UNIVERSIDAD TECNOLÓGICA METROPOLITANA
UTEM del Estado de Chile

Semestral. Volumen 19, n.º 2, Diciembre 2025

REVISTA CHILENA DE ECONOMÍA Y SOCIEDAD

19

ARTÍCULO

https://doi.org/10.58560/rches.v19.n02.01

LA RESPONSABILIDAD CIVIL EN EL ECOSISTEMA DE FINANZAS DESCENTRALIZADAS (DeFi): UN ANÁLISIS CRÍTICO DESDE EL DERECHO CHILENO A LA LUZ DE LA LEY FINTECH

CIVIL LIABILITY IN THE DECENTRALIZED FINANCE ECOSYSTEM (DEFI): A CRITICAL ANALYSIS FROM CHILEAN LAW IN LIGHT OF THE FINTECH LAW

Tomás A. Valenzuela R.*

Luis A. Valenzuela Silva**

* Abogado. Máster en Derecho Digital, Universidad de la Rioja, España. Investigador independiente. Correo electrónico: tvalenzuelar@gmail.com ORCID: https://orcid.org/0009-0003-0124-0479

** Profesor titular, Departamento de Economía, Recursos Naturales y Comercio Internacional, Facultad de Administración y Economía, Universidad Tecnológica Metropolitana, Santiago de Chile. Correo electrónico:luis.valenzuela@utem.clutem.cl. ORCID: https://orcid.org/0009-0004-8136-8962

RESUMEN

Una de las aplicaciones de la tecnología disruptiva blockchain son las finanzas descentralizadas (DeFi), que constituyen uno de los desafíos más transformadores en el ámbito financiero. Su complejidad inherente a un sistema digital, junto con la ausencia de marcos regulatorios precisos, genera un escenario de ambigüedad jurídica, especialmente en lo que respecta a la atribución de responsabilidad civil cuando se producen daños. El presente artículo es un análisis crítico de la aplicabilidad del régimen de responsabilidad civil al contexto del ecosistema DeFi, a la luz de los diferentes instrumentos disponibles por el legislador en forma de Código Civil, Ley No. 19.496, Ley de Protección de los Derechos de los Consumidores (LPDC) y el caso relativamente reciente de la legislación Fintech. Se destacan los principales vacíos regulatorios, deficiencias y tensiones interpretativas en estos aspectos como un medio para cubrir las principales lagunas, así como se describen una serie de criterios y reespecificaciones normativas según las cuales se puede abordar la responsabilidad de los diferentes actores. El objetivo final es proporcionar ideas relevantes para generar un análisis más exhaustivo, que pueda servir de base para la próxima reforma de la legislación o argumentos doctrinales o tratamiento judicial en esta área. En este contexto, se propone la implementación de estándares de diligencia elevados para los desarrolladores y auditores de protocolos, así como la diferenciación de criterios de responsabilidad para los diversos actores involucrados. Los desafíos probatorios y procesales exigen soluciones innovadoras y, en particular, el recurso a mecanismos alternativos de resolución de conflictos. Es crucial alcanzar un equilibrio entre la protección efectiva de los usuarios y el fomento de la innovación, mediante la construcción de un marco jurídico robusto, predecible y tecnológicamente neutro para DeFi en Chile que, si bien considere la experiencia comparada, se adapte de manera idónea a la realidad nacional.

PALABRAS CLAVE: cadena de bloques, contratos inteligentes, responsabilidad civil, seudoanonimato, proposiciones

ABSTRACT

One of the applications of disruptive blockchain technology is Decentralized Finance (DeFi), which constitutes one of the most transformative challenges in the financial sphere. Its inherent complexity as a digital system, together with the absence of precise regulatory frameworks, creates a scenario of legal ambiguity, especially with regard to the attribution of civil liability when damages occur. This article is a critical analysis of the applicability of the civil liability regime to the context of the DeFi ecosystem, in light of the different instruments available to the legislator in the form of the Civil Code, Law No. 19.496, the Consumer Rights Protection Law (LPDC), and the relatively recent case of Fintech legislation. The main regulatory gaps, deficiencies, and interpretative tensions in these areas are highlighted as a means of addressing the main shortcomings, and a series of criteria and regulatory re-specifications are described according to which the responsibility of the different actors can be addressed. The ultimate goal is to provide relevant ideas for a more comprehensive analysis that can serve as a basis for the next legislative reform or doctrinal arguments or judicial treatment in this area. In this context, the implementation of high standards of diligence for protocol developers and auditors is proposed, as well as the differentiation of liability criteria for the various actors involved. The evidentiary and procedural challenges call for innovative solutions, in particular the use of alternative dispute resolution mechanisms. The evidentiary and procedural challenges call for innovative solutions, particularly the use of alternative dispute resolution mechanisms. It is crucial to strike a balance between effective user protection and the promotion of innovation by building a robust, predictable, and technologically neutral legal framework for DeFi in Chile that, while considering comparative experience, is ideally suited to the national reality.

Keywords: blockchain, smart contracts, civil liability, pseudo-anonymity, propositions

Códigos JEL: E22, E44, G10, G21

Fecha de recepción: 7 de octubre 2025
Fecha de aceptación: 15 de octubre 2025
Fecha de publicación 31 de diciembre 2025.

INTRODUCCIÓN

El surgimiento de las finanzas descentralizadas (DeFi) representa en el ámbito financiero uno de los desarrollos más transformadores. (Kuznetsov et al., 2023). Estos protocolos, que se basan fundamentalmente en la tecnología *blockchain*, facilitan replicar y reconfigurar los servicios financieros convencionales, incluidos los préstamos, las bolsas de activos y los seguros, prescindiendo de intermediarios centralizados y funcionando mediante la ejecución autónoma de contratos inteligentes (Ali & Dembo, 2024).

La garantía de mayor transparencia, eficiencia y accesibilidad ha impulsado una expansión considerable, que actualmente supera los 170 mil millones de dólares en valor total bloqueado (TVL)[1], pero también este rápido avance ha hecho que los usuarios sean, al mismo tiempo, susceptibles a peligros considerables derivados de las vulnerabilidades tecnológicas, las manipulaciones del mercado y las deficiencias regulatorias (Dos Santos et al., 2022).

La complejidad inherente a estos sistemas, junto con la ausencia de marcos regulatorios precisos, genera un escenario de ambigüedad jurídica, especialmente en lo que respecta a la atribución de responsabilidad civil cuando se producen daños (Joggerst et al., 2018).

En Chile, con la promulgación de la Ley N° 21.521 (Ley Fintech) en febrero de 2023[2], se ha dado un primer paso hacia la regulación de servicios financieros basados en tecnología. Esta Ley promueve la competencia e inclusión financiera, estableciendo un marco para la supervisión de plataformas de financiamiento colectivo, sistemas alternativos de transacción, y otros servicios Fintech (Figueroa, 2023).

Como discutiremos más adelante, sin embargo, su metodología parece estar mejor adaptada para organizaciones centralizadas que para protocolos genuinamente descentralizados que definen DeFi, lo que plantea algunas preguntas a nivel regulatorio sobre la responsabilidad civil que permanecen abiertas. Esta Ley no trata la naturaleza distribuida que presenta la gobernanza de las Organizaciones Autónomas Descentralizadas (DAOs), así como tampoco los diferentes atributos de los contratos inteligentes (*smart contracts*) en lo relativo a las obligaciones o responsabilidades de participantes como los oráculos o auditores de seguridad. La naturaleza descentralizada, seudónima y transnacional de DeFi presenta desafíos para la aplicación de regímenes tradicionales de responsabilidad civil (Dhanya et al., 2025).

Naturalmente, esto plantea las preguntas de: ¿Cómo identificar la responsabilidad cuando un protocolo falla debido a fallos en el *software* de programación? ¿Quién puede asumir la responsabilidad cuando una DAO, gobernada por titulares de *tokens* anónimos, hace algo que es perjudicial para las personas que esta DAO representa? ¿Qué constructos legales tradicionales como culpa, causalidad o imputabilidad emplear con los sofisticados sistemas algorítmicos que operan más allá de las fronteras de la soberanía nacional? La falta de intermediarios identificados y la ejecución por dicho código autoejecutable también dificultan la aplicación directa de categorías dogmáticas tradicionales.

Este artículo es un análisis crítico de la aplicabilidad del régimen de responsabilidad civil al contexto del ecosistema DeFi: los diferentes instrumentos disponibles del legislador en forma de Código Civil, Ley No. 19.496 o Ley de Protección de los Derechos de los Consumidores (LPDC) y el caso relativamente reciente de la legislación Fintech. Se destacan los principales vacíos regulatorios, deficiencias y tensiones interpretativas en estos aspectos como un medio para cubrir las

1. Según CoinDesk en artículo de 18 septiembre 2025, el valor total bloqueado en DeFi supera US$170.000 millones, regresando a niveles previos a Terra con un crecimiento más mesurado y una creciente adopción institucional. Disponible en: https://www.coindesk.com/es/business/2025/09/18/defi-tvl-rebounds-to-usd170b-erasing-terra-era-bear-market-losses

2. Ley N°21.521 que promueve la competencia e inclusión financiera a través de la innovación y tecnología en la prestación de servicios financieros, Ley Fintech, disponible en: https://www.bcn.cl/leychile/navegar?idnorma=1187323

principales lagunas, se describen una serie de criterios y reespecificaciones normativas según las cuales se puede abordar la responsabilidad de los diferentes actores para los respectivos actores.

Se sostiene que, hasta la fecha, si bien el sistema legal existente ofrece las herramientas para gestionar algunos aspectos de la responsabilidad de DeFi, persisten desafíos clave, y que las interpretaciones volutivas necesarias de los principios legales tradicionales deben complementarse con interpretaciones especiales basadas en desarrollos normativos específicos que aún son necesarias para la protección del usuario y un diseño amigable con la innovación sin sofocar la innovación. El objetivo es proporcionar ideas relevantes para generar un análisis más exhaustivo, que pueda servir de base para una eventual reforma legislativa, argumentos doctrinales o tratamiento judicial en esta área.

1. MARCO CONCEPTUAL Y TECNOLÓGICO DE LAS DeFi

1.1. Definición y características esenciales.

Las DeFi constituyen un ecosistema de aplicaciones financieras construidas sobre cadenas de bloques, es decir, redes *blockchain* -principalmente *Ethereum*- que brinda acceso abierto a los servicios financieros sin intermediarios, replicando y reinventando servicios financieros tradicionales mediante contratos inteligentes, y permitiendo el acceso a los mercados de capital para varios proyectos (Moro-Visconti & Cesaretti, 2023).

Sus características más importantes incluyen: (1) Descentralización: operan sin autoridades centrales, basándose en protocolos distribuidos y gobernanza comunitaria, aunque el grado de descentralización real varía significativamente entre protocolos; (2) Contratos inteligentes: estos contratos programables ejecutan las transacciones automáticamente, lo que reduce la dependencia de los intermediarios y mejora la eficiencia (Carapella et al., 2022); (3) No custodia: permiten a los usuarios mantener control directo sobre sus claves privadas y, por tanto, sobre sus activos, reduciendo el riesgo de contraparte asociado a intermediarios; (4) Transparencia: el código fuente de los contratos inteligentes y el historial de transacciones suelen ser públicos y verificables en la *blockchain*, permitiendo auditoría pública; y (5) Composabilidad: los protocolos DeFi pueden interactuar entre sí como "bloques de lego financieros", creando nuevas funcionalidades complejas y potencialmente amplificando riesgos sistémicos (Schär, 2020). Ejemplos comunes incluyen plataformas de intercambio descentralizado (DEX) como Uniswap[3], protocolos de préstamo como Aave[4] o Compound[5], derivados sintéticos como Synthetix[6], y seguros descentralizados como Nexus Mutual[7].

