Cold memory and hot memory

Custody, encryption and transcendence of personal memories

Cris Olmedo and Kurt Sommer
Divina Machina Research Group

Working paper · State of the art and proposal
DM-2026-11, version 1.0 · 1 November 2026

Abstract. When an agent remembers a person, the decisive question is not where the memory is kept, but who holds the key. We propose to think about personal memory with the vocabulary of cryptocurrency wallets: a hot memory, online and within the agent's reach, and a cold memory, encrypted and out of its reach, which opens only with its owner's signature or, once the owner is gone, with that of their custodians.

We review the state of the art on three fronts. In key custody: cold and hot wallets, usability problems, secret sharing and social recovery. In distributed ledgers and data protection: the 2026 European guidelines on blockchain recommend keeping personal data off-chain, and W3C verifiable credentials offer an issuer, holder and verifier model. In the memory of those who are gone: the digital afterlife industry, the ethics of deadbots, the theory of continuing bonds in grief and Apple's and Google's legacy mechanisms.

On that basis we propose a three-temperature memory architecture, with rules for cooling, warming, inheriting and retiring memories, and we read it through *After Yang*. This is conceptual work without own data: the architecture is a design hypothesis, not a built or audited system.

Keywords: personal memory; key custody; cold wallet; social recovery; blockchain; GDPR; digital grief; deadbots; After Yang.

1. Introduction

In *After Yang*, an android's memory appears when he no longer works. His family discovers that Yang kept fragments of his life, that the manufacturer had denied it and that those memories contain other people. They decide to preserve and share them [1]. Without saying so, the film asks who holds custody of a memory when its bearer is gone [INT].

Conversational agents are beginning to remember their users [2, 3], and the companion paper DM-2026-10 reviews how [4]. This paper deals with what comes after remembering: protecting, authorising, inheriting and retiring. The cryptocurrency world has spent more than a decade solving a similar problem, holding a valuable secret that cannot be replaced if lost, and it has produced a useful vocabulary [INT].

1.1. Contributions

1. A review of the state of the art in key custody, distributed ledgers holding personal data and the memory of deceased people.
2. An explicit mapping between wallet concepts and memory concepts, with its limits.
3. A three-temperature memory architecture, with transition rules and a threshold inheritance scheme.
4. A reading of *After Yang* as a case of custody and legacy.

2. Key custody in cryptocurrencies

2.1. Hot and cold

In industry practice, a wallet is hot when the private key sits on an internet-connected device and cold when the key stays offline; to sign from a cold wallet, the unsigned transaction is taken to the offline device, approved there, and the signed transaction returns to a connected device to be broadcast [5]. We found no normative definition; we use the practitioners' one [DEF]. The hot wallet is convenient and more exposed; the cold one is inconvenient and safer.

2.2. The problem is human

Eskandari and colleagues evaluated key management in six Bitcoin clients and concluded that it shares the classic key-management problems of other domains, although it could be an opportunity to rethink it for end users [6] [EMP]. A seed phrase protects against loss but not against theft, and keeping it without losing it requires continuous effort [7].

2.3. Sharing the secret

Shamir proposed splitting a secret S into n shares so that any group of k shares reconstructs it and no group of $k-1$ obtains any information about it [8]. A random polynomial of degree $k-1$ is chosen whose constant term is the secret,

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

and any k points determine q and, with it, $S = q(0)$ [DEF].

2.4. Social recovery

Buterin advocates wallets with social recovery: a signing key for daily use and a set of guardians, at least three, a majority of whom can replace the key if it is lost; adding or removing guardians requires a delay of days, and no guardian can move funds on their own [7]. His example uses seven guardians with a threshold of four.

3. Distributed ledgers and data protection

A ledger such as Bitcoin's orders transactions into timestamped chained blocks, so that altering the past becomes very costly [9]. That immutability, its virtue, clashes with the right to erasure in the General Data Protection Regulation [10].

Guidelines 02/2025 of the European Data Protection Board, in version 2.0 adopted on 7 July 2026, call for data minimisation, storage limitation and the effective exercise of the rights to erasure and rectification to be applied by design. They describe off-chain storage, with only a reference in the transaction; they note that encrypting data on-chain limits access to whoever holds the key without ruling out breaches; and they mention key derivation functions, keyed message authentication codes (HMAC) or other one-way functions so that only values obtained with a secret key are placed on-chain, keeping the original data off-chain [11] [FAB].

The reading for memory is clear [INT]: a memory never goes on a chain. At most a keyed fingerprint goes there, allowing one to prove later that a memory existed at a given date and has not been altered,

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

where m is the memory, t its date and K a key held by the person. If m is deleted off-chain and K is destroyed, h can no longer be linked to anyone; whether that suffices as erasure depends on the case and on legal analysis, not on this paper [HIP].

