DNS for Digital Identity: Evolving a Trusted Internet Protocol

Dr. Balaji Rajendran

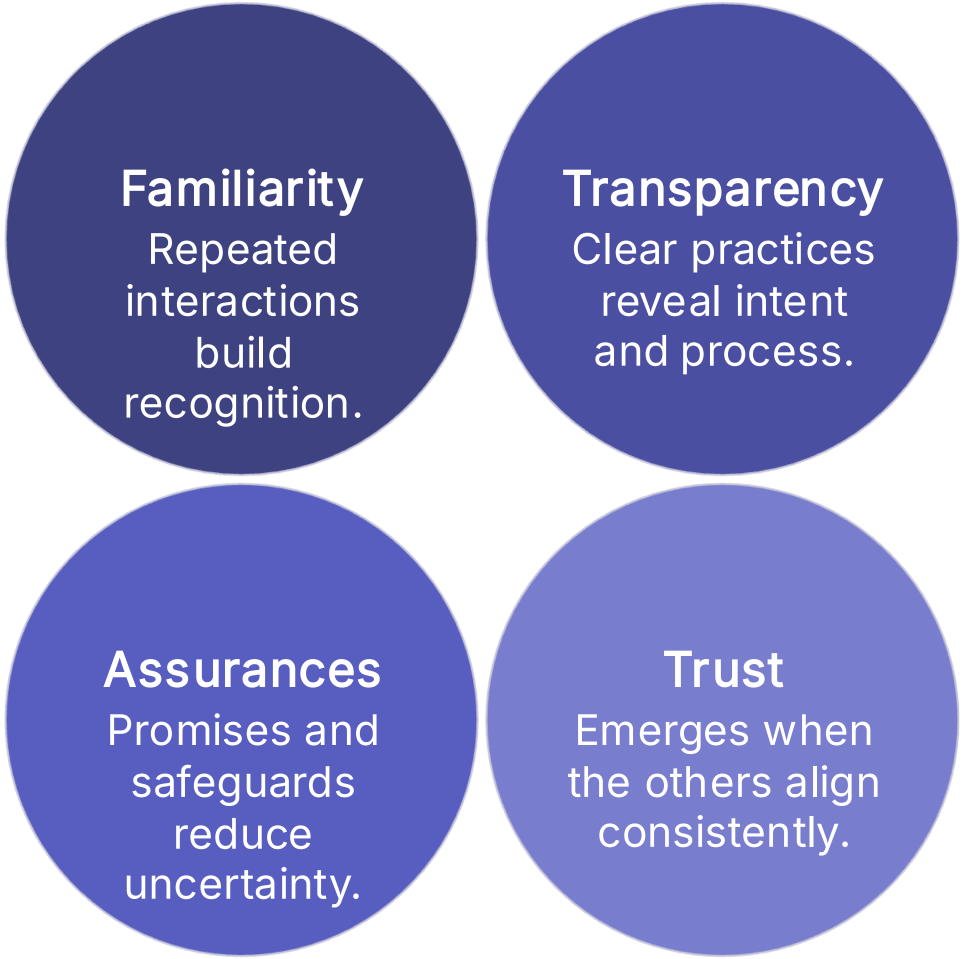
Scientist F

Centre for Development of Advanced Computing (C-DAC)

Ministry of Electronics and Information Technology (MeitY)

Government of India

Reflections on Trust



Familiarity
Repeated interactions build recognition.
Transparency
Clear practices reveal intent and process.
Assurances
Promises and safeguards reduce uncertainty.
Trust
Emerges when the others align consistently.