3. Uniwap constituye un protocolo DEX en la cadena de bloques *Ethereum*. Permite intercambios de tokens a través de fondos de liquidez y contratos inteligentes, eliminando intermediarios centralizados. El protocolo de código abierto emplea un modelo de creadores de mercado automatizados (AMM), lo que permite a los usuarios proporcionar liquidez y ganar comisiones. Disponible en: https://app.uniswap.org/

4. Aave constituye un protocolo que permite prestar y pedir prestada criptomoneda de forma descentralizada sin intermediarios; y además contempla el *token* Aave, la criptomoneda nativa de este protocolo, utilizada para gobernanza, *staking* y descuentos en tarifas. Disponible en: https://aave.com/

5. Compound es una plataforma descentralizada en *Ethereum* que facilita los préstamos a través de contratos inteligentes. Los prestamistas ganan intereses al depositar criptoactivos, mientras que los prestatarios proporcionan garantías para la liquidez. Las tasas de interés son ajustadas automáticamente por el protocolo. Disponible en: https://compound.finance/

6. Synthetix, sistema financiero descentralizado que permite la creación y comercialización de activos sintéticos sin propiedad directa. Synthetix sirve como garantía para emitir activos como sUSD y sBTC. En este caso, los titulares tienen participación en el gobierno de protocolos, recibiendo recompensas por ello. Disponible en: https://www.synthetix.io/

7. Nexus Mutual es una comunidad descentralizada que ofrece una alternativa a los seguros tradicionales a través de la cadena de bloques *Ethereum* para compartir riesgos y protección de pérdidas financieras en DeFi y riesgos digitales. Funciona como una organización mutua, facultando a los miembros para gobernar y participar en un sistema colectivo de gestión de riesgos desprovisto de intermediarios centralizados. Disponible en: https://nexusmutual.io/

1.2. Principales actores del ecosistema.

En el núcleo del ecosistema DeFi se encuentran una variedad de actores diferentes con distintos tipos de participación, y las interacciones de estos actores definen la complejidad y el perfil de amenaza del conjunto: a) los desarrolladores, que son los arquitectos del sistema, son responsables de escribir el código de los contratos inteligentes que son la base de los protocolos. La filiación de estos equipos puede ser abierta, pero también anónima o seudónima, lo cual hace complejo asignar responsabilidades (Sant'Ana Costa, 2024); b) los auditores de seguridad son las empresas o especialistas en ciberseguridad que examinan el contrato codificado en busca de posibles amenazas de seguridad antes de su lanzamiento y mientras está en operación. Sus informes son importantes para mantener la confianza en el mercado; el alcance real de su trabajo y su grado de responsabilidad continúan siendo un tema de debate (Xiao et al., 2024); c) los proveedores de interfaces, o DApps; son responsables de diseñar las aplicaciones web y móviles (DApps) que facilitan la interacción del usuario en la gestión de la complejidad de los contratos inteligentes de manera sencilla. En la práctica, sirven como intermediarios, lo que puede significar que tienen ciertas responsabilidades hacia el público responsable en cuanto a información y seguridad (Lallai et al., 2020); d) Oráculos: servicios, centralizados y descentralizados—Chainlink es uno de los más conocidos[8]-, que conectan los contratos inteligentes con el mundo exterior. Su función es suministrar datos cruciales, como la cotización de activos o el resultado de eventos, que son indispensables para la correcta ejecución de los protocolos. La fiabilidad y seguridad de estos oráculos son, por tanto, de vital importancia (Manda & Katneni, 2024); e) Organizaciones Autónomas Descentralizadas (DAOs): entidades cuya gobernanza recae en los poseedores de *tokens*, quienes votan para tomar decisiones clave sobre el futuro del protocolo, como la implementación de actualizaciones, el ajuste de parámetros o la gestión de los fondos de la tesorería. El estatus jurídico de estas organizaciones y la responsabilidad legal de sus miembros son aún áreas de gran incertidumbre (Thomason & Ivwurie, 2023); f) Proveedores de liquidez: usuarios que aportan capital a los protocolos depositando sus activos. Esta liquidez es fundamental para facilitar operaciones como intercambios y préstamos, y a cambio reciben comisiones o recompensas, asumiendo a su vez riesgos específicos (Aigner & Dhaliwal, 2021); y g) Usuarios finales: individuos e instituciones que utilizan los protocolos DeFi para acceder a una variedad de servicios financieros. Este grupo es muy heterogéneo, con niveles muy dispares de conocimiento técnico y de aversión al riesgo (Gogol et al., 2024).

1.3. Riesgos y vulnerabilidades específicas.

Las finanzas descentralizadas (DeFi) constituyen un nuevo arquetipo de innovación financiera, que están vulnerables a una serie de riesgos que han significado pérdidas cuantiosas para sus usuarios (Komal, 2024). Desafíos y amenazas que no pueden ser mirados a la ligera y que se manifiestan en múltiples niveles del ecosistema.

En el núcleo técnico, las vulnerabilidades en los contratos inteligentes constituyen una de las amenazas más críticas. Errores de programación (*bugs*), como los ataques de reentrada (*reentrancy*), desbordamientos de enteros o una lógica de permisos defectuosa, pueden ser explotados por actores maliciosos para comprometer los fondos de un protocolo (Dhillon & Mehrotra, 2024).

Otro vector de ataque relevante es la manipulación de oráculos. Dado que los contratos inteligentes dependen de fuentes de datos externas para operar, la alteración de esta información —por ejemplo, manipulando precios a través de préstamos *flash*— puede inducir liquidaciones indebidas y extraer valor de manera fraudulenta.

8. Chainlink es una red Oracle descentralizada que facilita la integración segura de *blockchain* y datos del mundo real para contratos inteligentes. Su *token* nativo, LINK, incentivará a los operadores de nodos para la validación de la información y la mejora de la seguridad de la red. Disponible en: https://chain.link/

Desde un punto de vista estructural, surgen riesgos de gobernanza y sistémicos. Las decisiones adoptadas por DAOs, aunque democráticas en teoría, pueden ser perjudiciales para la estabilidad del protocolo si actores con intereses maliciosos logran acumular suficiente poder de voto. Además, la alta interconexión entre protocolos —una característica clave de DeFi conocida como "componibilidad"— puede amplificar los fallos, generando efectos en cascada donde la crisis de un solo protocolo se propaga a otros dependientes.

Finalmente, el ecosistema está expuesto a riesgos de mercado y regulatorios. La notoria volatilidad de los criptoactivos, junto con fenómenos como la pérdida transitoria en los pools de liquidez y los fallos en los mecanismos de estabilización de *stablecoins* algorítmicas, cuyo ejemplo más notorio fue el colapso de Terra/Luna, exponen a los usuarios a pérdidas abruptas. A esto se suma la incertidumbre del marco legal, la posibilidad de acciones regulatorias y la ausencia de los mecanismos de protección al inversor que caracterizan las finanzas tradicionales (Weaver, 2018).

2. MARCO JURÍDICO CHILENO APLICABLE A DeFi.

2.1. Análisis de la Ley N° 21.521 (Ley Fintech) y su alcance en materia de DeFi.

La Ley N° 21.521, promulgada el 3 de febrero de 2023, representa el primer esfuerzo legislativo en Chile por establecer un marco general para los servicios financieros basados en tecnología (Quezada, 2024). Su objetivo conforme a su artículo 1° es "*establecer un marco general para incentivar la prestación de servicios financieros a través de medios tecnológicos*", conocida como Ley Fintech, descansa en principios fundamentales como la inclusión financiera, la promoción de la competencia, la protección al cliente, el resguardo de datos y la estabilidad financiera, buscando fomentar la innovación sin desatender la seguridad del sistema (Luco & Santander, 2023). En ese sentido, la naturaleza intrínsecamente descentralizada de DeFi plantea desafíos interpretativos y de aplicación que la Ley, en su concepción actual, no logra abordar de manera exhaustiva.

Esta Ley, en su afán por abarcar la novedad, opta por una definición amplia de "activos financieros virtuales o criptoactivos", describiéndolos en su artículo 3, numeral 3°, como "*representación digital de unidades de valor, bienes o servicios, con excepción de dinero [...] que pueden ser transferidos, almacenados o intercambiados digitalmente*". Esta amplitud, aunque inicialmente parece una ventaja, soslaya una distinción fundamental entre las múltiples tipologías de criptoactivos que proliferan en el ecosistema DeFi, tales como los *tokens* de pago, de utilidad, de seguridad o de gobernanza (Sotelo, 2024). La ausencia de una categorización más fina no es un detalle menor. Por el contrario, siembra ambigüedades en la aplicación de la normativa a la vasta y a menudo desconcertante gama de *tokens* que dan vida a los protocolos descentralizados (Castillo, 2025). A modo de ejemplo, en un *token* de gobernanza que confiere derechos de voto en una DAO, su naturaleza podría no amoldarse con facilidad a las categorías tradicionales de valores o instrumentos financieros, complicando sobremanera su encuadre regulatorio (Dotan et al., 2023).

El artículo 2 de la Ley N° 21.521 despliega un catálogo de servicios financieros tecnológicos bajo su órbita regulatoria mediante la fiscalización de la Comisión para el Mercado Financiero (CMF)[9], abarcando desde plataformas de financiamiento colectivo hasta sistemas alternativos de transacción, pasando por la asesoría crediticia y de inversión, y la custodia de instrumentos financieros (Hormazábal, 2023). Es innegable que, a primera vista, algunos de estos servicios hallen resonancia funcional en el universo DeFi; los *exchanges* descentralizados (DEX), por ejemplo, operan como sistemas alternativos de transacción, y los protocolos de préstamo descentralizados bien podrían conside-

9. La Comisión paras el Mercado Financiero, disponible en: https://www.cmfchile.cl

rarse análogos a plataformas de financiamiento (Zhou & Qin, 2024). Una lectura atenta de la Ley sugiere que su marco conceptual se diseñó pensando en la regulación de entidades centralizadas que se valen de la tecnología para ofrecer servicios financieros, y no tanto en la idiosincrasia de los protocolos intrínsecamente descentralizados, cimentados en contratos inteligentes y gobernados por DAOs (Sotelo, 2024).

Un aspecto crucial es la sujeción de los prestadores a la fiscalización de la CMF, requiriendo inscripción en un Registro de Prestadores de Servicios Financieros, conforme lo dispone el artículo 4 de la Ley Fintech y, para ciertos servicios y actividades, autorización previa según lo dispuesto en el artículo 7 del mismo cuerpo legal. La traslación de estos requisitos al ámbito de los protocolos DeFi, que a menudo carecen de una entidad central identificable o que son gobernados por DAOs con participantes anónimos o pseudónimos, se revela como una tarea de complejidad mayúscula. La interrogante cardinal de ¿quién debe inscribirse? o ¿quién ha de solicitar la autorización? permanece sin una respuesta clara, lo que pone de manifiesto una laguna regulatoria de considerable calado frente a la naturaleza distribuida de las finanzas descentralizadas.

La Ley Fintech, en su intento de asegurar la protección del cliente en el modelo financiero tradicional, impone a los prestadores una serie de obligaciones sustantivas: deberes de información (artículo 8), idoneidad (artículo 9), garantías (artículo 10), mantenimiento de un patrimonio mínimo (artículo 11) y la adopción de estructuras de gobierno corporativo (artículo 12) (González-Gutiérrez, 2025). De este modo, la transposición de estas exigencias al intrincado contexto de DeFi no es un ejercicio trivial, sino que se topa con desafíos estructurales.

