Enigma Blockchain (ENB)

A Tokenless Smart-Contract Ledger for Verifiable Records

IAIC TECHNICAL REPORTS

IAIC-TR-2026-01 • November 2026

https://doi.org/10.66693/iaic.tr.2026.1

Andrey Nechesov, PhD

Founder and Principal Architect
IAIC AI Research & Trading FZCO
Chair, International AI Committee

IAIC AI Research & Trading FZCO
Dubai, United Arab Emirates
iaic.world • enigma.ist • enb.world

Smart contracts licensed under Apache 2.0.
This document is licensed under Creative Commons Attribution 4.0 (CC BY 4.0).

Abstract

Enigma Blockchain (ENB) is an EVM-compatible proof-of-authority ledger operated for the ENIGMA platform: the scholarly publishing service **enigma.ist**, its journals and conferences, and the Enigma messenger. It has one purpose: to give records that people need to rely on later (who published what, who reviewed it, who held which role, what a service reported about itself on a given day) a form that anyone can read and that the operator cannot quietly rewrite.

ENB has no coin, no token and no fee market. The genesis block allocates no balances, blocks carry no reward, and the gas price is zero, so the supply of the chain's native unit is zero and stays zero. Nothing on the chain can be bought, sold, held or transferred as an asset. The chain carries smart contracts that record identities, attestations signed by both the issuing institution and the person concerned, subscriptions and memberships, and the platform's own operational reports.

This paper specifies the chain (QBFT consensus, validator and access model, external anchoring), a data policy that separates what may be written in clear from what may be written only as a salted commitment and what is never written, the five-contract suite (Registry, Track, Router, Relayer, Subscription), the trust model with dual signatures, the operations of the ENIGMA platform that already run on the public testnet, its foundations in the task approach and in learning theory, the application of the same design to AI-native government, its relation to the IAIC 101 standard for autonomous AI systems, governance, regulatory position, the state of implementation in November 2026, and the conditions for a mainnet launch.

Keywords. permissioned blockchain; proof of authority; QBFT; tokenless ledger; smart contracts; verifiable records; scholarly publishing; AI-native governance; dual-signature attestation; EIP-2771 meta-transactions; data minimisation; external anchoring.

Suggested citation. Nechesov, A. (2026). *Enigma Blockchain (ENB): A Tokenless Smart-Contract Ledger for Verifiable Records.* IAIC Technical Reports, IAIC-TR-2026-01. IAIC AI Research & Trading FZCO, Dubai, UAE. https://doi.org/10.66693/iaic.tr.2026.1

Contents

Abstract ii

1 Introduction 1

2 Problem Statement 1

2.1 The scholarly record is fragile 1

2.2 Peer review cannot be verified 1

2.3 Credentials do not travel 1

2.4 Platforms report on themselves . . . 2
2.5 Why a ledger, and which kind . . . 2
3 Design Principles 2
4 Chain Architecture 3
4.1 A chain without a native asset . . . 3
4.2 Consensus . . . 3
4.3 Validators . . . 4
4.4 Who can write and who can read . . . 4
4.5 External anchoring . . . 4
4.6 Hosting and operations . . . 5
5 On-Chain Data Policy 5
5.1 Three classes . . . 5
5.2 The decision rule . . . 5
5.3 Salted commitments . . . 6
5.4 Erasure . . . 6
5.5 Size limits . . . 6
6 Smart Contract Suite 6
6.1 ENBRegistry: identity and self-claimed records . . . 7
6.2 ENBTrack: records attested by institutions . . . 7
6.3 ENBRouter: one use per content hash . . . 8
6.4 ENBRelayer: submission on the user's behalf . . . 8
6.5 ENBSubscription: memberships and plans . . . 8
6.6 Shared component: ERC2771ContextMutable . . . 8
6.7 Size and tests . . . 9
7 Trust Model 9
7.1 Two tiers of record . . . 9
7.2 Dual signature . . . 9
7.3 Positive records only . . . 10
7.4 What the model does not establish . . . 10
8 Identifiers and the Publication Flow 10
8.1 Record identifiers . . . 10
8.2 Binding a file to its identifier . . . 10
8.3 Relation to the DOI . . . 10
9 Operations of the ENIGMA Platform on Chain 11
9.1 The messenger's pulse and daily digest . . . 11
9.2 Journals . . . 12
9.3 Conferences . . . 12
9.4 Goals . . . 12
9.5 Key directory . . . 12
9.6 Software releases . . . 12

10 Foundations: the Task Approach and Learning Theory 12
10.1 The task approach . . . 13
10.2 Learning theory and the hierarchy of knowledge . . . 13
10.3 What the ledger takes from them . . . 14
11 AI-Native Governance 14
11.1 Governments are making AI part of how they decide . . . 14
11.2 The question such a government must be able to answer . . . 15
11.3 How the design maps to it . . . 15
11.4 Data about citizens . . . 15
11.5 Sovereign deployment . . . 16
11.6 What this does not provide . . . 16
12 Relation to the IAIC 101 Standard 16
12.1 The standard . . . 16
12.2 What the standard asks of a record . . . 16
12.3 Where a ledger of this kind fits . . . 17
12.4 Independence of the standard . . . 17
13 Identity and Key Management 18
13.1 One secret, separate addresses . . . 18
13.2 Custody . . . 18
13.3 Recovery . . . 18
14 Governance and Upgrades 18
14.1 Roles . . . 18
14.2 Timelocks . . . 19
14.3 What upgradeability costs . . . 19
14.4 Path to shared governance . . . 19
15 Regulatory Positioning 19
15.1 Jurisdiction . . . 19
15.2 Virtual assets . . . 19
15.3 Data protection . . . 20
15.4 Publishing norms . . . 20
16 Privacy 20
16.1 What an observer of the chain learns . . . 20
16.2 Reducing linkage . . . 20
16.3 What is not claimed . . . 20
17 Further Fields of Use 21
17.1 Education . . . 21
17.2 Professional credentials . . . 21
17.3 Clinical research . . . 21
17.4 Conditions . . . 21
18 Implementation Status and Roadmap 21

18.1 State in November 2026 21
18.2 Roadmap 22
19 Risks and Mitigations 23
20 Relation to Existing Systems 23
20.1 ORCID and DOI 23
20.2 Preprint servers and repositories 23
20.3 Public blockchains 24
20.4 Timestamping services 24
20.5 Enterprise ledgers 24
20.6 Token-based science projects 24
21 Conclusion 24
References 24
A Network Parameters and Contract Addresses 28
B Format of the Messenger's Daily Digest 28
C Document History 28
D About the Author 29

1. Introduction

A platform that publishes research, runs conferences and carries private conversations asks its users for a great deal of trust. Authors trust that the record of their paper will not change. Reviewers and editors trust that their work will stay attributable to them. Readers trust that "peer reviewed" means what it says. Users of a messenger trust the figures the service publishes about itself. In each case the usual guarantee is the operator's word, backed by a database the operator can edit.

ENB replaces that word with a record. A fact that matters is written to a ledger that is sealed block by block, readable by anyone, and administered so that no single party can change what has been written. The ledger is an Ethereum-compatible chain, which means that the rules for writing a record are programs (smart contracts [12]) whose code and whose every execution are public.

The ledger carries no coin and no token. An asset would add regulatory exposure and a speculative association that working researchers and public institutions distrust, and it would contribute nothing to the property users actually want, which is that a record can be checked.

The contract suite is built around two kinds of record, those a person claims for themselves and those an institution attests with the person's consent. A public test network has been running since April 2026, and since November 2026 the Enigma messenger writes a verifiable digest of each day to it. Section 18 states precisely what is running, what is implemented but not deployed, and what is still design.

2. Problem Statement

2.1 The scholarly record is fragile

Journal websites go offline, archives are rebranded after acquisitions, and a publisher can alter or withdraw a paper without leaving a trace that a reader can inspect. Archiving services reduce the loss, but none of them lets a reader verify that the file in hand is the file that was published.