01

Identity + Events

02

Familiarity

03

Trust

> *For the Internet, the DNS is the ultimate human-friendly identity anchor.*

DNS: A Foundational Element for Trust

Globally Unique Namespace

Maintains distinct domain names, preventing conflicts and supporting global addressing

Hierarchical Delegation

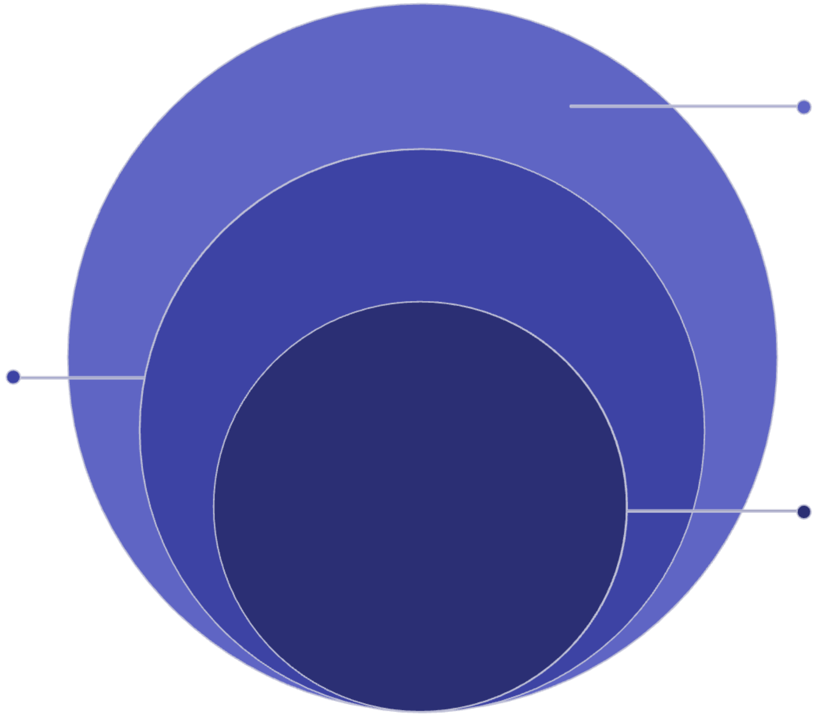
A structured approach enabling distributed management

Operational Resilience

Anycast routing, redundancy, and diverse infrastructure, supporting service availability.

DNSSEC Chain of Trust

Cryptographic security for DNS ensuring the authenticity of DNS data.



SLDs & Subdomains

Second-level domains and their delegated subdomains

Top-Level Domains

Delegation zones like .com, .org, .net

Root Servers

Global authoritative servers for delegating TLDs

The Expanding Role of Names

Domain names have developed beyond their initial function of resolving IP addresses. They now serve as identifiers and trust mechanisms within an expanding range of digital applications.

01

Address Mapping

The foundational role of DNS, translating human-readable domain names into IP addresses for network routing.

02

Authentication Anchor

Evolution with DNSSEC, serving as a critical infrastructure component for cryptographically validating domain origins and enhancing security.

03

Brand Trust Signal

Domain names as indicators of legitimacy and credibility, contributing to online business operations and consumer confidence.

04

Digital Asset Linkage

Integration with distributed ledger technologies for associating decentralized identifiers, digital wallets, and related assets with human-readable names.

05

AI/API Agent Identity

The role of DNS in providing verifiable identities for automated systems, APIs, and AI agents within machine-to-machine interactions is under exploration.

The Case for a Universal Name Resolution Service

A Universal Name Resolution Service addresses the critical infrastructure challenge of namespace fragmentation, providing unified resolution across traditional and emerging identity systems while maintaining security and governance standards.

The Need: Breaking the Silos

- Prevents the fragmentation of the Internet by providing a unified resolution layer across disparate namespace systems.
- Without universal resolution, each namespace operates in isolation, creating security gaps, user confusion, and governance challenges

The Importance: Integrated AI Defense

- As namespaces proliferate, the probability of malicious domains increases exponentially.
- A universal resolver enables **cross-system threat intelligence, behavioral analysis, and coordinated security responses** creating a unified system that detects attack patterns invisible to isolated namespace systems.

The Benefit: Seamless Access

- One-time configuration enables users to navigate effortlessly between classical and decentralized namespaces without understanding underlying protocol differences.
- This eliminates friction, reduces user error.

The Universal Name Resolution Service (UNRS): Extending the Resolver Logic

Input

User Queries

High-Speed Routing

All incoming DNS queries are received and classified by the Smart Forwarder before dispatch to functional cores.

Central Bus

The Smart Forwarder

Protocol-Aware Dispatch

The forwarder identifies query type - classical, decentralized and routes accordingly.

