NOTO Protocol
The Universal Source of Truth for the Decentralised Internet.

Light Paper Q4 2023 - Version 11.05

F.Costa & D.Vicini

Strictly private and confidential

Abstract

The Noto Protocol It’s the world's first infrastructural solution with an advanced and complex architecture, designed to serve as the central pillar for accessing and managing the Internet in web3. Noto Protocol, with its extraordinary uniqueness, positions itself as the B2B protocol destined to empower billions of users. The Noto Protocol vision is to be the “source of truth” empowering the decentralized use of the internet.

What distinctly characterizes Noto is its ability to synergistically integrate with major existing Blockchains and all web3 Domain Name Registries. This distinctive feature enables Noto to transcend traditional challenges associated with online identity management, offering advanced solutions tailored to the web3 ecosystem for handling name collision cases, resolution processes, indexing, DNS administration, web3 browsing security and abuse prevention.

Noto distinguishes itself for its flexibility through seamless API integration with third parties, opening doors to an unparalleled digital ecosystem. In this new paradigm, web3 naming system management emerges as reliable processes, assured by the robustness and security offered by the Noto protocol.

Introduction

In the use of the traditional internet, the regulatory oversight provided by institutions such as ICANN/IANA has played a pivotal role in ensuring streamlined processes and guaranteeing a secure browsing experience. However, in the context of web3, the landscape becomes markedly more complex due to its decentralized nature. Navigating the decentralized web3 space poses inherent challenges in maintaining the same level of ease and security experienced within the traditional internet. It is within this complex and evolving environment that the Noto Protocol emerges as a pioneering solution and strives to be the universal source of truth for the web3 internet.

Its core objective is to extend the fundamental principles that currently underpin the traditional use of the internet and technologically expand these principles into the internet usage within the Blockchain framework. The Noto Protocol is designed as an extension of the sound principles that currently regulate and facilitate the conventional internet, aiming to adapt and apply these principles in the context of decentralized technology.

By doing so, it seeks to bridge the gap and extend the ease, safety, and structured operation found within traditional internet usage into the decentralized sphere, addressing the challenges posed by the nature of web3. In response to this, Noto Protocol has emerged as the leading technical solution designed to empower the management of the intricacies in the evolving web3 Internet ecosystem. Its genesis was born from the demand for a resilient system capable of effectively managing the uncertainties and complexities arising from a multitude of web3 Registrars operating in several different Blockchains.

This White Paper traverses the architecture and functionalities of Noto, covering its background, inception, and core technological elements. Subsequent sections delve into the resolution process, indexing mechanisms, collision handling, and the intricate abuses signal management, aimed at mitigating potential abuses and vulnerabilities within the web3 environment. Moreover, the paper discusses the distinctive custom DNS capability, highlighting its substantial contribution to the web3 Domain Name space.

This paper continues into detailing the real-world implementation of this groundbreaking technology, emphasizing its unique features that position Noto as a standout solution. The analysis extends to potential applications and the industrial impact of Noto, underlining its significance in reshaping digital interactions within the dynamic, evolving landscape of web3 internet. Furthermore, it analyzes the data structure and management within the Noto framework, emphasizing its role in organizing and securing information. Finally, it will underscore the numerous benefits offered by the Noto Protocol, solidifying its role in ensuring a secure, efficient, and scalable environment for web3 interactions.

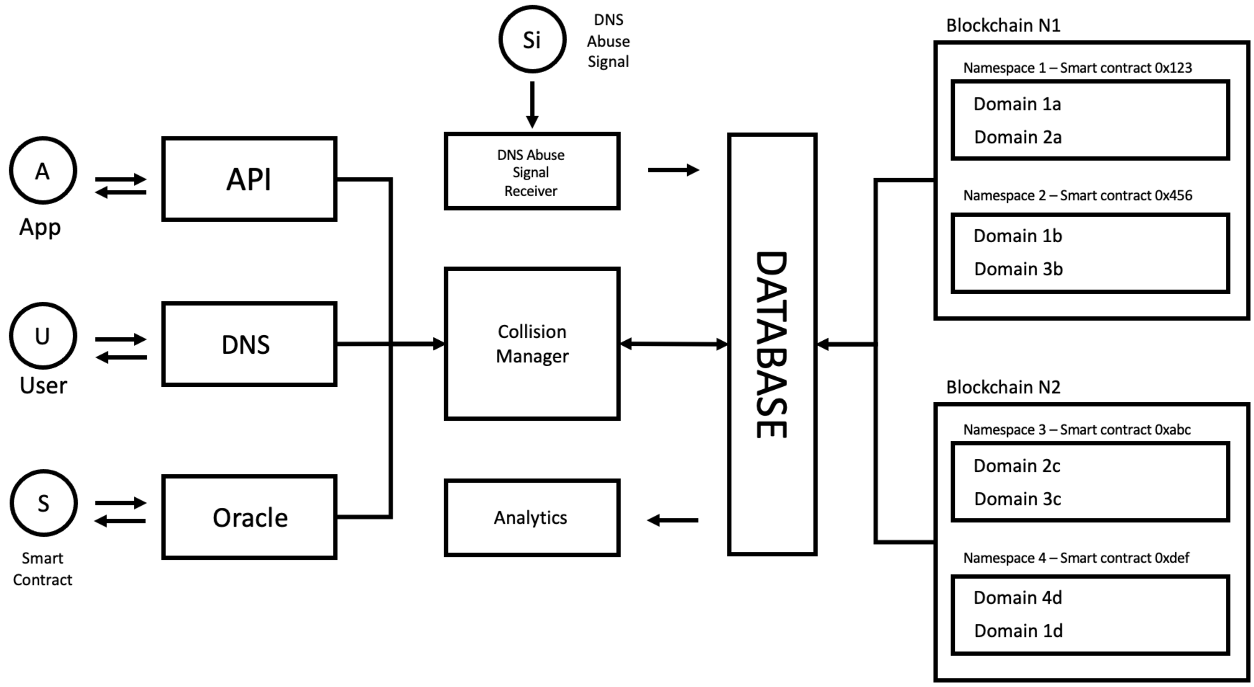
Description of the Invention

This invention introduces a fully integrated infrastructure allowing browsers, devices, users, and developers to access and resolve Domain Names within web3 namespaces not associated with the standard ICANN IANA root. Through this infrastructure, a wide range of consumers can seamlessly connect to and resolve domains.

Granting access to an unregulated web3 domain name space introduces the potential risk of domain name collisions across differing web3 namespaces. Additionally, there is the inherent risk of accessing domain names linked to illicit and hazardous content.

