Memoria fría y memoria caliente

Custodia, cifrado y trascendencia de los recuerdos personales

Cris Olmedo y Kurt Sommer
Grupo de investigación Divina Machina
Documento de trabajo · Estado del arte y propuesta
DM-2026-11, versión 1.0 · 1 de noviembre de 2026

Resumen. Cuando un agente recuerda a una persona, la pregunta decisiva no es dónde se guarda el recuerdo, sino quién tiene la llave. Proponemos pensar la memoria personal con el vocabulario de las carteras de criptomonedas: una memoria caliente, en línea y al alcance del agente, y una memoria fría, cifrada y fuera de su alcance, que solo se abre con una firma de su dueño o, cuando el dueño ya no está, con la de sus custodios.

Revisamos el estado del arte en tres frentes. En custodia de claves: carteras frías y calientes, problemas de usabilidad, compartición de secretos y recuperación social. En registros distribuidos y protección de datos: las directrices europeas de 2026 sobre blockchain recomiendan dejar los datos personales fuera de la cadena, y las credenciales verificables del W3C ofrecen un modelo de emisor, titular y verificador. En la memoria de quienes ya no están: la industria del más allá digital, la ética de los deadbots, la teoría de los vínculos continuos en el duelo y los mecanismos de legado de Apple y Google.

Con ello proponemos una arquitectura de memoria en tres temperaturas, con reglas para enfriar, calentar, heredar y retirar recuerdos, y la leemos con *After Yang*. Es un trabajo conceptual y sin datos propios: la arquitectura es una hipótesis de diseño, no un sistema construido ni auditado.

Palabras clave: memoria personal; custodia de claves; cartera fría; recuperación social; blockchain; RGPD; duelo digital; deadbots; After Yang.

1. Introducción

En *After Yang*, la memoria de un androide aparece cuando él ya no funciona. Su familia descubre que Yang guardaba fragmentos de su vida, que el fabricante lo había negado y que esos recuerdos contienen a otras personas. Deciden conservarlos y compartirlos [1]. La película pregunta, sin decirlo, quién custodia una memoria cuando su portador falta [INT].

Los agentes conversacionales empiezan a recordar a sus usuarios [2, 3], y el documento compañero DM-2026-10 revisa cómo [4]. Este documento se ocupa de lo que viene después de recordar: proteger, autorizar, heredar y retirar. El mundo de las criptomonedas lleva más de una década resolviendo un problema parecido, custodiar un secreto valioso que no puede reponerse si se pierde, y ha producido un vocabulario útil [INT].

1.1. Contribuciones

1. Una revisión del estado del arte en custodia de claves, registros distribuidos con datos personales y memoria de personas fallecidas.
2. Una correspondencia explícita entre conceptos de carteras y conceptos de memoria, con sus límites.
3. Una arquitectura de memoria en tres temperaturas, con reglas de transición y un esquema de herencia con umbral.
4. Una lectura de *After Yang* como caso de custodia y legado.

2. Custodia de claves en criptomonedas

2.1. Caliente y frío

En la práctica del sector, una cartera es caliente cuando la clave privada está en un dispositivo conectado a internet y fría cuando la clave permanece desconectada; para firmar desde una cartera fría, la transacción sin firmar se lleva al dispositivo desconectado, se aprueba allí y la transacción firmada vuelve a un dispositivo conectado para emitirse [5]. No encontramos una definición normativa; usamos la de la práctica [DEF]. La cartera caliente es cómoda y está más expuesta; la fría es incómoda y más segura.

2.2. El problema es humano

Eskandari y colaboradores evaluaron la gestión de claves de seis clientes de Bitcoin y concluyeron que comparte los problemas clásicos de gestión de claves de otros dominios, aunque podría ser una oportunidad para repensarla para usuarios finales [6] [EMP]. Una frase semilla protege contra la pérdida pero no contra el robo, y conservarla sin perderla exige un esfuerzo continuo [7].