Output

Verified Resolution

Pre-Screening

AI-Security Core is consulted before any query proceeds, ensuring threat signals are intercepted at the bus level.

UNRS provides modular architecture that helps resolution in traditional and decentralized namespace systems while maintaining security and cross-namespace threat detection.

Building Upon Existing Standards

This proposes to leverage established RFCs and standards, and at the same time resolve Decentralized Digital Identifiers.

1

RFC 1034 / 1035

Defines the fundamental architecture and protocols for the Domain Name System, establishing the hierarchical naming structure and resolution mechanisms that underpin the internet.

2

DNSSEC (RFC 4033–4035)

Introduces cryptographic security to the DNS, providing authentication of DNS data origin and integrity protection against various attacks like cache poisoning.

3

RFC 8806 (Hyperlocal Root)

Proposes methods for operating a root name server instance close to a DNS resolver, enhancing privacy, resilience, and performance for local resolution.

4

RFC 6698 (DANE)

Specifies a protocol for binding X.509 certificates to DNS names using DNSSEC, enabling secure distribution of cryptographic keys and enhanced service authentication.

5

Emerging DNS-based DID

Provision a Gateway to resolve Decentralized Identifiers (DID) via a Unified Interface.

AI in the DNS Ecosystem

DGA Detection

Identifying Domain Generation Algorithm patterns used by malware to generate domain names for command-and-control servers.

Phishing Detection

Recognizing suspicious domain patterns, typosquatting attempts, and other indicators of phishing campaigns.

Fast-Flux Analysis

Detecting rapidly changing DNS records and IP addresses associated with malicious infrastructure to evade detection.

Abuse Mitigation

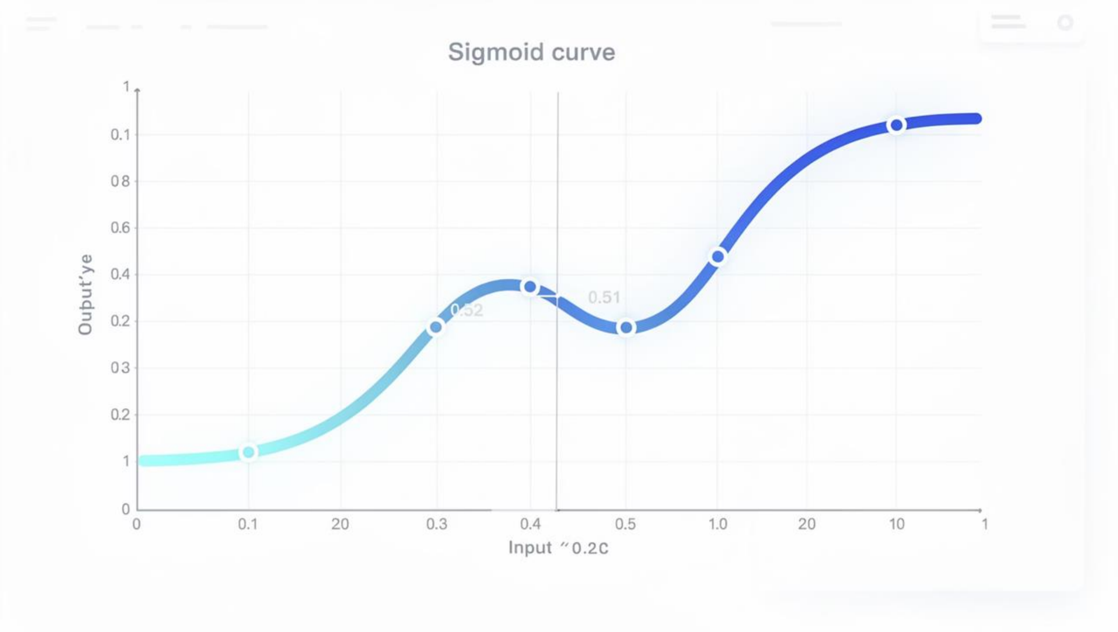
Automating responses to DNS-based threats and policy violations, enabling more timely and extensive protective actions.

These developments are being discussed within the IETF, particularly by the AINetOps working group and in various DNSOP drafts concerning AI agent naming. This reflects ongoing efforts to integrate AI within established internet standards and governance frameworks.