Addressing the concerns of naming collisions and DNS misuse are fundamental aspects of the Noto Protocol. Through this invention, the Protocol seeks to proactively confront and mitigate these challenges, ensuring safe and secure access within an unregulated domain landscape.

By bridging the standard web infrastructure with the web3 domain environment, this invention also delivers the necessary technical tools to normalize browsing experiences. This encompasses conventional website features such as DNS servers, SSL certificates, and analytical tools designed for in-depth industry monitoring and research.



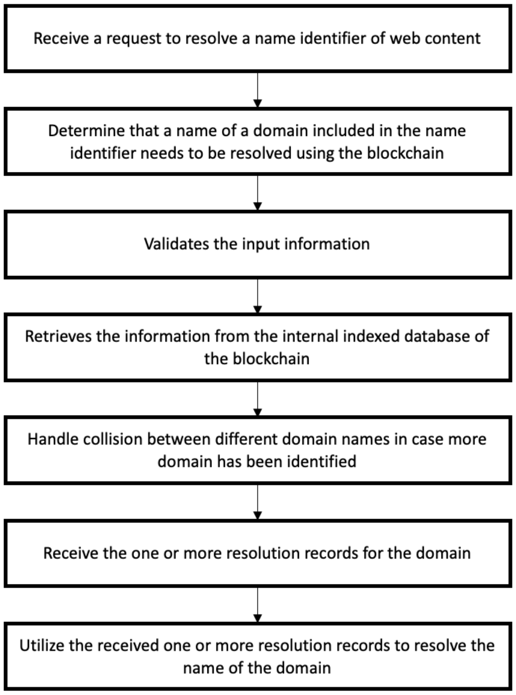
Resolution process

A Resolution Process is the moment where there is a request for having content of a Domain Name. This request can come from a browser that wants to access a website from a domain, it can come from a Terminal where a domain is converted into an IP address to run a FTP or SSH connection. For resolution we can identify the process of retrieving records information attached to a Domain Name. This normally happens with DNS servers in standard Web2 Domain infrastructure, but in web3 this scenario is normally not achievable because web3 domains reside outside the DNS root infrastructure bringing the impossibility to resolve them without an additional technology.

In Noto the resolution process starts from a request that can come from an application based on a user request or because of a software that requires specific data. All the requests access into a funnel of Application Program Interface to be handled. The funnel can be differentiated based on the device, the technology and the tools used. These interfaces are called Layers and are:

REST API Layer:
Accessible via HTTPS, the REST API interface caters to the application layer of the ISO/OSI model. Requests must conform to the prescribed API format and utilize the HTTPS protocol. This interface is particularly well-suited for web and mobile applications aiming to support web3 domain resolution. Additionally, it offers authentication features to limit API usage to a predefined user base. A noteworthy aspect of this API layer is its context-aware capabilities, adapting behavior based on authenticated user preferences and intended usage patterns.

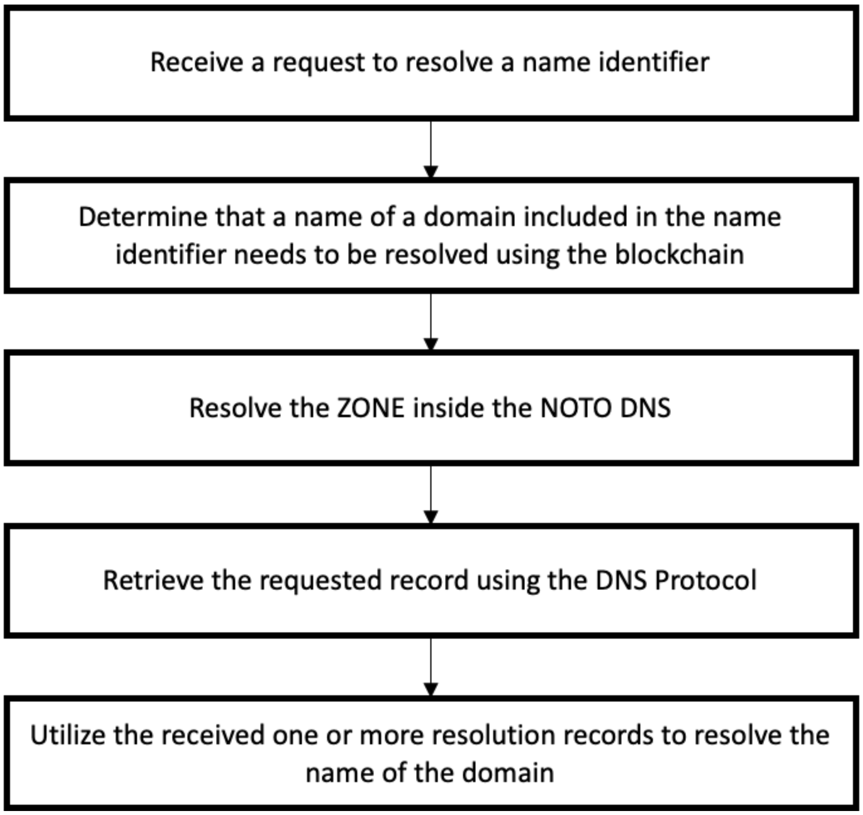
Resolve a domain with the API Layer


Receive a request to resolve a name identifier of web content
Determine that a name of a domain included in the name identifier needs to be resolved using the blockchain
Validates the input information
Retrieves the information from the internal indexed database of the blockchain
Handle collision between different domain names in case more domain has been identified
Receive the one or more resolution records for the domain
Utilize the received one or more resolution records to resolve the name of the domain

DNS Layer:

This layer provides DNS infrastructure for domain resolution, aligning with standard ICANN/IANA protocols. By leveraging TCP/IP, DNS enables device-level resolution of web3 domains, extending support to networks, routers, operating systems, and applications dependent on internet connectivity. Protocols such as FTP, HTTPS, and SSH are compatible with this DNS-level resolution.

