simultáneamente, dando a luz un Alma.

9.2 Billeteras de recuperación comunitaria

Aunque las billeteras de hoy carecen de recuperación comunitaria, cada una tiene fortalezas y debilidades relativas en cuanto a ser hogares, o quizás úteros gestacionales, para los SBTs. Los protocolos de proof or personhood (PoP) o prueba de personalidad tienen la ventaja de que ya experimentan con mecanismos de resolución de disputas sociales, que son la base de la recuperación comunitaria. Además, muchas DAOs usan PoP para facilitar la gobernanza, lo que las convierte en las primeras emisoras naturales de SBTs. Sin embargo, a pesar del liderazgo natural de los PoP, estos protocolos aún no se han ganado una amplia confianza para albergar tokens valiosos, mientras que las billeteras de custodia sí lo han hecho.

Las billeteras de custodia, a pesar de ser centralizadas, pueden ofrecer una vía de acceso natural para usuarios minoristas menos sofisticados. Dichas billeteras de custodia también podrían crear herramientas para que las comunidades minoristas emitan tokens revocables que luego se conviertan (o quemen y vuelvan a emitir) en SBTs o incluso herramientas para emisores más "corporativos", muchos de los cuales están buscando formas de construir bases de clientes leales en la Web3 pero carecen de experiencia en términos de custodia. Una vez que los mecanismos de recuperación de la comunidad se hayan formalizado y hayan sido probados, estas billeteras de custodia podrían descentralizarse en la recuperación comunitaria, mientras que los custodios pasarían a proporcionar otros servicios valiosos en DeSoc (como la gestión de la comunidad, emisiones de SBTs, etc.)

Para los usuarios de la Web3 más sofisticados, las billeteras descentralizadas sin custodia (o billeteras de recuperación social sin custodia como Argent y Loopring) son un punto de partida natural para impulsar los mecanismos de recuperación comunitaria. Las billeteras sin custodia tienen la ventaja de ser nativas de la Web3 y de código abierto y la flexibilidad de anunciar previamente y experimentar con mecanismos de manera incremental a un subconjunto de usuarios voluntarios y sofisticados para probar incentivos y combinar mecanismos (por ejemplo, multi-sig). Todos estos enfoques (PoP, con custodia y sin custodia) desempeñan un papel importante en la experimentación y la incorporación de usuarios con diferentes grados de sofisticación y tolerancia al riesgo.

9.3 Proto Almas

Las normas también pueden guiar a las Almas a la existencia. A medida que repensamos los tokens y las billeteras, también podemos replantear nuestra forma de pensar sobre ciertas clases de NFTs y tokens que están destinados a indicar una cierta membresía. En particular, podemos introducir una norma de no transferir NFTs y POAPs emitidos por instituciones acreditadas que reflejen asistencia a una conferencia, experiencia laboral o credenciales educativas. Tales transferencias de tokens de membresía, si se intercambian por valor, podrían disminuir la reputación de una billetera y tal vez desalentar a los emisores a seguir emitiendo tokens de membresía o POAPs para esa billetera. En el ecosistema sin custodia, un número significativo de usuarios ya ha logrado

una reputación financiera significativa y participación en sus billeteras, lo que podría funcionar como una garantía efectiva para que no abusen de las expectativas de intransferibilidad.

Si bien todos estos caminos contienen sus respectivos desafíos, esperamos que la variedad de enfoques aumente la posibilidad de convergencia a nuestro estado de cuasi-equilibrio en el mediano plazo a través de un pequeño conjunto de pasos.

§10 CONCLUSIÓN

A pesar de lo ambiciosos que hemos sido al imaginar lo que DeSoc podría permitir, en muchos sentidos, los puntos anteriores son sólo los primeros pasos. Hay más de un camino hacia DeSoc, incluyendo una serie de marcos que no están basados en blockchain, como Spritely, ACDC y Backchannel, que se basan en almacenes de datos vinculados a máquinas locales en lugar de registros globales. Estos marcos eventualmente pueden ofrecer una confianza aún mayor a través de la distancia social, porque pueden aprovechar la transitividad de las relaciones de confianza, como presentaciones confiables, en lugar de depender de SBTs emitidos por instituciones conocidas y de alto nivel (como universidades o DAOs). Además, las aplicaciones que describimos anteriormente son sólo el comienzo de lo que DeSoc puede potenciar, sin tocar los mundos virtuales: su física, sociedad y su compleja intersección con el mundo físico. Todo esto sugiere que incluso las amplias ambiciones que expresamos anteriormente son sólo el comienzo de lo que DeSoc puede llegar a ser.

