Transitioning from DNS to IPvX with NFT Identifiers. Proposal for cooperation

Project X

Introduction

Network: The network, which we call now the Internet, began from a network of a size, smaller, than modern local area networks in mid-size offices.

IP Addresses: At first, it was possible to keep the IP addresses of network nodes in memory.

DNS System: With network grow, the DNS system was introduced, to maintain a list of network nodes names, aligned with their IP addresses.

Domains: Then, there came domain zones and domain names - the hierarchy of DNS names and systems. And at last, the DNS upgraded to support non-latin symbols.

Background on IPvX

DNS Limitations:

- **Centralized control**
- Naming limitations
- Reactive to changes
- No security by design
- No resource identification
- Cyber-attacks

Each zone is capable to run independently, and as you are an administrator of the zone, it is capable to run trustworthily to the zone parties.

Problems begin when you follow hierarchy and establish interconnections with neighbour zones.

The point of trust moves to the superior zone, until root. That’s why you cannot run your zone independently any more.

At last, each f the domains relies on DNS root operability.

Background on IPvX

DNS Limitations:

- Centralized control
- **Naming limitations**
- Reactive to changes
- No security by design
- No resource identification
- Cyber-attacks

Your domain and corresponding website meet limitations on its naming.

It is mandatory to have all of superior zones name trailers, separated by comma.

From security considerations there came conventional rules for domain namings, individual for a given zone. For ex., you cannot mix symbols from different layouts, or you cannot use some special symbols.

Background on IPvX

DNS Limitations:

- Centralized control
- Naming limitations
- **Reactive to changes**
- No security by design
- No resource identification
- Cyber-attacks

From scalability limitations, there came a DNS cache extension.

When you query a website, having several zones in domain name, your DNS resolver queries each zone DNS server, beginning from root level. Obviously, top-level servers, especially root zone, could not bear such load for the whole Internet.

DNS caching was introduced, when you define a lifetime for your DNS record. And servers across Internet remember it.

When you make changes, there is a possibility, that there can be some DNS server in Internet, that still remembers your old record, until caching time expires.

Background on IPvX

DNS Limitations:

- Centralized control
- Naming limitations
- Reactive to changes
- **No security by design**
- No resource identification
- Cyber-attacks

Initially, the network was small, and every party relied on others.

Nobody tried to make attacks on DNS system.

With the network growth there had to be changes done to DNS protocols, but security issues had not been addressed.

Scalability performed only in terms of availability.

Background on IPvX

DNS Limitations:

- Centralized control
- Naming limitations
- Reactive to changes
- No security by design
- **No resource identification**
- Cyber-attacks

There is no resource identification in DNS system.

You can only be sure, that a given domain name belongs to a given IP address. But you can not identify the owner of a resource or the querying party.

DNSSEC security extension was introduced. But it addresses integrity only, and not authenticity or non-repudiation.

