FIBON
YELLOW PAPER

Revised Edition, 20.04.2026

Contents

13. References

14. Team and Operational Structure

15. Appendix – Audit Reference

0. LEGAL NOTICE AND TECHNICAL SCOPE

This Yellowpaper is provided for informational and technical reference purposes only. It is intended to complement the Fibon Whitepaper by describing selected technical, architectural, operational, and token-mechanics components of the Fibon ecosystem in greater detail.

The Fibon project is operated and maintained by Global Alliance A.Ş., which is responsible for the development, management, legal representation, and operation of Fibon-related technologies, platforms, and services.

This Yellowpaper does not constitute a prospectus, an offer of securities, a solicitation to invest, or a recommendation to purchase, sell, hold, or transfer any asset in any jurisdiction where such activity would be unlawful or require registration, licensing, or approval.

FIBON is described as a utility-oriented digital token within the Fibon ecosystem and related infrastructure. Nothing in this Yellowpaper shall be interpreted as granting equity rights, ownership rights, debt claims, dividend entitlement, revenue share, profit participation, or any comparable financial or governance right in Global Alliance A.Ş. or the Fibon project, unless expressly stated in a separate legally binding agreement.

This Yellowpaper contains technical descriptions, design intentions, workflow models, architectural assumptions, token-logic explanations, and forward-looking implementation concepts. Such materials may evolve over time due to technical development, legal requirements, compliance constraints, security findings, governance decisions, market conditions, or strategic reprioritization.

Where this Yellowpaper and the current official Fibon Whitepaper are read together, the Whitepaper should be understood as the primary strategic and positioning document, while this Yellowpaper should be understood as the more technical and operational companion document.

If any statement in this Yellowpaper conflicts with:
applicable law,
binding legal documentation,
final deployed smart contract behavior,
exchange disclosures,
or the most current official project documentation,
the latter shall prevail.

References in this Yellowpaper to ISO 27001, SOC 2-aligned practices, cryptographic protocols, security design, governance controls, or infrastructure modules should be interpreted as design and operational statements unless otherwise confirmed through separate official certifications, audits, or legal materials.

All readers, participants, counterparties, and users are responsible for conducting their own legal, technical, financial, and regulatory assessment before relying on this document or engaging with the Fibon ecosystem.

1. DOCUMENT PURPOSE AND RELATIONSHIP TO THE WHITEPAPER

The purpose of this Yellowpaper is to explain how Fibon is intended to work, rather than to restate the broader strategic narrative already described in the Whitepaper.

The Whitepaper presents Fibon as:
a verifiable identity and trust infrastructure project,
supported by modular blockchain-based trust components,
with AI-assisted verification,
Polygon-aligned infrastructure logic,
utility-oriented token mechanics,
and governed smart contract administration.

This Yellowpaper therefore serves a narrower function. It is intended to provide additional detail on:

system architecture,
credential and compliance workflows,
token mechanics,
vesting and treasury logic,
smart contract governance,
privacy and cryptographic building blocks,
and implementation-oriented design principles.
Scope of this Yellowpaper
This document is intended to clarify:
which layers of the Fibon system are designed to be on-chain and which are not,
how token mechanics relate to ecosystem operations,
how verification and trust workflows may function in practice,
how governance and smart contract controls are structured,
and how privacy-aware and cryptographic modules support the overall architecture.
What this Yellowpaper is not

This document is not intended to:

replace the Whitepaper,
function as a marketing brochure,
make financial promises,
provide legal advice,
or serve as a final deployment specification for every future implementation.

Its role is explanatory and technical.
Why the Yellowpaper needs revision

The current legacy Yellowpaper still reflects an earlier structure centered on:
a broader KYC/AML platform description,
BSC-oriented architecture discussion,
older token usage language,
and a less modular product narrative.

The current Whitepaper, by contrast, now frames Fibon in a more focused way around:
verifiable identity,
AI-assisted verification,
modular infrastructure,
Polygon-backed trust logic,
updated token treatment,
and controlled governance.

This Yellowpaper revision is therefore intended to bring the technical documentation into alignment with the project's current strategic positioning.

2. TECHNICAL EXECUTIVE SUMMARY

Fibon is being developed as a modular digital infrastructure designed to support verifiable identity, compliance-enabling workflows, auditable trust records, and utility-oriented ecosystem coordination.

From a technical perspective, the system is not intended to rely on blockchain as a universal execution layer for every feature. Instead, Fibon uses blockchain selectively where distributed trust, tamper evidence, attestation, auditability, and programmable coordination provide clear value. This allows the system to preserve technical discipline while remaining adaptable to product and compliance requirements.

The core technical model of Fibon is built around four ideas:
verifiable identity and credential workflows,
privacy-aware and compliance-sensitive process logic,
modular verification and AI-assisted extensions,
and utility-oriented token mechanics tied to ecosystem operations.

In this design, the primary smart contract and token layer serve as the auditable and governed core of the system. More dynamic features—especially verification modules that may evolve more rapidly over time—can be implemented in modular layers outside the primary token core where appropriate. This reduces unnecessary smart contract complexity and supports faster iteration without weakening governance discipline.

Fibon's infrastructure direction also includes the use of Polygon as the principal blockchain environment for selected ecosystem functions. Polygon's EVM compatibility, cost efficiency, and operational accessibility make it suitable for a system that seeks to balance auditability, interoperability, and scalable implementation.

Accordingly, this Yellowpaper should be read as a technical companion to the Whitepaper. Its purpose is to explain how Fibon's architecture, workflows, token mechanics, governance controls, and cryptographic modules are intended to function at a system level.

3. SYSTEM SCOPE AND DESIGN PRINCIPLES

This Yellowpaper focuses on the technical and operational scope of the Fibon ecosystem.
Its purpose is not to describe every theoretical use case or every possible future market extension. Instead, it concentrates on the system layers that are currently most relevant to

Fibon’s technical identity:

identity and credential workflows,
compliance-enabling coordination logic,
privacy-aware verification architecture,
blockchain-based trust anchoring,
token-enabled operational mechanics,
and governed smart contract controls.

3.1 System Scope

At a system level, Fibon is intended to support:
creation, registration, presentation, and validation of identity-linked or credential-linked workflows;
auditable event and process records where traceability matters;
modular support for onboarding, due diligence, verification, and related trust-sensitive interactions;
token-enabled access, participation, and operational coordination;
and integration paths with selected external service environments, including verification, identity, analytics, or compliance-related providers where appropriate.

The project is not designed as a claim that every workflow must be fully decentralized or fully on-chain. Nor is it positioned as a replacement for public authorities, regulated financial institutions, or licensed compliance service providers. Its technical scope is narrower and more practical: to provide a structured infrastructure layer for trust, verification, and coordination across digital ecosystems.

3.2 Design Principles

Fibon’s system design is guided by the following principles:

A. Selective Use of Blockchain

Blockchain is used where integrity, attestation, timestamping, auditable records, or programmable coordination benefit from distributed trust. It is not used indiscriminately for all product logic.

B. Modularity

System components should remain sufficiently modular to allow controlled evolution of features, especially in areas such as verification, analytics, and AI-assisted process support.

C. Auditability and Controlled Governance

Sensitive token, treasury, and administrative functions should operate under governed

controls rather than unilateral execution, with auditability preserved wherever technically and operationally appropriate.

D. Privacy-Aware Architecture

Identity and credential workflows should be structured in ways that support user control, selective disclosure, and privacy-conscious handling of sensitive information.

E. Interoperability

The system should remain compatible with relevant external environments, tools, and integration paths where this improves ecosystem usability without compromising design discipline.

F. Utility Orientation

Token mechanics and system interactions should correspond to operational ecosystem logic rather than symbolic or purely speculative positioning.

3.3 Technical Boundary

A critical technical boundary within Fibon is the distinction between:

the auditable smart contract and token core, and

the faster-moving functional and verification layers.

This distinction is intentional. It allows the core to remain more stable and governable, while allowing additional capabilities to evolve with greater implementation flexibility. This is particularly relevant in areas where verification methods, fraud patterns, and product expectations may change faster than the token core should.