Mathematical Foundations

AI models deployed in DNS security utilize relevant mathematical functions to convert raw model outputs into probabilities for threat detection and mitigation efforts.

Converting Outputs to Probabilities



Maps Raw Model Output to 0–1 Probability

The Sigmoid function accepts any real number as input and transforms it into a value strictly between 0 and 1. This conversion allows the model's output to be interpreted as a probability score, supporting structured analysis.

Supports Risk Scoring Thresholds

The Sigmoid function assists in setting defined thresholds for automated responses, in accordance with established policies.

For example, a probability score exceeding 0.8 could initiate an alert for high-risk activity on a domain based on pre-defined operational rules.

Brief on Model Training

These AI models are trained by minimizing **loss functions** (such as cross-entropy), employing optimization algorithms like **gradient descent**.

AI for DNS Abuse Mitigation

- AI models contribute to DNS security by employing a feature-based risk scoring approach.
- This facilitates the identification and mitigation of various forms of DNS abuse by providing data-driven insights.

Key Features Analyzed for Risk Scoring

Lexical Entropy

Analyzes the randomness in domain name characters, an indicator for detecting Domain Generation Algorithms (DGAs) often used in malware.

TTL Volatility

Monitors anomalous changes in Time-To-Live (TTL) values, which may indicate attempts to evade detection or manipulate DNS resolution.

Registration Age Anomalies

Identifies newly registered domains or those with unusual historical patterns associated with malicious campaigns.

IP Reputation

Assesses the historical behavior and known threat intelligence associated with the IP addresses linked to a domain, to assess potential risk.