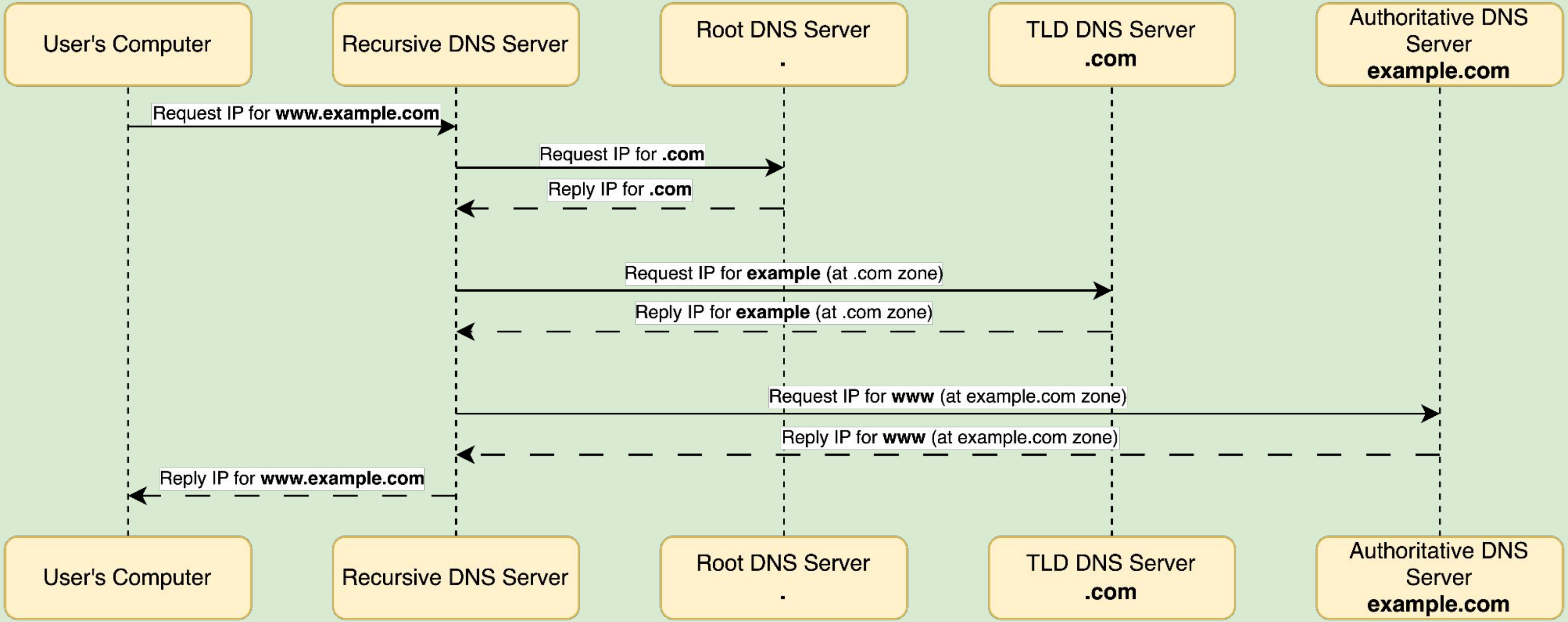
Background on IPvX

DNS Limitations:

- Centralized control
- Naming limitations
- Reactive to changes
- No security by design
- No resource identification
- **Cyber-attacks**

- DNS Spoofing (DNS Cache Poisoning)
- DNS DDoS
- DNS Tunneling
- DNS Amplification
- Man-in-the-Middle
- Domain Hijacking
- NXDOMAIN Attack
- DNS Rebinding

DNS Query Process



What is IPvX?

IPvX is a new paradigm of Internet addressing, routing, and entity identification.