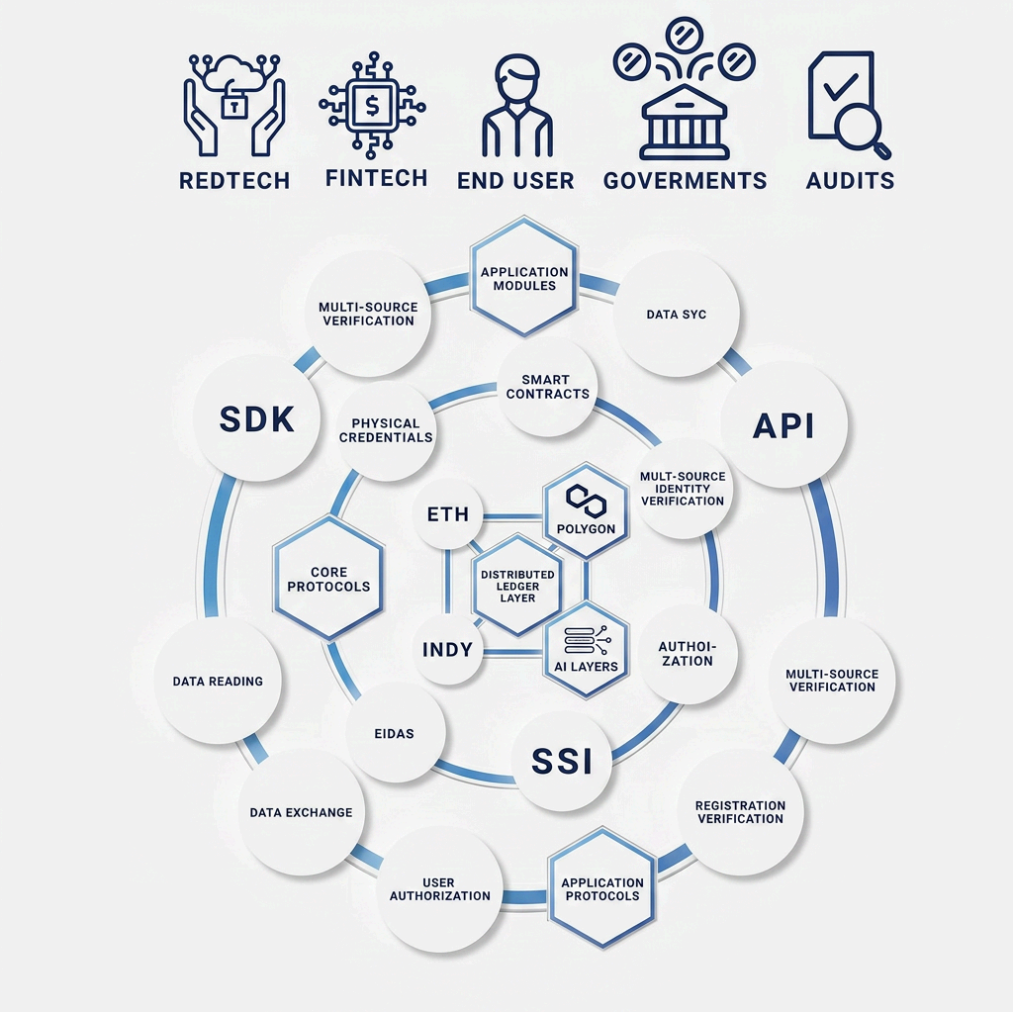
4. ARCHITECTURE OVERVIEW

Fibon is designed as a multi-layer technical architecture rather than a single monolithic blockchain application.

The system can be understood through five interacting layers:
4.1 Identity and Credential Layer
This layer supports the logic associated with identity, credentials, and verifiable trust artifacts.
It is intended to handle workflows such as:

credential registration,
credential presentation,
verification support,
privacy-aware disclosure,
and identity-linked process coordination.

This layer is central to Fibon’s technical direction because it addresses the repeated-friction problem in onboarding, verification, and trust establishment.



4.2 Workflow and Verification Layer

This layer supports process execution and decision-support logic around onboarding, review, due diligence, verification-sensitive approvals, and other trust-relevant operational workflows.
Depending on implementation scope, this may include:
rule-based workflow logic,
modular verification routines,
risk-oriented process support,
auditable event creation,
and compatibility with external verification or analytics modules.
This layer may combine on-chain and off-chain elements depending on security, compliance, and usability requirements.

4.3 AI-Assisted Extension Layer

This layer is intended to support AI-assisted verification and related modular intelligence capabilities.
Its role is not to replace institutional judgment or regulated human review. Rather, it may support:
signal detection,
document or interaction assessment,
credential consistency checks,

fraud-aware assistance,
and verification-related process enhancement.
This layer is intentionally designed to remain more modular than the primary token core. That separation allows technical iteration without unnecessarily expanding the complexity or governance burden of the core smart contract environment.

4.4 Blockchain and Smart Contract Layer

This layer provides the trust infrastructure required for:
attestation,
tamper-evident records,
governed token logic,
programmable coordination,
timestamped process evidence,
and selected ecosystem-level smart contract operations.

The role of this layer is not to absorb every product interaction. Its role is to support those parts of the system where distributed trust and auditable execution are genuinely useful.
Within this framework, smart contracts may support token mechanics, vesting logic, controlled administrative functions, and other selected workflow components.

4.5 Token and Ecosystem Coordination Layer

This layer describes how FIBON interacts with the broader ecosystem as a utility-oriented token.
Its technical role may include:
access to selected modules or services,
transaction-related infrastructure logic,
token-enabled ecosystem participation,
coordination across users, service environments, and counterparties,
and other live utility flows as implemented in the ecosystem.

This layer should not be understood in isolation from the rest of the architecture. Its meaning depends on the surrounding infrastructure, workflow logic, governance, and legal framework.

4.6 Supporting Security and Privacy Layer

Across all architectural layers, Fibon may use supporting privacy and security components including:
verifiable credentials,
selective disclosure logic,
user authorization protocols,
cryptographic integrity checks,
multi-signature governance controls,
and advanced privacy-oriented methods such as zero-knowledge proofs, secure multiparty computation, and homomorphic encryption where applicable.
These components are not independent marketing features. They are supporting mechanisms that strengthen the system’s broader trust and verification design.

4.7 Architectural Outcome

Taken together, Fibon's architecture is intended to achieve a balanced model in which:
blockchain is used where trust infrastructure matters,
modular layers are used where adaptability matters,
governance is used where control matters,
and privacy-aware design is used where identity and verification matter.

This architecture is intended to make the system more practical, more governable, and more adaptable than a design that treats blockchain as the default location for every function.

5. IDENTITY, CREDENTIAL, AND COMPLIANCE WORKFLOWS

Fibon is intended to support identity-sensitive and compliance-sensitive workflows through a structured combination of credential logic, verification processes, auditability, and privacy-aware architecture.

This section describes the core operational workflows that form the technical basis of the Fibon system. These workflows should not be interpreted as replacing legal, institutional, or regulated review. Rather, they are intended to support more efficient and interoperable trust processes in environments where identity verification, due diligence, and risk-sensitive interactions are operationally necessary.

At a high level, Fibon's workflow model is designed to support:

customer and user identification,
due diligence and enhanced due diligence support,
risk classification and scoring inputs,
onboarding and credential registration flows,
proof-oriented verification of digital asset control,
and chain-related risk signal assessment.
These workflow categories were already central to the legacy Yellowpaper and remain relevant, but they are now reframed within the narrower and more disciplined infrastructure model set out in the current Whitepaper.

5.1 CUSTOMER IDENTIFICATION

Customer identification is the initial verification stage in which the system records, validates, or references the core identity attributes required for a trust-sensitive interaction.

In practical terms, this stage may include collection and verification of information such as:

name or legal entity name,
address or residency-related information,
date of birth where applicable,
identification number or comparable identity reference,
and supporting document or credential evidence where required.

Within Fibon, customer identification should not be understood as a single rigid process. Depending on the context, implementation model, and applicable law, identification may rely on:
physical identity documents,
digital representations of physical credentials,
externally issued digital credentials,
or previously verified trust artifacts that can be presented and validated in a verifiable format.

The technical objective of this stage is to reduce duplication and ambiguity in downstream workflows by establishing a more structured starting point for verification, onboarding, and trust transfer.