En cuanto a los conceptos de gobernanza corporativa en las DAOs, la idea misma de aplicar requisitos de gobernanza corporativa en una DAO, en la que las determinaciones corresponden a una comunidad de poseedores de *tokens*, es conceptualmente difícil. Las DAOs, por definición y estructura, carecen de los cuerpos administrativos y de gestión que caracterizan a las estructuras empresariales convencionales**.** Su gobernanza se estructura mediante mecanismos algorítmicos y votaciones en cadena, lo que requiere de una aguda reinterpretación de los requisitos legales o incluso de una reforma legislativa que reconozca la singularidad de estas arquitecturas (Ding et al., 2023).

2.2. La Responsabilidad civil en la Ley Fintech: Una remisión genérica.

En materia de responsabilidad civil, la Ley Fintech es escueta. El artículo 10 en su inciso primero se limita en señalar que los prestadores responderán *"por los eventuales perjuicios que pudieren ocasionar a sus clientes por sus acciones u omisiones en la prestación de los servicios. Las entidades antes indicadas responderán de culpa leve en la prestación de los servicios antes mencionados"*. Asimismo, el inciso segundo del mismo artículo dispone *"La garantía deberá constituirse mediante boleta bancaria o póliza de seguros por el monto que determine la Comisión, según los parámetros establecidos mediante norma de carácter general en consideración al impacto o perjuicio potencial que pueda ocasionar la entidad a su cliente en atención al o los servicios prestados, la calidad del gobierno corporativo y gestión de riesgos de la entidad"*. Esta remisión genérica, lejos de ofrecer un marco claro, implica que la determinación de la responsabilidad civil en el complejo universo DeFi debe, forzosamente, anclarse en las normas generales del Código Civil y en otras leyes especiales, como la Ley de Protección de los Derechos de los Consumidores (LPDC). La ausencia de un régimen de responsabilidad diseñado específicamente para las particularidades de los protocolos descentralizados no hace sino generar un vacío legal, una zona de penumbra que sume en la incertidumbre jurídica a operadores y usuarios, quienes se ven obligados a transitar un terreno donde los principios tradicionales del derecho chocan frontalmente con la vertiginosa innovación tecnológica (Reyes & Gárate, 2021).

En síntesis, la Ley Fintech representa un paso adelante en la regulación de los servicios financieros tecnológicos en Chile, al reconocer la existencia de los criptoactivos y establecer un marco para ciertos prestadores. Pese a ello, su enfoque, centrado en intermediarios centralizados, deja lagunas y desafíos sin resolver en lo que respecta a la naturaleza descentralizada de DeFi, especialmente en la identificación de los sujetos obligados y la aplicación de los regímenes de responsabilidad. Esta situación subraya la necesidad de una evolución regulatoria que contemple las especificidades de la descentralización para garantizar una protección efectiva y una seguridad jurídica adecuada en este sector emergente.

2.3. Régimen general de responsabilidad civil en el Código Civil chileno

Dada la ausencia de un régimen específico de la Ley Fintech en lo que a responsabilidad civil se refiere, la búsqueda de un marco jurídico que permita dirimir los conflictos que surgen en el ecosistema de las DeFi nos reconduce, ineludiblemente, a las normas generales del Código Civil (CC). Este cuerpo normativo, pilar del derecho privado concebido en una era predigital, ofrece una regulación amplia para la responsabilidad contractual y extracontractual. Además, su aplicación a las singularidades de DeFi no es una tarea mecánica, sino que, al contrario, produce tensiones y desafíos interpretativos de una magnitud considerable (Weidenslaufer & Wilkins, 2020).

2.3.1. La responsabilidad contractual y la noción de contrato en DeFi.

La responsabilidad contractual, como es sabido, encuentra su génesis en el incumplimiento de una obligación que emana de un contrato legalmente celebrado (Barros, 2008). El artículo 1545 del CC, con su célebre adagio de que "*todo contrato legalmente celebrado es una Ley para los contratantes*", constituye un principio fundamental que consagra la siguiente locución latina "*pacta sunt servanda*"[10]. De este modo, al adentrarnos en el universo DeFi nos topamos con una dificultad primordial, cual es la determinación misma de la existencia de un "contrato válido" en el sentido que el derecho civil tradicional le ha consagrado. Con mayor detalle deben considerarse las siguientes observaciones:

a) La formación del consentimiento en la era de los contratos inteligentes**:** la doctrina civilista, con su arraigada tradición, demanda conforme al artículo 1445 CC para su validez la concurrencia de los siguientes elementos de todo contrato: consentimiento, capacidad, objeto y causa (Vial, 2003). En el universo de los contratos inteligentes la expresión de la voluntad se materializa mediante interacciones directas con el código en la cadena de bloques (Joshi et al., 2023). Aquí surge la pregunta medular: ¿es esta interacción equiparable a la formación de un consentimiento genuinamente libre e informado? Aun cuando el derecho contemple la validez de los contratos electrónicos, la peculiaridad de los *smart contracts* se manifiesta en que la "contraparte" constituye esencialmente un código autoejecutable, no una persona jurídica o natural en el sentido clásico (Nazarov, 2024). Esta particularidad abre un abanico de interrogantes sobre la verdadera voluntad de las partes y si la mera interacción con un algoritmo puede satisfacer los exigentes requisitos de consentimiento que el Código Civil establece, máxime cuando el usuario promedio podría carecer de una comprensión cabal de la lógica intrincada que subyace al código ("Consent to Automated Reputational Profiling Requires Transparency of the Underlying Algorithm" 2022); b) La elusiva identificación de las partes: la esencia seudónima o, en ocasiones, completamente anónima de un sinnúmero de participantes en el ecosistema DeFi se posiciona como una barrera para la identificación de las partes contratantes. Este es un requisito sine qua non para

10. Por esto se entiende que "los pactos deben cumplirse", puesto que los acuerdos y contratos obligan a las partes a cumplirlos, por ser son legalmente vinculantes. Es esencial tanto en el derecho civil, para la validez de los contratos, como en el derecho internacional, para asegurar que los tratados se respeten de buena fe.

la correcta configuración de la relación jurídica y, por consiguiente, para la atribución de responsabilidad contractual. En ausencia de un deudor o un acreedor claramente individualizado, la aplicación de las normas de responsabilidad se convierte, en la práctica, en una quimera (Napieralska & Kepczynski, 2024); y c) Términos de servicio y la sombra de los contratos de adhesión[11]: aunque los términos de servicio que acompañan a las interfaces web, las cuales fungen como puertas de entrada a los protocolos DeFi, podrían en una primera aproximación ser asimilados a contratos de adhesión, su validez y, sobre todo, su alcance jurídico, se prestan a una discusión profunda (Abdullah & Yihan, 2022). Esta controversia se agudiza si tales documentos incluyen estipulaciones que eximen de manera desproporcionada la responsabilidad o que, por su contenido, podrían ser tildadas de abusivas. Los contratos inteligentes son en esencia meros protocolos que ejecutan términos preestablecidos, a pesar de que no siempre logran satisfacer la totalidad de los requisitos jurídicos que el derecho civil chileno exige para la correcta formación del consentimiento contractual (Ferreira, 2023).

En caso de admitirse un vínculo contractual, el incumplimiento de las "promesas" de rendimiento o seguridad -expresadas en *whitepapers* o interfaces- podría generar responsabilidad. Si bien en materia de responsabilidad contractual la culpa se gradúa, el estándar de diligencia aplicable sería la regla general, que constituye la culpa leve, regulada en el artículo 44 CC[12].

11. Un contrato de adhesión constituye un acuerdo legal en el que una de las partes (el proveedor) delinea los términos y disposiciones con anticipación, mientras que a la otra parte (el consumidor o suscriptor) se le otorga la única opción de aceptar o rechazar el contrato en su totalidad, sin la capacidad de participar en la negociación o alteración de los términos estipulados. Estos contratos son utilizados para facilitar la contratación de servicios estandarizados.

12. La culpa leve, conforme al artículo 44 del Código Civil, es la falta de la diligencia y cuidado que una persona ordinaria emplea en sus propios asuntos. Esta de culpa se vincula con el patrón de comportamiento de un "buen padre de familia" y se aplica en casos donde no hay otra especificación de culpa, significando una responsabilidad por el descuido que una persona común cometería en sus negocios.

2.3.2. La responsabilidad extracontractual y los desafíos de la descentralización.

La responsabilidad extracontractual, fundamentada en el artículo 2329 CC bajo el principio "*todo daño que pueda imputarse a malicia o negligencia de otra persona debe ser reparado por ésta*", se aplica en ausencia de un vínculo contractual y requiere la concurrencia de un hecho ilícito mediante una conducta dolosa o culposa conforme lo dispone el artículo 44 CC, que cause daño y una relación de causalidad entre ambos en los términos del artículo 2314 CC (Corral, 2013). Esto podría ser relevante para situaciones donde no hay una relación contractual clara, es decir, entre proveedores de oráculos, miembros de DAO, o incluso los desarrolladores iniciales de un protocolo. Sus requisitos pueden verificarse de la siguiente manera:

a) El acto ilícito y la figura del agente de daño: en el caso de DeFi, un acto ilícito puede realizarse de diferentes maneras en el espacio DeFi, ya sea hackeando el protocolo, explotando una vulnerabilidad de un contrato inteligente, o incluso manipulando el mercado (Carpentier-Desjardins et al., 2025). Vale la pena destacar que el anonimato o el seudonimato de los actores en la *blockchain* dificulta sobremanera la atribución de un hecho ilícito a una persona o entidad específica. Cuando un contrato inteligente ejecuta una acción que deviene en daño debido a un error en su lógica, la pregunta sobre la responsabilidad se torna compleja: ¿recae en los desarrolladores originales, aun cuando el protocolo sea inmutable y ya no ejerzan control sobre él? ¿En los validadores de la red? ¿En los poseedores de *tokens* de gobernanza que, mediante su voto, aprobaron una actualización defectuosa? La ausencia de una persona natural o jurídica claramente identificable como agente complica, en grado sumo, la aplicación de este principio fundamental del derecho (Linoy et al., 2021); b) Culpa o dolo en entornos descentralizados: la responsabilidad extracontractual requiere la prueba de la culpa o dolo (Schiele & Tocornal, 2010). En DeFi, la culpa podría configurarse por negligencia en el desarrollo (desplegar código con vulnerabilidades

conocidas o fácilmente detectables), en la auditoría (realizar una revisión superficial que omite errores críticos) o en la gobernanza (aprobar propuestas riesgosas sin la debida diligencia) (Ma et al., 2023). En materia extracontractual, la culpa es una sola, no se gradúa; y c) Daño y causalidad: la existencia de un daño y una relación de causalidad directa entre el hecho ilícito y el daño son elementos indispensables (Cárdenas, 2006). La volatilidad característica de las criptomonedas hace difícil la medición del daño patrimonial. Asimismo, establecer un nexo causal directo entre una falla del protocolo y el perjuicio sufrido por un usuario puede ser extremadamente complejo, especialmente en un ecosistema interconectado donde un fallo en un protocolo puede tener efectos en cascada sobre otros (Liu et al., 2023).