W3C verifiable credentials, a Recommendation since May 2025, define an issuer who makes and signs claims, a holder who keeps and presents them, and a verifier who checks them cryptographically [12] [DEF]. We propose using them for consent: the person issues a credential authorising an agent to remember with a scope and an expiry; the agent presents it when storing; anyone can verify it and the person can revoke it [HIP].

4. The memory of those who are gone

Öhman and Floridi distinguish four types of services in the digital afterlife industry: information management, posthumous messaging, online memorials and recreation services that generate new messages imitating the deceased; they propose taking as an ethical basis the codes museums use for human remains [13]. Hollanek and Nowaczyk-Basińska study deadbots or griefbots through design fiction and, according to their centre's release and the press, call for the person's explicit consent before their data feed a deadbot, transparency that one is talking to an AI, protection of minors, dignified procedures for retiring these systems and attention to the rights of the living, not only of the deceased [14, 15]. Lindemann shifts the discussion from the dignity of the deceased to the dignity and autonomy of the bereaved [16]. The theory of continuing bonds, as opposed to the detachment model, holds that grief can include maintaining a relationship with the person who died [17] [EMP]; that explains both the appeal of these systems and their risk [INT].

Platforms already have inheritance mechanisms. Apple lets people designate legacy contacts: the person generates an access key they give to their contact, who needs it, together with a death certificate, to request access; content purchases and iCloud Keychain are excluded, and each contact can make decisions about the data, including deleting it [18, 19] [FAB]. Google's Inactive Account Manager sends notices after a period of inactivity and lets trusted contacts download the selected data [20]. In our terms, they are cold wallets with an heir: an offline key and proof of death [INT].

In Europe, the Artificial Intelligence Act requires people to be informed that they are interacting with an AI [21]. The General Data Protection Regulation does not apply to the data of deceased persons [10], so the custody of that memory currently lies, to a large extent, in the hands of contracts and platforms [INT].

5. Mapping wallets to memory

Table 1 sets out the mapping. The analogy works for custody and fails on the nature of the asset [INT]: money moves, memories are copied; money belongs to one person, a memory belongs to several.

6. A three-temperature architecture

We propose three memory temperatures [HIP], illustrated in Figure 1.

- *Hot.* What is said in the ongoing conversation. The agent reads it. It expires at the end unless stored with permission. In GAIA it is the only temperature that exists for visitors.
- *Warm.* The memory of a person who has consented to be remembered, encrypted and revocable, tagged with scope, provenance and expiry (DM-2026-10). The agent reads it when the conversation needs it.
- *Cold.* An encrypted vault with keys held by the person, out of the agent's reach. It keeps what the person wants to preserve but not use every day: stories, voice, memories of others. Warming a memory requires an explicit signature.

Transition rules [HIP]:

1. Nothing moves from hot to warm without verifiable consent.
2. Warm memory cools on expiry; it is not deleted unless the person asks.
3. Cold memory is warmed only with the person's signature and with a limited scope.
4. Whatever mentions third parties is stored in summary form, never verbatim.
5. Each transition leaves a keyed fingerprint in the ledger, without content.
6. When the person dies, the vault is sealed. A threshold of custodians, k of n according to Equation (1), can open it, preserve chosen memories, share them

Table 1. Mapping between cryptocurrency custody concepts and personal memory concepts. The limits column matters as much as the equivalences.

Crypto	Memory	Limit of the analogy
Hot wallet	Memory the agent can read in the conversation	A memory is not spent; it can be copied without the owner knowing
Cold wallet	Encrypted vault out of the agent's reach	Opening it is not signing a transaction: it is letting someone see
Private key and seed	Master key of a person's memory	If it is lost, the cold memory is lost with it
Signing a transaction	Authorising a memory to be warmed or shared	The authorisation must have a scope and an expiry
Guardians, threshold k of n	Custodians who can open the vault after death	Heirs are not neutral; they also appear in the memories
Immutable ledger	Keyed fingerprints proving existence and integrity	Content never goes on the chain; immutability clashes with erasure
Holder credential	Verifiable, revocable consent	Revoking does not delete copies already made