Design Considerations

The customer identification stage is intended to be:

modular, rather than dependent on a single document type;
privacy-aware, rather than based on indiscriminate data exposure;
auditable, where process traceability matters;
and interoperable, where credential reuse is lawful and technically feasible.

5.2 CUSTOMER DUE DILIGENCE AND ENHANCED DUE DILIGENCE

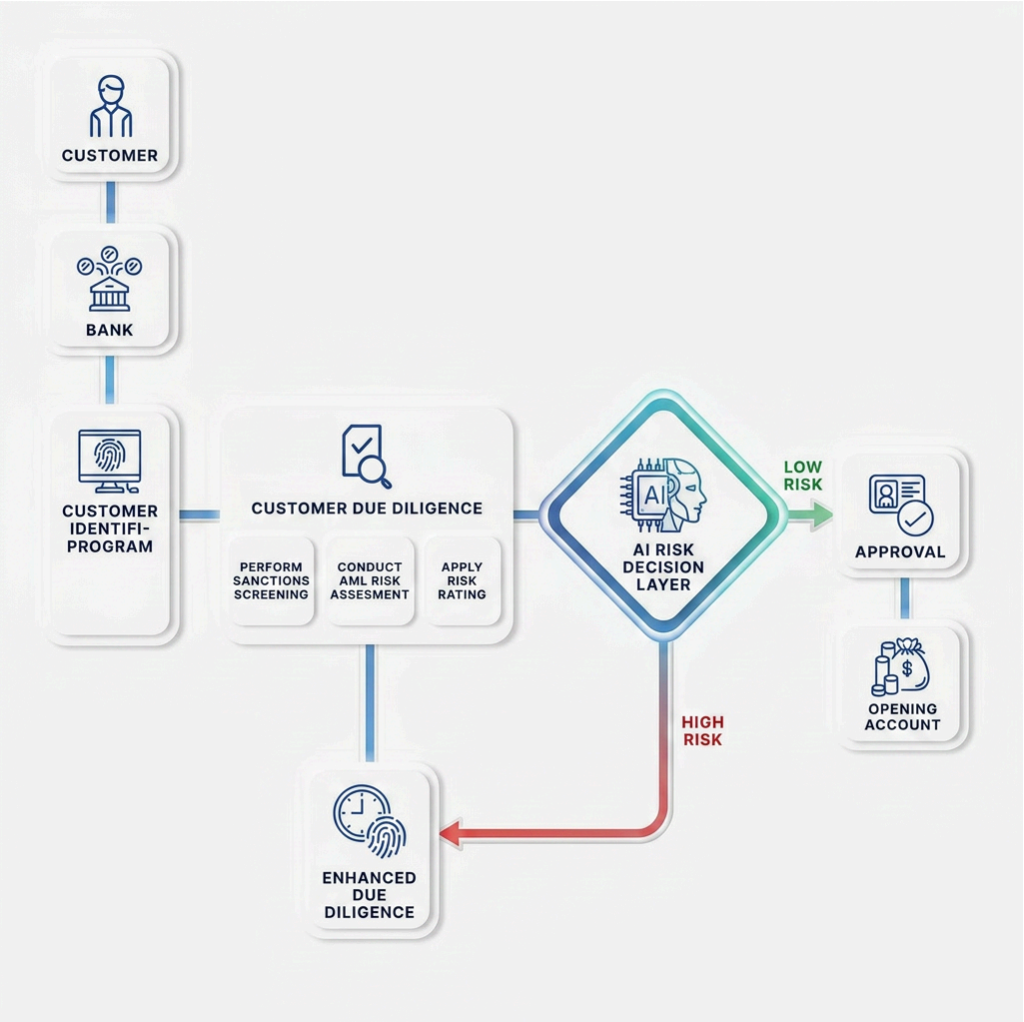
Following identification, the system may support due diligence workflows that help structure the collection, review, and interpretation of relevant risk-related information.

Customer Due Diligence (CDD)

CDD refers to the structured evaluation of a user, counterparty, or entity profile in order to determine whether the relationship presents low, moderate, or elevated operational or compliance risk. In the legacy Yellowpaper, this logic was framed around evaluating client profiles for money laundering or terrorist financing concerns and assigning risk categories accordingly.

In the updated Fibon model, CDD should be understood more broadly as a compliance-enabling workflow that may support:

identity-linked review,
structured information gathering,
credential validation,
contextual risk assessment,
and traceable onboarding logic.
Enhanced Due Diligence (EDD)



EDD applies in situations where elevated risk requires stronger review, additional supporting evidence, or more intensive monitoring logic.

Examples of higher-risk circumstances may include:

politically exposed persons (PEPs),
negative watchlist or adverse profile findings,
unusual ownership structures,
non-face-to-face onboarding conditions,
higher-risk jurisdictions,
or relationships requiring deeper source-of-funds or source-of-wealth review.

Within Fibon, EDD is not treated as a separate ideology but as an intensified branch of the same trust workflow model: higher uncertainty should trigger more structured scrutiny.

5.3 RISK SCORING LOGIC

Fibon’s workflow architecture may incorporate risk scoring logic to support structured decision-making in onboarding, due diligence, review prioritization, and other trust-sensitive processes.

The goal of risk scoring is not to produce a magical number that replaces judgment.

Its purpose is to:
organize risk-relevant inputs,
stratify profiles or relationships into usable categories,
and support more consistent downstream review logic.

In the legacy Yellowpaper, risk scoring was described in terms of client type, ownership, business category, jurisdiction, and inherent risk rating examples.
In the updated model, the same logic can be retained, but expressed more clearly as a modular scoring framework.

Possible Risk Inputs

Risk scoring may draw on inputs such as:

identity or credential status,
document consistency,
jurisdictional exposure,
behavioral anomalies,
historical interaction patterns,
counterparty characteristics,
source-of-funds or source-of-wealth indicators,
chain-related risk signals,
and external or partner-provided verification data.
Functional Purpose

Risk scoring is intended to support:

workflow prioritization,
escalation into enhanced review,
traceable approval or rejection logic,
reduction of purely ad hoc decision-making,
and more consistent interpretation of trust-sensitive information.

Where AI-assisted logic is used, risk scoring may also benefit from modular analytical support, but the resulting output should still be understood as an input into process logic rather than an automatic legal conclusion.

5.4 FIBON ONBOARDING WORKFLOW

The Fibon onboarding model is intended to support a structured trust flow in which a user or participant can move from identification toward credential registration, presentation, and verification.

The legacy Yellowpaper described onboarding in three parts:

installation,
credential registration,
and credential presentation.
That structure remains useful, but it should be written more clearly in the updated Yellowpaper.

Step 1 — Initialization

A user enters the system through a wallet, application environment, or equivalent access layer capable of supporting identity-linked and credential-linked interactions.

At this stage, the system may establish:

a wallet or account environment,
a public-private key structure or comparable credentialing basis,
and an identity-linked reference suitable for later trust interactions.
Step 2 — Credential Registration

The user presents identification or supporting credentials through the relevant workflow.

Depending on implementation, this may involve:

direct submission of physical or digitized credentials,
verification support from a trusted provider,
generation of a signed or hashed reference,
and registration of trust-relevant outputs in a governed system layer.

The objective is not to store every raw document on-chain, but to create a verifiable and auditable basis for later trust confirmation.

Step 3 — Credential Presentation

A user may later present a credential, claim, or trust artifact to a verifier, service provider, or counterparty.

Where the system supports reusable verification, the receiving party may:

validate the credential or proof,
confirm its consistency against previously registered trust data,
and decide whether new onboarding steps are necessary or whether prior verification can be reused in a controlled way.

This is one of the key efficiency gains in the Fibon model: reducing redundant trust reconstruction where comparable verification has already been performed and can be reused lawfully and technically.

5.5 PROOF OF VIRTUAL ASSET OWNERSHIP

Fibon may also support workflows related to demonstrating control or verified association with a digital asset or blockchain address.

The legacy Yellowpaper addressed this as a distinct use case and correctly recognized that simple asset transfer is not always the best way to demonstrate control.

In the updated model, proof of virtual asset ownership should be understood as a verification-support workflow rather than a payment workflow.,

Functional Logic

A proof-of-ownership process may support:

demonstration of control over a wallet or address,
confirmation that a party can sign with the relevant private key,
structured presentation of ownership-related attestations,
and support for audit, due diligence, or counterparty verification scenarios.
Important Technical Distinction

Control and legal ownership are not always identical.