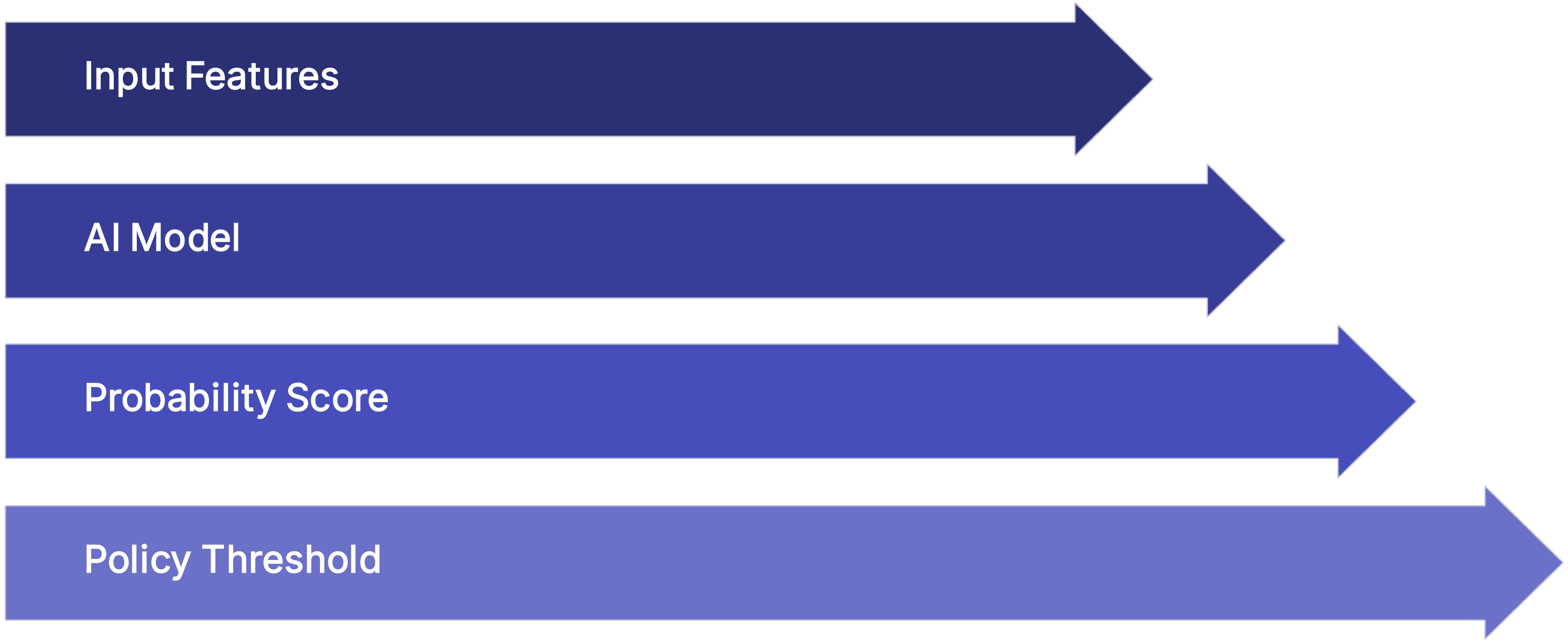
Behavioral Deviations

Detects anomalous changes in query patterns, traffic volumes, or other behavioral metrics that may suggest a new threat.

AI as a Supporting Tool for Governance

Decision Flow: AI-Powered Risk Assessment

- Diverse input features are processed by the AI model to yield a probability score
- This is evaluated against predefined policy thresholds for a decision.



Input Features

AI Model

Probability Score

Policy Threshold

Emerging Trends: AI & DNS in IETF Discussions

- The intersection of Artificial Intelligence (AI) and the Domain Name System (DNS) is an area of ongoing standardization efforts within the Internet Engineering Task Force (IETF).
- Numerous drafts and working groups are dedicated to examining the challenges and considerations presented by this convergence.

1

DNS-Native AI Agent Naming Draft

A proposal to standardize methods for identifying and resolving AI agents directly through the DNS infrastructure, facilitating integration.

2

DNSOP Draft on DNS for Internet of Agents

Discussions within the DNS Operations (DNSOP) Working Group focusing on the implications of agent-to-agent communication and naming conventions for the DNS.

3

AINetOps Operational AI Draft

The AI for Network Operations (AINetOps) Working Group is exploring practical applications of AI to enhance the operational efficiency and resilience of network infrastructure.

Digital Asset Transformation: A Value Proposition for DNS

The conversion of classical domain ownership into Non-Fungible Tokens represents a significant value addition for all stakeholders of the Ecosystem.

Classical to Tokenized Assets

- **NFT tokenization** transforms domains into **verifiable digital assets** with cryptographically secured ownership records.
- The blockchain-based approach ensures that every transaction, transfer, and modification is permanently recorded, creating an unalterable chain of custody that establishes provenance and authenticity.

Day Zero Audit Trail

- Recording ownership and behavior from Day Zero enables tracking of domain reputation.
- Historical data such as ownership transfers becomes quantifiable, allowing algorithmic assessment of trustworthiness.
- Creates a **reputation economy** where domain value is directly tied to verifiable behavior.