Resolves a domain with DNS Layer

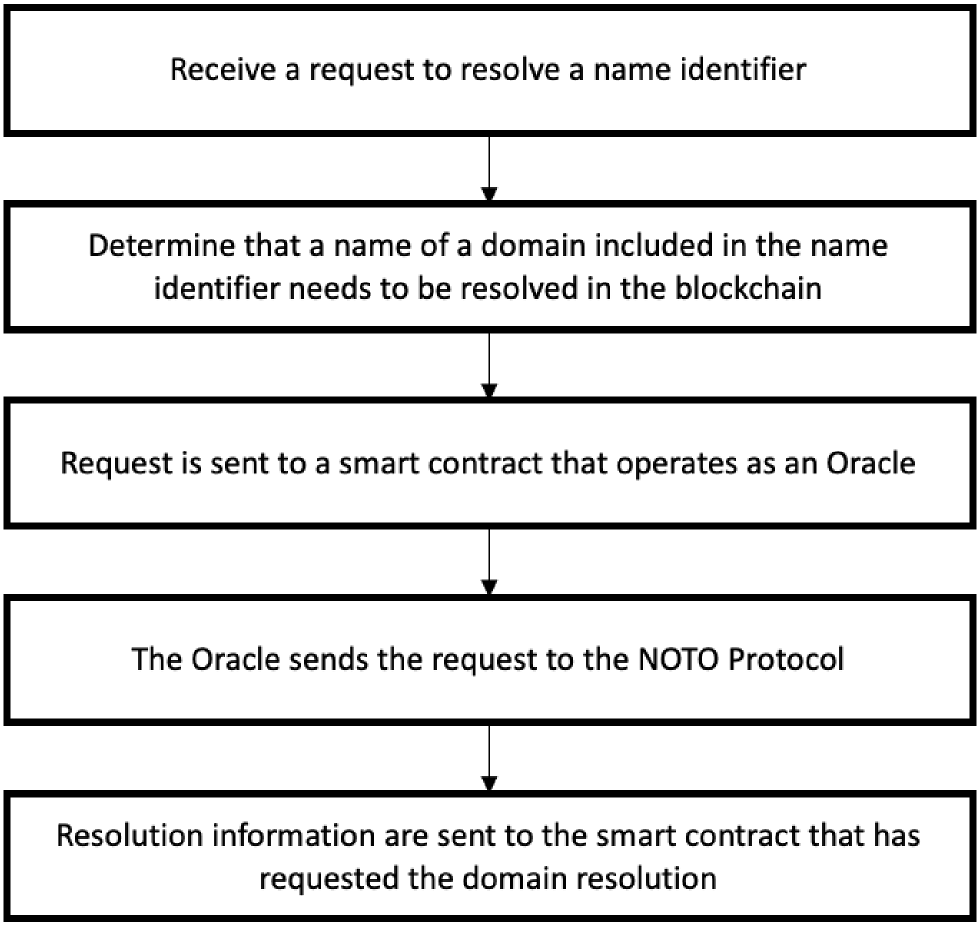

Receive a request to resolve a name identifier
Determine that a name of a domain included in the name identifier needs to be resolved using the blockchain
Resolve the ZONE inside the NOTO DNS
Retrieve the requested record using the DNS Protocol
Utilize the received one or more resolution records to resolve the name of the domain

Decentralized Oracles for On-Chain data Provisioning:
An Oracle serves as a bridge, sourcing data from off-chain resources (such as weather reports, databases, and applications) and then embedding them into the blockchain.

Within the Noto Protocol, this interface layer streamlines domain resolution and validation for blockchain-based smart contracts. Although blockchain data is typically isolated from the wider internet, specialized oracle technologies enable internal information sharing about domain names and content, offering web3 domain resolution for smart contracts and digital assets.

In this way the acknowledgment of the existence of a domain registered in another blockchain, the block of resolution of a domain or a collision is handled by bringing off-chain logic inside the blockchain through the Oracles.

Resolve domain from the blockchain


Receive a request to resolve a name identifier
Determine that a name of a domain included in the name identifier needs to be resolved in the blockchain
Request is sent to a smart contract that operates as an Oracle
The Oracle sends the request to the NOTO Protocol
Resolution information are sent to the smart contract that has requested the domain resolution

Indexing Process

The Indexing Process serves as the backbone for the aggregation of diverse blockchain and namespace data into a fully optimized storage repository for domain names. It ensures that all data are normalized and structured for efficient querying, retrieval, and utilization within the Resolution Process. The collection of all the domain indexed and their information is important since its the way that Noto Protocol uses for running the resolution of domains but also to provide to end users insights, analytics and reports about the web3 Domain Name space.

An indexer is a specialized tool designed to scan blockchain ledgers and events systematically, aiming to identify and record relevant metadata, transactions data and activities data. In the context of the Noto Protocol solution, these are called "block indexers," focusing on domain-related transactions within various Blockchains.

Technical Process Behind Indexing Data on the Blockchain

1. Event Listening: The indexing process commences with real-time event monitoring on multiple blockchain networks. This is achieved through the use of specialized tools, known as block indexers, that continuously scan for activities such as domain registration or modification within existing domains. This event listener runs on the blockchains where supported web3 namespaces reside.

2. Event Detection and API Handling: When an event is detected, it triggers a communication to a dedicated Application Programming Interface (API) for internal processing. This is where the event listener tools transmit essential details like the identification code of the affected domain, the originating blockchain, and the domain's namespace.

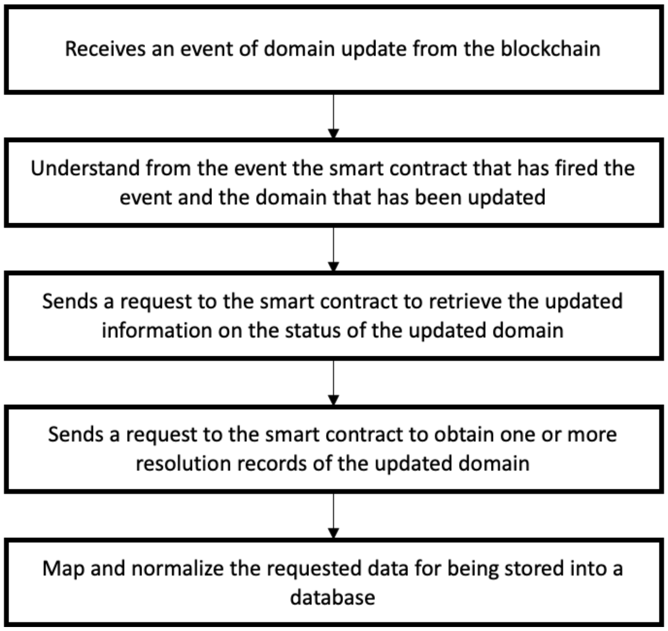
3. Blockchain Data Retrieval: Leveraging the received information, the indexer establishes a direct connection with the corresponding blockchain. It fetches all relevant data tied to the registered or modified domain.

