TECHNICAL WHITE PAPER · VERSION 2.0 · NOVEMBER 2026

The Sovereign Memory Architecture.

Sovereign Personal AI, the ETERNITY network, Bitcoin proof, Ethereum succession and generational memory transmission.

YOUR MEMORY. YOUR INTELLIGENCE. YOUR LEGACY.

BOTTLE ON THE SEA
Preserving Humanity's Memory

Status: pre-seed, closed development. Describes a proposed architecture — not a live, deployed or audited service.
Bottle on the Sea Sp. z o.o. · KRS 0001268323 · bottleonthesea.com

01

Executive summary

A life should never disappear. Yet the photos, voices, letters and values that make a person who they are sit today in accounts governed by terms of service, tied to a single provider and frequently lost when their owner dies or the provider changes course.

Bottle on the Sea is developing a **sovereign digital memory infrastructure**. Its purpose is to let individuals preserve, understand, protect and transmit their personal memories across generations, by combining five interconnected components:

— **Sovereign Personal AI** — an intelligence that knows you, without owning you.

— **ETERNITY network** — decentralised, encrypted storage across independent nodes.

— **Bitcoin** — permanent, independent cryptographic proof of integrity.

— **Ethereum** — programmable authorisation and digital succession.

— **Generational memory transmission** — what you leave behind should not disappear with you.

Bottle on the Sea is not another AI chatbot or storage service. It is an infrastructure in which individuals keep control of their memories, their encryption keys and the conditions under which their legacy is transmitted.

> **Honest scope.** Bottle on the Sea is pre-seed and in closed development. No live vault service is operating. Every section distinguishes existing technologies, proposed architecture, work in development and future capabilities. Nothing here is presented as an operational product, and nothing is claimed to be unhackable or guaranteed forever.

Label	Meaning
Existing technology	Proven, publicly available technology we build on.
Proposed architecture	Our design, documented here, not yet implemented end-to-end.
In development	Being engineered now in closed development or pilots.
Future capability	Long-term research or roadmap item; not promised for the first vault.

02

Founding principles

Principle	Design commitment
Your memory belongs to you	Data is encrypted on the owner's device. The operator never holds a usable key and cannot read the vault.
An intelligence that knows you, without owning you	The Personal AI reasons only over authorised material, never trains shared models and labels every answer Said, Inferred or Unknown.
Decentralised by trust, not by hype	Decentralisation is used only where it removes a single point of failure or control: storage, key custody, integrity anchoring.
Your keys, your legacy	Transmission follows conditions the owner writes. Keys are released only through verified, multi-party processes.
Portability and continuity	Open formats, data export at any time, and an exit-proof protocol designed to keep vaults recoverable if the company disappears.

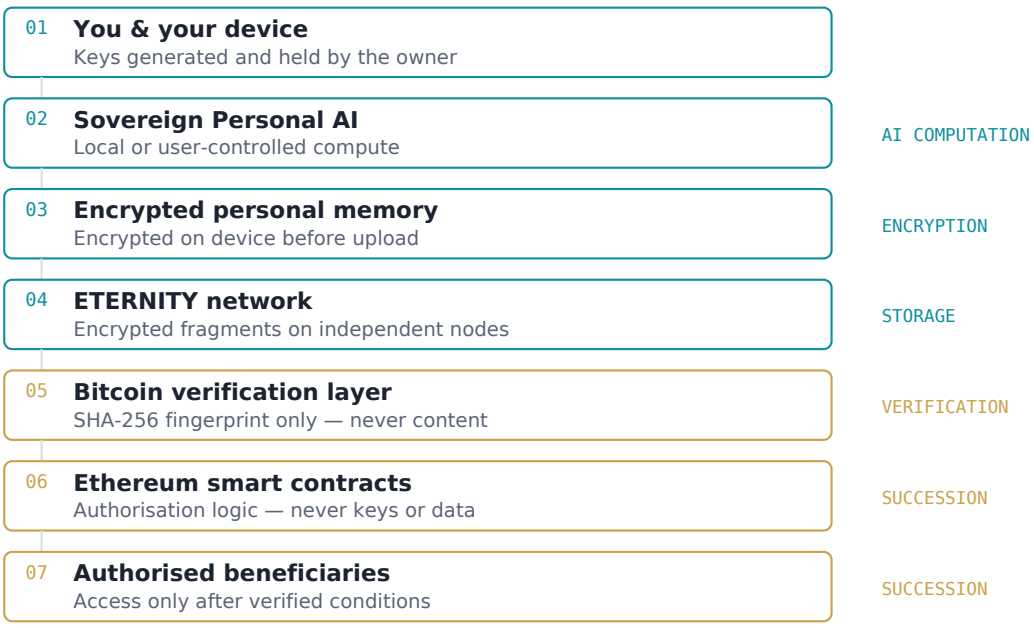
Three legacies, one vault

The vault is designed to carry an emotional legacy (memories, voices, moments), an intellectual legacy (knowledge, experience, reasoning) and a moral legacy (values, convictions, intentions). The aim is not simply to preserve files, but the human context, knowledge and personality behind them.