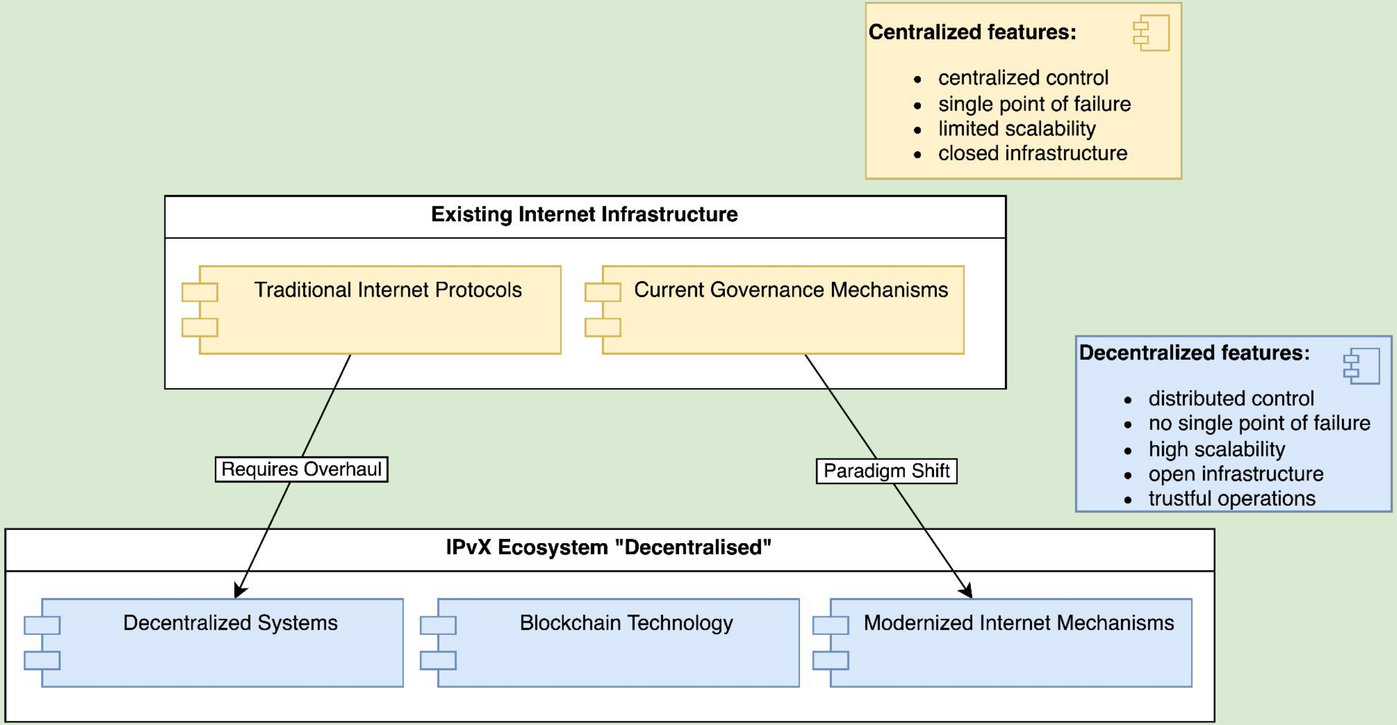
The goal is to power the transition from traditional ecosystem with architecture, protocols, procedures, etc.

IPvX is a new network model layer, interacting with applications, network access media, and the **blockchain** as a source of distributed databases, including new **resolving system - DRS (Distributed Resolver Service)**.

IPvX addresses and solves known network and **DNS** limitations, utilizing modern computing power and databases growth.

CIAAN (Confidentiality, Integrity, Availability, Authenticity, Non-repudiation) - by design in IPvX Ecosystem.

Decentralized Nature of IPvX



Centralized features:

- centralized control
- single point of failure
- limited scalability
- closed infrastructure

Existing Internet Infrastructure

Traditional Internet Protocols

Current Governance Mechanisms

Requires Overhaul

Paradigm Shift

Decentralized features:

- distributed control
- no single point of failure
- high scalability
- open infrastructure
- trustful operations

IPvX Ecosystem "Decentralised"