Con todo, los artículos 2320 y siguientes del CC, establecen presunciones de responsabilidad, en que se presume culpabilidad en ciertos daños que no ocurrirían sin negligencia; a modo de ejemplo, responsabilidad de los progenitores respecto a los hechos de sus hijos, responsabilidad de los dueños de animales causados por los mismos animales, explosión, ruina de edificio, entre otros. De este modo, esta responsabilidad podría aplicarse por analogía a fallos catastróficos en protocolos DeFi que, según estándares técnicos, no deberían ocurrir sin negligencia grave.

2.4. Aplicabilidad de la Ley N° 19.496 sobre protección de los derechos de los consumidores.

La Ley N° 19.496, promulgada en 1997 y cuya última modificación data de 2021 (Ley N° 21.320), conocida como Ley de Protección de los Derechos de los Consumidores (LPDC)[13], está diseñada para salvaguardar los intereses de los usuarios frente a las relaciones de consumo (Baraona, 2014). Su aplicación al ecosistema DeFi es complejo y se convierte en un campo abierto para el debate jurídico, toda vez que la naturaleza misma de DeFi desafía los mecanismos de protección tradicionales que la LPDC contempla.

La LPDC es aplicable si se configura una relación de consumo, en virtud del artículo 1, donde personas naturales o jurídicas en su calidad de consumidores o usuarios adquieren o disfrutan servicios DeFi de "proveedores" -desarrolladores, DAOs, interfaces- que habitualmente desarrollan estas actividades. Aunque muchos protocolos no cobran tarifas directas, podría argumentarse onerosidad por comisiones de transacción o incentivos *tokenizados* que tienen valor económico (Sompolinsky & Zohar, 2017).

2.4.1. La Relación de consumo: Los roles de proveedor y consumidor en DeFi

La piedra angular de la LPDC es la existencia de una "relación de consumo", que se configura entre un "proveedor" y un "consumidor".

El consumidor en el laberinto DeFi: la LPDC, en su artículo 1 N° 1, define al consumidor como "*la persona natural o jurídica que, en virtud de cualquier acto jurídico oneroso, adquiere, utiliza o disfruta, como destinatario final, bienes o servicios*". A priori, un cliente que interactúa con un protocolo DeFi, sea el motivo pedir un crédito, intercambiar criptomonedas o aportar liquidez, podría en teoría caer en esta definición, siempre y cuando su móvil sea el uso final y no la agregación en una cadena productiva o comercial. A mayor abundamiento, la frontera entre el "inversor" (quien asume riesgos de mercado y por ende no goza de la protección de la LPDC) y el "consumidor" (quien busca un servicio para su uso personal y está amparado por la ley) se torna difusa en el contexto DeFi. Un número considerable de usuarios se adentra en este ecosistema con un claro ánimo especulativo o de inversión, persiguiendo rendimientos financieros, lo que lo distingue del arquetipo de consumidor tradicional. A ello se suma la sofisticación técnica que a menudo se requiere para operar con ciertos protocolos, así como la participa-

13. La Ley 19.496, establece normas sobre Protección de los Derechos de los Consumidores, disponible en: https://www.bcn.cl/leychile/navegar?idNorma=61438

ción en la gobernanza de DAOs o en la provisión de liquidez, elementos que podrían argumentarse que los distancian del perfil de consumidor pasivo que la LPDC busca tutelar (De la Maza, 2021).

El proveedor en el ecosistema DeFi: la noción de "proveedor" se torna aún más compleja. La LPDC en su numeral 2° del artículo 1, lo concibe como "*las personas naturales o jurídicas, de carácter público o privado, que habitualmente desarrollen actividades de producción, fabricación, importación, construcción, distribución o comercialización de bienes o de prestación de servicios a consumidores, por las que se cobre un precio o tarifa*". Sin embargo, en el universo DeFi, la identificación de un proveedor en el sentido tradicional es en la mayoría de los casos una verdadera quimera, por las siguientes razones: a) Protocolos autónomos y la inmutabilidad de los contratos inteligentes: una porción considerable de los servicios DeFi se articula a través de protocolos autónomos, que operan mediante contratos inteligentes inmutables desplegados en una *blockchain*. Estos protocolos, por su propia naturaleza, no son personas naturales ni jurídicas, que una vez puestos en marcha, pueden funcionar sin que se requiera la intervención directa del hombre. Atribuir la calidad de proveedor a un mero código representa un desafío conceptual y práctico de envergadura, por su naturaleza impersonal; b) Organizaciones autónomas descentralizadas (DAOs) y la ausencia de personalidad jurídica: las DAOs, que con frecuencia ejercen la gobernanza de los protocolos DeFi, son estructuras de toma de decisiones distribuidas que carecen de la personalidad jurídica tradicional. Calificarlas como proveedor resulta complejo, pues no se ajustan a la definición legal. La imputación de responsabilidad de proveedor a una DAO, que es una colectividad de individuos, muchas veces seudónimos y dispersos geográficamente, genera un obstáculo (Hassan & De Filippi, 2021); y c) Desarrolladores y contribuyentes: los desarrolladores que inicialmente crearon un protocolo pueden haber cedido completamente su control. Los contribuyentes posteriores pueden operar en el anonimato. La idea de que un desarrollador sea responsable de forma indefinida por un protocolo sobre el cual ya no ejerce control choca frontalmente con los principios de la descentralización. Solo aquellos intermediarios centralizados que facilitan el acceso a los protocolos DeFi mediante interfaces de usuario o servicios de oráculo podrían, con mayor plausibilidad, ser considerados proveedores bajo la LPDC, dado que actúan como entidades identificables que prestan un servicio a cambio de una remuneración (Nadler et al., 2023).

Así, la dificultad para identificar al proveedor crea un vacío de responsabilidad. Si no hay un sujeto claramente identificable a quien exigir el cumplimiento de las obligaciones de la LPDC, la protección del consumidor se vuelve ilusoria.

2.4.2. Disposiciones clave de la LPDC y sus barreras de aplicación en DeFi.

La LPDC, en su espíritu protector, consagra una serie de derechos y deberes que, en principio, buscan salvaguardar al consumidor. Pero, su aplicación en el ecosistema DeFi se torna engorrosa por las siguientes razones:

a) El derecho a la información en la descentralización (artículo 3 letra b y 10 LPDC): consagra el derecho inalienable de los consumidores a recibir información veraz, oportuna, clara y comprensible sobre los bienes y servicios que se les ofrecen, incluyendo sus riesgos y condiciones (Perret et al., 1999). En el universo DeFi, la información técnica relativa al funcionamiento de los protocolos -el código subyacente, los riesgos inherentes a los contratos inteligentes, la volatilidad de los activos- es abundante. Ahora bien, esta riqueza informativa se ve empañada por su frecuente inaccesibilidad o, peor aún, por su incomprensibilidad para el usuario promedio. Surge entonces una pregunta crucial: ¿quién asume la responsabilidad de decodificar y traducir esta información técnica a un lenguaje que el consumidor pueda asimilar en un entorno tan descentralizado? (Arancibia & Rojas, 2024); b) El derecho a la seguridad en el consumo (artículo 3 letra d y 23 LPDC): este derecho fundamental implica

que los servicios ofrecidos no deben entrañar riesgos irrazonables para la seguridad de los consumidores. En el ecosistema DeFi, los riesgos de seguridad no son una excepción, sino una característica inherente. Las vulnerabilidades en los contratos inteligentes, ataques informáticos (hackeos) y manipulaciones de mercado son peligros latentes. La pregunta que emerge con fuerza es: ¿quién asume la responsabilidad por esta seguridad cuando no existe un proveedor centralizado? La "seguridad" en DeFi se cimienta en la robustez del código y en la calidad de las auditorías. De igual manera, la experiencia ha demostrado que incluso los protocolos más rigurosamente auditados pueden ser objeto de fallos o ataques, dejando a los usuarios en una posición de vulnerabilidad (Ruggieri,2021); c) La prohibición de cláusulas abusivas (artículo 16 LPDC): la LPDC, en su afán por proteger al consumidor, proscribe aquellas cláusulas que "*causen un desequilibrio importante en los derechos y obligaciones que para las partes se deriven del contrato*". Conviene recordar que los contratos inteligentes, al ser esencialmente código, no contienen "cláusulas" en el sentido tradicional del derecho. A pesar de ello, la lógica programada en su interior podría en la práctica generar resultados que, si se tratara de un contrato convencional, serían indudablemente considerados abusivos. La dificultad cardinal reside entonces en cómo discernir, identificar y, más aún, anular una "cláusula abusiva" incrustada en un código inmutable y autoejecutable, una tarea que desafía la intervención judicial en la autonomía de la voluntad (García, 2020); d) La responsabilidad por productos o servicios defectuosos (artículo 20 LPDC): esta disposición confiere al consumidor el derecho a elegir entre la reparación, el reemplazo o la devolución del dinero ante la presencia de defectos en un producto o servicio. En el ámbito DeFi un "servicio defectuoso" podría materializarse en un contrato inteligente que, debido a un error o *bug*, ocasiona pérdidas a los usuarios. Igualmente, la inmutabilidad inherente a la tecnología *blockchain*, sumada a la ausencia de una entidad central que pueda ser compelida a ejecutar estas acciones reparadoras, genera barreras significativas e, incluso, insuperables para la efectiva reparación o devolución, dejando al consumidor en una posición de desamparo (Wilkins, 2019); y e) Los procedimientos colectivos (artículos 50 y siguientes LPDC): se prevé la existencia de procedimientos colectivos, concebidos para la tutela de intereses difusos o colectivos de los consumidores. En teoría, un incidente como un hackeo masivo que afecte a múltiples usuarios de un protocolo DeFi podría, en principio, justificar la interposición de una acción colectiva. De este modo, la ausencia de un proveedor claramente identificable contra quien dirigir tal acción constituye un obstáculo insalvable, dejando esta valiosa herramienta de protección colectiva en gran medida inoperante en el ámbito descentralizado (Bozzo, 2019).

2.4.3. El precedente de sentencia N° 189/2023 en causa rol C N° 349-18: TDLC rechaza demandas de Surbtc SpA, Cryptomkt SpA y Orionx SpA en contra de bancos por abuso de posición dominante colectivo.

Por sentencia de 21 de diciembre de 2023, el Tribunal para la Defensa de la Libre Competencia (TDLC) desestimó demandas de Surbtc SpA, Cryptomkt SpA y Orionx SpA en contra de los bancos Itaú-Corpbanca, Banco del Estado de Chile, Scotiabank Chile, Banco de Chile, Santander-Chile, Banco Bice, Banco Bilbao Vizcaya Argentaria Chile S.A., Banco Internacional y Banco Security por presuntamente infringir los incisos primero y segundo letra b) del artículo 3° del D.L. N° 211, de ejercer un abuso de posición dominante colectivo con el objeto de impedir, restringir o limitar la participación de intermediarios de criptomonedas, a través del cierre de cuentas bancarias o por medio de la negativa a su apertura. Los demandantes también alegaron conductas auto protectoras y diversas formas de conducta anticompetitiva en contra de los bancos. El Tribunal reconoció la posible presión competitiva de los demandantes sobre los servicios bancarios, pero encontró pruebas insuficientes para clasificarlos como competidores. Ahora bien, la Corte examinó elementos estructurales y conductuales pertinentes al presunto abuso de dominio colectivo.