En ese camino, sin embargo, quedan muchos desafíos y preguntas abiertas. Las ideas expuestas anteriormente deben ser evaluadas holísticamente y desde la perspectiva de un adversario. Muchas de ellas son más sugerentes que totalmente prescriptivas. ¿Cómo pueden las DAOs mantener su estado de publicidad mientras comparan cuidadosamente los patrones de las Almas y las correlaciones entre SBTs para ejecutar las protecciones de Sybil y la descentralización? ¿Qué tan compatible con los incentivos es adquirir SBTs frente a varios esquemas de descuento por correlación? ¿Cuál es el nivel de conflicto entre la privacidad, el descuento por correlación y otros diseños de mecanismos de DeSoc? ¿Cómo podemos medir la desigualdad de una manera social y, sin embargo, apropiadamente privada (contextualmente integral)? ¿Cómo deberían funcionar las herencias en el marco de la recuperación comunitaria? ¿Hay límites que se puedan dibujar o incluso integrar en protocolos para evitar escenarios distópicos? ¿O deberíamos simplemente competir para construir mejores escenarios primero? Estas preguntas son sólo el comienzo de lo que se espera que sea una agenda de investigación que abarque años y que evolucione junto con el ecosistema DeSoc.

Sin embargo, el potencial que ofrece DeSoc no sólo parece valer el precio de navegar estos difíciles desafíos, sino que quizás sea necesario para garantizar nuestra supervivencia. Albert Einstein dijo en la conferencia de desarme de 1932 que las fallas del “poder organizador del hombre” para seguir el ritmo de “sus avances técnicos” habían puesto una “navaja en las manos de un niño de 3 años”. En un mundo donde su observación parece más profética que nunca, aprender a programar

futuros que codifican la *sociabilidad*, en lugar de escribir sobre la confianza, parece un curso requerido para que la vida humana en este planeta persista.

APÉNDICE

Ajuste de mecanismos cuadráticos para la cooperación preexistente

Debido a que los mecanismos cuadráticos incentivan la colaboración desde una base de egoísmo, son vulnerables a los grupos que *ya son* cooperativos. Si los SBTs reflejan la membresía comunitaria que individualiza a un Alma para reflejar sus parcialidades, los SBTs pueden ayudarnos a descartar la cooperación preexistente e inclinar la balanza a favor de la cooperación *a través de las diferencias*. Aquí proporcionamos una ilustración de un primer intento de un modelo cuadrático refinado y otras direcciones futuras para la investigación. Este mecanismo no está optimizado y sin duda tiene vulnerabilidades: se entiende como un ejemplo ilustrativo para estimular la experimentación y la investigación futura. Si bien ilustramos con la financiación cuadrática o Quadratic Funding (QF), los mismos principios y fórmulas también se aplican a la votación cuadrática o Quadratic Voting (QV), donde las contribuciones individuales simplemente se sustituyen por créditos de voz.

En QF, una comunidad iguala las contribuciones individuales a proyectos compartidos con fondos en proporción al cuadrado de la suma de las raíces cuadradas de las contribuciones individuales. Para niveles de contribución fijos, los fondos de emparejamiento crecen como el cuadrado del número de contribuyentes individuales, pero tienen rendimientos decrecientes para las contribuciones individuales. Hay rendimientos decrecientes en la acción individual concentrada, pero rendimientos crecientes en la acción colectiva. Por ejemplo, si Abdu, Shou y Belle fueran personas que no cooperaran, contribuyendo con A, S y B unidades monetarias respectivamente, los fondos de emparejamiento a sus donaciones en un programa de QF (por ejemplo, Gitcoin Grants) deberían ser proporcionales (con una escala determinada por fondos disponibles) al cuadrado de la suma de las raíces cuadradas de las donaciones individuales.

$$\textit{Compensación Simple} \sim (\sqrt{A} + \sqrt{S} + \sqrt{B})^2 - (A + S + B)$$

Membresía única

Ahora supongamos un modelo simplificado en el que Abdu, Shou y Belle se diferencian por una sola membresía (lugar de trabajo) y los fondos de emparejamiento están disponibles para emprendimientos, empresas y proyectos de código abierto (nuevamente, en el espíritu de Gitcoin). Debido a que las personas del mismo lugar de trabajo tienen un fuerte incentivo para contribuir a su propio lugar de trabajo para maximizar los fondos de emparejamiento para su empresa, deberíamos esperar que se coordinen. Un enfoque extremo sería suponer que los trabajadores comparten plenamente los objetivos y coordinan plenamente su comportamiento. Sin embargo, incluso en este caso simple, hay varias formas en que podríamos compensar en la fórmula.