A system may verify that an entity controls a key, signs a message, or demonstrates access to a given address. That does not automatically settle every legal question regarding title, beneficial ownership, or off-chain claims. Accordingly, this workflow should be understood as a technical trust signal that may support broader review, not as a universal legal conclusion.

This distinction is important in:

audit support,
asset verification,
counterpart risk review,
and trust-sensitive digital interactions involving wallets or on-chain assets.

5.6 CHAIN SCORING AND RISK SIGNALS

In addition to identity and credential workflows, Fibon may support blockchain-related risk analysis through chain scoring and related signal processing.

The legacy Yellowpaper already positioned this as a use case relevant to anti-money laundering and suspicious activity detection, including examples such as suspicious transaction volumes, rapid in-and-out transfers, repeated asset conversion, anonymity tools, and suspicious source-of-funds indicators.

In the updated Yellowpaper, this should be reframed as a modular risk-signal layer.

Purpose of Chain Scoring

The purpose of chain scoring is to support:

risk-sensitive review of blockchain-linked activity,
structured interpretation of transaction behavior,
interaction with third-party analytics or RegTech tools where relevant,
and more informed trust or due-diligence workflows in digital asset contexts.
Possible Signal Categories

Signal categories may include:

unusual transaction volume or velocity,
repetitive cross-platform movement,

clustering patterns,
high-risk source or destination indicators,
mixing or anonymization exposure,
rapid asset cycling,
and other anomalous or policy-sensitive behaviors.
System Role

Chain scoring should be understood as:

an input into risk-sensitive process logic,
a support mechanism for compliance-oriented workflows,
and a modular analytical component rather than a standalone accusation engine.

It is intended to improve visibility and prioritization, not to replace formal investigation, legal process, or regulated judgment.

6. AI-ASSISTED VERIFICATION LAYER

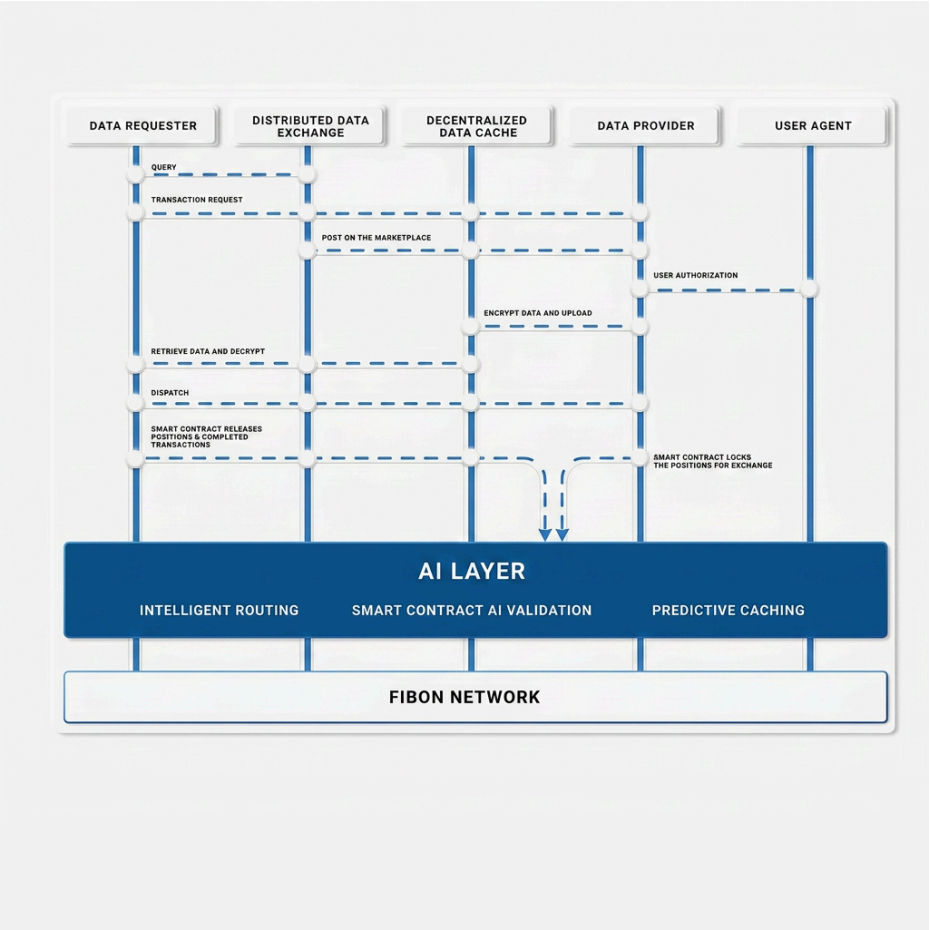
Fibon is being developed with the recognition that verification systems can no longer rely only on static rules or document checks. The increasing sophistication of fraud, synthetic identity activity, manipulated media, and document inconsistency requires more adaptive verification support. This logic is already explicit in the current Whitepaper, which positions Fibon as an AI-assisted verifiable identity infrastructure with modular extensions rather than a static blockchain-only system.

6.1 Functional Role

The AI-assisted layer may support:

credential consistency checks,
document and interaction assessment,
fraud-aware signal detection,
anomaly recognition,
and workflow support for trust-sensitive processes.

Its purpose is to improve speed, consistency, and operational responsiveness in environments where manual review alone may be too slow, too repetitive, or too expensive.



6.2 Non-Replacement Principle

AI in Fibon is not intended to replace:

legal judgment,
institutional accountability,
regulated review,
or human oversight where such oversight remains necessary.

The role of AI is assistive. It is a technical support layer, not an autonomous legal authority.

6.3 Modular Separation from the Core Contract Layer

A key design principle of Fibon is that fast-evolving verification logic should not automatically be embedded into the primary token and smart contract core.

Accordingly, AI-assisted features are better treated as modular layers that can evolve without unnecessarily expanding:

contract complexity,
governance burden,
audit surface,
or deployment rigidity.

This allows the auditable token core to remain more controlled while allowing verification intelligence to adapt more dynamically over time. That modular separation

is one of the clearest differences between the updated architecture and the older monolithic narrative.

6.4 Strategic Relevance

This layer is important because the verification environment is changing faster than traditional process design.

As fraud techniques evolve, static systems become less reliable. A modular AI-assisted layer gives Fibon a more realistic path for adapting to:

new fraud patterns,
evolving user behavior,
changing risk signals,
and broader operational demands across identity-sensitive digital ecosystems.

7. BLOCKCHAIN ROLE AND POLYGON INFRASTRUCTURE

Fibon uses blockchain selectively as a trust and coordination layer rather than as a default execution layer for every product feature.

The purpose of blockchain within the Fibon architecture is to support functions such as:

verifiable attestations,
tamper-evident records,
timestamped workflow evidence,
programmable coordination logic,
and utility-linked ecosystem operations where distributed trust is beneficial.

This approach reflects an important architectural principle: a system that attempts to place all application logic, verification routines, and business workflows directly on-chain becomes harder to govern, more expensive to update, and less adaptable to real-world product and compliance requirements.

Accordingly, Fibon's blockchain architecture is designed to preserve the strengths of on-chain infrastructure while avoiding unnecessary feature overload.

7.1 Design Rationale for Selective On-Chain Use

The system distinguishes between:

functions that benefit from immutable or auditable trust infrastructure, and
functions that are better handled through modular or off-chain layers.

On-chain logic is most appropriate where the system requires:

attestation,
integrity preservation,
governed token mechanics,
auditable event references,
or programmable coordination between ecosystem participants.

Off-chain or modular logic is more appropriate where the system requires:

rapid feature iteration,
more complex review workflows,
privacy-sensitive processing,
AI-assisted verification,
or adaptive logic that may change faster than the core contract layer should.

This separation is intended to improve:

governance clarity,
implementation flexibility,
security discipline,
and long-term maintainability.

7.2 Polygon Deployment Logic

Fibon's infrastructure direction includes the use of Polygon as the principal blockchain environment for selected ecosystem functions.

Polygon is suitable for Fibon's technical direction because it offers:

EVM compatibility,
lower transaction costs compared with more congested environments,
faster execution for selected operational flows,
and compatibility with established tooling, wallets, and development practices.