2.2 Peer review cannot be verified

A journal states that a paper was reviewed by independent experts; a reviewer states that they reviewed for a journal. Neither statement can be checked by a third party, and the reviewer has no credential that survives the journal.

2.3 Credentials do not travel

Editorial positions, memberships, conference talks and awards live in the databases of the bodies that granted them. When the body changes its systems, merges or closes, the credential becomes an unverifiable line in a curriculum vitae.

2.4 Platforms report on themselves

A service that publishes its own usage figures, uptime or release history asks to be believed. Nothing stops the figures being revised later, and a reader has no means to tell whether they were.

2.5 Why a ledger, and which kind

These four problems share one requirement: a statement made at a given time must remain exactly as it was made, and anyone must be able to confirm that. A cryptographic ledger with several independent operators provides this. A token does not add to it.

The requirement does not call for an open, anonymous network either. The parties that issue records here (journals, universities, conference committees, the platform) are known institutions that can be held to account. A permissioned network of such institutions gives fast, final settlement at negligible cost. Its weakness is that a small validator set could collude to rewrite history, and Section 4.5 addresses that with commitments to a public chain that the validators do not control.

ENB therefore claims a narrow result: *records with public verifiability and no single party able to rewrite them.* It does not claim to decentralise publishing or to replace peer review.

3. Design Principles

1. **No asset.** The chain has no coin, no token and no fees. No contract accepts, holds or transfers value.
2. **Records, with rules.** A smart contract is used where a rule must be enforced by something other than the operator: who may issue a record, whose consent is required, what cannot be changed afterwards.
3. **Consent by signature.** An institution cannot write a record about a person without that person's cryptographic signature, or that of a signer the person has appointed.
4. **The least data that proves the point.** Public facts may be written in clear. Anything private is written only as a salted commitment. Personal data is never written in clear (Section 5).
5. **Extension without redeployment.** Kinds of institution, kinds of record and kinds of annotation are entries in on-chain lists managed by governance. A new field of use needs new entries and no new contract.
6. **Open to read, permissioned to write.** Every block, transaction and contract state is public. Writing is limited to known institutions and to users acting through the platform's relayer.
7. **Stated trust assumptions.** Where the design depends on the operator's good conduct (validator set at bootstrap, upgrade keys), the paper says so and gives the mechanism that limits the dependence.

8. **No user needs a wallet balance.** Users sign messages; the relayer submits them. There is nothing to acquire before using the system.

4. Chain Architecture

4.1 A chain without a native asset

Every Ethereum-compatible chain [1] defines a native unit in which account balances and fees are denominated. ENB sets every quantity of that unit to zero:

- the genesis block contains no account allocation;
- the block reward is zero;
- the minimum gas price accepted by validators is zero and the base fee is fixed at zero;
- no contract in the suite has a payable function.

Under these four conditions no account can ever hold a balance, because there is no source from which a balance could arise. The unit exists as a field in the protocol and nowhere else. Gas remains as a measure of computation, used to bound the work in a block; it is not paid for.

4.2 Consensus

ENB uses **QBFT** [2, 3], a Byzantine-fault-tolerant [4] proof-of-authority protocol, as implemented in Hyperledger Besu [5]. Validators are known institutions that take turns proposing blocks; a block is final once a supermajority of validators has signed it.

Parameter	Value
Consensus	QBFT proof of authority
Client	Hyperledger Besu
Block period	5 seconds
Finality	Immediate (a sealed block is not reorganised)
Fault tolerance	$f = \lfloor (n-1)/3 \rfloor$ faulty validators out of n
Gas limit per block	15,000,000
Gas price and base fee	0
Block reward	0
Native balances at genesis	None
Chain identifiers	31415 (mainnet), 31416 (testnet)

The present test network runs Clique on go-ethereum. Go-ethereum removed Clique signing in release 1.14.0 [7], so a Clique network must stay on the 1.13 series, which no longer receives fixes. QBFT on Besu is maintained, gives immediate finality where Clique gives probabilistic finality, tolerates faulty validators by design, and supports zero-fee networks as a documented configuration [6]. The production network therefore starts under QBFT from its own genesis

(Section 18).

4.3 Validators

The security of a proof-of-authority chain is the independence of its validators. A network whose validators all belong to one organisation offers ordering and public readability but no protection against that organisation. ENB distinguishes two states and commits to naming them accurately in public material:

- **Operator-run.** All validators are operated by IAIC FZCO. This is the state of the testnet and the permitted state of a bootstrap network. In this state the guarantee against rewriting rests on external anchoring alone.
- **Consortium.** At least four validators, operated by at least three legally independent institutions, so that no single institution can halt or rewrite the chain and the network tolerates one faulty validator. Only a network in this state is described as a consortium chain.

Validators are added and removed by vote of the existing validators, as provided by QBFT. Candidate validators are universities, publishers and research organisations that issue records on the chain and therefore have their own interest in its integrity. Validators receive no on-chain payment.

4.4 Who can write and who can read

With a zero gas price, fees cannot serve as protection against abuse. Access control takes their place:

- **Writing.** Validators accept transactions only from allowlisted sender accounts: the platform relayer, registered institutions (journals, universities, conference committees), and governance. Individual users do not submit transactions directly. They sign typed messages, and the relayer submits them within per-user rate limits (Section 6.4).
- **Reading.** Unrestricted. The chain is served through a public explorer at `enb.world`, a read-only RPC endpoint and a JSON interface. Any institution may run an observer node that follows the chain and verifies every block without taking part in consensus.

4.5 External anchoring

Validators that collude, or a single operator during bootstrap, could in principle produce an alternative history. To make such a rewrite detectable by anyone, ENB commits the hash of a recent final block to the Bitcoin blockchain [8] at regular intervals, using the OpenTimestamps protocol [9]. OpenTimestamps aggregates many commitments into one Bitcoin transaction through public calendar servers, so the operator of ENB needs no cryptocurrency and pays no fee. Each proof is published alongside the block it covers. A reader who holds a proof can confirm that the ENB history up to that block existed at the time of the Bitcoin block, whatever the

ENB validators later claim.

Anchoring is specified and not yet active; it is a condition of mainnet launch.

4.6 Hosting and operations

The testnet runs on a single virtual server in Helsinki. This is sufficient for the present volume, which is under two thousand transactions a day, and is disclosed here as a single point of failure for availability. Consortium validators run on infrastructure chosen by each institution.

5. On-Chain Data Policy

A rule of "hashes only" is safe but wasteful: some information is public by nature, and writing only its hash forces every reader to fetch the content elsewhere and trust that it will remain available. ENB permits clear text where publication is the purpose, and applies a strict rule to everything else.

5.1 Three classes

Class	Written as	Examples
P, public	Clear text or structured data, with its hash	Aggregate usage figures of the messenger; journal and issue identifiers; titles and DOIs of published articles; conference programme entries; versions and file hashes of released software; identifiers of published standards; governance decisions
C, committed	Salted cryptographic commitment only	Manuscripts under review; review reports; contracts; individual goals and their outcomes; membership of a person in a body; attendance of a person at an event; any record about an identifiable person
N, never	Not written in any form	Message content and message metadata; contact lists; private keys; payment details; health data; identity documents

5.2 The decision rule

A datum may be written in clear only if all three conditions hold:

1. it is already public, or publishing it is the purpose of the record;
2. it is meant to stay public permanently, with no foreseeable reason to withdraw or correct it other than by a later record;
3. it contains no personal data. Names count as personal data even where they are already public, because a person may later have the right to have a name corrected or removed,

and a ledger cannot comply.

If any condition fails, the datum is class C or class N. The rule is applied when a record type is registered: each record type declares whether it may carry clear text. Enforcement of that declaration by the contracts, together with the size limits below, is part of the release build (Section 18).