En el elemento estructural, la Corte reconoció la interdependencia estratégica en el mercado, pero concluyó que no se cumplían los criterios de dominio colectivo. En cuanto al elemento conductual, la Corte determinó que las cuentas bancarias no son insumos esenciales debido a la falta de limitaciones y ausencia de pruebas de comportamiento colectivo abusivo. En última instancia, el Tribunal evaluó y ponderó la evidencia ofrecida respecto de la conducta de cada banco acusado, descartando que se hubieran configurado las conductas imputadas, en cuanto se acreditó la existencia de hechos que justifican las decisiones adoptadas por los demandados, o bien la inexistencia de una intención seria de contratar por parte de las demandantes.[14]

3. RESPONSABILIDAD CIVIL DE LOS ACTORES EN EL ECOSISTEMA DeFi.

3.1. Desarrolladores de protocolos y contratos inteligentes.

Los desarrolladores de protocolos y contratos inteligentes ocupan una posición clave en el ecosistema DeFi, dada su capacidad para configurar la arquitectura fundamental y las reglas operacionales de las plataformas. La evaluación de su responsabilidad civil debe efectuarse bajo un estándar de diligencia cualificado, que excede la mera diligencia de un buen padre de familia o comportamiento cuidadoso y se aproxima a la *lex artis* propia de profesionales especializados. Este estándar se justifica por la naturaleza intrínsecamente financiera de los sistemas que diseñan, la inmutabilidad inherente a gran parte del código una vez desplegado, la asimetría informativa que existe entre desarrolladores y usuarios, y la previsibilidad de ataques o vulnerabilidades en un entorno de alto valor económico.

La *lex artis* en el desarrollo de software seguro para el ámbito DeFi implica la observancia de un conjunto de mejores prácticas y estándares de la industria. Entre estas se incluyen la realización de auditorías de seguridad por terceros independientes y con probada competencia técnica, la implementación de pruebas exhaustivas que abarquen desde unidades individuales hasta la integración completa del sistema, incluyendo técnicas como el *fuzzing*[15] y, cuando sea aplicable, el análisis formal, la incorporación de mecanismos de seguridad intrínsecos al diseño del protocolo, tales como pausas de emergencia, bloqueos temporales, límites de transacción y sistemas de actualización robustos y seguros. Adicionalmente, recae sobre los desarrolladores un deber de diligencia en la selección y verificación de componentes de terceros que sean integrados en el protocolo, asegurando su fiabilidad y seguridad. La responsabilidad que emane de estas acciones u omisiones podría ser de naturaleza contractual, en aquellos casos donde exista un vínculo jurídico directo con los afectados, o extracontractual, conforme a las reglas generales del Código Civil, particularmente el artículo 2314 y siguientes, que establecen la obligación de indemnizar el daño causado por dolo o culpa a otro (Parisi & Budorin, 2024).

3.2 Auditores de seguridad.

Los auditores de seguridad desempeñan un rol crítico en la validación de la robustez y fiabilidad de los protocolos DeFi. Su responsabilidad primaria es de índole contractual frente al cliente que los contrata -generalmente el equipo desarrollador del protocolo-, obligándose a cumplir diligentemente con el encargo de auditoría. Además, su esfera de responsabilidad puede extenderse al ámbito extracontractual frente a terceros, específicamente usuarios que, de manera razonable, confían en los informes de auditoría publicados para tomar decisiones de inversión o participación en el protocolo.

14. Sentencia N° 189/2023 en causa rol C N° 349-18 ante el Tribunal de Defensa de la Libre Competencia, disponible en: https://www.tdlc.cl/wp-content/uploads/2023/12/Sentencia_N_189-23.pdf

15. *Fuzzing* son métodos utilizados en seguridad informática para identificar vulnerabilidades y errores de software mediante la entrada de datos aleatorios.

La determinación de la culpa en la actuación de un auditor se evaluaría considerando diversos factores: el alcance explícito de la auditoría, es decir, qué aspectos del código o del diseño del protocolo se comprometió a revisar; la metodología empleada, verificando si se adhirió a estándares reconocidos en la industria de la seguridad *blockchain* (como los propuestos por la *Ethereum Security Network* o similares); la exhaustividad del análisis realizado en relación con la complejidad del código auditado; la correcta comunicación de los hallazgos, incluyendo la identificación precisa de vulnerabilidades y la adecuada ponderación de su severidad; y las representaciones públicas que el auditor haya realizado respecto a la seguridad del protocolo (Guandaru, 2023). La publicación de un informe de auditoría, al servir como una señal de seguridad y generar confianza legítima en la comunidad, impone un deber de cuidado hacia los usuarios que se basan en dicha información. Por cierto, la responsabilidad que se le pueda exigir a sus auditores debe estar dentro de cánones razonables. Las auditorías, por su propia naturaleza, no constituyen una garantía absoluta contra la ocurrencia de todo tipo de hackeos o explotación de vulnerabilidades, especialmente aquellas de carácter novedoso o que emergen de ataques altamente sofisticados. Un estándar de responsabilidad excesivamente riguroso podría tener el efecto contraproducente de desincentivar la actividad de auditoría o de elevar sus costos a niveles prohibitivos, lo que en última instancia podría mermar la seguridad general del ecosistema DeFi (Bourveau et al., 2024). La aplicación de los artículos 2314 y siguientes del CC sería el marco para evaluar esta responsabilidad extracontractual, siempre que se acrediten los elementos de daño, culpa y relación de causalidad.

3.3. Proveedores de interfaces (DApps).

Los proveedores de interfaces, comúnmente conocidos como DApps (aplicaciones descentralizadas), actúan como el principal punto de interacción entre la complejidad subyacente de los protocolos DeFi y el usuario final. Esta posición les confiere responsabilidades particulares, que se distinguen de las que recaen sobre el protocolo mismo.

Debido a su función habilitadora, los proveedores de DApps deben proporcionar detalles veraces y completos sobre los riesgos asociados con el uso del protocolo, cómo funciona y las tarifas aplicables, de acuerdo con los requisitos del Artículo 1546 del Código Civil en relación con la buena fe en la ejecución de contratos, y el Artículo 3 de la Ley de Protección al Consumidor referente al derecho a información clara y oportuna.

Adicionalmente, se les exige un deber de usabilidad y diseño seguro, que minimice la probabilidad de errores por parte del usuario y que advierta de manera explícita sobre operaciones críticas. Esto implica una interfaz intuitiva y mecanismos de confirmación robustos para transacciones significativas. También recae sobre ellos un deber de actualización constante de la interfaz para reflejar cambios o mejoras en el protocolo subyacente, y un deber de verificación básica (*due diligence* mínima) para evitar la promoción negligente de protocolos manifiestamente fraudulentos o inseguros. Su responsabilidad civil se torna relevante ante representaciones erróneas o engañosas, diseños de interfaz que inducen a error, fallos propios de la aplicación (por ejemplo, la visualización de datos incorrectos) o la promoción irresponsable de protocolos de alto riesgo. La LPDC parece ser particularmente aplicable a estos actores, dado que en muchos casos constituyen la cara visible del servicio para el consumidor final, estableciendo un marco de protección que puede ser invocado por los usuarios afectados por su negligencia o dolo. La responsabilidad podría derivar de los artículos 23 y 28 de la LPDC, que sancionan la información falsa o engañosa y el incumplimiento de las condiciones ofrecidas, respectivamente, sin perjuicio de la aplicación de las normas generales de responsabilidad extracontractual del CC.

3.4 Oráculos.

Los oráculos cumplen una función esencial en el ecosistema DeFi al suministrar datos externos (como precios de activos, tasas de interés o resultados de eventos) a los contratos inteligentes, permitiendo que estos interactúen con el mundo real. Dada la criticidad de la información que proveen, la responsabilidad de los oráculos puede ser tanto contractual, frente a los protocolos que los utilizan y con los cuales han establecido un acuerdo de servicio, como extracontractual, frente a los usuarios finales que resulten afectados por la inexactitud o manipulación de los datos (Eskandari et al., 2021).

La apreciación de la culpa de un oráculo se focalizaría en la celeridad empleada en su operación. Esto abarca la metodología de recolección y agrupamiento de datos; las precauciones tomadas para prevenir un manejo indebido de los datos; la claridad relativa a las limitaciones propias del servicio, como los retrasos en la actualización de datos o los riesgos de centralización; y la velocidad y eficacia en la corrección de datos incorrectos una vez descubiertos. La responsabilidad de los oráculos es muy importante en contextos donde pueden producirse ataques de manipulación de precios, como los *flash loans*[16], atrasos considerables en la actualización de datos cuando hay una alta volatilidad de mercado, o problemas técnicos deriven en datos claramente erróneos, lo que puede desatar liquidaciones innecesarias de posiciones o ejecuciones contractuales lesivas. Por su relevancia para la estabilidad y seguridad de los variados protocolos DeFi, podría aducirse la imposición de un deber de diligencia fortalecido para los oráculos, equivalente al que se aplica a las infraestructuras críticas del mercado financiero tradicional (Calderón Marenco et al., 2025). Los artículos 2314 y siguientes del CC serían el fundamento para la acción de responsabilidad extracontractual, requiriendo la prueba del daño, la culpa del oráculo y el nexo causal entre la acción u omisión culposa y el perjuicio sufrido por el usuario.

3.5. Miembros de DAOs.

La calificación jurídica de las DAOs en el ordenamiento jurídico chileno representa uno de los desafíos más complejos, ya que su naturaleza distribuida, la ausencia de una personalidad jurídica tradicional y la participación seudónima de sus miembros dificultan su encuadre en las categorías existentes (Kim & Jung, 2024). Podrían en principio asimilarse a figuras como las sociedades de hecho (artículos 2057 y 2094 del CC), comunidades (artículo 2304 del CC) o asociaciones de hecho, aunque ninguna de estas analogías es perfecta. Si se les considerara sociedades de hecho, los miembros podrían enfrentar una responsabilidad personal e ilimitada por las obligaciones sociales, si bien la identificación de los responsables y la ejecución de sentencias se presentarían como obstáculos prácticos de gran envergadura.

Alternativamente, podría explorarse una responsabilidad extracontractual individual de aquellos miembros que hayan participado activamente en la toma de decisiones, por ejemplo, votando a favor de propuestas manifiestamente negligentes o dañinas. Esta responsabilidad sería particularmente exigible a aquellos con roles especiales dentro de la DAO, como desarrolladores principales, miembros de comités técnicos o grandes tenedores de *tokens* de gobernanza, quienes por su influencia y/o conocimiento podrían tener un deber de diligencia reforzado (Kitzler et al., 2023). La mera posesión pasiva de *tokens* de gobernanza, sin una activa participación en la gobernanza o en la toma de decisiones que causen un daño, difícilmente generaría responsabilidad personal. La aplicación práctica de estos principios enfrenta desafíos considerables, incluyendo la identificación de miembros seudónimos, la determinación de la jurisdicción aplicable en un entorno global y la prueba de la relación de causalidad entre un voto individual y el daño producido. La falta

16. Los *flash loans* son préstamos descentralizados, sin garantías, facilitados por la tecnología *blockchain*. El monto prestado y una tarifa mínima deben ser devueltos dentro de la transacción originaria, o la transacción será anulada.

de una regulación particular para las DAOs en Chile compele a una interpretación analógica y creativa de las normas existentes, teniendo eso sí siempre presente los principios generales que rigen la responsabilidad civil y la protección de aquellos que son afectados.

3.6. Usuarios.

La participación de los usuarios en el ecosistema DeFi no los exime de toda responsabilidad, especialmente en lo que respecta a la diligencia que deben observar al interactuar con estos protocolos. La figura de la culpa de la víctima, contemplada en el artículo 2330 del CC, puede operar como un factor atenuante o incluso eximente de responsabilidad para los demás actores, si se demuestra que el usuario actuó con una falta de diligencia básica. Esto podría incluir no realizar una investigación mínima sobre el protocolo, ignorar advertencias explícitas de riesgo, utilizar protocolos experimentales de manera consciente sin comprender sus implicaciones, interactuar con el sistema sin una comprensión fundamental de su funcionamiento, o ser negligente en la custodia de sus claves privadas (Saengchote et al., 2023).