2.3. Compartir el secreto

Shamir propuso dividir un secreto S en n partes de modo que cualquier grupo de k partes lo reconstruya y ningún grupo de $k-1$ obtenga información sobre él [8]. Se elige un polinomio aleatorio de grado $k-1$ cuyo término independiente es el secreto,

$$\begin{aligned} q(x) &= S + a_1 x + \cdots + a_{k-1} x^{k-1}, \\ D_i &= q(i), \quad i = 1, \ldots, n, \end{aligned} \tag{1}$$

y k puntos cualesquiera determinan q y, con él, $S = q(0)$ [DEF].

2.4. Recuperación social

Buterin defiende las carteras con recuperación social: una clave de firma para el uso diario y un conjunto de guardianes, al menos tres, cuya mayoría puede sustituir la clave si se pierde; añadir o quitar guardianes exige

una espera de días, y ningún guardián puede mover fondos por su cuenta [7]. El ejemplo que da es de siete guardianes con un umbral de cuatro.

3. Registros distribuidos y protección de datos

Un registro como el de Bitcoin ordena transacciones en bloques encadenados con sellos de tiempo, de modo que alterar el pasado resulta muy costoso [9]. Esa inmutabilidad, que es su virtud, choca con el derecho a la supresión del Reglamento general de protección de datos [10].

Las directrices 02/2025 del Comité Europeo de Protección de Datos, en su versión 2.0 adoptada el 7 de julio de 2026, piden aplicar desde el diseño la minimización de datos, la limitación del plazo de conservación y el ejercicio efectivo de los derechos de supresión y rectificación. Describen el almacenamiento fuera de la cadena, con solo una referencia en la transacción; señalan que cifrar los datos en la cadena limita el acceso a quien tiene la clave sin descartar filtraciones; y mencionan funciones de derivación de claves, códigos de autenticación de mensajes con clave (HMAC) u otras funciones unidireccionales para poner en la cadena solo valores obtenidos con una clave secreta, guardando los datos originales fuera [11] [FAB].

La lectura para la memoria es clara [INT]: un recuerdo nunca va a una cadena. A lo sumo va una huella con clave que permite demostrar, más tarde, que un recuerdo existía en una fecha y no se ha alterado,

$$h = \mathrm{HMAC}_K(m \,\|\, t), \tag{2}$$

donde m es el recuerdo, t su fecha y K una clave que custodia la persona. Si m se borra fuera de la cadena y K se destruye, h deja de poder vincularse a nadie; que eso baste como supresión depende del caso y del análisis jurídico, no de este documento [HIP].

Las credenciales verificables del W3C, recomendación desde mayo de 2025, definen un emisor que hace afirmaciones y las firma, un titular que las conserva y presenta, y un verificador que las comprueba criptográficamente [12] [DEF]. Proponemos usarlas para el consentimiento: la persona emite una credencial que autoriza a un agente a recordar con un alcance y una caducidad; el agente la presenta al guardar; cualquiera puede verificarla y la persona puede revocarla [HIP].

4. La memoria de quienes ya no están

Öhman y Floridi distinguen cuatro tipos de servicios en la industria del más allá digital: gestión de información, mensajes póstumos, memoriales en línea y servicios de recreación que generan mensajes nuevos imitando al fallecido; proponen tomar como base ética los códigos con que los museos tratan los restos humanos [13]. Hollanek y Nowaczyk-Basińska estudian los deadbots o griefbots mediante ficción de diseño y, según la nota de su centro y la prensa, piden consentimiento explícito de la persona antes de que sus datos alimenten un deadbot, transparencia de que se habla con una IA, protección de menores, procedimientos dignos para retirar estos sistemas y atención a los derechos de los vivos, no solo del fallecido [14, 15]. Lindemann desplaza la discusión de la dignidad del fallecido a la dignidad y la autonomía de quienes están de duelo [16]. La teoría de los vínculos continuos, frente al modelo de desapego, sostiene que el duelo puede incluir mantener una relación con quien murió [17] [EMP]; eso explica el atractivo de estos sistemas y también su riesgo [INT].