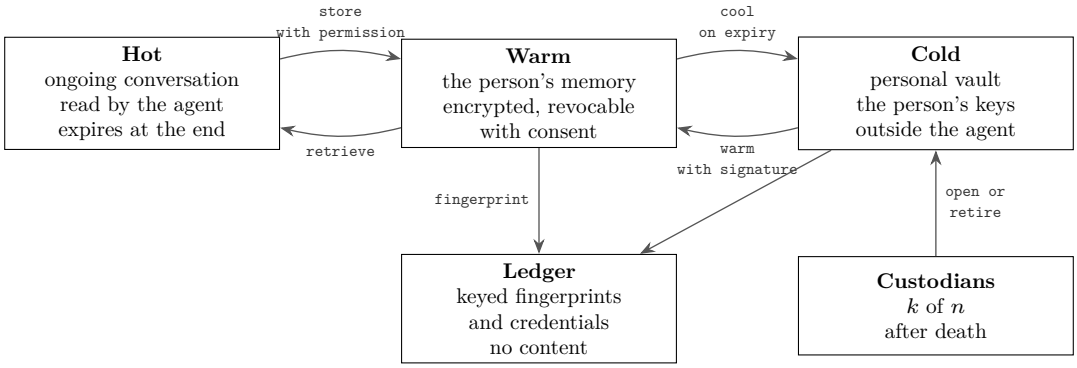


Figure 1. Three-temperature memory architecture. The agent reads only hot memory and, with permission, warm memory; cold memory opens only with the person's signature or, after their death, that of a threshold of custodians.

or retire it through a dignified procedure. No custodian decides alone.

7. A deadbot is not built by default: it requires the person to have authorised it during their lifetime, explicitly and separately.

With seven custodians and a threshold of four, as in Buterin's example, opening the vault withstands the loss of three keys and collusion by three custodians [7] [DEF].

7. After Yang, read as custody

Yang's family does, without a protocol, what the architecture proposes [INT]. It discovers a memory the manufacturer hid, that is, a memory without consent. It opens it thanks to a technician and a museum specialist, third parties without a mandate. It finds Ada in the memories, someone who did not agree to be there. And in the end it decides to preserve and share those memories with the people to whom Yang mattered, without displaying his body [1]. That final gesture is rule 6: a threshold of people who decide together what to do with a memory when its bearer is gone.

8. Threats to validity

- Targeted review, without own data or a built system.
- The definition of cold and hot wallets comes from industry practice, not from a standard.
- Hollanek and Nowaczyk-Basińska's recommendations were taken from their centre's release and the press, not from the full text.
- The legal reading on erasure and key destruction is a hypothesis; it requires legal analysis.
- The analogy between money and memory has structural limits, set out in Table 1.

9. Recommendations for the community

1. Separate hot, warm and cold memory, and declare who holds the key to each.
2. Do not put memories on a chain; at most, keyed fingerprints.
3. Ask for verifiable consent, with scope and expiry, before remembering a person.
4. Design inheritance before death: custodians, threshold and retirement procedure.
5. Do not build representations of deceased people without their express authorisation during their lifetime.

10. Conclusions

An agent's memory will be as trustworthy as the custody of its keys. Cryptocurrency wallets offer a proven vocabulary for that custody; data protection sets its limits; and the ethics of digital grief reminds us that

a memory never belongs only to whoever keeps it. Between hot and cold, between remembering and retiring, there is room to design a transcendence that is not an imitation, but a legacy held in custody.

Signed. Cris Olmedo and Kurt Sommer, Divina Machina Research Group. *How to cite*: Olmedo, C. and Sommer, K. (2026). Cold memory and hot memory. Working paper DM-2026-11, v 1.0. Divina Machina Research Group. Divina Machina by Qs Ventures.

References

Sources consulted up to 1 November 2026.

[1] Wikipedia. After Yang. English-language article. URL https://en.wikipedia.org/wiki/After_Yang. Credits, cast, source material and plot.

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

[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. What Yang keeps. memory in conversational agents. Working paper DM-2026-10. Divina Machina Research Group, 2026.

[5] Ripple. Cold wallet and hot wallet. Ripple Learn. URL https://ripple.com/learn/cold-wallet-and-hot-wallet/. Practitioner definition, not a standard.

[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. Personal blog, 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] European Parliament and Council. Regulation (EU) 2016/679, General Data Protection Regulation. Official Journal of the European Union, 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. Version 2.0, adopted 7 July 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 May 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. Recommendations consulted via the Leverhulme Centre release and press; full text not accessible at the time of consultation.

[15] Leverhulme Centre for the Future of Intelligence. Deathbots, griefbots and the digital afterlife. University of Cambridge news release, 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, n.d.. URL https://support.apple.com/102631.

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

[20] University of Manitoba. Digital death directory. google. Platform entry. URL https://digitaldeathdirectory.cs.umanitoba.ca/platforms/google. Secondary description of Google's Inactive Account Manager.

[21] European Parliament and Council. Regulation (EU) 2024/1689, Artificial Intelligence Act. Official Journal of the European Union, 2024. URL https://eur-lex.europa.eu/eli/reg/2024/1689/oj.