5.3 Salted commitments

A class C record stores $h = H(s \,\|\, d)$, where d is the canonical serialisation of the data, s is a random 256-bit salt generated for that record, and H is SHA-256 or Keccak-256. The data and the salt stay off chain with the party that owns the record.

The salt is needed because much real data has little entropy: a name, a date, a decision of "accept" or "reject". An unsalted hash of such data can be reversed by trying the candidates. With a salt, the commitment reveals nothing to anyone who lacks the salt, and a holder of the data and salt can prove at any later time that the record matches.

5.4 Erasure

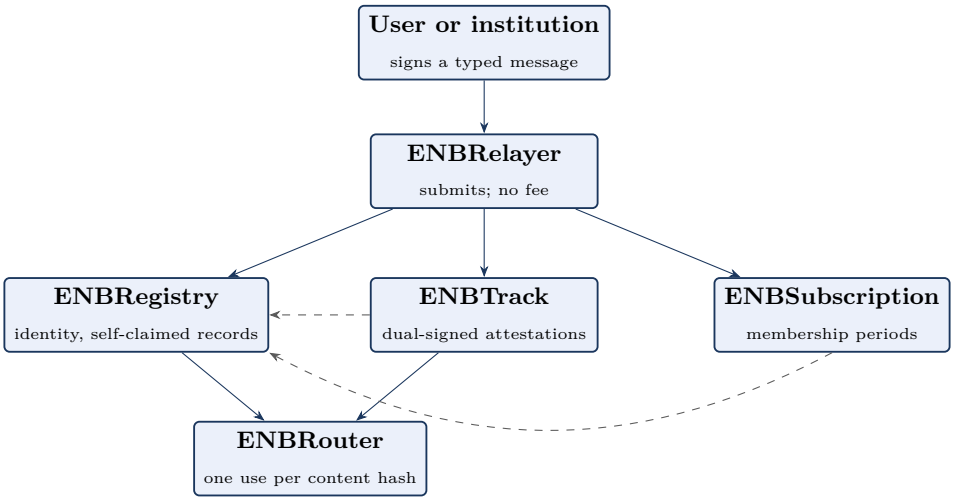
A ledger cannot delete. Where a person is entitled to erasure, the owner of the record deletes the data and the salt. The commitment that remains on chain can no longer be linked to the person by any party. Data-protection authorities have not settled whether this satisfies an erasure right under the General Data Protection Regulation [23] in every case, which is why the policy does not rely on it for anything that can be kept off chain entirely: class N exists so that the question does not arise for the most sensitive data.

5.5 Size limits

Clear-text payloads are capped per record type, with a general ceiling of 4 kilobytes. The ledger is a place for facts and proofs. Documents, files and media are stored off chain and referenced by hash.

6. Smart Contract Suite

The suite consists of five contracts and one shared component. All are written in Solidity 0.8.24 on OpenZeppelin Contracts 5 [18], licensed under Apache 2.0, and deployed behind upgradeable proxies [16, 17] whose upgrades pass through timelocks (Section 14).



Solid arrows are calls. Dashed arrows are read-only lookups of owners and access grants in the Registry.

6.1 ENBRegistry: identity and self-claimed records

Every participant begins by obtaining an **ENB ID**, a globally unique integer bound to one address. The Registry holds:

- the identifier counter and the mapping between identifiers and owner addresses;
- **meta tags**, key and value pairs the owner sets and deletes at will (a link to a profile, a commitment to a biography);
- **trusted signers**, addresses the owner authorises to sign on their behalf, optionally limited to one institution and with an expiry. Only the owner can appoint or revoke them, and the power cannot be delegated further;
- **self-claimed records**, statements the owner makes about themselves, such as a preprint or a talk given. They carry no third-party verification and are displayed as such;
- **access grants**, by which the owner permits one institution to receive records held by another, for stated record types and until a stated date. The grant and its revocation are on chain; the data itself travels off chain, encrypted between the two institutions.

6.2 ENBTrack: records attested by institutions

The Track holds the registry of institutions and every record an institution issues.

- **Contexts.** An institution (a journal, a university, a conference, the platform itself) is registered by governance as a *context* with an owner address and a type. Governance can flag or deactivate a context; records issued earlier remain, and readers see the changed status.
- **Taxonomies.** Context types, record types and annotation types are lists in contract storage, extended by governance at run time.
- **Anchors.** A person's first record under a context is an anchor, which establishes their consent to hold records with that institution.

- **Attestations.** A record under a context is valid only with two signatures over the same content: the institution's and the subject's (Section 7).
- **Annotations.** An institution may annotate its own earlier record without the subject's signature. Annotations bind the final file of a published article to its identifier, and record corrections and retractions.
- **Data publication.** Under an access grant, the sending institution records the hash and location of the encrypted payload, and the receiving institution may record that it received it. The exchange leaves an audit trail without exposing the data.

6.3 ENBRouter: one use per content hash

Before the Registry or the Track accepts a record, it asks the Router to mark the record's content hash as used. The Router refuses a hash that has been used before, by either contract. The same content therefore cannot be claimed twice, for example once by its author as a self-claimed record and again, unchanged, as an institutional attestation in another name. Only contracts authorised by governance may call the Router.

6.4 ENBRelayer: submission on the user's behalf

The Relayer implements EIP-2771 meta-transactions [15]. A user signs an EIP-712 typed message [14] that names the target contract, the call, a nonce and a deadline. The Relayer verifies the signature, the nonce and the deadline, and forwards the call to an authorised target, which reads the user's address from the forwarded data and treats the user as the caller.

The Relayer charges nothing and settles nothing. Abuse is limited by the write allowlist at the validators and by rate limits applied per user at the relaying service.

6.5 ENBSubscription: memberships and plans

The Subscription contract records periods of membership as an append-only history. Governance registers a *plan* (for example a premium tier of the messenger, or membership of the International AI Committee) and names the address entitled to activate periods for it. Each activation stores a start and an expiry for an ENB ID; a renewal adds a period and leaves earlier ones in place.

Payment is outside the contract and outside the chain. Subscriptions are sold in fiat currency through ordinary payment processors, and the contract receives only the resulting dates. What the chain adds is a credential: that a given identifier held a given membership over a given interval can be shown to any third party.

6.6 Shared component: ERC2771ContextMutable

Contracts that accept forwarded calls must know which forwarder to trust. This component stores the trusted forwarder's address in upgrade-safe storage and lets governance replace it, so that the Relayer can be upgraded without redeploying the contracts that depend on it.

6.7 Size and tests

Contract	Lines	Test functions	Upgrade timelock
ENBRegistry	597	42	24 hours
ENBTrack	994	52	24 hours
ENBRouter	327	36	48 hours
ENBRelayer	376	22	48 hours
ENBSubscription	533	52	24 hours
ERC2771ContextMutable	164	(via the above)	n/a
Total	**2,991**	**204**	

Line and test counts are those of the source repository in November 2026; seven integration tests are additional. The figures will be restated, with a test report, when the release is tagged (Section 18).

7. Trust Model

7.1 Two tiers of record

- **Tier 1, attested.** A record in the Track, signed by an active institution and by the subject. Interfaces show it with the institution's name.
- **Tier 2, self-claimed.** A record in the Registry, signed by its owner alone. Interfaces show that no third party has verified it. A tier 1 record whose institution is later deactivated is displayed with the same caution.

The tier is a property of where and how the record was written. A reader does not need to trust the interface that displays it.

7.2 Dual signature

For every attestation, the Track verifies two EIP-712 signatures over the same context, record type, content hash and parent record:

1. the **institution's declaration**, recovered to the owner address of an active context;
2. the **subject's consent**, recovered to the owner of the subject's ENB ID or to a trusted signer the subject appointed, valid for that context and not expired.

Each signature carries its own nonce and deadline and can be used once. The consequence is that an institution cannot attribute a record to a person who has not agreed to it, and a person cannot obtain an institutional record the institution has not issued. This is enforced by the contract and does not depend on the conduct of the operator.