Las plataformas ya tienen mecanismos de herencia. Apple permite designar contactos de legado: la persona genera una clave de acceso que entrega a su contacto, quien la necesita, junto con un certificado de defunción, para solicitar el acceso; quedan fuera las compras de contenidos y el llavero de iCloud, y cada contacto puede tomar decisiones sobre los datos, incluido borrarlos [18, 19] [FAB]. El gestor de cuentas inactivas de Google avisa tras un periodo de inactividad y deja que contactos de confianza descarguen los datos elegidos [20]. Son, en nuestros términos, carteras frías con un heredero: una clave fuera de línea y una prueba del fallecimiento [INT].

En Europa, el Reglamento de inteligencia artificial obliga a informar a las personas de que interactúan con una IA [21]. El Reglamento general de protección de datos no se aplica a los datos de personas fallecidas [10], por lo que la custodia de esa memoria queda hoy, en gran parte, en manos de contratos y plataformas [INT].

5. Correspondencia entre carteras y memoria

La tabla 1 recoge la correspondencia. La analogía funciona en la custodia y falla en la naturaleza del bien [INT]: el dinero se mueve, el recuerdo se copia; el dinero es de uno, el recuerdo es de varios.

6. Una arquitectura en tres temperaturas

Proponemos tres temperaturas de memoria [HIP], ilustradas en la figura 1.

- *Caliente.* Lo dicho en la conversación en curso. La lee el agente. Caduca al terminar salvo que se guarde con permiso. En GAIA es la única temperatura que existe para los visitantes.
- *Templada.* La memoria de una persona que ha consentido ser recordada, cifrada y revocable, etiquetada con alcance, procedencia y caducidad (DM-2026-10). El agente la lee cuando la conversación lo necesita.
- *Fría.* Una bóveda cifrada con claves que custodia la persona, fuera del alcance del agente. Guarda lo que la persona quiere conservar pero no usar a diario: relatos, voz, recuerdos de otros. Calentar un recuerdo exige una firma explícita.

Reglas de transición [HIP]:

1. Nada pasa de caliente a templada sin consentimiento verificable.

Tabla 1. Correspondencia entre conceptos de custodia de criptomonedas y de memoria personal. La columna de límites es tan importante como la de equivalencias.

Cripto	Memoria	Límite de la analogía
Cartera caliente	Memoria que el agente puede leer en la conversación	Un recuerdo no se gasta; puede copiarse sin que el dueño lo sepa
Cartera fría	Bóveda cifrada fuera del alcance del agente	Abrirla no es firmar una transacción: es dejar que alguien vea
Clave privada y semilla	Clave maestra de la memoria de una persona	Si se pierde, la memoria fría se pierde con ella
Firmar una transacción	Autorizar que un recuerdo se caliente o se comparta	La autorización debe tener alcance y caducidad
Guardianes, umbral k de n	Custodios que pueden abrir la bóveda tras el fallecimiento	Los herederos no son neutrales; también aparecen en los recuerdos
Registro inmutable	Huellas con clave que prueban existencia e integridad	El contenido nunca va a la cadena; inmutable choca con supresión
Credencial del titular	Consentimiento verificable y revocable	Revocar no borra copias ya hechas

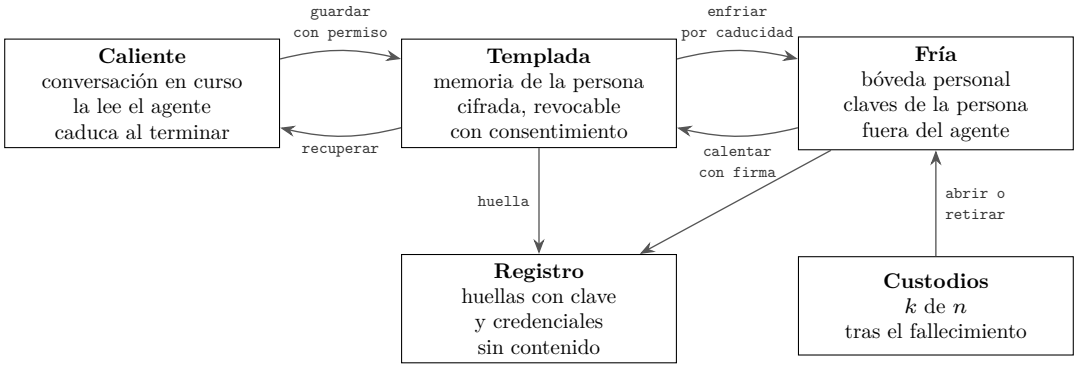


Figura 1. Arquitectura de memoria en tres temperaturas. El agente solo lee la memoria caliente y, con permiso, la templada; la fría solo se abre con la firma de la persona o, tras su fallecimiento, de un umbral de custodios.