Decentralized Systems

Blockchain Technology

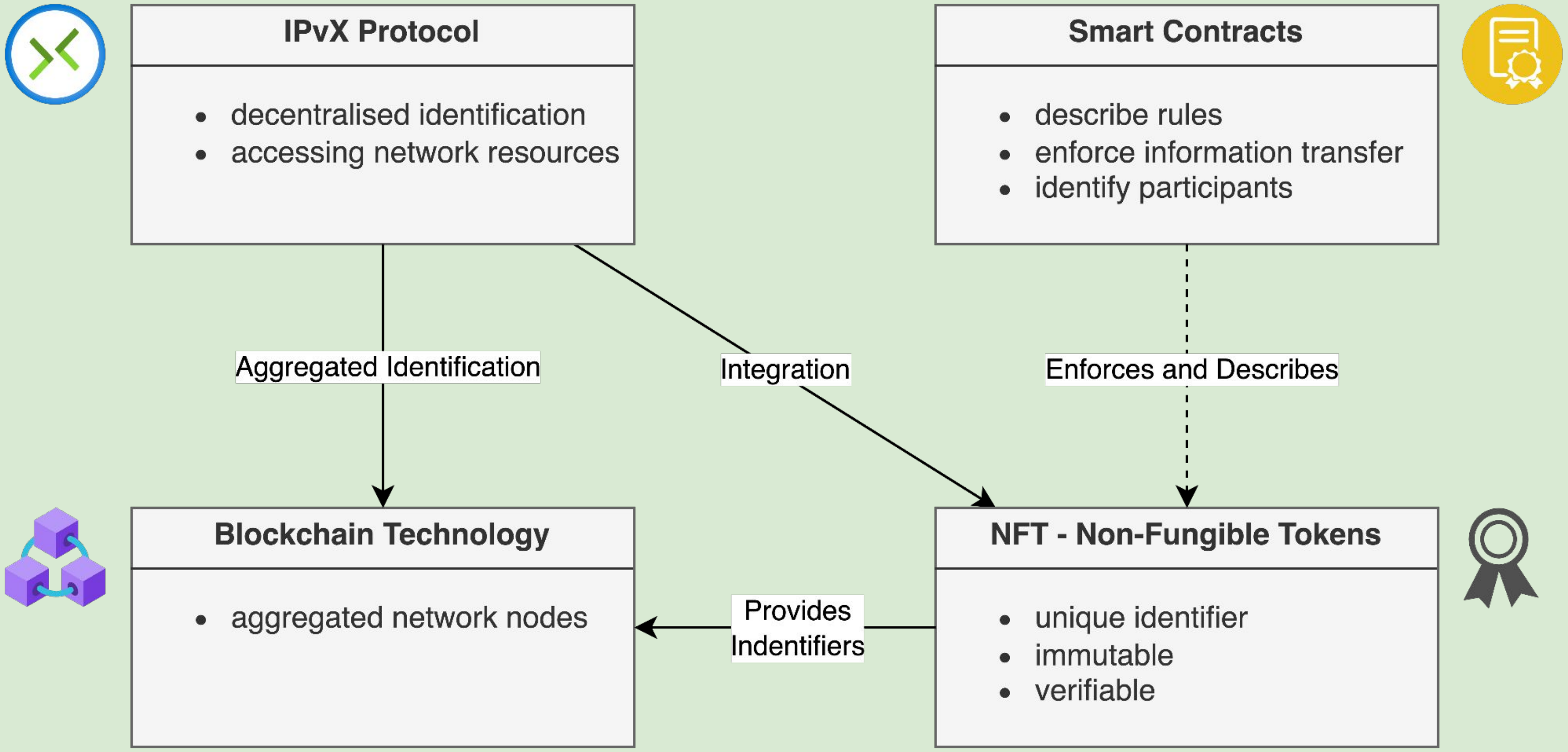
Modernized Internet Mechanisms

Decentralized Nature of IPvX

Key features:

- **No root** - no single point of trust
- **Flat design** - no complicated hierarchy, “zoneless” names
- **Distributed databases** - no single database entry, no single responsible party
- **Distributed resolvers** - multiple resolvers, choose closest
- **Peer-to-peer** - any nodes can reach each other (if not restricted by either node)