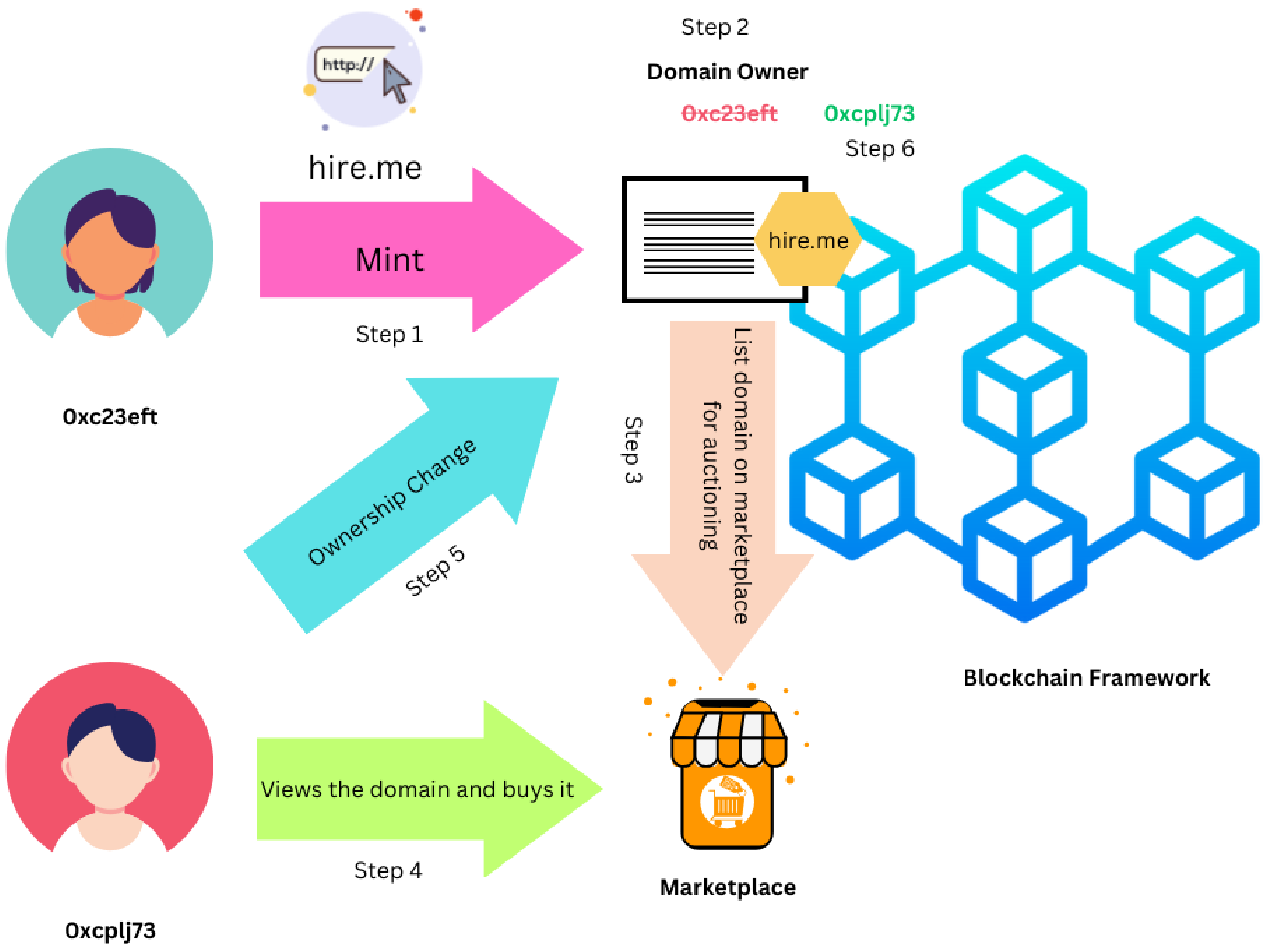
Case Study: Tracking malicious domains through permanent ledger records prevents re-registration and enables proactive threat identification across the namespace.

Reputation-Based Leasing

- **Domain-as-a-Service** (DaaS) enables high-reputation domains to function as Verified Digital Identities available for short-term leasing.
- Organizations can leverage established trust without permanent acquisition, while domain owners can monetize reputation capital.

Technical Anchor: NFTs incorporate legally valid digital signatures within smart contracts, establishing cryptographic proof of authenticity and enhancing credibility in secondary markets.