Un enfoque simple, que llamamos "agrupación", pondría a dos compañeros de trabajo "bajo la misma raíz cuadrada" en la fórmula cuadrática para compensar su tendencia a coordinarse. Si Abdu y Shou fueran compañeros de trabajo (pero no Belle), la contribución de Abdu y Shou se sumaría y se calcularía la raíz cuadrada, mientras que la contribución de Belle se calcularía sola, lo que daría más peso a su contribución.

$$\textit{Emparejamiento Agrupado} \sim (\sqrt{A} + \sqrt{S} + \sqrt{B})^2 - A - S - B$$

Si Abdu y Shou estuvieran perfectamente coordinados, siempre sería óptimo para ellos dividir su contribución conjunta igualmente, por lo que podemos suponer $A = S$, permitiéndonos simplificar:

$$(\sqrt{2A} + \sqrt{B})^2 - (2A + B)$$

En este caso, es fácil ver cómo el agrupamiento conduce a la optimización (o maximización del bienestar) bajo el mismo argumento que para QF de manera más general. Si Abdu y Shou están perfectamente coordinados, actúan efectivamente como un solo agente y la fórmula de emparejamiento de agrupamiento es la fórmula QF para dos agentes: el agente conjunto Abdu-Shou y el agente Belle. Otro ajuste que también logra la optimización es lo que llamamos "Emparejamiento Compensatorio":

$$\textit{Emparejamiento Compensatorio} \sim \left(\frac{\sqrt{A} + \sqrt{S}}{\sqrt{2}} + \sqrt{B}\right)^2 - A - S - B$$

La lógica en el Emparejamiento Compensatorio es que debido a que Abdu y Shou son parte de un grupo de tamaño 2 perfectamente coordinado, podemos reducir el peso de sus votos por un factor de 2 para compensar la coordinación. Esto conduce al mismo resultado que el Emparejamiento Agrupado, ya que siempre es óptimo que Abdu y Shou ($A = S$) perfectamente coordinados hagan contribuciones iguales y, en este caso:

$$\textit{Emparejamiento Compensatorio} \sim \left(\frac{\sqrt{A} + \sqrt{S}}{\sqrt{2}} + \sqrt{B}\right)^2 - A - A - B$$

$$= (\sqrt{2A} + \sqrt{B})^2 - (2A + B)$$

Membresías Múltiples

El ejemplo anterior asume que Abdu, Shou y Belle tienen una sola membresía: el lugar de trabajo. Sin embargo, en casi todos los casos, esto sería una gran simplificación. Las personas tienen múltiples membresías comunitarias, relaciones cooperativas e incluso intersecciones informales. Abdu y Belle podrían ser familia extendida, Shou y Belle podrían haber asistido a la misma escuela, o Shou y Abdu podrían ser poseedores de tokens del mismo protocolo de capa 1, y así sucesivamente. Para facilitar la cooperación a través de las diferencias, estas correlaciones en las membresías entre

individuos deben reconocerse de una manera menos binaria. Ahora consideraremos extender cada uno de los enfoques anteriores para hacer esto. Nuevamente nos enfocaremos en el ejemplo más simple que sea suficiente para ilustrar este punto. A continuación, planteamos fórmulas más generales.

Nos centramos en un ejemplo en el que Abdu y Shou comparten una afiliación, Abdu y Belle comparten una afiliación diferente y Shou tiene una afiliación con un grupo que incluye a otros miembros, pero ninguno participa en esta ronda de contribuciones. Este es el conjunto completo de afiliaciones.

Para extender el Emparejamiento Agrupado a este caso, incluimos un grupo o "cluster" para cada grupo de alianzas compartidas y distribuimos las contribuciones de cada individuo entre todos los grupos en los que participa por igual con coeficientes de sus contribuciones que suman uno.

$$\textit{Emparejamiento Agrupado} \sim \left(\sqrt{\frac{S}{2} + \frac{A}{2}} + \sqrt{\frac{A}{2} + B} + \sqrt{\frac{S}{2}}\right)^2 - A - B - C$$