De la misma manera, la determinación de la culpa del usuario debe ser ponderada cautelosamente, teniendo en cuenta la asimetría informativa, el grado de dificultad técnica de los protocolos DeFi y las facilidades de uso desarrolladas por los proveedores de interfaces. La validez del consentimiento informado, a menudo materializado a través de *disclaimers* o términos de servicio, requiere que la información sobre los riesgos específicos sea clara, comprensible y oportuna, y no meras cláusulas genéricas que busquen una renuncia anticipada de derechos (Farkas et al., 2023). En este sentido, la LPDC en su artículo 16 limita la validez de cláusulas abusivas que impliquen una renuncia anticipada de derechos por parte del consumidor. Es crucial distinguir entre usuarios sofisticados, quienes por su experiencia y conocimiento podrían tener un mayor deber de diligencia en la comprensión y evaluación de los riesgos, y usuarios minoristas (*retail*), que por su menor experticia merecen una mayor protección jurídica y a quienes se les debe exigir un estándar de diligencia menos riguroso. La aplicación de la culpa de la víctima debe ser contextualizada y no puede servir como un pretexto para eximir de responsabilidad a actores que han incumplido sus propios deberes de diligencia y transparencia.

4. CAUSALIDAD Y DAÑO EN ENTORNOS DESCENTRALIZADOS.

4.1. Desafíos probatorios de la relación causal.

La determinación del nexo causal entre una acción específica, como la implementación de código vulnerable, y el perjuicio resultante, ejemplificado por la pérdida de fondos en el ámbito de DeFi, presenta una dificultad que se acentúa por la naturaleza algorítmica de las interacciones, la composabilidad intrínseca entre diversos protocolos, la concurrencia de múltiples factores causales, que pueden incluir vulnerabilidades de código, ataques maliciosos, manipulaciones de oráculos y decisiones de DAO, así como la opacidad funcional que a menudo caracteriza a estos sistemas. En este contexto, la prueba pericial informática emerge como un elemento central para dilucidar la cadena de eventos, aunque no está exenta de limitaciones significativas, tales como la escasez de expertos cualificados, los elevados costos asociados y la dificultad para que los órganos jurisdiccionales comprendan claramente las complejidades técnicas involucradas.

Frente a estas barreras, se podría considerar la aplicación de presunciones de causalidad, particularmente en situaciones donde se evidencian vulnerabilidades manifiestas o fallos catastróficos que, por su magnitud, difícilmente habrían ocurrido sin una negligencia grave. Un precedente relevante en la jurisprudencia chilena es la doctrina de la pérdida de oportunidad, la cual podría ofrecer un marco para indemnizar la privación de una posibilidad seria y real de evitar un daño. Por ejemplo, si una auditoría negligente no detectó un riesgo crítico, impidiendo así la adopción de medidas preventivas, la

víctima podría ser compensada por la pérdida de esa oportunidad de salvaguardar sus activos.

4.2. Tipología y cuantificación de daños.

La tipología y cuantificación de daños en el ecosistema DeFi exige una clasificación precisa y una metodología de medición adaptada a sus características:

a) Daño emergente: está referido a la pérdida de criptomonedas. Su valoración constituye un desafío considerable debido a la extrema volatilidad de estos activos y la necesidad de su conversión a moneda nacional para efectos indemnizatorios, conforme a lo establecido en el artículo 1556 del CC. Una aproximación metodológica podría consistir en valorar los activos al momento del incidente, actualizando dicho valor de manera objetiva, por ejemplo, mediante el Índice de Precios al Consumidor (IPC) o bien, al momento de fijarse un determinado valor dictada la sentencia, si esta última opción resulta más favorable para la víctima.

b) Lucro cesante: corresponde a la ganancia legítima que la víctima dejó de percibir como consecuencia directa del daño. En este rubro, la indemnización se limitaría a los rendimientos regulares y previsibles que se habrían obtenido, como los intereses generados por actividades de *staking* o *lending*, excluyendo expresamente las ganancias meramente especulativas o hipotéticas. La procedencia de esta indemnización exige una prueba de certeza rigurosa sobre la existencia y cuantía de la ganancia frustrada.

La distinción entre ambos deriva de que el daño emergente es el empobrecimiento real y efectivo que sufre el patrimonio del deudor, y el lucro cesante la utilidad que deja de percibir el acreedor por el incumplimiento o cumplimiento tardío de la obligación (Abeliuk, 2014).

c) Daño moral: abarca la afectación extrapatrimonial que el incidente pueda haber causado, incluyendo el estrés, la ansiedad o el daño reputacional. Aunque tradicionalmente asociado a contextos no comerciales, su procedencia es viable incluso en el ámbito de las transacciones financieras, siempre que se acredite de manera concreta la existencia y magnitud de la afectación sufrida por la víctima.

4.3. El problema de la reparación efectiva.

La restitución en especie (devolución de activos en su estado original) a menudo se vuelve imposible, ya sea porque los fondos se han mezclado con otros, se han transferido a billeteras inaccesibles o se han dispersado en múltiples direcciones. Además, la ejecución de sentencias puede volverse desafiante debido a una variedad de factores, incluidos, pero no limitados a, el anonimato o seudonimato de los actores, la dispersión global de las operaciones y la complejidad de incautar criptoactivos (Cheong, 2023). A la luz de esta situación, se están estudiando posibles soluciones para mitigar el impacto de los daños, como la creación de fondos de compensación financiados por los propios protocolos, a través de reservas o tesorerías de DAO, la implementación de seguros descentralizados, el desarrollo de mecanismos técnicos de recuperación, como bloqueos de tiempo, sistemas *multisig*, o la posibilidad de realizar bifurcaciones de cadena, y la ejecución sobre activos identificables que puedan encontrarse en plataformas centralizadas como los intercambios.

5. EXIMENTES Y LIMITACIONES DE RESPONSABILIDAD

Hay hechos que excluyen la existencia de culpa o dolo y otros en que no se responde o se modifica la responsabilidad.

5.1. Validez de cláusulas eximentes.

La validez de las cláusulas exonerativas o limitativas de responsabilidad en el contexto de DeFi en Chile es restrictiva y se rige por principios jurídicos específicos:

a) En el ámbito de las obligaciones contractuales, las disposiciones eximentes, limitativas o agravantes de responsabilidad se consideran válidas de conformidad con el artículo 1547 CC. Esta estipulación, junto con el último párrafo del artículo 1558 CC, que sirve para interpretar la probable intención de las partes involucradas, sugiere la posibilidad de modificar la responsabilidad, incluida la posibilidad de su derogación total, según ciertas interpretaciones. El artículo 1547 CC delimita el grado de culpabilidad y falta en relación con las prestaciones contractuales, haciendo hincapié en que las estipulaciones explícitas de las partes tienen prioridad. El artículo 1558 refuerza esta afirmación al permitir a las partes modificar las normas prescritas en relación con los daños. Estas disposiciones establecen un espacio libre para la autorregulación dentro del marco legal. El principio de autonomía de la voluntad subyace a estos mecanismos. Las cláusulas de exención están regidas por el Artículo 12 del Código Civil (González, 2011); b) Efectividad parcial por negligencia leve: las cláusulas que limitan la responsabilidad por negligencia leve pueden tener efectividad parcial, siempre que no distorsionen las obligaciones esenciales del contrato y hayan sido objeto de una negociación efectiva entre las partes. Debe tenerse presente que en el ámbito de los contratos de adhesión, predominantes en el ecosistema DeFi, demostrar una negociación real es extremadamente difícil; c) Abusividad bajo la Ley de Protección al Consumidor: es muy probable que tales cláusulas sean estimadas abusivas bajo la LPDC, particularmente si implican una exención absoluta de responsabilidad o limitan derechos esenciales del consumidor, de acuerdo con el Artículo 16 letra e) de dicha ley; y d) Requisitos de forma y contenido: la efectividad de estas cláusulas también depende de su exposición clara y comprensible, del conocimiento real por parte del usuario y de la ausencia de representaciones contradictorias, como las que podrían surgir entre el marketing del protocolo y las advertencias contenidas en los descargos de responsabilidad.

5.2. Caso fortuito y hecho de tercero.

La aplicación de las eximentes de responsabilidad por caso fortuito o hecho de tercero en el ámbito de DeFi es sumamente restrictiva. La mayoría de los ataques y vulnerabilidades, como los ataques de reentrada o los préstamos *flash*, son en principio previsibles y evitables mediante la aplicación de una diligencia adecuada, que incluye la realización de auditorías de seguridad rigurosas y la adopción de buenas prácticas de desarrollo. Las vulnerabilidades inherentes al código no pueden ser consideradas como un factor "externo" al desarrollador, sino que forman parte de su esfera de control y responsabilidad.

El deber de prevención que recae sobre los desarrolladores y operadores de protocolos DeFi limita significativamente la eficacia del hecho de tercero como eximente, salvo en situaciones de sofisticación sin precedentes, como ataques de día cero - *zero-day exploits*-, o circunstancias extraordinarias e irresistibles, como por ejemplo un fallo catastrófico de la red *blockchain* subyacente.

6. DESAFÍOS PROCESALES Y JURISDICCIONALES

Las DeFi, por su naturaleza global y descentralizada, plantea importantes desafíos en el ámbito procesal y jurisdiccional, que demandan una adecuación de los criterios tradicionales:

- Jurisdicción: la determinación de la jurisdicción competente se dificulta por la inoperancia de los criterios clásicos como el domicilio del demandado o el lugar de cumplimiento de la obligación. En este contexto, se indagan enfoques alternativos, como el del mercado meta, el domicilio de los usuarios o consumidores y la presencia de activos ejecutables en el territorio chileno. Ello exige una interpretación flexible de las normas existentes o, en su defecto, una adaptación normativa específica.

- Identificación y notificación: el anonimato o seudonimato característico de los participantes en DeFi obstaculiza la identificación de los responsables y la consecuente notificación de las acciones judiciales. Para superar estos obstáculos se consideran posibles soluciones como la solicitud de medidas prejudiciales para obtener datos de intermediarios (como *exchanges* centralizados o proveedores de *hosting*), la notificación por equivalentes funcionales (utilizando los canales digitales habituales de comunicación de los demandados) y la adopción de medidas cautelares sobre los activos involucrados.

- Valor probatorio: los registros inmutables de la *blockchain* poseen un valor probatorio considerable, siendo equiparables a documentos electrónicos bajo la Ley N° 19.799[17] y valorados conforme a las reglas de la sana crítica. No obstante, la prueba pericial informática es un elemento clave, cuya implementación es costosa y compleja, demandando peritos altamente especializados y una capacitación judicial continua para su correcta apreciación.

- Mecanismos alternativos de resolución de conflictos (ADR): ante la ineficacia de los cauces judiciales tradicionales, emergen los ADR como alternativas más eficientes y adaptadas a la idiosincrasia de DeFi. Estos incluyen el arbitraje especializado, la mediación tecnológicamente asistida, los jurados técnicos descentralizados (como Kleros[18]) o la resolución de disputas *on-chain*[19]. Si bien estas opciones requieren una base consensual entre las partes, plantean desafíos en cuanto a su ejecutabilidad y el respeto al debido proceso.