These characteristics make Polygon a practical environment for a system that seeks to balance:

scalability,
interoperability,
technical accessibility,
and operational efficiency.

From Fibon's perspective, Polygon is not chosen as a branding decision. It is chosen as an infrastructure environment aligned with the system's need for efficient on-chain coordination and trust anchoring without unnecessary execution overhead.

7.3 Smart Contract Layer and Modularity

The smart contract layer is intended to support the governed core of the system.

This may include:

token logic,
vesting and release controls,
administrative protections,
auditable governance-linked actions,
and selected ecosystem-level utility functions.

A central architectural rule is that the core smart contract layer should remain more stable, more auditable, and more governable than rapidly evolving product logic.

For this reason, Fibon separates:

the core token and contract layer, and
the modular functional layer, which may include verification support, AI-assisted analysis, workflow-specific logic, and other adaptable service components.

This separation is intended to:

reduce smart contract complexity,
contain governance burden,
limit unnecessary audit surface expansion,
and allow product capabilities to evolve without destabilizing the token core.

7.4 Practical Infrastructure Outcome

Taken together, Fibon's blockchain infrastructure is intended to produce a balanced technical outcome:

on-chain where trust anchoring matters,
off-chain or modular where adaptability matters,
governed where administrative sensitivity matters,
and interoperable where ecosystem participation requires compatibility.

This is the sense in which blockchain functions inside Fibon: not as a slogan, but as a controlled infrastructure layer.

8. FIBON TOKEN MECHANICS

FIBON is the utility-oriented digital token of the Fibon ecosystem. Its technical role is to support defined operational functions inside the broader infrastructure rather than to represent corporate ownership, debt, guaranteed return, or comparable financial entitlement. That framing is consistent with the revised whitepaper and also replaces older yellowpaper language that treated the token more broadly as service payment currency across the ecosystem.

The token layer should therefore be understood in relation to:

ecosystem access,
infrastructure coordination,
governed supply and release logic,
token-enabled workflow participation,
and selected operational interactions linked to the Fibon architecture.
8.1 Token Role in the Ecosystem

At a system level, FIBON may support:

access to selected modules or services,
token-enabled participation logic,
transaction-related infrastructure functions,
credential-linked or verification-linked interaction flows,
and coordination across users, partners, and service environments.

The token is not described as existing in isolation from the rest of the system. Its role depends on the surrounding architecture, live ecosystem implementation, legal framework, and operational deployment model.

8.2 Supply Structure

FIBON has a defined maximum supply of 5,882,000,000 tokens.

Within this structure:

972,410,000 tokens are categorized as unlocked,
and 4,909,590,000 tokens are categorized as locked.

This means the current supply structure distinguishes between:

a controlled unlocked allocation base,
and a much larger locked reserve structure intended to support staged availability and release discipline.

The supply model is intended to align token availability with:

ecosystem growth,
launch readiness,
strategic expansion,
treasury planning,
and controlled release timing.

8.3 Allocation and Distribution Logic

The token allocation model is intended to reflect operational ecosystem needs rather than symbolic distribution.

Existing allocation categories include:
Shareholders,
P. Launch Partners,
ICO 1,
Bonus for ICO 1,
ICO 2,
Bonus for ICO 2,
ICO 3,
Bonus for ICO 3,
Liquidity Provision and DEX,
Marketing,
Research & Development,
and Strategic Partnerships.

These categories indicate that the token model is intended to support:

stakeholder alignment,
phased market-entry structure,
liquidity preparation,
ecosystem growth,
technical development,
and strategic integrations.

The allocation logic should be read together with vesting, treasury, and governance sections, because allocation without controlled release logic does not by itself create a disciplined token system.

FIBON TOKEN ALLOCATION

Detailed breakdown of unlocked coins

UNLOCKED COINS	NUMBER OF TOKENS	% OUT OF TOTAL TOKEN SUPPLY	% OUT OF UNLOCKED COINS	CLIFF PERIOD (MONTHS)	VESTING PERIOD (MONTHS)
Shareholders	268,700,000.00	4.57%	27.63%	0	36
P.launch Partners	58,820,000.00	1.00%	6.05%	3	3
ICO 1	58,820,000.00	1.00%	6.05%	0	0
Bonus for ICO 1	26,424,000.00	0.45%	2.72%	3	12
ICO 2	44,000,000.00	0.75%	4.52%	0	0
Bonus for ICO 2	17,420,000.00	0.30%	1.79%	6	12
ICO 3	25,176,000.00	0.43%	2.59%	0	0
Bonus for ICO 3	11,000,000.00	0.19%	1.13%	12	12
Liquidity Provision and DEX	346,550,000.00	5.89%	35.64%	0	24
Marketing	44,000,000.00	0.75%	4.52%	0	36
Research & Development	50,000,000.00	0.85%	5.14%	0	6
Strategic Partnerships	21,500,000.00	0.37%	2.21%	6	24
TOTAL	**972,410,000.00**	**16.53%**	**100.00%**	-	-

Revised Edition, 20.04.2026

8.4 Vesting, Release, and Treasury Controls

FIBON's token structure includes release discipline through cliff periods and vesting periods across different categories. Existing tables already show that different allocations may follow different timing structures, including immediate availability for some categories and multi-month cliffs or vesting schedules for others.

The purpose of vesting and release controls is to:

reduce sudden supply pressure,
align medium- and long-term stakeholders with ecosystem execution,
protect launch stability,
and preserve treasury discipline.

Treasury controls may also include:

designated treasury wallets,
governed transfer authorization,
multi-signature approval logic,
auditable movements,
and controlled release procedures for sensitive categories.

This framework is intended to keep token availability tied to execution discipline rather than uncontrolled release behavior.

8.5 ICO and Public Distribution Structure

The current token structure includes three ICO phases, each with base token amounts and bonus components. The total ICO coin allocation, including bonuses, is listed as 182,840,000 tokens. Price and timing fields in the current tables remain marked as TBA.

This phased structure indicates that public-facing distribution is intended to be staged rather than released through a single unrestricted allocation event.

The ICO logic should be understood as a structured distribution mechanism connected to broader launch, treasury, and ecosystem planning.

FIBON ICO PHASES OVERVIEW

Detailed breakdown of token allocation by ICO phases

ICO 1

ICO PHASES	NUMBER OF TOKENS	% OUT OF TOTAL TOKEN SUPPLY	BONUS %	PRICE PER TOKEN (IN USD)	CLIFF PERIOD (MONTHS)	VESTING PERIOD (MONTHS)	DATE
ICO 1	58,820,000.00	1.00%	-	TBA	0	0	TBA
Bonus for ICO 1	26,420,000.00	0.45%	44.92%	-	3	12	-
TOTAL ICO 1	**85,244,000.00**	**1.45%**	**-**	**-**	**-**	**-**	**-**

ICO 2

ICO PHASES	NUMBER OF TOKENS	% OUT OF TOTAL TOKEN SUPPLY	BONUS %	PRICE PER TOKEN (IN USD)	CLIFF PERIOD (MONTHS)	VESTING PERIOD (MONTHS)	DATE
ICO 2	44,000,000.00	0.75%	-	TBA	0	0	TBA
Bonus for ICO 2	17,420,000.00	0.30%	39.59%	-	6	12	-
TOTAL ICO 2	**61,420,000.00**	**1.04%**	**-**	**-**	**-**	**-**	**-**

ICO 3

ICO PHASES	NUMBER OF TOKENS	% OUT OF TOTAL TOKEN SUPPLY	BONUS %	PRICE PER TOKEN (IN USD)	CLIFF PERIOD (MONTHS)	VESTING PERIOD (MONTHS)	DATE
ICO 3	25,176,000.00	0.43%	-	TBA	0	0	TBA
Bonus for ICO 3	11,000,000.00	0.19%	43.69%	-	12	12	-
TOTAL ICO 3	**36,176,000.00**	**0.62%**	**-**	**-**	**-**	**-**	**-**

TOTAL ICO COIN ALLOCATION (INCLUDING BONUSES)	**182,840,000**

Revised Edition, 20.04.2026

8.6 Token Interaction and Operational Flows

FIBON is intended to function as part of a live ecosystem.