Like a hive that survives the loss of any single bee, a vault should never depend on one server, one company or one person.

Architecture overview

The diagram separates AI computation, encryption, storage, blockchain verification and digital succession. Information flows top to bottom; no blockchain ever stores personal memory files.



03

Sovereign Personal AI

STATUS · IN DEVELOPMENT

The objective is a personal AI that operates independently from external AI providers. It is designed to run locally on the owner's device, or within a user-controlled computing environment, and to read the owner's encrypted memory without sending personal conversations to third-party AI APIs.

— **Personal AI** — one intelligence per person, built from their memories, voice, values and reasoning.

— **Local inference** — on-device models where hardware allows; quantised open-weight models are the primary candidates.

— **Private memory** — retrieval over the decrypted vault happens only inside the owner's environment.

— **User-controlled intelligence** — the owner decides what the AI may read, and can revoke it.

— **Independence from external AI APIs** — no default dependence on outside providers for personal memory processing.

> Not every device can run every AI model locally today. Heavier tasks will use isolated, ephemeral compute that the owner controls. During closed development, the private web app uses a secure AI service under a no-retention arrangement; replacing it with sovereign inference is part of this roadmap.

The truth-grounding protocol

Label	Meaning
SAID	A direct quote or documented fact from the archive, with its source cited.
INFERRED	An interpretation explicitly permitted by the owner's documented values — always marked as such.
UNKNOWN	The archive does not contain the answer. The AI says so rather than invent one.

The AI speaks *about* a person, from their sources. It never claims to be them, and owner data is excluded from every machine-learning training pipeline.

04

ETERNITY network architecture

STATUS · PROPOSED ARCHITECTURE · IN DEVELOPMENT

ETERNITY is the decentralised storage infrastructure being developed for Bottle on the Sea. Its purpose is to reduce dependence on centralised storage providers while ensuring that network participants never have access to original, unencrypted memories.

Stage	Mechanism
1 · Encrypt	Data is encrypted on the user's device before it leaves it.
2 · Fragment	Ciphertext is split into fragments with erasure coding, so the whole can be rebuilt from a subset.
3 · Distribute	Fragments are placed on independent nodes run by separate operators, across jurisdictions.
4 · Verify	Nodes periodically prove they still hold their fragments; integrity is checked cryptographically.
5 · Retrieve	The owner or an authorised beneficiary collects enough fragments, verifies them and reconstructs the ciphertext locally.
6 · Decrypt	Decryption happens only on the authorised device, with user-controlled keys.

Decentralised storage is not durable by default. It requires redundancy above the expected node-loss rate, incentives that keep operators online, continuous monitoring, repair of lost fragments and documented recovery procedures. All five are part of the ETERNITY design and will be validated in pilots before any launch.

05

Encryption and key management

Device-side encryption

EXISTING TECHNOLOGY — All media, text and voice data are designed to be encrypted locally with AES-256-GCM (or ChaCha20-Poly1305 on mobile hardware) before transmission. The Data Encryption Key is generated on the device and never leaves it in plaintext.

Key custody — Shamir's Secret Sharing (3 of 5)

PROPOSED ARCHITECTURE — The master key is never stored whole. It is split into five fragments; any three reconstruct it, any two reveal nothing.

Share	Holder & release condition
1 · Owner	The owner's primary trusted device, optionally a hardware key.
2 · Beneficiary	Encrypted escrow, releasable only once transmission conditions are verified.
3 · Independent custodian	A regulated party such as a notarial practice or an EU digital trust.
4 · Distributed network	Held in ETERNITY with time-locked release conditions.
5 · Operator escrow	Held by Bottle on the Sea — useless without two other shares.

Recovery and post-quantum readiness

— Secure recovery through the owner's own shares, without the operator ever seeing a usable key.

— Standards-aligned with NIST FIPS 203, 204 and 205 (ML-KEM, ML-DSA, SLH-DSA), hybrid with classical algorithms during migration.