7. PROPUESTAS NORMATIVAS E INTERPRETATIVAS.

Para abordar los desafíos identificados en el marco de la responsabilidad civil en DeFi, se plantean las siguientes propuestas normativas e interpretativas:

7.1. Criterios para estándares de diligencia.

Es imperativo establecer criterios jurisprudenciales o normativos -posiblemente a través de la Comisión para el Mercado Financiero (CMF)- que definan los estándares de diligencia exigibles a los actores del ecosistema DeFi. Estos criterios deberían basarse en los siguientes principios:

1) Proporcionalidad al riesgo: la diligencia exigida debe ser proporcional al nivel de riesgo inherente a cada protocolo o servicio; 2) Conformidad con mejores prácticas: adopción y cumplimiento de las mejores prácticas de la industria, incluyendo guías de seguridad y estándares técnicos reconocidos; 3) Transparencia y documentación: obligación de proporcionar información clara, completa y accesible sobre el funcionamiento, riesgos y características de los protocolos; 4) Testeo riguroso: implementación de pruebas exhaustivas antes del despliegue de código y funcionalidades; 5) Auditorías independientes: realización de auditorías de seguridad por terceros especializados de manera periódica; 6) Mecanismos de seguridad y contingencia: desarrollo e implementación de sistemas robustos de seguridad y planes de contingencia ante posibles incidentes; 7) Monitoreo y respuesta a incidentes; 8) Establecimiento de capacidades de monitoreo continuo y protocolos de respuesta rápida ante eventos adversos; y 9) Actualización continua: compromiso con la mejora y actualización constante de los protocolos y sus medidas de seguridad.

17. Ley 19.799, de 2002, sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma, disponible en: https://www.bcn.cl/leychile/navegar?idNorma=196640

18. Kleros es un servicio de resolución de disputas descentralizado basado en *blockchain* que ofrece una alternativa equitativa, rápida y rentable a los sistemas legales convencionales para disputas mundanas y digitales en la economía global en evolución. Funciona de manera similar a un jurado digital, en el que participantes incentivados, seleccionados por el sistema a través de criptomonedas, resuelven los conflictos en línea. Disponible en: https://kleros.io/es/

19. La resolución de disputas en cadena utiliza la tecnología *blockchain* para documentar y ejecutar los procesos de arbitraje. Los contratos inteligentes se emplean para automatizar este proceso, garantizando que los resultados sean inmutables y aplicables.

7.2. Adaptaciones necesarias al marco normativo.

Se requiere una serie de adaptaciones y desarrollos normativos para integrar adecuadamente el fenómeno DeFi en el ordenamiento jurídico chileno:

1) Clarificación del estatus jurídico de las DAOs: es fundamental regular su naturaleza jurídica, los requisitos para su constitución, sus mecanismos de gobernanza y el régimen de responsabilidad aplicable. Esto podría lograrse mediante una modificación a la Ley Fintech o la promulgación de una ley especial; 2) Regulación de los contratos inteligentes: se necesita clarificar su validez jurídica, los principios para su interpretación, sus efectos vinculantes y el tratamiento de los vicios del consentimiento en un entorno automatizado. Una reforma al Código Civil o una ley específica podrían abordar esta cuestión; 3) Adaptación de las normas procesales: es imprescindible facilitar la identificación de las partes, la notificación de las acciones y la práctica de la prueba en entornos descentralizados. Esto implicaría una reforma al Código de Procedimiento Civil; 4) Desarrollo normativo de estándares de diligencia: la CMF podría desarrollar una normativa específica que establezca estándares de diligencia basados en principios y proporcionalidad, complementando así el marco legal; 5) Creación de un marco para seguros descentralizados: se requiere una regulación que reconozca las particularidades tecnológicas de estos productos, ya sea mediante una modificación a la Ley de Seguros o una normativa específica de la CMF; 6) Fomento de ADR especializados: es necesario establecer un marco legal que promueva y regule el arbitraje y la mediación adaptados a las especificidades de DeFi, lo que podría implicar una reforma a la Ley de Arbitraje o una ley especial; 7) Clarificación de criterios de jurisdicción: se deben establecer criterios claros para determinar la jurisdicción en operaciones transfronterizas, lo que podría abordarse mediante una reforma al Código de Bustamante o a través de la consolidación de jurisprudencia; y 8) Refuerzo de la protección al consumidor: es crucial adaptar la Ley de Protección al Consumidor a los servicios ofrecidos en el ecosistema DeFi, ya sea mediante una reforma a la LPDC o a través de normativa específica del Servicio Nacional del Consumidor (SERNAC).

CONCLUSIONES

La irrupción de las Finanzas Descentralizadas (DeFi) representa un desafío significativo para el derecho chileno, que exige ir más allá de las disposiciones incipientes de la Ley Fintech. Se hace indispensable una interpretación adaptativa tanto del Código Civil como de la Ley de Protección de los Derechos de los Consumidores (LPDC), complementada con el desarrollo de un marco normativo específico. La tensión inherente entre la inmutabilidad tecnológica y la necesidad de seguridad jurídica se posiciona como un eje central de esta problemática. En este contexto, se propone la implementación de estándares de diligencia elevados para los desarrolladores y auditores de protocolos, así como la diferenciación de criterios de responsabilidad para los diversos actores involucrados. Los desafíos probatorios y procesales demandan la adopción de soluciones innovadoras, incluyendo el recurso a mecanismos alternativos de resolución de conflictos. Es crucial alcanzar un equilibrio entre la protección efectiva de los usuarios y el fomento de la innovación, mediante la construcción de un marco jurídico robusto, predecible y tecnológicamente neutro para DeFi en Chile que, si bien considere la experiencia comparada, se adapte de manera idónea a la realidad nacional.

REFERENCIAS BIBLIOGRÁFICAS

Abeliuk, R. (2014). Las Obligaciones. Sexta Edición actualizada, Editorial Thomson Reuters.

Abdullah, J., & Yihan, G. (2022). Making Smart Contracts a Reality: Confronting Definitions, Enforceability, and Regulation. Capítulo 3 (pp. 70–78). Oxford University Press.
https://academic.oup.com/oxford-law-pro/book/43175/chapter-abstract/362294932?redirectedFrom=fulltext

Aigner, A., & Dhaliwal, G. (2021). UNISWAP: Impermanent Loss and Risk Profile of a Liquidity Provider. arXiv: Trading and Market Microstructure.
https://www.researchgate.net/publication/352679908_UNISWAP_Impermanent_Loss_and_Risk_Profile_of_a_Liquidity_Provider#read

Ali, A. A., & Dembo, S. A. (2024). Decentralized Finance (DeFi) and Its Impact on Traditional Banking Systems: Opportunities, Challenges, and Future Directions.
https://www.preprints.org/frontend/manuscript/5c1d21b73a8064a9c360eb4010fe1d36/download_pub

Arancibia, L., & Rojas, C. (2024). Mecanismos de resolución de controversias por medios electrónicos en la Ley 19.496: Antecedentes, conceptualización y propuestas de diseño para un mecanismo ODR de consumo. Revista Chilena de Derecho y Tecnología.
https://www.scielo.cl/scielo.php?pid=S0719-25842024000100206&script=sci_arttext

Baraona, J. (2014). La regulación contenida en la Ley 19.496 sobre Protección de los Derechos de los Consumidores y las Reglas del Código Civil y Comercial sobre Contratos: Un marco comparativo. Revista chilena derecho, vol.41, N°2.
https://www.scielo.cl/scielo.php?pid=S0718-34372014000200002&script=sci_arttext

Barros, E. (2008). Tratado de Responsabilidad Extracontractual, primera edición, Editorial Jurídica de Chile.

Bourveau, T., Brendel, J., & Schoenfeld, J. (2024). Decentralized Finance (DeFi) assurance: early evidence. Review of Accounting Studies.
https://link.springer.com/content/pdf/10.1007/s11142-024-09834-8.pdf

Bozzo, S. (2019). Eres consumidor, defiende tus derechos. Guía práctica para la defensa de los derechos del consumidor.
https://ediciones.uautonoma.cl/index.php/UA/catalog/download/30/57/66?inline=1

Calderón Marenco, E. A., Garzón Solano, J. E., Sánchez Silveyra, R., Sal, G. O., & Ravelo-Franco, G. (2025). Responsabilidad civil del oráculo: intersección entre el derecho privado y los contratos inteligentes. IDP, 0(42).
https://raco.cat/index.php/IDP/article/view/430703/526488

Carapella, F., Dumas, E. B., Gerszten, J., Swem, N., & Wall, L. D. (2022). Decentralized Finance (DeFi): Transformative Potential & Associated Risks. Finance and Economics Discussion Series, 2022(057), 1–33.
https://www.federalreserve.gov/econres/feds/decentralized-finance-defi-transformative-potential-and-associated-risks.htm

Cárdenas, H. (2006). La relación de causalidad: ¿Quaestio facti o quaestio iuris?, Comentario a sentencia de Corte Suprema, 26 de enero de 2004. Revista Chilena de Derecho, vol. 33 N°1 (pp. 167 – 176).
https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-34372006000100011

Carpentier-Desjardins, C., Paquet-Clouston, M., Kitzler, S., & Haslhofer, B. (2025). Mapping the DeFi crime landscape: an evidence-based picture. Journal of Cybersecurity, 11(1).
https://academic.oup.com/cybersecurity/article-pdf/11/1/tyae029/61510649/tyae029.pdf

Castillo, A. (2025). Regulación de criptoactivos en Chile, opinión. Diario Constitucional.
https://www.diarioconstitucional.cl/2025/06/24/regulacion-de-criptoactivos-en-chile-por-alicia-castillo/

Cheong, B. C. (2023). Doctrinal Issues in Recovering NFTs That Have Been Wrongfully Taken Away. Social Science Research Network.
https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID4636419_code4186833.pdf?abstractid=4572629&mirid=1&type=2

Consent to Automated Reputational Profiling Requires Transparency of the Underlying Algorithm (2022), GRUR International, Volume 71, Issue 6, June 2022, Pages 581–583.
https://academic.oup.com/grurint/article-abstract/71/6/581/6565352?redirectedFrom=fulltext

Corral, H. (2013). Lecciones de Responsabilidad Civil, Segunda edición actualizada. Legal Publishing by Thomson Reuters.