Classical Domains as NFT



The NFT Identity for DNS - Example

The Day Zero Reputation Anchor

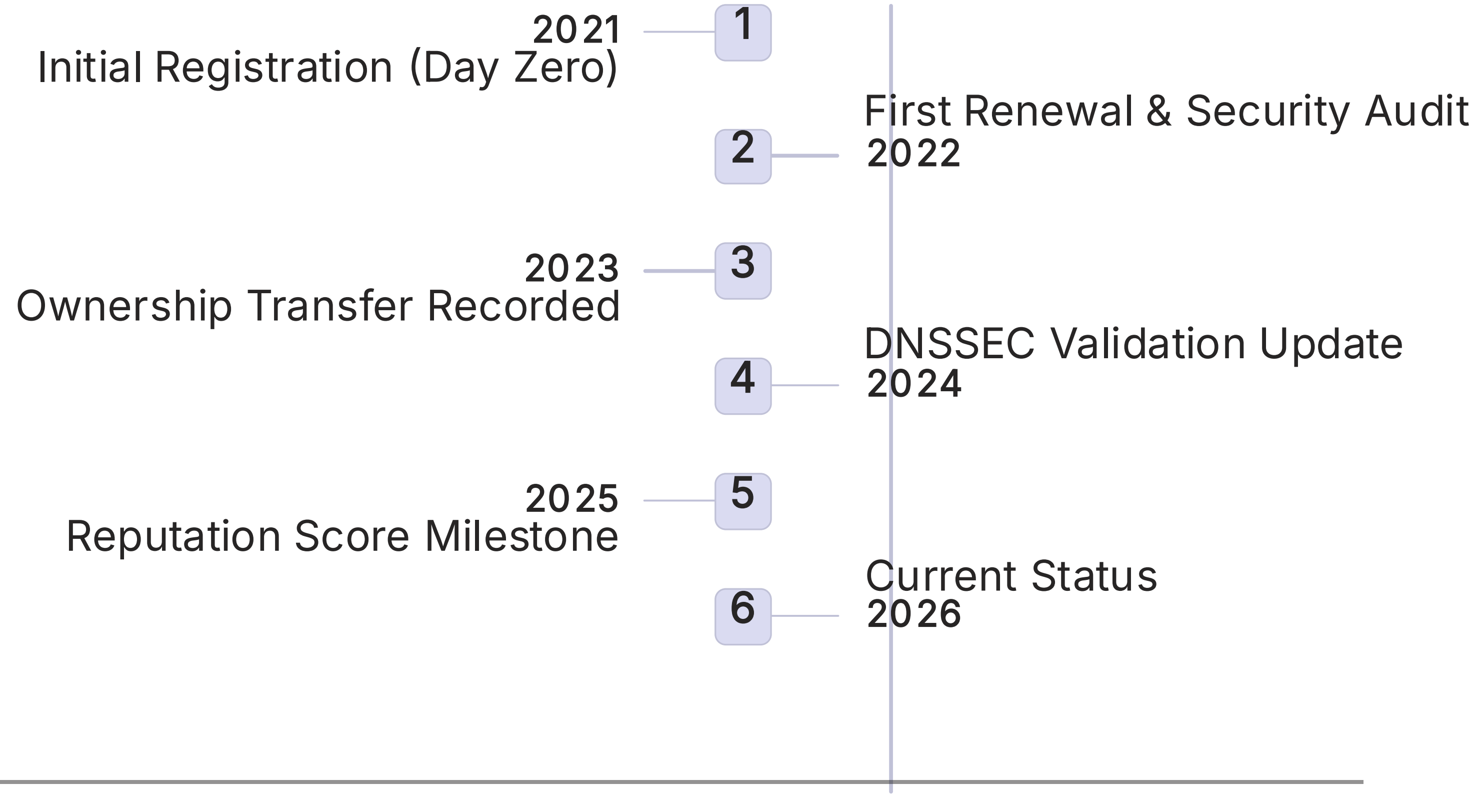
Digital Identity Instrument

1

finance.trust

Registered: 2021
Reputation Score: 98/100
Verified via DNSSEC
Owner: [Organization Name]
Status: Active

Immutable Lifecycle Ledger



1 — 2021 Initial Registration (Day Zero)
2 — First Renewal & Security Audit 2022
3 — 2023 Ownership Transfer Recorded
4 — DNSSEC Validation Update 2024
5 — 2025 Reputation Score Milestone
6 — Current Status 2026

Functional Architecture:

- Tokenization creates an unalterable history, ensuring that reputation cannot be erased or faked
- Every event is cryptographically recorded on the blockchain, providing non-repudiable evidence
- The NFT serves as an identity instrument that carries verifiable reputation