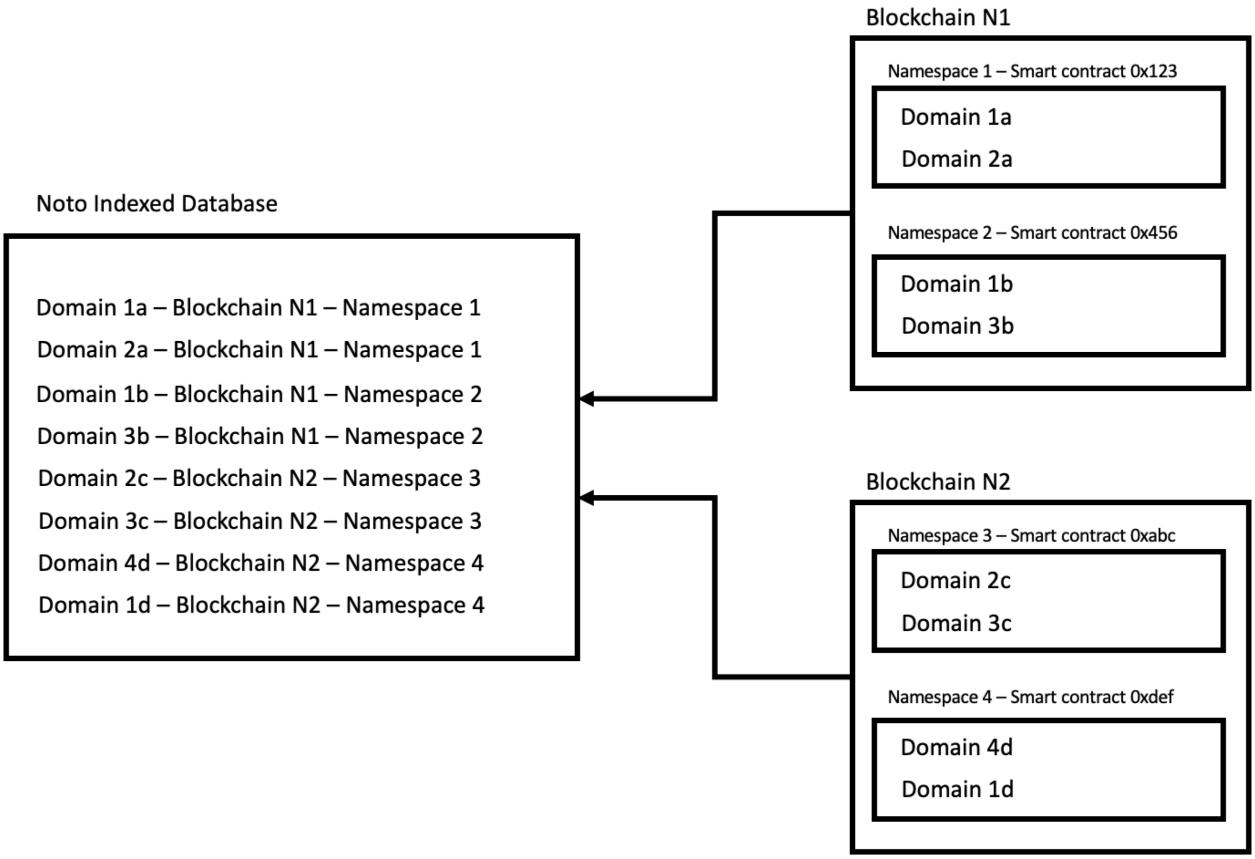
4. Normalization: Post-retrieval, the data undergoes a normalization process. This involves standardizing various data types and structures to conform to a unified schema, thereby facilitating easier database storage and subsequent querying.

5. Database Storage: Finally, the normalized data is committed to a centralized database, which serves as the go-to repository for all domain-related information.

By incorporating diverse event listener triggers, this indexing process streamlines data acquisition, ensuring direct data sourcing from the originating blockchains without the need for third-party intermediaries. This enhances both the integrity and reliability of the indexed data, making it robust and dependable for real-time domain data uses.

Indexing of a domain from the blockchain


Receives an event of domain update from the blockchain
Understand from the event the smart contract that has fired the event and the domain that has been updated
Sends a request to the smart contract to retrieve the updated information on the status of the updated domain
Sends a request to the smart contract to obtain one or more resolution records of the updated domain
Map and normalize the requested data for being stored into a database


Blockchain N1
Namespace 1 – Smart contract 0x123
Domain 1a
Domain 2a
Namespace 2 – Smart contract 0x456
Domain 1b
Domain 3b
Noto Indexed Database
Domain 1a – Blockchain N1 – Namespace 1
Domain 2a – Blockchain N1 – Namespace 1
Domain 1b – Blockchain N1 – Namespace 2
Domain 3b – Blockchain N1 – Namespace 2
Domain 2c – Blockchain N2 – Namespace 3
Domain 3c – Blockchain N2 – Namespace 3
Domain 4d – Blockchain N2 – Namespace 4
Domain 1d – Blockchain N2 – Namespace 4
Blockchain N2
Namespace 3 – Smart contract 0xabc
Domain 2c
Domain 3c
Namespace 4 – Smart contract 0xdef
Domain 4d
Domain 1d

Collision Management process

The Collision Management Process is the workflow of activities and technologies used to manage naming collisions that can occur during the process of Domain Resolution.

The Collision Management Engine serves as an integral component of the solution, essential for navigating the complexities of domain resolution and mitigating conflicts between similar web3 domains originating from multiple namespaces.

Rule-Based Resolution

The engine operates based on a database of governing parameters, called "Rules", that dictate how to process specific requests and manage domain collisions with a precise resolution result.

Each rule is comprised of the following attributes:

- Phase of Execution: Specifies whether the rule is to be applied before ("Pre-resolution") or after ("Post-resolution") the domain resolution process.
- Conditional Criteria (“Where Condition”): Establishes the prerequisite conditions that trigger the rule's execution.
- Priority Ranking: Designates the rule's rank, particularly useful when there's a conflict between multiple rules.
- Authority Level: Indicates the hierarchical level of the authority that registered the rule.
- Action to be Taken: Specifies the engine's operational behavior if the rule is executed, such as blocking or redirecting requests.

Rules for managing naming collisions can be created by the User who sets the profiling for the resolution, or automated by the Score Based Collision Algorithm.