Para extender el Emparejamiento Compensatorio, tenemos que resolver los coeficientes de la contribución de cada individuo para compensar la coordinación que beneficia a ese individuo. En particular, si asumimos que la mitad de Belle internaliza la mitad del valor de Abdu, que la mitad de Abdu internaliza la mitad del valor de Belle y un cuarto del valor de Shou, y que un cuarto de Shou internaliza un cuarto el de Abdu, entonces necesitamos resolver los coeficientes:

$$\alpha_A + \frac{\alpha_B}{2} + \frac{\alpha_S}{4} = 1$$

$$\alpha_B + \frac{\alpha_A}{2} = 1$$

$$\alpha_S + \frac{\alpha_A}{4} = 1$$

La solución a esta ecuación es $\alpha_A = \frac{4}{11}$, $\alpha_B = \frac{9}{11}$, $\alpha_S = \frac{10}{11}$. Entonces:

$$\textit{Emparejamiento Compensatorio} \sim \left(\sqrt{\frac{4A}{11}} + \sqrt{\frac{9B}{11}} + \sqrt{\frac{10S}{11}}\right)^2 - A - B - C$$

El Emparejamiento Compensatorio, si bien en algunos aspectos es las más simple, es casi el menos transparente, asignando a cada individuo un peso en función de su centralidad social que compensa el poder que esto otorga.

Fórmulas generales

Para cada individuo $i = 1, \ldots N$, definamos el número de afiliaciones que tiene como T ; en general, podemos dar diferentes pesos a diferentes afiliaciones, pero en este momento asumimos que todas son iguales. Σ será el conjunto de todos los "grupos de afiliación", proyectos del conjunto de poseedores de una afiliación dada sobre el conjunto de participantes en la contribución equivalente, con un elemento típico σ. Tenga en cuenta que $T_i = \sum_{j=1}^{|\Sigma|} 1_{i\epsilon\sigma}$, dónde 1 es el indicador de la función. Denote la contribución de i individual como c_i. La fórmula general para el Emparejamiento Agrupado es:

$$\textit{Emparejamiento Agrupado} \sim \left(\sum_{j=1}^{|\Sigma|} \sqrt{\sum_{i=1}^{|\sigma_j|} \frac{c_i}{T_i}} \right)^2 - \sum_{i=1}^{N} C_i$$

Defina la Puntuación de Correlación entre cualquier par ordenado de individuos i y k como:

$$S_{i,k} = \frac{\sum_{j=1}^{|\Sigma|} 1_{i\epsilon\sigma j} 1_{k\epsilon\sigma j}}{T_i}$$

Luego, el Emparejamiento Compensatorio se deriva de los coeficientes de compensación, α_i que resuelven el sistema de ecuaciones, una para cada individuo i:

$$\alpha_i + \sum_{k \neq i}^{N} \alpha_k s_{k,i} = 1$$

Esto producirá genéricamente una solución única para el vector α, que es aproximadamente una medida inversa de la centralidad de la red de individuos en la red de solidaridad. Después:

$$\textit{Emparejamiento Compensatorio} \sim \left(\sum_{i=1}^{N} \sqrt{\alpha_i c_i} \right)^2 - \sum_{i=1}^{N} C_i$$

Una característica atractiva de esta solución es que generalmente conducirá a la optimización suponiendo que la solidaridad mide correctamente la internalización efectiva de la utilidad. Una característica menos atractiva es que parece poco probable que sea particularmente "robusta": en particular y en contraste con otros casos, no siempre será óptimo para cualquier individuo dar todas sus contribuciones a través la contribución equivalente en lugar de externamente, dadas las penalizaciones.

Emparejamiento por Pares

Un tercer mecanismo, al que llamamos "Emparejamiento por Pares", sugerido por Buterin (2019) adopta un enfoque diferente. El Emparejamiento por Pares tiene la desventaja de que no logra la optimización sino que se enfoca en limitar las pérdidas de ataques específicos, pero tiene la importante ventaja de que no requiere una fuente extrínseca para especificar quién está coordinando y quién no. En cambio, esta información se extrae de los propios valores de la contribución.

El Emparejamiento por Pares sólo se puede definir de manera significativa en el contexto de múltiples proyectos y un límite de emparejamiento por par, M. Por cada pareja de agentes (A, B), si aportan $x_{A\to P}$ y $x_{B\to P}$ al mismo proyecto P, obtienen una subvención[12].

$$Emparejamiento_{AB\to P} = \frac{2M\sqrt{x_{A\to P}x_{B\to P}}}{M + PuntuaciónDeCorrelación_{AB}}$$

Donde M es un parámetro del sistema y:

$$PuntuaciónDeCorrelación_{AB} = \sum_{todos\ los\ proyectos\ P} \sqrt{x_{A\to P}x_{B\to P}}$$

La $PuntuaciónDeCorrelación$ pretende reflejar en qué medida dos participantes contribuyen a los mismos proyectos. Si dos participantes A y B contribuyen con x a algún proyecto, entonces la $PuntuaciónDeCorrelación_{AB}$ aumenta en x. Si aportan cantidades diferentes, la $PuntuaciónDeCorrelación_{AB}$ aumenta por la media geométrica de sus dos aportaciones.