Depending on implementation scope, token interactions may include:

access to services or modules,
workflow-linked participation,
token-enabled coordination,
selected infrastructure actions,
verification-linked ecosystem interactions,
and partner or service-linked operational logic.

For technical clarity, token interaction can be viewed across three categories:

A. User-Facing Interactions

These may include access, participation, and workflow actions performed by end users within the ecosystem.

B. System-Level Interactions

These may include internal coordination logic, transaction-linked infrastructure behavior, or selected utility execution inside the governed environment.

C. Partner or Integration-Level Interactions

These may include token-linked logic connected to approved partners, service environments, or interoperable ecosystem functions.

This interaction framework should be understood as ecosystem mechanics, not as a guarantee that every token function is live in every jurisdiction, release phase, or product version.

8.7 Use of Funds Logic

The existing token documentation also includes an indicative use-of-funds structure organized across:

Product Development,
Corporate Operations,
Marketing & Communication,
and Reserve & Liquidity Buffer.

This indicates that collected funds are intended to support:

technical buildout,
legal and operational setup,
communication and ecosystem growth,
and liquidity or reserve planning.

That use-of-funds logic should be read as an operational planning framework rather than as a promise of outcome or return.

8.8 Token Mechanics Summary

Taken together, FIBON's mechanics are intended to support:

controlled supply structure,
defined allocation logic,
staged release discipline,
governed treasury handling,
structured public distribution,
and utility-oriented ecosystem participation.

The token layer should therefore be understood as part of Fibon's broader infrastructure model rather than as a standalone speculative object.

9. GOVERNANCE, ADMINISTRATIVE CONTROLS, AND AUDIT STATUS

Fibon's governance and smart contract control model is designed to support operational discipline, auditability, and controlled administration across the token and related contract environment.

The system is not designed around the assumption that all administrative power should be absent. Instead, it is designed around the principle that sensitive actions must be governed, restricted, and auditable.

9.1 Governance Objective

The objective of the governance layer is to balance:

operational continuity,
treasury and token discipline,
controlled emergency response,
vesting integrity,
and resilience against unilateral administrative action.

This means the contract environment is intended to preserve enough control to protect the system, while avoiding unconstrained single-actor authority.

9.2 Multi-Signature Administrative Control

Critical smart contract functions are intended to operate under a multi-signature authorization model.

This means that protected actions should require coordinated approval from a predefined governance set rather than execution by a single individual or wallet. In practical terms, this approach is intended to reduce:

unilateral control risk,
unauthorized administrative action,
governance fragility,
and operational concentration around a single actor.

The current Whitepaper and audit-oriented materials already describe this as a core design principle of the system.

9.3 Controlled Privileges

Some contract-level privileges may be retained intentionally for operational stability and system protection.

These may include:

supply-related controls,
blacklist-related controls,
governed transfer fee adjustment,
upgrade-related administrative actions,
and other contract-level intervention points where system continuity or risk mitigation may require a controlled response.

Such privileges should not be interpreted as arbitrary discretionary rights. Their intended role is limited to:

governed administration,
emergency protection,
technical continuity,
and ecosystem risk management.

9.4 Supply and Fee Governance

The Fibon contract model is designed to allow governed flexibility in specific parameters such as supply management and transfer-fee adjustment, where such flexibility is required by ecosystem design or operational necessity.

However, this flexibility is intended to remain subject to:

governance restrictions,
multi-signature authorization,
and auditable administrative logic.

The purpose of this design is to preserve technical adaptability without sacrificing oversight.

9.5 Vesting Integrity and Release Discipline

The vesting environment is intended to distinguish clearly between:

tokens that remain unvested and therefore still subject to defined administrative logic under the relevant rules,
and tokens that have vested and should no longer be retroactively altered.

This distinction is essential because it creates a boundary between:

controlled pre-vesting administration, and
post-vesting finality.

From a governance perspective, vesting integrity is one of the core mechanisms used to align release discipline with operational trust.

9.6 Emergency Governance Controls

The system may also include emergency governance controls across token, ICO, vesting, or related smart contract layers.

These controls are intended for:

incident response,
system protection,
risk mitigation,
and continuity management in exceptional situations.

They should not be interpreted as open-ended management rights. Their purpose is defensive rather than discretionary.

9.7 Audit Status

According to the current project materials, the Fibon token and related smart contracts were audited by 0xGuard, with the referenced audit dated March 2025. The current documentation states that the reviewed contract structure included strict multi-signature-controlled mechanisms, governed administrative protections, and vesting-related controls aligned with the project’s security and administration model.

The public audit reference is linked through the 0xGuard repository and should be treated as the externally referenced audit source for the smart contract layer.

9.8 Governance Interpretation

Fibon's governance layer should be understood as a controlled infrastructure model.

It is not a claim that the ecosystem is unmanaged. It is also not a claim that governance alone eliminates operational risk.

Rather, the governance model is intended to support:

administrative safety,
treasury discipline,
vesting reliability,
audit-linked trust,
and launch-ready contract control.

In this sense, governance is part of the technical trust model of Fibon, not merely an organizational afterthought.

9.9 Section Summary

Taken together, Fibon's governance model is intended to reflect:

multi-signature control rather than single-actor dependence,
governed flexibility rather than rigid fragility,
vesting discipline rather than uncontrolled release,
and audit-linked administration rather than undocumented token control.

This framework is intended to support the system's broader goal of building a technically credible and operationally disciplined trust infrastructure.

10. PRIVACY, CRYPTOGRAPHY, AND SECURITY MODULES

Privacy, cryptographic integrity, and controlled authorization are central to Fibon's architecture.

The project's technical direction depends not only on token mechanics or smart contracts, but also on the reliability of the trust and privacy layer that supports identity, verification, and credential-related workflows. The legacy Yellowpaper already contained strong technical material in this area, particularly around verifiable credentials, authorization, secure data exchange, multiparty computation, homomorphic encryption, and zero-knowledge proofs.

10.1 Design Purpose

The role of privacy and cryptography within Fibon is to support:

user control over trust-sensitive information,
selective disclosure of credential data,
verifiable claims and attestations,

secure authorization logic,
integrity-preserving data exchange,
and advanced privacy-preserving computation where applicable.

These modules are not separate marketing features. They are supporting technical components that strengthen the broader identity and trust infrastructure.

10.2 Verifiable Credentials

Verifiable credentials form one of the foundational trust objects in the Fibon architecture.

A verifiable credential may be understood as a digitally signed representation of an attribute, relationship, or claim that can be:

issued,
stored,
presented,
verified,
and, where necessary, revoked or expired.

The legacy Yellowpaper already framed verifiable credentials in this way and emphasized that they can represent the same information as physical credentials while becoming more tamper-evident through cryptographic signatures.

Within Fibon, verifiable credentials are relevant because they support:

reusable trust,
machine-verifiable identity artifacts,
selective information sharing,
and structured trust transfer across participants.
10.3 Multi-Source Authentication

Fibon may support identity and trust workflows that rely on more than one source of validation.

This includes the possibility of combining:

self-held identity artifacts,
external trust references,
ecosystem-issued claims,
and contextual trust indicators.

The legacy Yellowpaper described this in terms of multi-source authentication and external trust certification. In the updated model, the same logic can be retained but framed more clearly as a way to reduce dependence on a single isolated trust source.

10.4 User Authorization Protocol

User authorization is a core privacy layer in the Fibon system.

The authorization model is intended to ensure that access to user-linked data, credential-linked resources, or other protected interactions is not assumed automatically. Instead, relevant actions should be governed through explicit

authorization logic.

This may include:

defined access policies,
delegated authorization,
resource-request workflows,
verifiable authorization proofs,
and fine-grained permission structures.

The purpose of this model is to preserve user control while still allowing structured ecosystem interactions where trust-sensitive data flows are required.

10.5 Distributed Data Exchange Protocol

Fibon may also support a privacy-aware and authorization-aware model for controlled data exchange.

The legacy Yellowpaper described a distributed data exchange protocol in which:

a data requester,
a data provider,
a data owner,
and a user agent
can interact through a controlled, contract-supported process that protects both transaction flow and authorization logic.

In the updated framing, the key point is this:

Fibon is not simply moving raw data around. It is attempting to structure how sensitive or valuable information can be:

requested,
authorized,
shared,
verified,
and settled
under a more trust-aware model than traditional opaque exchange flows.