7.3 Positive records only

The contract has no function by which an institution can write an adverse statement about a person, and the consent requirement would defeat one in any case. Institutions that need to say something adverse do so through their own channels. A retraction is an annotation by the institution on its own publication; an author who disagrees can publish a self-claimed record in reply.

7.4 What the model does not establish

A signature proves that the holder of a key signed. It does not prove that an institution's judgment was sound, that a review was careful, or that a figure reported by a service is true. ENB makes such statements attributable and unchangeable, which is the precondition for holding their authors to account. It does not replace that accountability.

8. Identifiers and the Publication Flow

8.1 Record identifiers

Every record has an integer identifier assigned by the contract at the moment of writing. It is displayed as `enb-N`, for example `enb-42157`. A published article carries this identifier alongside its Crossref DOI. A journal's own numbering remains available as a convenience for readers, and has no standing on chain.

8.2 Binding a file to its identifier

An article should display its identifier inside the PDF. The identifier cannot then be derived from the PDF, since inserting it changes the file. The flow separates the two steps:

1. **Issue.** On acceptance, the journal and the author co-sign an attestation of type `Paper`. The contract returns the identifier.
2. **Typeset.** The journal places the identifier and the DOI in the final PDF.
3. **Bind.** The journal writes an annotation of type `PdfFinalized` to the record, carrying the hash of the final file.

A reader verifies a copy by reading the identifier from the file, looking up the record, hashing the file and comparing the result with the latest `PdfFinalized` annotation. Corrections add annotations; the identifier does not change.

8.3 Relation to the DOI

The DOI remains the identifier that indexing services require, and its resolution depends on the registration agency and the publisher. The ENB identifier adds what the DOI lacks: a commitment to the exact content, verifiable without relying on either.

9. Operations of the ENIGMA Platform on Chain

This section lists the operations of the platform that are, or are to be, organised through the ledger, with the class of data each one writes (Section 5) and its state in November 2026.

Operation	What is written	Class	State
Messenger: pulse each minute	Aggregate counts for the current day	P	Live on testnet
Messenger: daily digest	Aggregate counts for the closed day, with SHA-256	P	Live on testnet
Journals: articles	Attestation and file-binding annotation; title and DOI in clear	P and C	Implemented; earlier contracts on testnet
Journals: peer review	Commitment to the report, co-signed by reviewer and journal	C	Implemented
Journals: editorial roles	Attestation of appointment and its end	C	Implemented
Subscriptions and memberships	Periods per identifier and plan	C	Implemented
Conferences	Programme entries in clear; participation as attestations	P and C	Record types to be registered
Goals in the messenger	Commitment to a goal and its criterion; later, to the outcome	C	Aggregates live; per-goal commitments designed
Key directory	Periodic commitment to the directory of users' public keys	P	Designed
Software releases	Version and file hash of each client build	P	Designed
Standards	Identifier and hash of each published standard	P	Designed

9.1 The messenger's pulse and daily digest

The Enigma messenger reports on itself in two records. Every minute it writes a *pulse*: the number of people using it at that moment and the running totals for the day. Once a day it writes a *digest* of the day that has closed: distinct devices that opened the application, number of openings, messages sent by people, calls started, conversations begun, goals set, goals confirmed as reached, and sign-ins. All days are counted in UTC.

Both records contain aggregates only. They identify no person and include no text, and they are class P under the policy: publishing them is their purpose.

Each digest is written by the platform's own address as a transaction whose data field holds the figures and their SHA-256 (Appendix B). Anyone can read the transaction from a node, recompute the hash and compare. Once a day is written, the platform cannot revise it. A service that later wished to present better figures for a past day would have to contradict its own record

on a ledger it does not solely control. This is the first operation of the platform to run on the chain.

9.2 Journals

The platform publishes five journals, covering mathematics and artificial intelligence, finance and artificial intelligence, bioinformatics, AI agents, and the standards of the International AI Committee. Each journal is a context in the Track. Articles follow the three-step flow of the previous section. A review is recorded as an attestation co-signed by the reviewer and the journal, which commits to the report without disclosing it or the reviewer's name; the reviewer can later prove authorship of the review to anyone they choose, by revealing the salt. Editorial appointments are attestations co-signed by the editor and the journal.

9.3 Conferences

A conference is a context. Its programme is public and may be written in clear. A talk, a role on the programme committee or attendance is an attestation co-signed by the participant and the organising committee. The MathAI conference series is the first intended user.

9.4 Goals

In the messenger, a user can set a goal with a criterion for success and later confirm whether it was reached. The daily digest already carries the aggregate numbers. The per-goal design commits to the goal and its criterion when it is set and to the outcome when it is closed, both as salted commitments. The user can then show a third party that a criterion was fixed before the outcome was known. The content of the goal never leaves the user's control.

9.5 Key directory

End-to-end encryption depends on each user receiving the genuine public keys of the people they talk to. A service that controls the key directory could substitute a key. Committing the directory's Merkle root [11] to the chain at regular intervals, in the manner of key-transparency systems [13], lets each client check that the key it was given is in the directory everyone else sees, and makes a substitution detectable.

9.6 Software releases

Each released build of the client applications is recorded with its version and file hash. A user or auditor can then confirm that an installer is the one the platform published.

10. Foundations: the Task Approach and Learning Theory

The design of the ledger follows from two lines of research on artificial intelligence that can be trusted. This section describes them and states what the ledger takes from each.

10.1 The task approach

The task approach was developed by E. E. Vityaev, S. S. Goncharov and D. I. Sviridenko and extended in joint work with the author of this paper [41, 42]. Its starting point is that an intelligent system should be described by the tasks it solves. A task is not a request in free form. It consists of a statement and a criterion, fixed in advance, that decides whether something offered as a solution is one. A system that receives a task without a criterion can produce an answer, but nobody, the system included, can establish that the answer is correct.

The joint work applies the approach to systems built on language models. Such systems reason well inside a formal framework and still produce statements that are false, a failure usually called hallucination. The task approach locates the cause: the system answers without a criterion against which the answer is checked. The remedy is to make the task and its criterion explicit, together with the axioms and theorems the task rests on and the limits within which it can be solved at all. A solution is then accepted on the ground that it was checked against the criterion.

The approach is grounded in semantic programming, in which a task is a formula and solving it means establishing that the formula holds in a model. The author's work on polynomially computable representations [44] and on polynomial analogues of Gandy's fixed-point theorem [38, 39] concerns the cost of this step: which criteria can be checked in feasible time.

10.2 Learning theory and the hierarchy of knowledge

The learning theory proposed by the author [43] builds on the task approach, semantic programming, computability theory and model theory. In it, learning is the growth of a knowledge base through solved tasks. A solved task, with its criterion and its solution, becomes knowledge that later tasks may use. Because each item of knowledge depends on the items used to obtain it, the knowledge base acquires a natural hierarchy, and the hierarchy records how the system came to know what it knows.

Two properties follow. A system organised in this way can keep learning without being rebuilt, since each new solved task extends the hierarchy. It can also explain a decision by the rules and earlier results the decision rests on, which a language model alone cannot do. The theory therefore points to hybrid systems, in which a statistical component proposes and a symbolic component checks and records.

10.3 What the ledger takes from them

In the theory	In ENB
A task has a criterion fixed in advance	A commitment to the goal and its criterion is written before the work begins (Section 9). Its block time shows that the criterion preceded the result.
A solution is one that passed the criterion	The outcome is a second record, linked to the first. Whoever holds the data can show a third party that the outcome meets the criterion that was committed.
Solved tasks become knowledge	Records are append-only and each can name its parent, so the record of an agent or an institution is a growing structure and not a list of unrelated entries.
Knowledge forms a hierarchy	Parent links and annotations preserve which result rests on which, including corrections.
A decision is explained by the rules it rests on	The version of each rule set is recorded when it is adopted, and a decision record commits to the version it applied (Section 11).