2. Lo templado se enfría al caducar; no se borra salvo que la persona lo pida.
3. Lo frío se calienta solo con la firma de la persona y con un alcance limitado.
4. Lo que menciona a terceros se guarda resumido, nunca en su forma literal.
5. Cada transición deja una huella con clave en el registro, sin contenido.
6. Al fallecer la persona, la bóveda se sella. Un umbral de custodios, k de n según la ecuación (1), puede abrirla, conservar recuerdos elegidos, compartirlos o retirarla con un procedimiento digno. Ningún custodio decide solo.
7. Un deadbot no se construye por defecto: requiere que la persona lo haya autorizado en vida, de forma explícita y separada.

Con siete custodios y umbral cuatro, como en el ejemplo de Buterin, la apertura resiste la pérdida de tres claves y la colusión de tres custodios [7] [DEF].

7. After Yang, leído como custodia

La familia de Yang hace, sin protocolo, lo que la arquitectura propone [INT]. Descubre una memoria que el fabricante ocultó, es decir, una memoria sin consentimiento. La abre gracias a un técnico y a una especialista de museo, terceros sin mandato. Encuentra a Ada en los recuerdos, alguien que no aceptó estar ahí. Y decide, al final, conservar y compartir esos recuerdos con quienes Yang importó, sin exhibir su cuerpo [1]. Ese gesto final es la regla 6: un umbral de personas que deciden juntas qué hacer con una memoria cuando su portador ya no está.

8. Amenazas a la validez

- Revisión dirigida, sin datos propios ni sistema construido.
- La definición de cartera fría y caliente procede de la práctica del sector, no de un estándar.
- Las recomendaciones de Hollanek y Nowaczyk-Basińska se tomaron de la nota de su centro y de la prensa, no del texto completo.
- La lectura jurídica sobre supresión y destrucción de claves es una hipótesis; requiere análisis legal.
- La analogía entre dinero y recuerdo tiene límites estructurales, recogidos en la tabla 1.

9. Recomendaciones para la comunidad

1. Separar memoria caliente, templada y fría, y declarar quién tiene la llave de cada una.
2. No poner recuerdos en una cadena; como mucho, huellas con clave.
3. Pedir consentimiento verificable, con alcance y caducidad, antes de recordar a una persona.

4. Diseñar la herencia antes del fallecimiento: custodios, umbral y procedimiento de retiro.
5. No construir representaciones de personas fallecidas sin su autorización expresa en vida.

10. Conclusiones

La memoria de un agente será tan digna de confianza como la custodia de sus llaves. Las carteras de criptomonedas ofrecen un vocabulario probado para esa custodia; la protección de datos marca sus límites; y la ética del duelo digital recuerda que una memoria nunca es solo de quien la guarda. Entre lo caliente y lo frío, entre recordar y retirar, hay espacio para diseñar una trascendencia que no sea una imitación, sino un legado custodiado.

Firman. Cris Olmedo y Kurt Sommer, Grupo de investigación Divina Machina. *Cómo citar*: Olmedo, C. y Sommer, K. (2026). Memoria fría y memoria caliente. Documento de trabajo DM-2026-11, v 1.0. Grupo de investigación Divina Machina. Divina Machina by Qs Ventures.

Referencias

Fuentes consultadas hasta el 1 de noviembre de 2026.

[1] Wikipedia. After Yang. Artículo en inglés. URL https://en.wikipedia.org/wiki/After_Yang. Ficha, reparto, fuente literaria y argumento.