10.6 Secure Multi-Party Computation (SMPC)

Secure Multi-Party Computation is relevant to Fibon because it allows multiple parties to compute over private inputs without revealing those inputs to each other beyond what is implied by the output.

This makes SMPC useful in situations where:

collaborative computation is needed,
privacy must be preserved,
and no single party should gain access to all underlying data.

The legacy Yellowpaper correctly positioned MPC as a privacy-enhancing tool for trust-sensitive environments and noted its relevance for practical applications where participants need joint results without surrendering their private data.

Within Fibon, SMPC should be understood as a potential advanced privacy module rather than a mandatory default layer for every interaction.

10.7 Fully Homomorphic Encryption (FHE)

Fully Homomorphic Encryption allows computation to be performed on encrypted data without first decrypting that data.

The legacy Yellowpaper already described this as an important privacy-enhancing capability, especially in cases where sensitive information may need to be processed in untrusted or distributed environments.

In the context of Fibon, FHE is relevant because it points to a long-term architectural possibility:

privacy-preserving computation,
secure off-chain or on-chain processing,
and stronger confidentiality protection in advanced trust workflows.

At the same time, FHE should be treated as an advanced technical capability whose practical implementation may depend on performance, readiness, and system design constraints.

10.8 Zero-Knowledge Proofs (ZKPs)

Zero-Knowledge Proofs are highly relevant to Fibon because they allow a party to prove that a statement is true without revealing the underlying sensitive information itself.

The legacy Yellowpaper already emphasized their usefulness in:

self-sovereign identity,
confidential transaction logic,
and privacy-preserving smart contract environments.

Within Fibon, ZKPs may support:

selective disclosure,
attribute proofs,
privacy-preserving credential presentation,
and verifiable trust logic without unnecessary data exposure.

This is especially aligned with Fibon’s broader positioning around privacy-aware and reusable trust infrastructure.

10.9 Security-Oriented Integration

These privacy and cryptographic modules should not be understood in isolation.

Their purpose is to strengthen the broader Fibon architecture by helping the system achieve:

stronger confidentiality where required,
higher trust in credential and verification flows,
better user control,
and more technically credible privacy protection across sensitive interactions.

This is also consistent with the project's broader alignment around security-conscious design, auditable infrastructure, and privacy-aware workflows.

10.10 Section Summary

Taken together, Fibon's privacy and cryptographic layer is intended to support a trust infrastructure in which:

credentials can be verified without unnecessary disclosure,
user authorization remains central,
sensitive computations may be protected through advanced privacy methods,
and trust-sensitive workflows can be supported by stronger technical guarantees than traditional fragmented systems.

This layer is a core technical differentiator of Fibon's architecture, even where implementation depth may vary by phase, product scope, and operational readiness.

11. ROADMAP AND IMPLEMENTATION PHASES

The roadmap below outlines the phased development and rollout of the Fibon ecosystem and related infrastructure. Each phase reflects a structured progression in product readiness, token deployment, ecosystem growth, and operational expansion.

All phases remain subject to change depending on technical readiness, legal and regulatory requirements, market conditions, exchange requirements, partner coordination, and product priorities.

PHASE 1 – FOUNDATION

Fibon documentation and ecosystem structure refinement
Core smart contract preparation and security review
Token utility, allocation, and treasury structure confirmation
Identity and verification architecture definition
Operational and compliance framework preparation

PHASE 2 – INFRASTRUCTURE READINESS

Completion of core smart contract audit and launch preparation
Finalization of token-related infrastructure and governance controls
Treasury, liquidity, and operational planning
Alignment of ecosystem modules with launch requirements
Readiness of investor, legal, and ecosystem documentation

PHASE 3 – PRIVATE PARTICIPATION AND EARLY SUPPORT

Early Backer onboarding
Strategic early-stage participation and ecosystem alignment

Controlled private entry under the defined token structure
Final pre-launch coordination across product, legal, and token operations

(at the time of writing, this phase is expected to include early-backer participation in the range of approximately USD 100,000, subject to change)

PHASE 4 – PUBLIC TOKEN LAUNCH
Public launch of FIBON on a DEX / exchange platform
Launch-phase token access and ecosystem visibility
Listing-related operational execution
Liquidity and market-entry support
Public communication aligned with ecosystem rollout

(at the time of writing, a public launch through an exchange platform such as MEXC is among the actively considered paths, subject to change)

PHASE 5 – POST-LAUNCH ECOSYSTEM SUPPORT
Post-launch market and ecosystem support
Token visibility, communication, and community coordination
Liquidity and operational follow-through
Ongoing ecosystem stabilization and launch-phase monitoring
Structured support for growth and user engagement

PHASE 6 – PRODUCT EXPANSION
Expansion of identity, credential, and verification-related workflows
Rollout of modular AI-assisted verification capabilities
Development of selected user-facing and ecosystem-facing modules
Strengthening of Fibon's trust infrastructure and operational utility

PHASE 7 – STRATEGIC INTEGRATIONS AND SCALE-UP
Expansion into selected ecosystem and enterprise integrations
Development of additional token-enabled and trust-based service flows
Progressive scaling of infrastructure, interoperability, and ecosystem use cases
Prioritized growth based on product readiness, market demand, and strategic fit

ROADMAP NOTE:

This roadmap is provided for planning and informational purposes only. Features, sequence, deployment timing, and scope may be revised, expanded, delayed, or removed as the project evolves.

12. GLOSSARY

Below is a revised glossary aligned with the updated Whitepaper and Yellowpaper structure. It keeps the useful technical base of the legacy glossary while removing outdated token and payment phrasing. The legacy Yellowpaper glossary already contains many of these core concepts, including AML, CDD, CIP, EDD, FIBON Token, SMPC, selective disclosure, verifiable credentials, and ZKPs.

Anti-Money Laundering (AML)

A set of policies, procedures, and controls designed to detect, prevent, and respond to money laundering, terrorist financing, and related illicit financial activity.

Attestation

A signed or otherwise verifiable statement asserting that a claim, credential, event, or relationship has been reviewed or confirmed by an authorized party.

Auditability

The property of a system or workflow that allows relevant actions, records, or logic to be independently reviewed, traced, or verified.

Credential

A structured set of claims, attributes, or identifying information associated with a subject. Credentials may exist in physical, digitized, or fully digital form.

Customer Due Diligence (CDD)

A review process used to assess the identity, profile, and risk characteristics of a customer, user, or counterparty.

Customer Identification (CIP / Customer Identification Phase)

The initial stage of identity-related review in which a participant’s credentials or identifying information are collected and checked.

Enhanced Due Diligence (EDD)

A more intensive review process applied in cases where elevated risk requires additional evidence, scrutiny, or monitoring.

FIBON

The utility-oriented digital token of the Fibon ecosystem, intended to support selected operational and coordination functions within the broader infrastructure.

Fully Homomorphic Encryption (FHE)

A cryptographic approach that allows computation to be performed on encrypted data without first decrypting that data.

Governance Layer

The set of controlled administrative and authorization mechanisms that govern sensitive smart contract, treasury, and token-related actions.

Identity Verification

The process of validating whether a participant’s credentials, claims, or trust signals are sufficient for a given interaction.

Initial Coin Offering (ICO)

A phased token distribution or fundraising structure used in earlier or current token planning materials. In Fibon documentation, ICO-related mechanics should be read together with current token allocation, vesting, and launch materials.

Know Your Customer (KYC)

A group of processes used to verify the legitimacy of a customer’s or participant’s identity and to evaluate associated risk.

Modular Architecture

A technical design approach in which system functions are separated into layers or components so that not all capabilities must evolve inside a single monolithic contract or codebase.

Multi-Signature Control

A governance model in which certain actions require authorization from more than one designated signer or controller.

Privacy-Aware Design

A system design principle focused on reducing unnecessary data exposure, supporting user control, and aligning workflows with privacy-sensitive handling.

Risk Scoring

A structured method for classifying or evaluating participants, transactions, or interactions according to defined risk indicators or criteria.

Secure Multi-Party Computation (SMPC / MPC)

A cryptographic method that allows several parties to compute over private inputs without revealing those inputs to one another beyond what is implied by the output.