— Crypto-agile key wrapping: algorithms can change without decrypting archive content.

06

Decentralised storage

Storage is separated into layers so that no single party controls confidentiality, integrity and availability at once.

Layer	Role	What it never holds
Owner device	Encryption, keys, local AI	—
ETERNITY nodes	Encrypted fragments, proofs of storage	Plaintext, keys
Operator services	Coordination, account, pilot hosting	Usable decryption keys
Bitcoin	Integrity fingerprints	Memories, personal data
Ethereum	Authorisation records	Memories, keys, personal data

Long-term preservation

— Open formats: PDF/A, FLAC/WAV, MP4, plain text and Markdown.

— Periodic format migration to newer open standards.

— Data portability: the owner can export the full vault at any time.

— Long-horizon research (future capability): DNA-on-silicon and other durable media, adopted only after independent validation; not required for the first vault.

07

Bitcoin integration

EXISTING TECHNOLOGY · INTEGRATION IN DEVELOPMENT

Bitcoin is proposed as an independent verification layer. Its role is to anchor cryptographic fingerprints of selected encrypted memory archives, so that anyone can later verify that an archive existed at a given time and has not been altered.

Encrypted memory → **SHA-256 hash** → **Bitcoin transaction** → **Verifiable proof**

— Personal memories are **never** stored on Bitcoin.

— Only a SHA-256 hash — typically the root of a Merkle tree covering many archives — is recorded in a transaction.

— The blockchain provides timestamping and tamper-evident proof of existence and integrity.

— Verification needs no trust in Bottle on the Sea: the archive's hash is recomputed and compared to the anchored value.

A hash proves integrity and existence; it does not prove authorship, nor does it make content retrievable. Availability is the role of ETERNITY, not Bitcoin.

08

Ethereum smart contracts

FUTURE CAPABILITY

Ethereum smart contracts can provide programmable authorisation and succession mechanisms: rules written by the owner today, honoured tomorrow, with a public and verifiable record of who was authorised and when.

— Beneficiary designation

— Conditional access

— Digital succession

— Time-based transmission

— Authorised release workflows

— Verifiable authorisation records

No personal information and no encryption key is ever placed in a public smart contract. Beneficiaries are referenced by pseudonymous identifiers. Contracts coordinate authorisation only; secure off-chain mechanisms — the Shamir custodians and the orchestration layer — manage keys and execute the actual transfer of access.

09

Digital succession

The most critical risk in digital legacy is premature — or failed — activation. The owner defines who receives what, and when. A typical high-assurance configuration requires two of three independent signals:

Signal	How it is verified
Temporal	A predefined date or beneficiary age is reached — e.g. a capsule for Julian, opened on his 25th birthday.
Proof-of-life lapse	The owner does not answer out-of-band verification requests over a grace period, e.g. 90 days.
Legal verification	A designated trusted party — a notary or family lawyer — submits a signed declaration of death or incapacity.

Once the threshold is met, the orchestration layer coordinates the release of the required key shares, the vault is decrypted for the beneficiary only, and access is delivered through a verified portal. Bottle on the Sea complements the notary; it does not replace them.

> In the current private app, owners can already designate beneficiaries and schedule transmissions. Automatic delivery is not active yet: nothing is sent.

10

Generational memory transmission

A parent creates a personal digital memory throughout their lifetime. They preserve conversations, photographs, videos, personal experiences, knowledge, reflections and messages. They decide which memories should eventually be accessible to their children, and under which conditions.

When those conditions are fulfilled and verified, an authorised process allows the designated beneficiaries to access the corresponding encrypted memories — and, if the owner allowed it, to ask the Personal AI questions grounded in those memories.

The purpose is not simply to preserve files. It is to preserve the human context, knowledge and personality behind them.

> “What if your children could still learn from your experiences, your stories and your way of seeing the world, long after you are gone?”

11

Security and privacy architecture

Property	Mechanisms
Confidentiality	Client-side encryption; user-controlled keys; zero-knowledge storage where technically applicable; isolated AI processing.
Integrity	Authenticated encryption; hashes per item; Merkle roots anchored on Bitcoin; signed authorisation records.
Availability	Erasure-coded redundancy on independent nodes; monitoring and repair; open formats; export at any time.

— No default dependence on external AI APIs for personal memory processing (target).

— Secure authorisation and recovery through multi-party key custody.

— Personal data never used to train general AI models.

— Any exceptional operator access would be logged and governed.