[2] OpenAI. Memory and new controls for ChatGPT, 2025. URL https://openai.com/index/memory-and-new-controls-for-chatgpt/. Actualización de abril de 2025.

[3] Bloomberg. Anthropic tries to win users from ChatGPT with memory feature, March 2026. URL https://www.bloomberg.com/news/articles/2026-03-03/anthropic-tries-to-win-users-from-chatgpt-with-memory-feature.

[4] C. Olmedo and K. Sommer. Lo que guarda Yang. memoria de agentes conversacionales. Documento de trabajo DM-2026-10. Grupo de investigación Divina Machina, 2026.

[5] Ripple. Cold wallet and hot wallet. Ripple Learn. URL https://ripple.com/learn/cold-wallet-and-hot-wallet/. Definición de práctica, no estándar.

[6] S. Eskandari, D. Barrera, E. Stobert, and J. Clark. A first look at the usability of Bitcoin key management. In *Workshop on Usable Security (USEC 2015), NDSS*, 2015. URL https://arxiv.org/abs/1802.04351.

[7] V. Buterin. Why we need wide adoption of social recovery wallets. Blog personal, January 2021. URL https://vitalik.eth.limo/general/2021/01/11/recovery.html.

[8] A. Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979. doi: 10.1145/359168.359176.

[9] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2008. URL https://bitcoin.org/bitcoin.pdf.

[10] Parlamento Europeo y Consejo. Reglamento (UE) 2016/679, reglamento general de protección de datos. Diario Oficial de la Unión Europea, L 119, 2016. URL https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[11] European Data Protection Board. Guidelines 02/2025 on processing of personal data through blockchain technologies. Versión 2.0, adoptada el 7 de julio de 2026, 2026. URL https://www.edpb.europa.eu/system/files/2026-07/edpb_guidelines_202502_blockchain_v2_en.pdf.

[12] M. Sporny, T. Thibodeau Jr, I. Herman, G. Cohen, and M. B. Jones. Verifiable credentials data model v2.0. W3C Recommendation, 15 de mayo de 2025, 2025. URL https://www.w3.org/TR/vc-data-model-2.0/.

[13] C. Öhman and L. Floridi. An ethical framework for the digital afterlife industry. *Nature Human Behaviour*, 2(5):318–320, 2018.

[14] T. Hollanek and K. Nowaczyk-Basińska. Griefbots, deadbots, postmortem avatars. on responsible applications of generative AI in the digital afterlife industry. *Philosophy & Technology*, 37 (2), 2024. doi: 10.1007/s13347-024-00744-w. Recomendaciones consultadas a través de la nota del Leverhulme Centre y prensa; texto completo no accesible en la consulta.

[15] Leverhulme Centre for the Future of Intelligence. Deathbots, griefbots and the digital afterlife. Nota de la Universidad de Cambridge, 2024. URL https://lcfi.ac.uk/news-events/news/deathbots-griefbots-and-the-digital-afterlife.

[16] N. F. Lindemann. The ethics of 'deathbots'. *Science and Engineering Ethics*, 28, 2022. doi: 10.1007/s11948-022-00417-x. URL https://pmc.ncbi.nlm.nih.gov/articles/PMC9684218/.

[17] D. Klass, P. R. Silverman, and S. L. Nickman, editors. *Continuing Bonds. New Understandings of Grief*. Taylor & Francis, Washington, DC, 1996.

[18] Apple. How to add a Legacy Contact for your Apple Account. Apple Support 102631, s. f. URL https://support.apple.com/102631.

[19] Apple. Request access to an Apple Account as a Legacy Contact. Apple Support 102678, s. f. URL https://support.apple.com/102678.

[20] University of Manitoba. Digital death directory. google. Ficha de la plataforma. URL https://digitaldeathdirectory.cs.umanitoba.ca/platforms/google. Descripción secundaria del Gestor de cuentas inactivas de Google.

[21] Parlamento Europeo y Consejo. Reglamento (UE) 2024/1689, reglamento de inteligencia artificial. Diario Oficial de la Unión Europea, 2024. URL https://eur-lex.europa.eu/eli/reg/2024/1689/oj.