Types of Rules

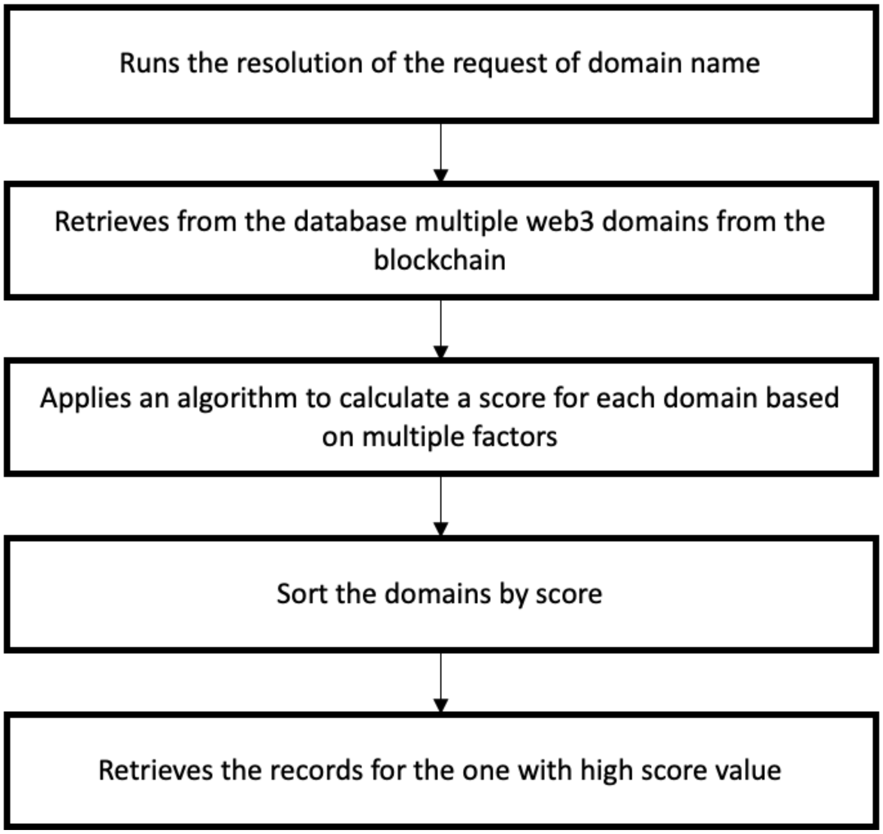
The rules can broadly be categorized into two:

- Resolution Rules: These could mandate the blocking of certain requests, redirecting queries to alternate domains, or predefined namespaces based on geographic or other criteria.
- Collision Management Rules: These guide the engine in prioritizing or sequencing namespaces during collisions.

Score-Based Collision Resolution

Upon the application of these rules, the engine may still yield a single or multiple domain results. When multiple outcomes are derived, it implies that a collision remains unresolved. To address this, the engine applies a scoring system to each domain, ranking them based on a proprietary algorithm that estimates the score based on qualitative and quantitative characteristics. It then retrieves the domain with the highest score as the definitive result to be resolved.

Resolve a domain and handle a collision


Runs the resolution of the request of domain name
Retrieves from the database multiple web3 domains from the blockchain
Applies an algorithm to calculate a score for each domain based on multiple factors
Sort the domains by score
Retrieves the records for the one with high score value

How Rules behave in the different Resolution Layers

The Resolution Process of Noto operates differently depending on the Resolution Layer Interface used by the consumer of the request of resolution.

Given that Noto Protocol integrates a Collision Management Engine that, using rules, handles domain resolution and collision management, it's important to take into account that it cannot be implemented in the same way on the different Resolution Layers, since these use different protocols of communication and technologies.

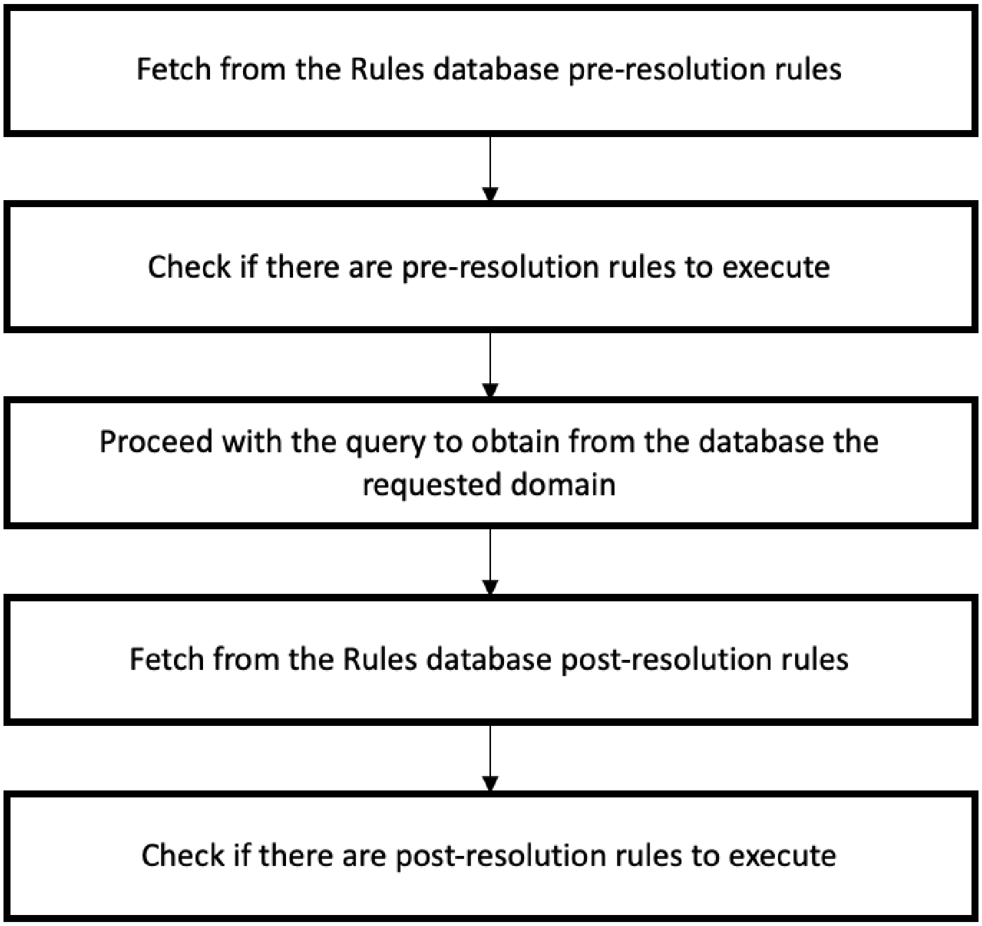
With this context, it's important to consider the limits of each Resolution Layer Interface. Starting with the API Layer, it fully implements the capabilities of the Collision Management Engine allowing a set of specific rules to be activated at the moment of the resolution of a request, these are:

- Pre-resolution rules: these rules triggers and runs before any query happens in the database layer checking if the profile contains any sort of setting available, these includes: censorship of specific domains, override of standard resolutions
- Context-aware rules: these rules occurs based on the context of the request, meaning that if the request comes from a country or an organization that blocks specific domains and overrides others, these are executed during the resolution
- Post-resolution collision management checks: if a collision between two or more namespaces happens for the same domain name, the platform handles the resolution following its own techniques and rules but also providing custom user logic setted up in context-level allowing the profile to set which one to prefer overriding existing logics.