Continuity & exit-proof commitment

In the event of bankruptcy, acquisition or cessation of operations, the decryption and key-recombination client would be released under an open-source licence, and external key-share holders would be bound to help beneficiaries reconstruct their vaults independently.

> We make no absolute claims such as ‘100% unhackable’, ‘impossible to access’ or ‘guaranteed forever’. Security is a process, validated by independent audit.

12

Technical development roadmap

Phase	Scope	Status
Now · 2026	Private web app (memories, timeline, voice & thoughts, Personal AI with sources, legacy planning); core cryptographic design; Shamir implementation.	In development
2027 · H1	Device-side encryption in production clients; iOS and Android apps; closed pilots with notarial practices and family offices; Bitcoin anchoring pilot.	Proposed
2027 · H2	Independent third-party security audit before any public launch; published report.	Committed
2028	ETERNITY network pilots with independent node operators; on-device Personal AI for capable hardware.	Proposed
2028+	Ethereum-coordinated succession; post-quantum key exchange; long-horizon storage research.	Future capability

Conclusion

Bottle on the Sea is building a sovereign digital memory infrastructure that combines personal artificial intelligence, decentralised storage, cryptographic verification and generational transmission. It proposes a different relationship between humans, artificial intelligence, digital memory and personal freedom: **your memories, your keys, your legacy.**

O. Aleksander, Co-Founder and Project Manager · Bottle on the Sea Sp. z o.o. · KRS 0001268323 · NIP 9512656702 · bottleonthesea.com

13

Five technical decisions

Before presenting the architecture to investors or technical partners, five decisions must be explicit. Each answer below is a **proposed direction**, not a deployed capability.

Topic	Decision	Proposed answer
Local AI	Which models and devices can run the AI?	Quantised small language models (1–3B parameters) on device neural accelerators for indexing, semantic search and fact extraction. Heavier synthesis runs in isolated confidential-computing enclaves (TEE), with memory decrypted only in volatile RAM and no logging. Open memory format (structured JSON + normalised vectors) so model changes never invalidate the archive.
ETERNITY	How to guarantee availability over decades?	Client-side encryption, then Reed-Solomon erasure coding (e.g. any 6 of 10 fragments rebuild the archive) across independent nodes; periodic proofs of retrievability; prepaid preservation endowment funding 20–50 years of retention; offline cold-archive export available at any time.
Cryptography	How to recover if the owner loses their keys?	Shamir secret sharing 3-of-5: owner device (secure enclave), offline backup (BIP-39 style), trusted person 1, trusted person or notary 2, zero-knowledge custody server. No single holder can read data; any three rebuild the key. No central password reset, no backdoor.
Ethereum	How to trigger succession without a single trusted third party?	Hybrid protocol (below). The contract only authorises key-fragment reassembly; it never stores personal data or keys.
Bitcoin	What level of proof, at what cost?	Merkle anchoring: each memory's SHA-256 hash is a leaf; only the periodic Merkle root is written via OP_RETURN. One transaction (a few euros) covers thousands of users; each memory keeps an independently verifiable inclusion proof.

Succession protocol — the death-oracle problem

A smart contract cannot know on its own that a person has died. The protocol therefore combines three safeguards, configurable by the owner in the My Legacy space:

Step	Mechanism	Owner setting
1. Presence signal	Owner silently confirms presence in the app (dead man's switch).	Every 3, 6 or 12 months
2. Grace & contestation	Missing signal opens multichannel alerts and a period during which the owner or anyone authorised can contest.	30, 60 or 90 days
3. Quorum release	Joint approval by m-of-n beneficiaries, plus independent verification (legal certificate or decentralised oracle), authorises key reassembly.	1 to 5 beneficiaries

Status. Owner settings are recorded in the app today. Automatic checks, alerts and on-chain execution are in development: nothing is released yet.

14

Sovereignty and technology identities

Sovereignty must not stop at storage. It also covers:

— **AI model updates** — signed, reversible and opt-in; the owner can keep a previous model.

— **Memory formats** — open, documented, versioned; readable without Bottle on the Sea.

— **Portability** — full encrypted export at any time, with keys held by the owner.

— **Hardware dependence** — no lock-in to a single chip, cloud or vendor; confidential compute is interchangeable.

Identity	Role
Bottle on the Sea	The platform and the human experience.
Sovereign AI	The personal intelligence that works with the owner's memories.
ETERNITY	The decentralised infrastructure that preserves memories.
Bitcoin & Ethereum	Complementary rails of trust (proof of integrity) and transmission (programmable succession).