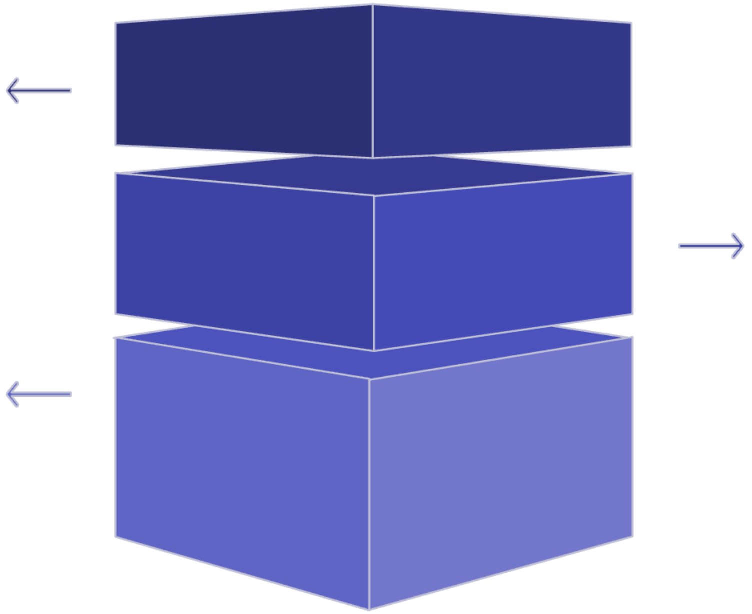
Technical Benefits:

- Day Zero recording establishes complete provenance
- Reputation scoring becomes mathematically verifiable
- Dispute resolution (UDRP) can gain access to complete audit trail
- Secondary market transactions include full transparency

Tokenize the domain to create an unalterable history, ensuring that reputation cannot be erased or faked.

Bridging Accountability: Compliance in a Layered Architecture

Separates resolution policy from audit history, enabling regulatory compliance without sacrificing accountability.



UNRS Operational Plane

This is where traffic flow is determined.

AI Policy Trigger

Resolution in action;

Blockchain / NFT as Audit Plane

This is the unchangeable record.

Technical Architecture

- **Blockchain provides the Witness (Audit); The DNS Resolver provides the Enforcement (Resolution)**
- Resolution suspension does not erase the audit trail, ensuring both legal compliance and forensic integrity
- Enables protocol stability, regulatory compliance, and enhanced accountability within a unified framework

This architecture ensures that legal compliance does not compromise the forensic chain of custody (Accountability).

What This Does NOT Do

This proposal summarizes the intent to complement existing internet infrastructure and governance

Does not establish an alternative root

- The ICANN root remains the authoritative source for the Domain Name System.
- No competing or parallel root systems are introduced through this proposal.

Does not circumvent ICANN governance

- All proposed modifications adhere to and operate within established ICANN multistakeholder processes.
- Existing governance structures remain preserved and authoritative.

Does not supersede PKI

- Public Key Infrastructure and Certificate Authorities continue to operate as foundational elements.
- This complements, rather than replaces, established trust mechanisms.

Does not mandate Blockchain integration

- Blockchain integration is **an optional component**, not a mandatory requirement.
- Traditional DNS operations maintain their existing functionality without modification.

Does not cause namespace fragmentation

- The unified, globally consistent DNS namespace is maintained.
- This approach avoids the introduction of namespace collisions or conflicting identifier systems.

Proposed Outcomes

The DNS is undergoing an evolution to address requirements for digital identity, ensuring secure interactions and maintaining its foundational principles of stability and interoperability within established frameworks.

1

Resolution Mechanisms

2

Trust Frameworks

3

Identity Coordination

1. Source of Trust

- The ICANN root acts as authoritative source.
- Avoidance of fragmentation

2. Adherence to multistakeholder governance

- Existing governance models are preserved and reinforced.
- Community-driven decision-making processes continue.

3. Sustained global interoperability

- Functional operation across traditional and evolving systems is ensured.
- Broad compatibility and accessibility are maintained.

4. Guided evolution

- A measured, standards-based approach informs development.
- Existing infrastructure is respected while accommodating future capabilities.

The Future of the Trusted Resolver

Orchestration

Beyond Classical DNS

Proposes a Gateway for Decentralized namespaces via a Unified Interface

Provenance

Blockchain & NFT Anchoring

Immutable lifecycle records from first registration.

Accountability

Forensic Integrity

Separation of Audit and Enforcement Planes

Intelligence

Targeted AI Defense

Reputation-based Threat Analytics.

Beyond resolving addresses; we will be engineering a verifiable foundation for digital trust.

Thank You

I Welcome Your Questions and Perspectives I

Dr. Balaji Rajendran | C-DAC Bangalore