The DNS layer, differently from the API Layer, handles the resolution by accessing a dump of the entire resolution of web3 domains where rules have been applied to consider all the possible collisions happening. This process uses a set of algorithms and rules defined by Noto Protocol. This resolution process gives access to a subset of the entire collection of domains allowing only the winners of resolution in case of collision and removing all censored or not accessible domains in specific regions. It is possible for users to set their own node of DNS that works with the specific logic; this process will be discussed further during the document.

Finally, the Oracle resolution works based on the logic of the blockchain where it resides. Its ability of computation and data provisioning depends on the capabilities of the Oracle implementation and how the information itself can be processed by the virtual machine of the blockchain adopted. This means that not all the features of resolution provided in both API Layer and DNS Layer can be processed, allowing only to acknowledge the existence of a domain, its owner, where it resides and which record uses for smart contracts.

Application of rules



Fetch from the Rules database pre-resolution rules

Check if there are pre-resolution rules to execute

Proceed with the query to obtain from the database the requested domain

Fetch from the Rules database post-resolution rules

Check if there are post-resolution rules to execute

Signal and resolution management for web3 abuses

Signal management plays a pivotal role in mitigating DNS abuses commonly encountered within the domain landscape. Such signals are generated and transmitted by DNS Abuse Management Providers. These entities aggregate DNS abuse reports, scrutinize the data, and then liaise with DNS providers to initiate appropriate corrective actions—be it blocking domains or modifying resolution records.

The Challenge of Unregulated web3 Domains

In the current ecosystem, web3 domains lack a dedicated DNS Abuse Management framework, leading to a governance void. This absence poses significant challenges as users transition to a new domain landscape fraught with potential threats in an unregulated market.

Integrated Abuse Management Mechanisms

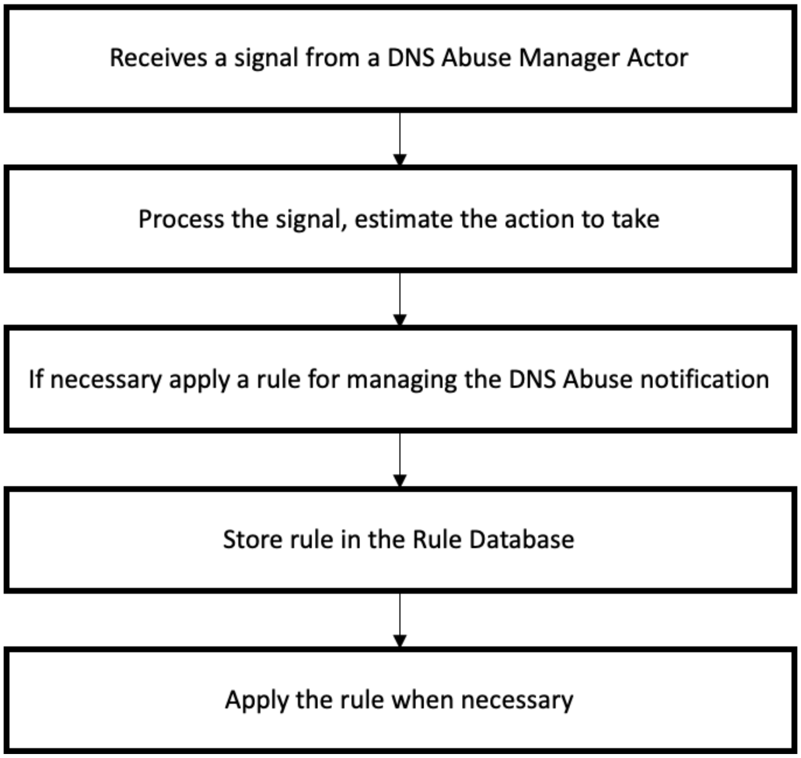
To address this inefficiencies, Noto Protocol incorporates a comprehensive suite of technologies designed to interpret DNS Abuse signals originating from established DNS Abuse Management Providers. These signals are integrated seamlessly into the existing abuse reporting infrastructure, extending its capabilities to cover web3 domains.

Rule-Based Handling of Abuse Signals

Upon receipt of an abuse report, the information is conveyed via signals to the Collision Management Engine. This engine, in turn, processes the signal and institutes a new rule aimed at either blocking or overriding the domain resolution in question. This rule-based approach ensures a scalable and efficient method to manage abuse in both DNS and web3 domain spaces.

By integrating this sophisticated abuse management mechanism, the solution fortifies the security posture of web3 domains, making them less susceptible to a range of potential abuses and ensuring a safer browsing experience for users.

Signal for DNS Abuse



Receives a signal from a DNS Abuse Manager Actor

Process the signal, estimate the action to take

If necessary apply a rule for managing the DNS Abuse notification

Store rule in the Rule Database

Apply the rule when necessary

Custom DNS

As previously discussed in the section titled “How Rules Behave in Different Resolution Layers,” the inherent technical constraints of the technology mean that DNS Layers cannot execute runtime rules for resolution and collision management. Consequently, resolutions via the DNS Layer lack customizable settings and rules, relying solely on the Default Rules outlined by the Noto Protocol.

However, within the Noto Protocol's infrastructure, there exists the capability to establish and launch a bespoke DNS server. This server seamlessly incorporates user-defined settings and rules as per the Noto Protocol's guidelines. Such an arrangement empowers enterprises and communities to operate a tailored DNS Node that not only supports web3 domains but also aligns with their unique business objectives.

This approach is ideally suited for corporations, browsers, ISPs, and VPNs seeking to grant users access to the web3 domain name landscape while simultaneously modulating or tailoring the navigation experience to reflect specific preferences.