The ledger does not implement these theories and proves nothing about a task. Checking a solution against a criterion is done by the system that solves the task, with whatever logical tools it uses. What the ledger adds is that the task, the criterion, the result and their order in time are fixed where neither the system nor its operator can change them. For an autonomous agent this turns a claim of competence into a record of tasks actually solved under criteria actually stated in advance.

11. AI-Native Governance

11.1 Governments are making AI part of how they decide

Public administrations are moving from using AI as a tool to building their operations around it. The United Arab Emirates has the most developed programme. In January 2025 the Government of Abu Dhabi published its Digital Strategy 2025–2027, with a stated investment of AED 13 billion and the aim of becoming the first fully AI-native government across its digital services by 2027, including more than 200 AI solutions in government services [28]. Dubai launched the Dubai Universal Blueprint for Artificial Intelligence in 2024 and appointed Chief AI Officers across its government entities [29]. At federal level, the Cabinet approved a Regulatory Intelligence Office in April 2025 to apply AI to the drafting and review of legislation [30], and it was announced in June 2025 that a National AI System would sit as an advisory member of the Cabinet from January 2026 [31].

Other jurisdictions are writing the corresponding duties into law. The European Union's Artificial Intelligence Act [25] requires high-risk AI systems to record events automatically over their lifetime (Article 12) and requires those who deploy them to keep the logs (Article 26). Estonia has for more than a decade protected the integrity of its state registries with hash-linked timestamping [32].

These programmes are cited as context. ENB has no affiliation with any of them, is not deployed in any government, and claims no endorsement.

11.2 The question such a government must be able to answer

When a system proposes or takes a decision that affects a person, an administration will be asked: which system acted, in which version, under which rule, on whose authority, and which official answers for it. The usual source for the answer is a log held by the agency that operates the system or by its vendor. A log that its owner can edit is weak evidence in an audit, an appeal or a court, and it is weakest where the owner has a reason to revise it.

The requirement is the one this paper started from: a statement made at a given time must remain as it was made, and a party other than its author must be able to confirm that. The section builds on the author's earlier work on the theory of blockchains [35] and on combining AI and blockchain in public administration [36]; requirements for autonomous AI systems themselves are set out in the IAIC 101 standard [45], discussed in Section 12.

11.3 How the design maps to it

What must be provable	Mechanism in ENB
Which rule was in force	The version of each policy or rule set is recorded when it is adopted. Public rules are written in clear; internal ones as commitments.
Which system acted	Each deployed model is recorded by an identifier and a hash of its released version, as software releases are (Section 9).
That an agent had authority	An official delegates signing authority to an agent as a trusted signer: limited to one agency, with an expiry, revocable in one transaction, and not delegable further.
What was decided, and on what basis	A decision is an attestation under the agency's context, carrying a salted commitment to the inputs, the model version, the rule version and the output.
Who answers for it	The attestation is valid only with two signatures: the agency's, and that of the accountable official or of the agent acting under that official's delegation.
That the criterion preceded the outcome	A goal and its criterion of success are committed before the action; the outcome is committed afterwards.
Correction and appeal	A reversal or correction is an annotation on the original record. The original stays visible.
That the record was not rewritten	Validators from separate bodies, and anchoring outside the network (Section 4.5).

11.4 Data about citizens

The data policy of Section 5 applies without exception. No data about a citizen is written in clear. A decision record is a commitment that reveals nothing without the salt, which stays with the agency. The case file stays in the agency's systems, under the law that governs it. Where

volume is high, decisions are committed in batches: one Merkle root per interval, with each decision provable against it.

11.5 Sovereign deployment

A government need not write its records to a network operated by a company. The contracts and the client are open source, and a state can run its own instance: validators operated by its agencies, its audit institution and its judiciary or ombudsman, so that the body that decides is not the only body that keeps the record; governance keys held under its own procedures; read access open to the public or limited to oversight bodies, as its law requires. Because the ledger has no coin or token, a public body can adopt it without holding, issuing or accounting for a digital asset.

11.6 What this does not provide

A record of a decision does not make the decision correct, lawful or fair, and it does not explain a model's reasoning. It establishes what was decided, by which system, under which rule and on whose authority, in a form that the deciding body cannot later change. Review of the substance remains the work of auditors, courts and the public. The design described in this section is a specification. It has not been deployed for any public body.

12. Relation to the IAIC 101 Standard

12.1 The standard

IAIC 101:2026, the *International Standard for Autonomous AI Systems* [45], was issued by the International Artificial Intelligence Committee on 7 September 2026. It runs to 145 pages and 167 acceptance items and is published under CC BY 4.0. It is written for the party that acquires an autonomous system: it states what a supplier must be asked before a bid can be evaluated, and what an evaluation may conclude from the answers. Its requirements are graded by deployment tier, a system is assessed only against tasks stated before purchase, and assurance is divided into six dimensions, none of which substitutes for another: provenance and identity attestation, data governance, control-channel isolation, behavioural verification, auditability, and human oversight.

12.2 What the standard asks of a record

Clause 10 of the standard starts from an observation that this paper shares. A record held, generated and attested entirely within the supplier's control does not establish what happened, because everything the acquirer can check about it was produced inside the boundary whose trustworthiness is the question. The standard therefore requires:

- a record taken at the decision layer: every step admitted or refused with the condition that decided it, every command with the principal that issued it, every change of goal with what set it, every change to the system, and every escalation to a person;

- entries that carry enough to re-execute a decision, and no field that purports to explain a learned component;
- entries signed by the system with a key it cannot surrender;
- a periodic commitment of the record placed outside the supplier's reach, and a time source the supplier does not control.

12.3 Where a ledger of this kind fits

The standard names no product and requires none. ENB is one way of meeting the parts of it that call for something outside the supplier's boundary.

Requirement in IAIC 101	**What ENB can supply**
Independent commitment of the record (clause 10)	The system, or its operator, writes the hash of each block of its decision record as a commitment. The record stays with the system; the commitment cannot be altered by the supplier.
Time source outside the supplier's control (auditability)	Block time fixed by validators that are not the supplier, and anchored to a public chain (Section 4.5).
Provenance and identity of what is running	The identifier and hash of each released version, recorded when it is released (Section 9).
Tasks stated before purchase (clause 5)	A commitment to the task and its criterion, written before acceptance and compared with the outcome afterwards.
Changes after acceptance (clause 11)	Each change is a new record linked to the one it supersedes; the earlier state stays visible.
Who commanded, and by what authority (clauses 13 and 16)	Delegation to a signer that is scoped, time-limited and revocable, and a record that carries the delegating party.
A named accountable person (human oversight)	A record that is valid only with the signature of that person, or of a signer acting under that person's delegation.

The commitment is useful only if the ledger is outside the reach of the supplier being assessed. A ledger whose validators the supplier controls does not meet clause 10, whatever its technology. This is the same condition as in Section 4.3, and for a sovereign deployment it is met by placing validators with bodies other than the one that operates the system.

12.4 Independence of the standard

The author of this paper is the author and editor-in-chief of IAIC 101, and IAIC FZCO, which operates ENB, publishes the standard. The standard addresses this in its foreword, and the same applies here: the standard does not require or name ENB or any other offering of the committee or of parties connected to it; using ENB gains a deployment nothing in an assessment under the standard; and any commitment mechanism outside the supplier's reach satisfies the same clauses. Where ENB is proposed in a deployment assessed under IAIC 101, that connection is a competing interest and is to be disclosed to the party relying on the assessment.

13. Identity and Key Management

13.1 One secret, separate addresses

A user holds one master secret of 256 bits, which may be kept as a 24-word BIP-39 mnemonic [20], a raw private key or an encrypted keystore file. The wallet derives separate addresses from it along hardened BIP-32 paths [19], so that the addresses cannot be linked to one another by anyone who sees only the chain:

Address	Derivation path	Use
Publishing	`m/44'/31416'/0'/0/0`	Owns the ENB ID; signs consents and self-claimed records
Governance	`m/44'/31416'/0'/2/0`	Signs governance actions, where the user is a signer
Editorial	`m/44'/31416'/0'/3/0`	Signs for an institution in which the user holds a role

The path `m/44'/31416'/0'/1/0` is reserved.