De la Maza, I. (2021). La Ley 19.496 como un supuesto de descodificación material y su relación con las leyes especiales a las que alude el artículo 2 bis. Revista de Derecho de la Pontificia Universidad Católica de Valparaíso N°56.
https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-68512021000100006

Dhanya, V. R., D'silva, R. R., & Joseph, D. (2025). Regulatory Challenges and Compliance in Decentralized Finance (DeFi). Advances in Finance, Accounting, and Economics Book Series, 71–100.
https://www.igi-global.com/gateway/chapter/full-text-pdf/368536

Dhillon, D., & Mehrotra, D. (2024). Smart Contract Vulnerabilities: Exploring the Technical and Economic Aspects (pp. 81–91). Springer Vienna.
https://link.springer.com/chapter/10.1007/978-3-031-49593-9_5

Ding, Q., Liebau, D., Wang, Z., & Xu, W. (2023). A Survey on Decentralized Autonomous Organizations (DAOs) and Their Governance. World Scientific Annual Review of Fintech, Vol 1.
https://www.worldscientific.com/doi/10.1142/S281100482350001X

Dos Santos, S., Singh, J., Thulasiram, R. K., Kamali, S., Sirico, L. J., & Loud, L. (2022). A New Era of Blockchain-Powered Decentralized Finance (DeFi) - A Review. Annual International Computer Software and Applications Conference, 1286–1292.
https://ieeexplore.ieee.org/document/9842637

Dotan, M., Yaish, A., Yin, H.-C., Tsytkin, E., & Zohar, A. (2023). The Vulnerable Nature of Decentralized Governance in DeFi.
https://arxiv.org/abs/2308.04267

Eskandari, S., Salehi, M., Gu, W. C., & Clark, J. (2021). SoK: Oracles from the Ground Truth to Market Manipulation. arXiv: Cryptography and Security.
https://dl.acm.org/doi/10.1145/3479722.3480994

Farkas, W., Fasser, F., Weingärtner, T., & Reis, P. (2023). Deciphering DeFi: A Comprehensive Analysis and Visualization of Risks in Decentralized Finance.
https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID4608294_code623849.pdf?abstractid=4607944&mirid=1&type=2

Ferreira, A. (2023). Smart Contracts and the Law (pp. 125–143).
https://link.springer.com/chapter/10.1007/978-94-6265-579-9_8

Figueroa J.V. (2023). Ley Fintech: Fenómeno Fintech, análisis del sistema registral y sistema de finanzas abiertas.
https://repositorio.uchile.cl/bitstream/handle/2250/192767/Ley-Fintech-fenomeno-Fintech-analisis-del-sistema-registral-y-sistema-de-finanzas-abiertas.pdf?sequence=1

García, C. (2020). Análisis de la sanción a las cláusulas abusivas en la doctrina y la jurisprudencia: una propuesta desde la nulidad absoluta.
https://www.revistaiusnovum.cl/index.php/REIN/article/download/58/36

Gogol, K., Killer, C., Schlosser, M., Bocek, T., Stiller, B., & Tessone, C. J. (2024). SoK: Decentralized Finance (DeFi) - Fundamentals, Taxonomy and Risks. https://arxiv.org/abs/2404.11281

González, J. (2011). Las cláusulas limitativas, exonerativas o agravantes de responsabilidad en materia contractual. validez y límites. Revista chilena derecho vol. 38, N°1. https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-34372011000100005

González-Gutiérrez, N. (2025). Ley 21.521, la prestación de servicios financieros fintech: El desafio de la comisión para el mercado financiero para regularlos. Universidad Autónoma de Chile. https://papers.ssrn.com/sol3/Delivery.cfm/5402289.pdf?abstractid=5402289&mirid=1

Guandaru, C. (2023). CryptoAudit and its inherent challenges. https://www.qeios.com/read/20TV8G

Hassan, S., & De Filippi, P. (2021). Decentralized Autonomous Organizations. Glossary of Distributed Technologies. https://eprints.ucm.es/id/eprint/62306/

Hormazábal, J. (2023). Normativa aplicable exclusivamente a la República de Chile, Aspectos Relevantes de la Ley Fintec N°21.521. Circula Verde. https://www.circuloverde.cl/aspectos-relevantes-de-la-ley-fintec-n21-521/#

Joggerst, L., Knoll, M., Hoppe, F., Wendt, J., & Groche, P. (2018). Autonomous Manufacturing Processes under Legal Uncertainty. Applied Mechanics and Materials, 885, 227–239. https://www.scientific.net/AMM.885.227.pdf

Joshi, S., Anuratha, K., Nandhini, J. M., & P, S. (2023). Digital I Will Using Blockchain. 1–6. https://ieeexplore.ieee.org/document/10395842

Kim, J., & Jung, B.-H. (2024). A Study on the Legal Status of Blockchain-Based Decentralized Autonomous Organizations (DAOs). Beopgwa Gieob Yeon-Gu. https://doi.org/10.35505/sjlb.2024.4.14.1.3

Kitzler, S., Balietti, S., Saggese, P., Haslhofer, B., & Strohmaier, M. (2023). The Governance of Decentralized Autonomous Organizations: A Study of Contributors' Influence, Networks, and Shifts in Voting Power. https://arxiv.org/abs/2309.14232

Komal, Ms. A. P. (2024). Decentralized Finance (DeFi): A Review of Applications and Risks in the Financial Ecosystem. Indian Scientific Journal Of Research In Engineering And Management, 08(11), 1–7. https://ijsrem.com/download/decentralized-finance-defi-a-review-of-applications-and-risks-in-the-financial-ecosystem/

Kuznetsov, A., Ilchenko, O., Kryvinska, N., Buravchenko, K., Smirnov, O., & (2023). An Empirical Assessment of Leading Blockchain Financial Services. https://ieeexplore.ieee.org/document/10548729

Lallai, G., Pinna, A., Marchesi, M., & Tonelli, R. (2020). Software engineering for DApp smart contracts managing workers Contracts. http://ceur-ws.org/Vol-2580/DLT_2020_paper_8.pdf

Linoy, S., Stakhanova, N., & Ray, S. (2021). De-anonymizing Ethereum blockchain smart contracts through code attribution. International Journal of Network Management, 31(1). https://onlinelibrary.wiley.com/doi/epdf/10.1002/nem.2130

Liu, J., Makarov, I. A., & Schoar, A. (2023). Anatomy of a Run: The Terra Luna Crash. Social Science Research Network. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4416677

Luco, D., & Santander, C. (2023). Las Fintech en Chile: Alternativa de bancarización para las personas naturales y jurídicas. Revista Summa de Arithmetica, N° 8, Universidad de Santiago.
https://www.revista-sda.cl/index.php/sda/article/download/52/55/196

Ma, W.-M., Zhu, C., Liu, Y., Xie, X., & Li, Y. (2023). A Comprehensive Study of Governance Issues in Decentralized Finance Applications.
https://arxiv.org/abs/2311.01433

Manda, V. K., & Katneni, V. (2024). The Critical Role of Blockchain Oracles in Web 3 (pp. 207–224). IGI Global.
https://www.igi-global.com/gateway/chapter/full-text-pdf/342266

Moro-Visconti, R., & Cesaretti, A. (2023). Decentralized Finance (DeFi) (pp. 287–340).
https://link.springer.com/chapter/10.1007/978-3-031-42971-2_9

Nadler, M., Bekemeier, F., & Schär, F. (2023). DeFi Risk Transfer: Towards A Fully Decentralized Insurance Protocol.
https://ieeexplore.ieee.org/document/10174937

Napieralska, A., & Kepczynski, P. (2024). Redefining Accountability: Navigating Legal Challenges of Participant Liability in Decentralized Autonomous Organizations.
https://arxiv.org/abs/2408.04717

Nazarov, A. (2024). Legal Nature and Classification of Smart Contracts in Crypto Exchanges: Challenges to Traditional Contract Law. International Journal of Law and Policy, 2(9), 1–15.
https://irshadjournals.com/index.php/ijlp/article/view/224/183

Parisi, C., & Budorin, D. (2024). DeFi Security. Future of Business and Finance, 3–18.
https://link.springer.com/chapter/10.1007/978-3-031-58002-4_1

Perret, L., YrarrAzaval A., Jara, R., Durán R., Hübner A., González M., Corral H., Zelaya P., Romera, O., Bofill J., & Romero A. (1999). Derecho del Consumo y Protección al Consumidor, Estudios sobre la Ley N° 19.496 y las principales tendencias extranjeras.
https://www.uandes.cl/wp-content/uploads/2019/03/Cuaderno-de-Extensi%C3%B3n-Jur%C3%ADdica-N%C2%B0-3-Derecho-del-Consumo-y-Protecci%C3%B3n-al-Consumidor.pdf

Quezada, I. (2024). Montt Group, Legal & Consulting.
https://monttgroup.com/es/alerta/publicacion-de-ley-n-21-521-que-regula-a-los-proveedores-de-servicios-financieros-por-medios-digitales-fintech-y-habilita-la-implementacion-del-sistema-de-finanzas-abiertas-open-banking/

Reyes, C., & Gárate, O. (2021). Proyecto de Ley Fintech: Innovación, inclusión y competencia, programa libre competencia UC. Opinión técnica N°16.
https://librecompetencia.uc.cl/images/AAA/Opinion/Op_16.pdf

Ruggieri, M. (2021). El derecho a la seguridad en el consumo del servicio de estacionamientos en la actual ley Nº 19.496. Repositorio de la Universidad Finis Terrae.
https://repositorio.uft.cl/xmlui/bitstream/20.500.12254/2183/1/Ruggieri_Silva_2021.pdf

Saengchote, K., Putniņš, T., & Samphantharak, K. (2023). Does DeFi remove the need for trust? Evidence from a natural experiment in stablecoin lending. Journal of Behavioral and Experimental Finance, 40, 100858.
https://www.sciencedirect.com/science/article/abs/pii/S2214635023000722?via%3Dihub

Sant'Ana Costa, C. L. (2024). DeFi: Concepts and Ecosystem.
https://arxiv.org/abs/2412.01357

Schär, F. (2020). Decentralized Finance: On Blockchain- and Smart Contract-based Financial Markets. Social Science Research Network.
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3571335

Schiele, C., & Tocornal, J. (2010). Artículo 2329 del Código Civil. La interpretación de presunción por hechos propios existe en la jurisprudencia. Revista Chilena de Derecho, vol. 37 N° 1 (pp. 123 – 139).
https://www.scielo.cl/pdf/rchilder/v37n1/art06.pdf

Sompolinsky, Y., & Zohar, A. (2017). Bitcoin's Underlying Incentives: The unseen economic forces that govern the Bitcoin protocol. ACM Queue, 15(5), 29–52.
https://spawn-queue.acm.org/doi/10.1145/3155112.3168362

Sotelo, C. (2024). Implementación de la Ley Fintec, Icare. Comisión para el Mercado Financiero (CMF).
https://www.cmfchile.cl/portal/prensa/615/articles-81931_doc_pdf.pdf

Sotelo, C. (2024). Ley Fintec: Avances en la Regulación de Criptoactivos. Comisión para el Mercado Financiero (CMF).
https://www.cmfchile.cl/portal/principal/613/articles-79589_doc_pdf.pdf

Thomason, J., & Ivwurie, E. (2023). Decentralized Autonomous Organizations: Governing by Code. IGI Global Scientific Publishing (pp. 84–101).
https://www.igi-global.com/gateway/chapter/full-text-pdf/325636

Vial, V. (2003). Teoría General del Acto Jurídico. Quinta edición actualizada, Editorial Jurídica de Chile.

Weaver, N. (2018). Risks of cryptocurrencies. Communications of The ACM, 61(6), 20–24.
https://dl.acm.org/doi/10.1145/3208095

Weidenslaufer, C., & Wilkins, J. (2020). Regulación de Fintech en Chile y el derecho comparado. Asesoría Técnica Parlamentaria.
https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/29556/2/BCN_Fintech_en_Chile_y_derecho_comparado_2020.pdf

Wilkins, J. (2019). Garantía legal del consumidor, marco regulatorio vigente y ejemplos en la legislación extranjera. Asesoría técnica parlamentaria.
https://www.bcn.cl/obtienearchivo?id=repositorio/10221/27235/1/PL_Proteccion_Consumidor__GARANTIA__Comparado.pdf

Xiao, M., Xu, Y., Li, Z., & Wan, H. (2024). Advanced Security Auditing Methods for Solidity-Based Smart Contracts. Electronics.
https://www.mdpi.com/2079-9292/13/20/4093/pdf?version=1729167910

Zhou, L., & Qin, K. (2024). DeFi '24: Workshop on Decentralized Finance and Security. 4907–4908.
https://dl.acm.org/doi/10.1145/3658644.3691552

UNIVERSIDAD TECNOLÓGICA METROPOLITANA
del Estado de Chile

UTEM

EDICIONES UNIVERSIDAD TECNOLÓGICA METROPOLITANA

ISSN (EN LÍNEA) 0719-0891
ISSN-L: 0718-3933