Integration of NFT



IPvX Protocol

- decentralised identification
- accessing network resources

Smart Contracts

- describe rules
- enforce information transfer
- identify participants

Aggregated Identification

Integration

Enforces and Describes

Blockchain Technology

- aggregated network nodes

Provides Indentifiers

NFT - Non-Fungible Tokens

- unique identifier
- immutable
- verifiable

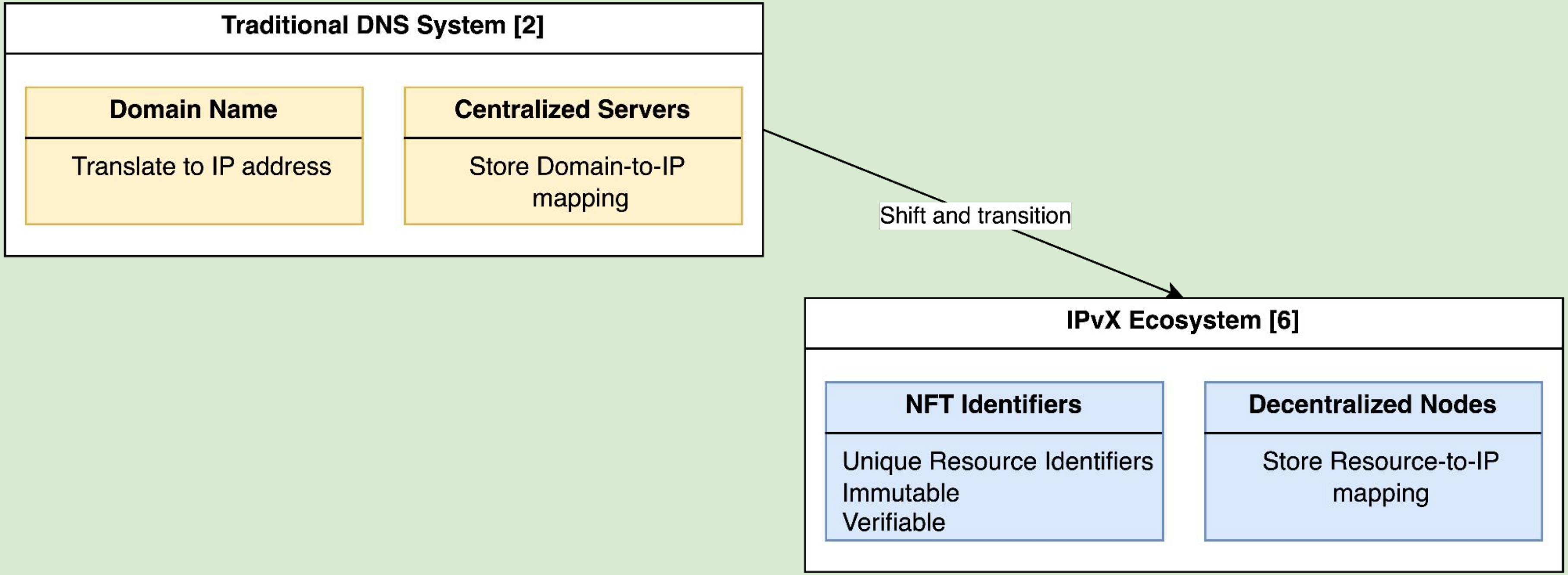
Integration of NFT

NFT (Non-Fungible Token) - is a unique digital asset verified on a blockchain, representing ownership and authenticity of an item

In IPvX we talk about these items:

- Traditional Domain Names
- IPvX Domain Names (aliases to IPvX addresses on a blockchain)
- IPvX Address
- Traditional network information
- New network information
- Legal entity (a person or a company)
- Any other entity, represented by NFT, if requested

DNS vs. IPvX Approach



Traditional DNS System [2]

Domain Name

Translate to IP address

Centralized Servers

Store Domain-to-IP mapping

Shift and transition

IPvX Ecosystem [6]

NFT Identifiers

Unique Resource Identifiers
Immutable
Verifiable

Decentralized Nodes

Store Resource-to-IP mapping

Comparison of DNS and IPvX

DNS	IPvX
Security Comparison	
Centralized - single root: ● DNS spoofing attacks ● DNS cache poisoning attacks ● DDOS attacks ● Security addons required (DNSSEC)	Decentralized - no root: ● Immutable records ● Authenticated transactions ● Nowhere to attack
Efficiency Comparison	
● Multiple servers cooperating ● Root problems lead to subdomain problems ● DNS cache timeouts	● Distributed resolver - immediate everywhere ● No root - sole responsibility on updates ● Lower latency - blockchain consensus
Scalability Comparison	
Various problems: ● Dependency to top-level ● Accreditation procedures ● Each “zone” requires DNS server sample	Pros: ● No “top-level” - feel free ● No need to be “accredited” - join blockchain ● Distributed resolver - no need for “server”

Transition from DNS to NFT Identifiers

The transition to IPvX Ecosystem and to usage of NFT identifiers could be done in stages:

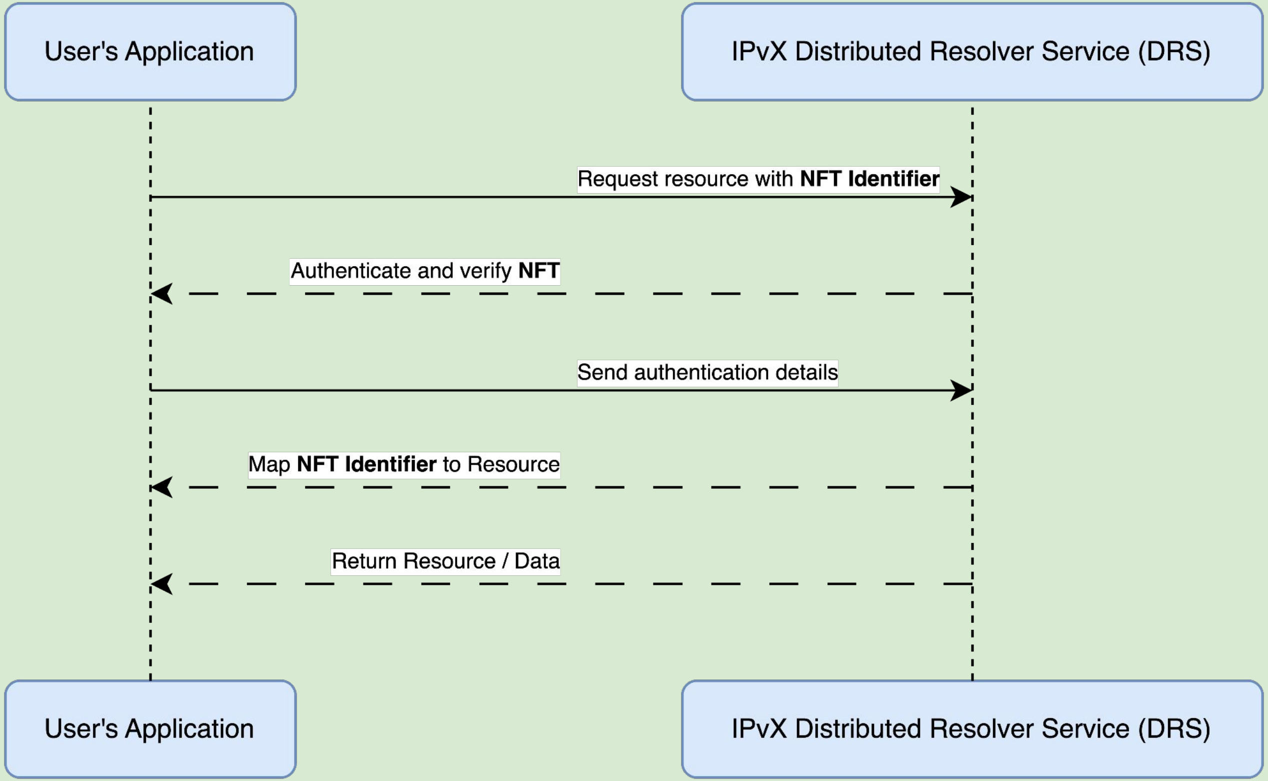
- **Database shifting** - The involved parties (Regional Registries, DNS systems, etc.) begin to store their database information in a blockchain
  - users still interact with old services, that serve as a bridge between users and new databases
  - **NFT identifiers** are applied to db entities alongside with classical db information
- **Direct interaction** - The users of these databases begin to append and query in direct
  - users are capable to query blockchain databases with a help of **Distributed Resolvers**, or on their own
  - **Distributed Resolvers** and users query **NFT identifiers**
- **“Zoneless” concept** - The DNS System is flat again, as it had been from scratch
  - with new addresses growth, the interest in domain-like addressing is declining
  - **NFT identifiers** prevail as a source of trust

Distributed Resolver Service (DRS) in IPvX

Distributed Resolver Service (DRS) - a service to carry several functions on a blockchain:

- Append and query address information - classical DNS, and IPvX requests from hosts
- Append and query routing information - classical RIPE, RADb, whois, etc. databases, transformed to the blockchain, and IPvX routing information
- Provide a backend and a frontend with blockchain interaction:
    - append and validate Smart Contracts
    - append and validate NFTs
    - etc.