13.2 Custody

- **Hosted custody** is the default. The platform stores the master secret as a Web3 Secret Storage keystore [21] encrypted under a key derived from the user's password with Argon2id [22]. The password is known only to the user and is required for each signature.
- **Self-custody.** The user exports the keystore or the mnemonic, and the platform keeps no copy.
- **Hardware wallet.** The secret stays on a BIP-32 device, which derives the addresses and signs.

Because no address holds any asset, the loss or theft of a key cannot cost the user money. The exposure is to their identity: a thief could sign consents in their name. Trusted signers with a narrow scope and an expiry, and hardware custody for institutional keys, limit that exposure.

13.3 Recovery

The contracts have no recovery mechanism. A user who loses the master secret loses control of the identifier, and its records remain. A new identifier can be linked to the old one by an off-chain statement signed through the user's institution and countersigned by the platform. Recovery is handled as an operational procedure, to keep the contracts small.

14. Governance and Upgrades

14.1 Roles

Administrative powers over the contracts are held by a multi-signature account, referred to in the code as the Foundation Safe. It registers and deactivates contexts, extends the taxonomies, authorises relayer targets and schedules upgrades. Its signers and threshold are published at mainnet launch, and changes to them are visible on chain.

14.2 Timelocks

Each contract sits behind a proxy whose implementation can be replaced only through a timelock controller. An upgrade is scheduled publicly, waits for the delay (24 hours for Registry, Track and Subscription; 48 hours for Router and Relayer), and only then takes effect. During the delay anyone can inspect the proposed code.

A separate emergency role can apply a fix after one hour. Its use emits a distinct event, and each use is to be followed by a published explanation.

14.3 What upgradeability costs

The contracts are upgradeable, because a defect in an immutable contract that holds identity records can be corrected only by abandoning the contract. The price is a trust assumption: the holders of the upgrade keys could, after the delay, install code that misbehaves. Three things bound this. The delay gives every observer time to object and every institution time to stop relying on the chain. An upgrade cannot alter blocks already sealed, so the history of what was recorded, and under which code, stays intact. External anchoring fixes that history beyond the reach of the key holders.

14.4 Path to shared governance

At bootstrap all signers of the Safe are appointed by IAIC FZCO. As institutions join as validators, they are added as signers, with the aim that no upgrade can be scheduled by the operator alone. The paper makes no promise about the date; the composition at any moment is public.

15. Regulatory Positioning

This section states the operator's position. It is not legal advice, and written confirmation from counsel in the United Arab Emirates is a condition of mainnet launch (Section 18).

15.1 Jurisdiction

IAIC AI Research & Trading FZCO is a free zone company incorporated in the Emirate of Dubai. Platform agreements are governed by the law of the Emirate of Dubai and applicable federal law of the United Arab Emirates.

15.2 Virtual assets

Regulation of virtual assets in Dubai, administered by the Virtual Assets Regulatory Authority [26], and comparable regimes elsewhere (the Markets in Crypto-Assets Regulation in the European Union [24], among others) attach to the issuance of, and services relating to, digital representations of value that can be traded, transferred or used for payment or investment.

ENB creates no such representation. There is no coin or token, no balance at genesis or afterwards, no fee, and no contract function that accepts or moves value. The operator issues nothing, sells

nothing on chain, holds nothing for users, and runs no exchange, transfer or custody service. Services of the platform are sold in fiat currency through ordinary payment processors and are not settled on the chain.

Should a later version introduce any transferable unit, that would be a new design, subject to legal review and to whatever licence the law then requires, before any deployment. Nothing in this version prepares for it: no supply is reserved and no allocation exists.

15.3 Data protection

The data policy of Section 5 is designed to meet the principle of data minimisation [23]. No personal data is written in clear. Records about persons are salted commitments, written with the person's signature. Rights of access, rectification and portability are exercised against the off-chain stores of the platform and of the issuing institutions. The limits of erasure on a ledger are disclosed in the terms of service and explained in Section 5.

15.4 Publishing norms

Editorial policy follows the guidance of the Committee on Publication Ethics [27]. Recording a review or an editorial decision on chain changes none of the obligations of confidentiality: the commitment discloses nothing.

16. Privacy

16.1 What an observer of the chain learns

An observer sees that an identifier holds a record of a given type under a given institution, and when it was written. The observer does not learn who owns the identifier, unless the owner has published the link, and does not learn the content of any class C record.

This is pseudonymity. It is weaker than anonymity. A person who publishes their identifier, or whose pattern of records is distinctive, can be recognised. Users are told so, and no record about a person is written without that person's signature.

16.2 Reducing linkage

Separate derived addresses keep a user's roles apart. Records submitted through the relayer can be batched, so that the time of a block need not reveal the exact time of the user's action.

16.3 What is not claimed

The design does not protect against an adversary who holds off-chain data, such as the platform's own databases or a payment processor's logs, and can correlate it with the chain. It raises the privacy of ordinary scholarly and commercial activity; it is not built for hostile environments.

17. Further Fields of Use

The contracts make no assumption about the subject matter of a record. A new field needs institutions registered as contexts, record types added to the taxonomy, and an agreed off-chain format for the data behind each commitment. The fields below are within the design and none is active.

17.1 Education

A university registers as a context and issues course completions and degrees as attestations co-signed by the graduate. A certificate can be verified without contacting the registrar.

17.2 Professional credentials

Employers and professional bodies attest positions held and qualifications gained. Through an access grant, a person lets a prospective employer receive records held by a previous one.

17.3 Clinical research

Trial protocols, endpoints and analysis plans are committed before a study begins, which lets anyone confirm afterwards that the published analysis is the registered one. Anonymised outcome datasets are committed at release. Under the data policy, health data about an identifiable person is class N and is never written, in any form. A patient's consent to share records between two clinics is expressed as an access grant; the records themselves pass between the clinics off chain.

17.4 Conditions

The value of a credential depends on the standing of its issuer. None of these fields is opened before recognised institutions have agreed to issue records and, for regulated fields, before the applicable rules have been reviewed.

18. Implementation Status and Roadmap

18.1 State in November 2026

Running.

- A public test network, chain identifier 31416, in operation since April 2026 with a block every five seconds. It runs Clique proof of authority on go-ethereum 1.13 with validators operated by IAIC FZCO, and is therefore operator-run in the sense of Section 4.3.
- A public explorer at `enb.world`: blocks, transactions, addresses and search.
- The messenger's pulse and daily digest, written to the testnet since November 2026 and verifiable from the explorer.
- An earlier generation of the contracts, deployed on the testnet.

Implemented, not deployed.

- The contract suite described in Section 6, with its tests, in the source repository.

Not yet done.

- A tagged release of the five-contract suite with a published test report.
- The QBFT network: genesis without allocations, zero-fee configuration, write allowlist.
- Clear-text payloads per record type, with the size limits of the data policy, in the Track.
- External anchoring.
- An independent security audit.
- Any validator operated by an institution other than IAIC FZCO.

The test network uses funded test accounts, as go-ethereum test networks ordinarily do. These are test values with no holder outside the operator, and they do not carry over: the production network starts from a genesis with no allocations.

18.2 Roadmap

The phases are ordered by dependency. Dates are published on `enb.world` as each phase is committed.