Implementation of the technology

The invention can be implemented in numerous ways, including as a process; an apparatus; a system; a composition of matter; a computer program product embodied on a computer readable storage medium; and/or a processor, such as a processor configured to execute instructions stored on and/or provided by a memory coupled to the processor. In this specification, these implementations, or any other form that the invention may take, may be referred to as tech-niques. In general, the order of the steps of disclosed processes may be altered within the scope of the invention.

Unless stated otherwise, a component such as a processor or a memory described as being configured to perform a task may be implemented as a general component that is temporarily configured to perform the task at a given time or a specific component that is manufactured to perform the task.

As used herein, the term processor resets to one a to devices, circuits, and/or processing cores configured to process data, such as computer program instructions.

A detailed description of one or more embodiments of the invention is provided below along with accompanying figures that illustrate the principles of the invention. The invention is described in connection with such embodi-ments, but the invention is not limited to any embodiment.

The scope of the invention is limited only by the claims and the invention encompasses numerous alternatives, modifications and equivalents. Numerous specific details are set forth in the following description in order to provide a thorough understanding of the invention. These details are provided for the purpose of example and the invention may be practiced according to the claims without some or all of these specific details. For the purpose of clarity, technical material that is known in the technical fields related to the invention has not been described in detail so that the invention is not unnecessarily obscured.

For the effective deployment of the Noto Protocol technology, any device, application, circuit, or process must utilize one of the previously mentioned interfaces for interaction and communication.

To facilitate the adoption of the infrastructure layer the Noto Protocol provides a platform that enables developers and organizations to set up their own account and from there the “Project” from which they can set up the resolution settings and to access to the right guides to make a perfect integration of the technology.

API Layer Implementation

To implement the API Layer it is necessary to follow the documentation provided for the API integration. This means using REST APIs via the HTTPS protocol and where each request is authenticated using an API KEY generated by the developer using the Noto Protocol Platform.

The API exposed for handling resolution are:

- Resolve: returns a resolution for a given domain. It processes the collision management and all the resolution logics.
- DeepResolve: retrieves the list of all possible domains sorted by the highest score. In case of collision, with this API both domains are returned.
- ReverseResolve: retrieves from a given wallet address the list of domains owned
- Exists: checks the existence of the domain

The API Layer can be easily implemented in both web and mobile applications, browsers, scripts and other code based software that can run API requests on the HTTPS protocol.

DNS Layer Implementation

To implement the DNS Layer, it is necessary to set up the DNS IP Address inside the Operative System of the Personal Computer used by the consumer, or to set it in the Default Gateway Settings of the router (or in case of ISP or VPN, as Default DNS IP address).

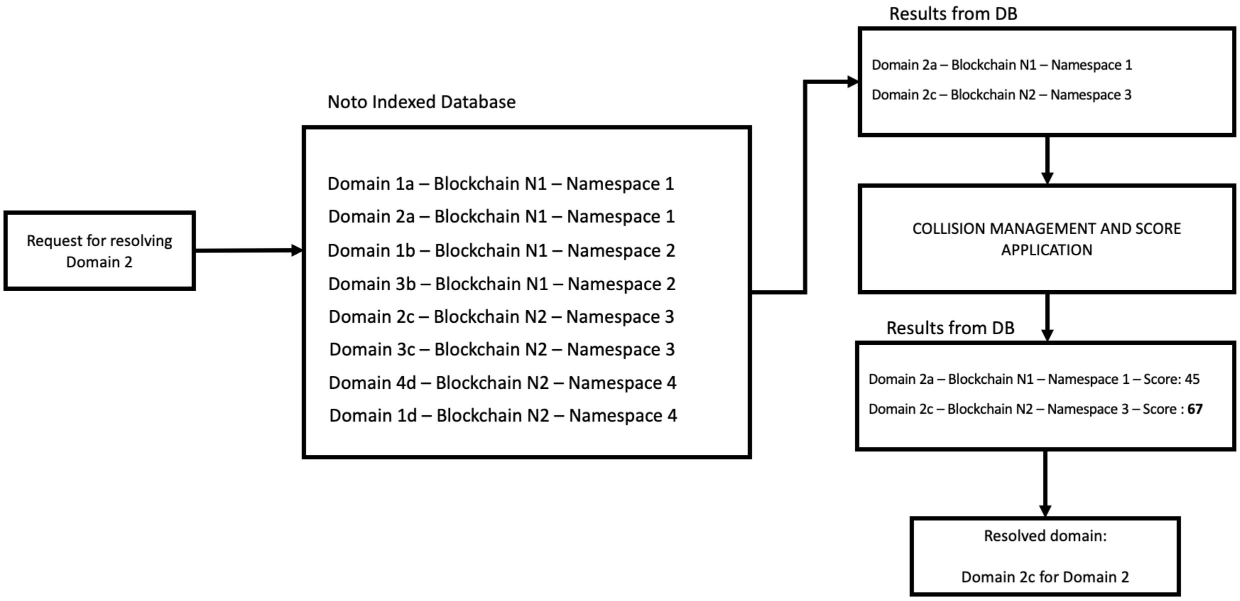
Using one of those approaches the DNS is automatically reached by all the incoming requests from devices and applications and can perform domain resolution for both web3 Domain Names and Web2 Domain Names.

Embracing the innovative technology of the Noto Protocol, the potential challenges of configuring a custom DNS IP address within a network router or on a Personal Computer have been seamlessly addressed. Noto Network offers a user-friendly installer tailored for all major operating systems, allowing the DNS IP application to be launched and operated effortlessly. This ensures that even those without technical expertise can enjoy the benefits with ease.

On-chain resolution using Oracle

The implementation of an Oracle for resolving web3 Domain Names requires skills and knowledge in building smart contracts for blockchain.

To implement the Oracle it is necessary to interact with the deployed smart contract Oracles of Noto that consuming an exact number of gas fees and LINK tokens it performs an off-chain query operation to check the existence of a domain and the retrievement of useful informations to understand where the domain exists and what records contains. This resolution, as for the DNS Layer implementation, works using the Default Resolution Algorithm of the Noto Protocol.