Selective Disclosure

The ability to reveal only the necessary part of a credential or claim without exposing the entire underlying data set.

Smart Contract

A programmable contract-like logic deployed in a blockchain environment that executes predefined conditions and actions in an auditable way.

Trust Layer

The part of the Fibon architecture that uses blockchain and related mechanisms selectively for attestation, integrity, and coordination.

Utility Token

A token designed primarily to support system functions, access, coordination, or ecosystem operations rather than equity, debt, or profit participation.

Verifiable Credential

A digitally signed credential that can be presented and validated in a cryptographically verifiable way.

Vesting

A controlled release mechanism through which tokens become available over time according to defined conditions.

Zero-Knowledge Proof (ZKP)

A cryptographic method that allows a party to prove that a statement is true without revealing the underlying sensitive information itself.

13. REFERENCES

This reference section should be updated rather than copied blindly from the legacy Yellowpaper. The legacy reference list is still useful for core technical foundations like Ethereum, FATF, FHE, ZKPs, Wolfsberg, Chainalysis, Scorechain, and Yao’s MPC work.

I would structure the updated reference section like this:

Standards, Frameworks, and Guidance

[1] W3C. Verifiable Credentials Data Model v2.0.

[2] European Commission. European Digital Identity Framework / European Digital Identity Wallet materials.

[3] FATF. Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing.

[4] NIST. Digital Identity Guidelines and fraud-related guidance relevant to identity proofing and verification.

Cryptography and Security Foundations

[5] Rivest, Adleman, Dertouzos. On Data Banks and Privacy Homomorphisms.

[6] Craig Gentry. Fully Homomorphic Encryption Using Ideal Lattices.

[7] Goldwasser, Micali, Rackoff. The Knowledge Complexity of Interactive Proof Systems.

[8] Andrew C. Yao. Protocols for Secure Computations.

Blockchain and Smart Contract Foundations

[9] Vitalik Buterin et al. Ethereum White Paper.

[10] Polygon documentation and technical materials relevant to EVM compatibility and PoS-based infrastructure.

Risk, Compliance, and Industry References

[11] Wolfsberg Group. Risk Assessment guidance relevant to AML / sanctions / bribery & corruption.

[12] Chainalysis public technical and product materials.

[13] Scorechain public technical and product materials.

Project-Specific References

[14] Fibon Whitepaper (current official edition).

[15] Fibon smart contract repository.

[16] 0xGuard audit report for Fibon smart contracts.

Reference Note

The reference section should include only:

materials actually cited or relied upon,

currently relevant standards and technical sources,

and project-specific documents that support the current Whitepaper / Yellowpaper alignment.

Old references that support abandoned architecture, outdated chain choices, or deprecated narratives should be removed.

14-TEAM AND OPERATIONAL STRUCTURE

All legal representations, contractual responsibilities, and regulatory filings related to the Fibon Project shall be exclusively managed and executed by Global Alliance A.Ş., a Turkish corporation duly established and governed under the provisions of the Turkish Commercial Code (TTK) and applicable financial services regulations, including but not limited to:

Law No. 6102 (Turkish Commercial Code)

Law No. 6362 (Capital Market Law)

Tax Procedure Law (VUK)

Relevant SPK (Capital Markets Board of Turkey) communiqués and guidelines

Global Alliance A.Ş. assumes full corporate accountability for the operational, legal, and regulatory aspects of the Fibon ecosystem, including:

Execution and management of investor documentation

Platform-related service contracts

Compliance and audit correspondence

Authorized representation before public institutions and regulatory bodies

Information disclosures required under local or international legal obligations

The executive team and advisors involved in the Fibon project act under the full authority and supervision of Global Alliance A.Ş. and do not bear personal legal liability unless explicitly disclosed by contract.

Duke A.
Equity and Investment
Director

Vladimir Prelevic
Business Development Officer
Corporate finance & business strategy

Orhan S. Dayıoğlugil
Chief Operation Officer
COO, Innovative solutions Designer / Project Maker / Team Leader. Consultant for major VCs and top e-business and digital projects.

Ahmet Çakmak
Chief Technology Officer
CTO, Information Security and Blockchain Engineer, Applied Cryptography, and Security Protocols. Currently working on DAO at an international company in *Silicon Valley*.

Elifcan Cetin
Financial Crime Prevention And QC (EU)
As a Financial Crime Prevention (KYC) Senior Expert with 15+ years of experience (ING BElgium, Akbank, Finansbank) She work bridges deep regulatory expertise (including EU AML developments) with hands-on process design, enabling teams to work smarter while staying fully aligned with evolving expectations.

Yasemin GÜLEÇYÜZ
Mehmet TEKÇE
Market Making & Listing Operations
As a market making and listing team they work on this topics,
team building and training in the market maker field, creation of market maker algorithms, unification and management of all exchanges in a single panel (project management and development), design and management of treasury, risk management, and monitoring screens, etc

Ömer Faruk Zorlu
Fullstack Blockchain Developer/ R&D Team Leader
CPO, Participated in *NATO's Information Technology* development projects during the period between 2013 and 2016. Experienced in highly complicated full-stack development with a proven track record in designing and developing websites, blockchain programming, embedded systems, networking, and managing databases. Currently working with IBM, Redhat, and top technology brands worldwide especially based in Silicon Valley.

Nathan Boomsma
Head of Design - UX Lead
A visionary professional who is adept at combining marketing initiatives with design technologies. Performed re-design works for *Microsoft, Apple, Mercedes, and Porsche*.

Bünyamin Atik
BC Development Team Lead
Engineering graduate and Product Development manager in the High-Tech industry, Telecom, and Financial technology sector.

Cem Başgül
Marketing Director
Ex-CMO of Vesbo France, International Business Development & CCM

Zeynep Altınok
DeFi Advisor
Founder of DigiFox and the DataDash YouTube Channel with over 473.000 Subscribers, Paratica brand ambassador.

15- APPENDIX - AUDIT REFERENCE

OXGuard Audit Report

Security and Governance Considerations
Audit Conducted by: 0xGuard
https://github.com/0xGuard-com/audit-reports/blob/master/Fibon/Fibon.pdf
Date: March 2025

The Fibon Token and related smart contracts were subject to a comprehensive audit conducted by 0xGuard. The audit confirmed the presence of strict, multi-signature-controlled mechanisms aligned with current best practices in smart contract governance and emergency response standards.

9.1 Controlled Privileges and Multi-Sig Authorization

Core contract functionalities such as minting and blacklisting have been intentionally retained to allow emergency intervention and platform stability. However, these functions are fully restricted through multi-signature control, which requires approval from a predefined group of trusted entities. No single actor can unilaterally modify critical parameters.

9.2 Supply Management without Hard Cap

FibonToken does not implement a hard cap on supply. This decision supports future adaptability for strategic requirements. Any supply expansion is strictly regulated by multi-signature consensus, preserving transparency and security over token inflation risks.

9.3 Dynamic Transfer Fee Adjustment

The system retains the capacity to modify transfer fees to adapt to ecosystem needs. Fee changes are restricted by multi-signature authorization, ensuring they are not executed arbitrarily and follow defined governance rules.

9.4 Vesting Contract Integrity

Within the FibonVesting contract:

Unvested tokens may be reclaimed if a vesting schedule is disabled (e.g., due to a breach or compliance issue).

Vested tokens, however, are immutable and cannot be altered post-vesting. This guarantees investors that vested rights are irrevocable, in compliance with trust-based vesting mechanisms.

9.5 Emergency Governance Controls

Emergency administrative actions across the token, ICO, and vesting layers are secured via multi-signature wallets. These mechanisms are designed solely for risk mitigation and system protection—not for discretionary intervention—and are in line with ISO 27001 standards for access control (Annex A.9) and SOC 2 principles related to system integrity.

9.6 Governance and Smart Contract Authorities

Smart contract functionalities such as supply control, fee adjustment, and contract upgrades are executed under an auditable multi-signature governance framework. This design provides resilience and transparency while minimizing centralization risk.

These governance functions do not convey any voting rights, shareholding, or profit participation.

They do not meet the criteria of a security or capital market instrument as per SPK Law No. 6362, Article 3.

The system is designed in accordance with best practices for decentralized administration and includes verifiable logging, controlled access, and change management consistent with ISO 27001 and SOC 2 requirements.