Phase	Work	Complete when
1. Release build	Finalise the five-contract suite; add clear-text payloads with limits	Tagged release; all tests pass; test report published
2. QBFT testnet	Relaunch testnet 31416 on Besu with zero fees and no allocations	Explorer shows the new network; digest and pulse written to it
3. Record carry-over	Re-submit testnet records to the new network with references to the original transactions	Every earlier digest is verifiable on the new network
4. Anchoring	Regular commitments through OpenTimestamps	Proofs published and checkable for each interval
5. Audit and legal review	Independent audit of the five contracts; written legal opinion	Audit report published; opinion received
6. Mainnet, operator-run	Launch chain 31415; journals, subscriptions, conference records	First article attested and bound on mainnet
7. Consortium	Onboard validators from independent institutions; add them as governance signers	Four validators across three institutions
8. Further operations	Per-goal commitments, key directory, software releases, standards	Each operation documented and verifiable

The mainnet may open in the operator-run state. Until phase 7 is complete it will be described as operator-run, and its guarantee against rewriting will be stated as resting on anchoring.

19. Risks and Mitigations

Risk	Likelihood	Impact	Mitigation
No independent validator joins	Medium	High	Anchoring from launch; network named operator-run until the threshold is met; validators recruited among institutions that issue records
Validator or governance key compromised	Medium	High	Hardware keys; multi-signature; timelocks; validator rotation by vote
Defect in a contract	Low–med.	High	Tests; independent audit before mainnet; timelocked upgrade path; emergency role with public trace
Abuse of free transactions	Medium	Medium	Write allowlist at validators; rate limits per user at the relayer; block gas limit
Personal data written by mistake	Low	High	Clear text restricted by record type; size limits; personal data excluded from clear text by rule; review of each new record type
Regulatory change	Medium	Medium	No asset on chain; legal opinion before mainnet; periodic review
Low adoption	Medium	Medium	The platform's own journals, conference and messenger supply records from the first day; value to others grows with each issuing institution
Availability of a small network	Medium	Medium	Several validators in separate facilities; observer nodes; public snapshots of the chain
Records outlive the operator	Low	High	Open-source contracts and client; any institution holding a copy of the chain can continue it or serve it read-only

20. Relation to Existing Systems

20.1 ORCID and DOI

ORCID [33] identifies researchers and DOIs [34] identify publications. Both are registries run by central bodies, and neither commits to content. ENB adds content commitments and co-signed attestations, and is used alongside them: an article carries a DOI and an ENB identifier.

20.2 Preprint servers and repositories

arXiv, Zenodo and institutional repositories store and serve documents. ENB stores proofs about documents and is not a repository. A preprint on any server can be recorded as a self-claimed record that commits to its file.

20.3 Public blockchains

A record could be written to a public chain such as Ethereum. That requires each writer to hold and spend a cryptocurrency, exposes users to fee volatility, and places an institutional record system inside an asset market. ENB uses a public chain for one purpose, anchoring, and through a protocol that needs no asset.

20.4 Timestamping services

A trusted timestamp [10] proves that a document existed at a time. It does not record who attested what about whom, with whose consent, or how a record was later corrected. ENB's contracts add those relations.

20.5 Enterprise ledgers

Permissioned ledgers are widely used within consortia of companies, usually with access restricted to members. ENB differs in being open to read by anyone, since its records are meant for third parties who are not members.

20.6 Token-based science projects

Several projects fund or reward research through tokens. ENB does not compete with them and shares none of their mechanisms.

21. Conclusion

ENB is a ledger with rules and without money. Its premise is that the records of scholarly and platform life should be checkable by anyone and alterable by no one, and that this requires no coin.

The design rests on four elements: a proof-of-authority chain on which no asset exists; a data policy that says what may be written in clear and what may not be written at all; five contracts that require an institution's signature and a person's consent for every record about that person; and an external anchor that holds even the validators to the history they have sealed.

Section 18 separates what exists from what is planned. A test network runs, and the messenger's daily record is on it. The release build, the QBFT network, the audit, the legal confirmation and the first independent validator are work to be done, in that order, before the network is called what this paper describes. Progress will be reported in later versions.

References

[1] Wood, G. *Ethereum: A Secure Decentralised Generalised Transaction Ledger* (Yellow Paper). https://ethereum.github.io/yellowpaper/paper.pdf

[2] Enterprise Ethereum Alliance. *QBFT Blockchain Consensus Protocol Specification.*

https://entethalliance.github.io/client-spec/qbft_spec.html

[3] Moniz, H. *The Istanbul BFT Consensus Algorithm*. arXiv:2002.03613 (2020). doi:10.48550/arXiv.2002.03613

[4] Castro, M. and Liskov, B. "Practical Byzantine fault tolerance and proactive recovery." *ACM Transactions on Computer Systems* 20(4), 398–461 (2002). doi:10.1145/571637.571640

[5] Hyperledger Besu documentation. *Configure QBFT consensus*. https://besu.hyperledger.org/private-networks/how-to/configure/consensus/qbft

[6] Hyperledger Besu documentation. *Configure free gas networks*. https://besu.hyperledger.org/private-networks/how-to/configure/free-gas

[7] go-ethereum. *Asteria (v1.14.0)*. Release notes (2024). https://github.com/ethereum/go-ethereum/releases/tag/v1.14.0

[8] Nakamoto, S. *Bitcoin: A Peer-to-Peer Electronic Cash System* (2008). https://bitcoin.org/bitcoin.pdf

[9] Todd, P. *OpenTimestamps: Scalable, Trust-Minimized, Distributed Timestamping with Bitcoin* (2016). https://petertodd.org/2016/opentimestamps-announcement

[10] Haber, S. and Stornetta, W. S. "How to time-stamp a digital document." *Journal of Cryptology* 3(2), 99–111 (1991). doi:10.1007/BF00196791

[11] Merkle, R. C. "A certified digital signature." *Advances in Cryptology, CRYPTO '89*, Lecture Notes in Computer Science 435, 218–238. doi:10.1007/0-387-34805-0_21

[12] Szabo, N. "Formalizing and securing relationships on public networks." *First Monday* 2(9) (1997). doi:10.5210/fm.v2i9.548

[13] Melara, M. S., Blankstein, A., Bonneau, J., Felten, E. W. and Freedman, M. J. "CONIKS: Bringing key transparency to end users." *24th USENIX Security Symposium* (2015). https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/melara

[14] Bloemen, R., Logvinov, L. and Evans, J. *EIP-712: Typed structured data hashing and signing* (2017). https://eips.ethereum.org/EIPS/eip-712

[15] Sandford, R., Siri, L., Tirosh, D., Weiss, Y., Forshtat, A. et al. *EIP-2771: Secure protocol for native meta transactions* (2020). https://eips.ethereum.org/EIPS/eip-2771

[16] Palladino, S., Giordano, F. and Croubois, H. *EIP-1967: Proxy storage slots* (2019). https://eips.ethereum.org/EIPS/eip-1967

[17] Barros, G. and Gallagher, P. *EIP-1822: Universal upgradeable proxy standard (UUPS)* (2019). https://eips.ethereum.org/EIPS/eip-1822

[18] OpenZeppelin Contracts, version 5. https://docs.openzeppelin.com/contracts/5.x/

[19] Wuille, P. *BIP-32: Hierarchical deterministic wallets* (2012). https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki

[20] Palatinus, M., Rusnak, P., Voisine, A. and Bowe, S. *BIP-39: Mnemonic code for generating deterministic keys* (2013). https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki

[21] Web3 Secret Storage Definition. https://ethereum.org/en/developers/docs/data-structures-and-encoding/web3-secret-storage/

[22] Biryukov, A., Dinu, D., Khovratovich, D. and Josefsson, S. *Argon2 Memory-Hard Function for Password Hashing and Proof-of-Work Applications*. RFC 9106 (2021). doi:10.17487/RFC9106

[23] Regulation (EU) 2016/679 (General Data Protection Regulation). OJ L 119, 4.5.2016. https://gdpr-info.eu/

[24] European Securities and Markets Authority. *Markets in Crypto-Assets Regulation (MiCA)*. https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/markets-crypto-assets-regulation-mica

[25] European Commission. *AI Act Explorer: Regulation (EU) 2024/1689, the EU Artificial Intelligence Act*. https://ai-act-service-desk.ec.europa.eu/en/ai-act-explorer