Request for resolving Domain 2
Noto Indexed Database
Domain 1a – Blockchain N1 – Namespace 1
Domain 2a – Blockchain N1 – Namespace 1
Domain 1b – Blockchain N1 – Namespace 2
Domain 3b – Blockchain N1 – Namespace 2
Domain 2c – Blockchain N2 – Namespace 3
Domain 3c – Blockchain N2 – Namespace 3
Domain 4d – Blockchain N2 – Namespace 4
Domain 1d – Blockchain N2 – Namespace 4
Results from DB
Domain 2a – Blockchain N1 – Namespace 1
Domain 2c – Blockchain N2 – Namespace 3
COLLISION MANAGEMENT AND SCORE APPLICATION
Results from DB
Domain 2a – Blockchain N1 – Namespace 1 – Score: 45
Domain 2c – Blockchain N2 – Namespace 3 – Score : 67
Resolved domain:
Domain 2c for Domain 2

Implementation of Analytics features

To implement analytics features and start to obtain data and business intelligence information about the Web3 Domain Name space, it is necessary to register and use the Noto Protocol Platform from where users can obtain an API KEY.

The API KEY is required to make api requests dedicated for querying domain names. These are:

- findOne: retrieves one result from a query
- findMany: retrieves one or more results from a query

Using these features it is possible to query and retrieve information from the Noto Protocol Database about Web3 Domains and the data they contain.

Potential Applications and Industrial Impacts

The applications of the Noto Protocol encompass diverse use cases within the infrastructural capabilities of functioning the new internet. These services include critical functionalities such as web3 naming collision management, resolution facilitation, DNS setup, abuse prevention, data analytics, DNS security, and SSL certificate issuance. Each service plays a distinct role in enhancing the functionality, security, and overall experience within the decentralized use of the internet.

Potential applications

- **Surf your web3 domains across all registries and chains.**
  The Noto Protocol's Collision Management service offers a comprehensive solution to oversee and resolve naming conflicts within the web3 space. It ensures that domain names remain unique across multiple registries and blockchains, enabling interoperable and conflict-free navigation for users across the internet.

- **Create and manage your own decentralized Top-Level Domain.**
  The Noto Protocol offers the capability for brands and large companies to independently create and manage decentralized Top-Level Domain (TLD). This service allows users to establish and control the identity and scope of their TLD independently within the decentralized web3 ecosystem, enabling greater customization and management of their domains, communities and users.

- **Surf any web3 domain straight from your favorite browser.**
  Allowing the use of web3-enabled DNS, Noto provides users with the capability to directly browse any web3 domain from any browser. This service simplifies and enhances the user experience, allowing direct access to decentralized websites and services without the need for any complex configurations.

- **Set your own web3-enabled DNS node.**
  With the DNS Node Generator, users can independently set up their own web3-enabled DNS node. This capability grants users' greater control over their DNS functionalities within the decentralized web3 environment, allowing for customized and personalized DNS management.

- **Gather usable data intelligence of the whole web3 internet.**
  Noto's Data Analytics service collects and analyzes valuable intelligence data regarding the usage and operation of the entire internet in web3. This service provides tools and insights to the internet industry stakeholders for better decision-making and technological improvements.

- **Use data analytics and signals to prevent onlines abuses and harms.**
  Using data analytics and specific signals, the Abuses Prevention service of Noto Protocol aims to prevent, report, and take swift action in the identification and prevention of any kind of online abuse. Noto Protocol plays a crucial role in maintaining a safer online environment by actively addressing and preventing abuse-related content.

- **Set your own browsing security parameters.**
  This service empowers users to establish their own browsing security parameters. Users can tailor their security preferences, enhancing their online preferred safety levels while navigating across the web3 internet.

- **Increase web3 security of your websites.**
  The Noto Protocol facilitates enhanced security by issuing and offering SSL certificates for web3 websites. This service significantly strengthens security measures for websites operating in the decentralized web, ensuring increased protection against potential cyber threats and vulnerabilities.

Industrial impact

- **Blockchain and web3 Internet Industry.**
  The Noto Protocol is positioned to have a transformative impact on the blockchain and web3 internet industry, especially considering the complex and fragmented nature of the web3 naming landscape. With the multitude of naming services operating across diverse blockchains, establishing uniformity and standardized rules becomes an increasingly challenging necessity. Noto steps in as a pioneer in bringing order and implementing rule-based approaches using advanced technology. Its emphasis on ensuring unique and conflict-free naming across an array of web3 domain name registries and blockchains lays a foundation for a more reliable and structured infrastructure within the web3 identity ecosystem, crucial for an harmonized web3 naming interoperability. These capabilities are particularly essential and highly sought after by various web3 infrastructural services such as wallets, decentralized browsers, website builders, smart contract developers, blockchain oracles, blockchain scanners, and more. The Noto Protocol's provision of these services is seen as invaluable, addressing the critical need for standardization and enhanced security within the evolving web3 landscape.

- **Internet Operators' Industry.**
  Within the internet operators' industry, the Noto Protocol plays a pivotal role in the internet operators' industry by prioritizing efficient resolution management, allowing traditional internet operators such as browsers to handle web3 complexities like indexing, resolution, and naming conflicts. It enables users to safely browse web3 domains using traditional DNS settings. The Noto Protocol's services are tailored to facilitate traditional mail providers in integrating decentralized technology into their current SMTP protocols, effectively managing new email addressing requests arising from the usage of the web3 internet. Additionally, by leveraging the web3 DNS

capabilities of the Noto Protocol, VPNs and ISPs can integrate their customized versions of private web3-enabled DNS. This concerted effort signifies a shift in operational strategies, demanding operators to adapt to an ever-evolving landscape that emphasizes decentralized security and resolution mechanisms, ensuring a safer and more secure use of the decentralized internet.

- **Traditional Registrars and Registry Industry.**
  For the traditional registrars and registry industry, the Noto Protocol presents a technology that will enhance the ability to include web3 domain names and in their offering. The ability to manage naming conflicts and provide solutions for robust and secure naming management via APIs across diverse web3 registries and Blockchains within can revolutionize and enhance the existing domain management practices. This stands to impact how traditional registrars operate, requiring adaptation to meet the demands of the evolving decentralized domain landscape facilitated by the Noto Protocol.

- **IP Protection Industry.**
  The Noto Protocol serves as a pivotal solution for the Intellectual Property (IP) protection industry, offering a robust infrastructure for managing digital identities and web3 assets within the decentralized naming system. Alongside enhanced security measures, it plays a vital role in protecting and securing intellectual property. Notably, the protocol extends its functionalities to assist IP protection services and brands by scanning the web3 naming system for potential IP infringements. It aids in the search for IPs to safeguard and offers data intelligence, empowering decisive actions to protect intellectual properties within the rapidly evolving decentralized internet landscape. Its capacity to prevent abuses, maintain naming integrity, and safeguard digital identities signifies a potential redefinition in the operations of IP protection mechanisms in the web3 landscape.