Si A y B tienen una $PuntuaciónDeCorrelación$ baja, suponemos que son agentes muy independientes y les damos casi el subsidio máximo cada vez que contribuyen a algún proyecto juntos. Pero si A y B contribuyen al mismo proyecto con frecuencia y/o en grandes cantidades, asumimos que están muy coordinados entre sí y actúan más como un solo agente, y descontamos los subsidios a los proyectos que cofinancian.

En el caso límite donde $x_{A\to P} \to 0$ para todos los agentes y proyectos, los puntajes de correlación son insignificantes, $A \to P \to 0$, por lo que la fórmula anterior es equivalente a la financiación cuadrática simple: $Emparejamiento_{AB\to P}$ se simplifica a $2\sqrt{x_{A\to P}x_{B\to P}}$. En el caso de tres agentes, donde tres agentes aportan A, S y B, esto se simplifica a:

[12] La descripción original difiere ligeramente en tanto que usa M en lugar de 2M. Técnicamente, 2M es correcto si sumamos sobre *pares desordenados* de agentes, y M es correcto si sumamos sobre *pares ordenados*. Aquí, estamos sumando sobre pares no ordenados.

$$EmparejamientoTotal_P = Emparejamiento_{AS\to P} + Emparejamiento_{BS\to P} + Emparejamiento_{AB\to P}$$

$$= 2\sqrt{AS} \ + \ 2\sqrt{BS} \ + \ 2\sqrt{AB}$$

$$= \left(\sqrt{A} \ + \ \sqrt{S} \ + \ \sqrt{B}\right)^2 - (A \ + \ S \ + \ B)$$

Pero si un par de agentes contribuye muchas veces o en grandes cantidades a los mismos proyectos, el puntaje de correlación de ese par aumenta, hasta que eventualmente cualquier número de contribuciones compartidas adicionales a un nuevo proyecto en su mayoría quitan subsidios de otras contribuciones compartidas que el mismo par de agentes ya ha efectuado. A medida que el total de emparejamientos se acerca al infinito, el subsidio total por par de agentes se acerca a $lim_{T\to\infty}\frac{2MT}{M+T}$ = *2M.*

Un objetivo de diseño clave de esta fórmula era limitar las pérdidas por identificar incorrectamente a un grupo en colusióncomo agentes independientes. En el Emparejamiento Simple, las pérdidas son ilimitadas: *N* agentes falsos o coludidos controlados por el mismo actor del mundo real puede contribuir *V* cada uno a un proyecto falso y extraer un subsidio de $V * (N^2 \ - \ N)$. En el Emparejamiento Agrupado, una extracción ilimitada similar es posible si el mecanismo de agrupamiento identifica erróneamente incluso a un grupo en colusión como agentes completamente independientes. En el Emparejamiento por Pares, por el contrario, las pérdidas de *N* agentes falsos o en colusión siempre están delimitadas superiormente por $M * (N, 2 - N)$, donde *M* es un parámetro del sistema.

Tenga en cuenta que el Emparejamiento por Pares no logra la optimización: los actores coludidos aún tienen el incentivo de reportar por demás cuánto valoran ciertos proyectos, e incluso pueden extraer algunos fondos contribuyendo a un proyecto falso controlado por ellos mismos. Más bien, este enfoque pretende ser el segundo mejor, optimizado para el caso en el que se dispone de información externa limitada sobre qué actores realmente coluden.

Habiendo dicho esto, el Emparejamiento por Pares se puede usar como una *plantilla filosófica* sobre cómo dar cuenta de la coordinación preexistente sin penalizarla en exceso: en lugar de que la puntuación de correlación sólo incluya valores de $\sqrt{x_{A\to P}x_{B\to P}}$ para ese sistema de financiación cuadrática en particular, podría intentar incluir términos similares para todos los casos en los que esos dos actores hayan obtenido algún beneficio al cooperar. Si los beneficios de la cooperación se valoran correctamente, mayor cooperación nunca sería perjudicial para ningún par de agentes; más bien, las ganancias netas de una mayor cooperación simplemente se acercarían a cero.