[26] Virtual Assets Regulatory Authority (VARA), Dubai. *Virtual Assets and Related Activities Regulations 2023*. https://rulebooks.vara.ae/rulebook/virtual-assets-and-related-activities-regulations-2023

[27] Committee on Publication Ethics (COPE). *Code of Conduct*. https://publicationethics.org/membership/code-of-conduct

[28] Abu Dhabi Media Office. *Abu Dhabi Government launches Digital Strategy 2025–2027* (January 2025). https://www.mediaoffice.abudhabi/en/government-affairs/abu-dhabi-government-launches-digital-strategy-2025-2027/

[29] Gulf News. *Sheikh Hamdan announces launch of Dubai Universal Blueprint for Artificial Intelligence* (April 2024). https://gulfnews.com/uae/government/sheikh-hamdan-announces-launch-of-dubai-universal-blueprint-for-artificial-intelligence-1.1714404361861

[30] Akin Gump. *UAE set to use AI to write laws*. AI Law and Regulation Tracker (2025). https://www.akingump.com/en/insights/ai-law-and-regulation-tracker/uae-set-to-use-ai-to-write-laws

[31] The National. *Sheikh Mohammed announces AI system to become advisory UAE Cabinet member from 2026* (20 June 2025). https://www.thenationalnews.com/news/uae/2025/06/20/sheikh-mohammed-announces-ai-system-to-become-advisory-uae-cabinet-member-from-2026

[32] e-Estonia. *KSI Blockchain*. https://e-estonia.com/solutions/cyber-security/ksi-blockchain/

[33] ORCID. https://orcid.org

[34] International DOI Foundation. *DOI Handbook*. https://www.doi.org/the-identifier/resources/handbook

[35] Goncharov, S. and Nechesov, A. “Axiomatization of blockchain theory.” *Mathematics* 11(13), 2966 (2023). doi:10.3390/math11132966

[36] Nechesov, A. and Ruponen, J. “Empowering government efficiency through civic intelligence: merging artificial intelligence and blockchain for smart citizen proposals.” *Technologies* 12(12), 271 (2024). doi:10.3390/technologies12120271

[37] Goncharov, S. and Nechesov, A. “Solution of the problem P = L.” *Mathematics* 10(1), 113 (2021). doi:10.3390/math10010113

[38] Goncharov, S. and Nechesov, A. “Polynomial analogue of Gandy’s fixed point theorem.” *Mathematics* 9(17), 2102 (2021). doi:10.3390/math9172102

[39] Nechesov, A. and Goncharov, S. “Functional variant of polynomial analogue of Gandy’s fixed point theorem.” *Mathematics* 12(21), 3429 (2024). doi:10.3390/math12213429

[40] Nechesov, A. and Puzarenko, V. “Gandy direct-limit theorem: polynomial-time prediction on operator-generated networks.” *IEEE Access* 14, 128869–128885 (2026). doi:10.1109/ACCESS.2026.3725439

[41] Nechesov, A., Vityaev, E., Goncharov, S. and Sviridenko, D. “The task-based approach: a new paradigm for building trustworthy artificial intelligence.” *The Bulletin of Irkutsk State University. Series Mathematics* 54, 96–112 (2025). doi:10.26516/1997-7670.2025.54.96

[42] Vityaev, E., Goncharov, S., Sviridenko, D. and Nechesov, A. “The power of task-based approach in building trustworthy AI systems.” *Mathematics & AI* 1(1), 1 (2026). doi:10.66693/mathai.1001

[43] Nechesov, A. “Learning theory and knowledge hierarchy for artificial intelligence systems.” *2024 IEEE International Multi-Conference on Engineering, Computer and Information Sciences (SIBIRCON)*, 299–302. doi:10.1109/SIBIRCON63777.2024.10758505

[44] Nechesov, A. “Semantic programming and polynomially computable representations.” *Siberian Advances in Mathematics* 33(1), 66–85 (2023). doi:10.1134/S1055134423010066

[45] Nechesov, A. *IAIC 101:2026, International Standard for Autonomous AI Systems.* International Artificial Intelligence Committee (IAIC), Dubai, United Arab Emirates, 7 September 2026. doi:10.66693/iaic.101.2026. `https://iaic.world/standards/101/`

A. Network Parameters and Contract Addresses

```
Testnet (running, Clique, to be relaunched under QBFT)
  ENB_TESTNET_CHAIN_ID   = 31416
  Explorer               = https://enb.world

Mainnet (not launched)
  ENB_CHAIN_ID           = 31415
  ENB_REGISTRY           = <assigned at launch>
  ENB_TRACK              = <assigned at launch>
  ENB_ROUTER             = <assigned at launch>
  ENB_RELAYER            = <assigned at launch>
  ENB_SUBSCRIPTION       = <assigned at launch>
  GOVERNANCE_SAFE        = <assigned at launch>
```

Addresses are proxy addresses and do not change when an implementation is upgraded.

B. Format of the Messenger's Daily Digest

The data field of a digest transaction is a UTF-8 JSON object with two members:

```
{"sha256": "<64 hex characters>", "digest": { ... }}
```

The member `digest` holds the day and its figures: devices, openings, messages, calls, conversations begun, goals set, goals reached, sign-ins. To verify a day:

1. read the transaction from any node and decode its data field as UTF-8;
2. serialise the value of `digest` as JSON with keys sorted and no whitespace;
3. compute SHA-256 of the result and compare it with `sha256`.

The explorer performs these steps in the reader's browser against the node. The same records are served as JSON at `api.enigma.ist/api/goals/enb/digests`.

C. Document History

Report	Date	Notes
IAIC-TR-2026-01	2026-11-14	Specification of the tokenless ledger: QBFT consensus, five-contract suite, on-chain data policy, platform operations on chain, foundations in the task approach and learning theory, AI-native governance, relation to the IAIC 101 standard, external anchoring, status and roadmap.

D. About the Author



Andrey Nechesov, PhD is a mathematician and the founder of **IAIC AI Research & Trading FZCO**, the Dubai company that builds the Enigma messenger, the ENIGMA research platform and the Enigma Blockchain, of which he is the principal architect.

He founded and chairs the **International AI Committee (IAIC)** and is the lead organiser of **MathAI**, the international conference series on the mathematics of artificial intelligence (2025, 2026, and 2027 in Abu Dhabi). He is editor-in-chief of the journal *Mathematics & AI*. He is the author and editor-in-chief of IAIC 101:2026, the International Standard for Autonomous AI Systems [45], issued by the committee in September 2026.

He is based in Abu Dhabi. His main research there is on AI-native government and the governance of autonomous AI, pursued with senior faculty of the emirate's research universities and with founders and executives of Hub71, Abu Dhabi's global technology ecosystem.

His research began in mathematical logic and computability. With Academician S. S. Goncharov he published *Solution of the Problem $P = L$* [37] and two papers on a polynomial analogue of Gandy's fixed-point theorem [38, 39]; with V. Puzarenko, a Gandy direct-limit theorem for polynomial-time prediction on operator-generated networks [40]. With E. E. Vityaev, D. I. Sviridenko and S. S. Goncharov he develops the task-based approach to trustworthy AI [41, 42], and he is the author of a learning theory with a hierarchy of knowledge for AI systems [43]. His work now concerns AI whose results can be checked: language models combined with formal logic, autonomous AI and robotic systems whose behaviour can be verified, and the theory of blockchains. His publications on the subject of this paper include *Axiomatization of Blockchain Theory* (with S. S. Goncharov, *Mathematics*, 2023) [35] and *Empowering Government Efficiency Through Civic Intelligence: Merging Artificial Intelligence and Blockchain for Smart Citizen Proposals* (with J. Ruponen, *Technologies*, 2024) [36].

Contact: `nechesov@iaic.world` • `iaic.world` • `nechesov.com`

© 2026 IAIC AI Research & Trading FZCO. Text licensed under CC BY 4.0.