IPvX DRS Query Process



User's Application

IPvX Distributed Resolver Service (DRS)

Request resource with **NFT Identifier**

Authenticate and verify **NFT**

Send authentication details

Map **NFT Identifier** to Resource

Return Resource / Data

User's Application

IPvX Distributed Resolver Service (DRS)

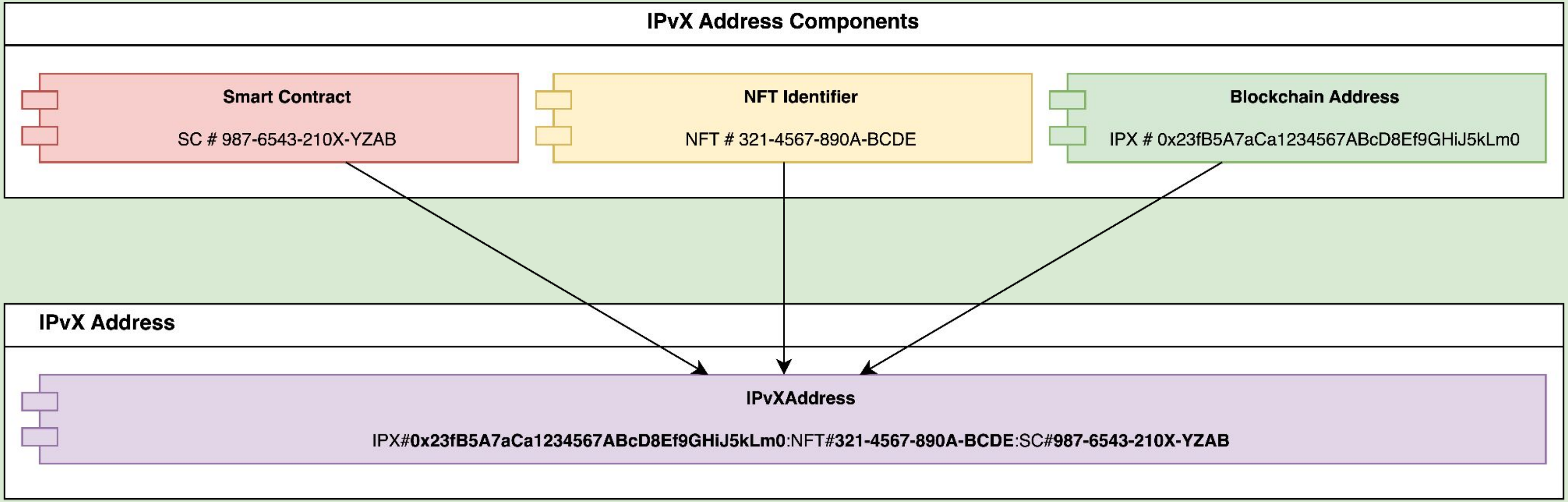
Advantages of NFT Identifier

The **NFT Identifier** represents authenticity of an entity.

We can outline several advantages of using NFT:

- NFT is issued to any type of content
- NFT can be used as the only technology to validate identities of entities of any kind in IPvX Ecosystem (and for traditional databases content for transitional period)
- NFT is tiny in size and able to point to content, stored at any accessible location (web url, ipfs cid)

IPvX Address Structure



IPvX Address Components

Smart Contract

SC # 987-6543-210X-YZAB

NFT Identifier

NFT # 321-4567-890A-BCDE

Blockchain Address

IPX # 0x23fB5A7aCa1234567ABcD8Ef9GHiJ5kLm0

IPvX Address

IPvXAddress

IPX#**0x23fB5A7aCa1234567ABcD8Ef9GHiJ5kLm0**:NFT#**321-4567-890A-BCDE**:SC#**987-6543-210X-YZAB**

Understanding IPvX Addressing

In **classic Internet** the resource address consists of several parts. In IPvX Ecosystem we also use several parts, with a slightly different meaning:

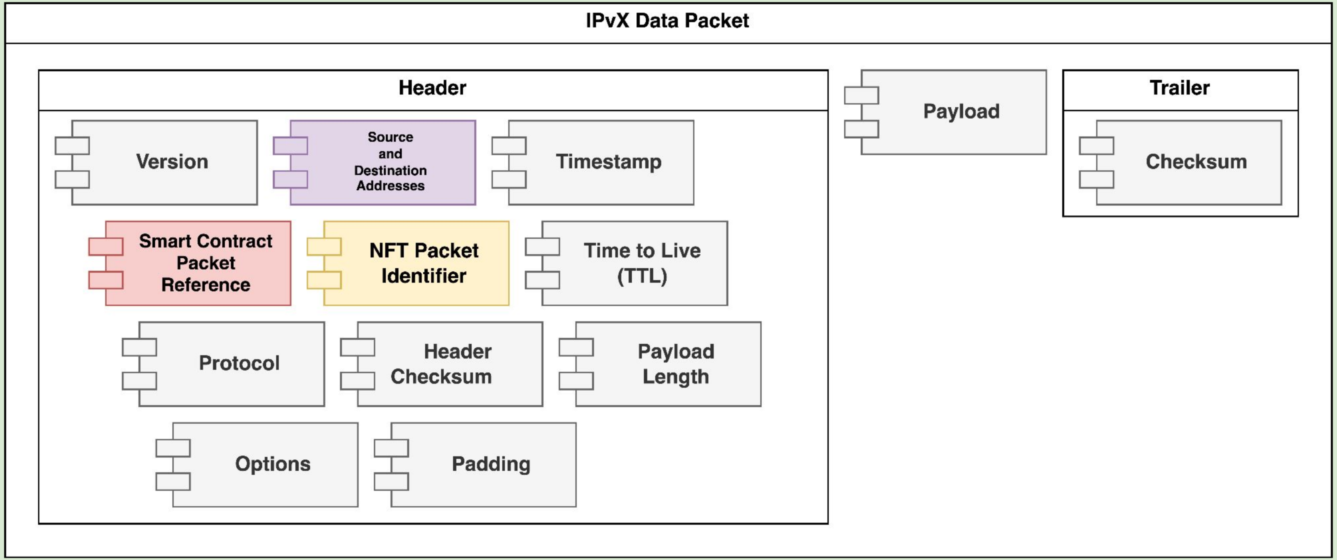
Classical

- scheme - *http*
- credentials - *{user}:{password}*
- server - *example.com*
- port - *:9090*
- path to resource - */billboard*

IPvX

- **IPX Address** - the address of a resource on a blockchain. It is an address of any possible entity in IPvX Ecosystem (person, route, webpage, alias, etc.)
- **NFT** - the authenticity of **IPX Address**
- **SC** - the rules how to handle the resource (to allow route or not, whether to firewall, the cost of a route, etc.)

IPvX Data Packet Structure



IPvX Data Packet

Header

Version

Source and Destination Addresses

Timestamp

Smart Contract Packet Reference

NFT Packet Identifier

Time to Live (TTL)

Protocol

Header Checksum

Payload Length

Options

Padding

Payload

Trailer

Checksum

Smart Contract Packet Reference — **Smart Contracts** revolutionize the concept of route formation and traffic conditions through network nodes

NFT Packet Identifier — **NFT Identifiers** are key in changing the approach to packet processing, control, and organisation

IPvX Data Packet Structure

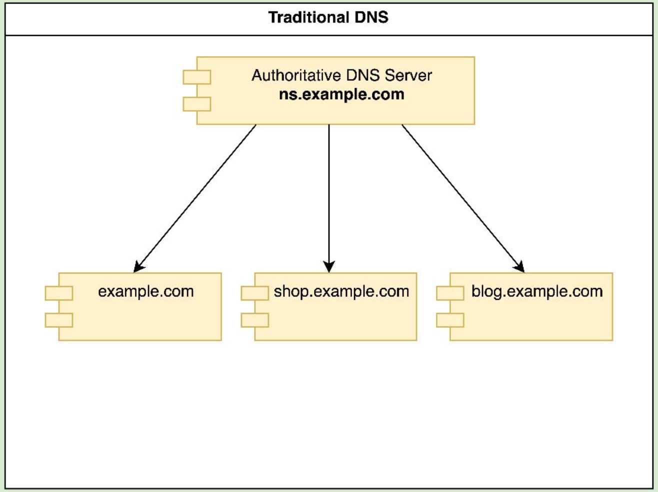
The paradigm of fragmenting information transfer into packets works well, so we advance with it.

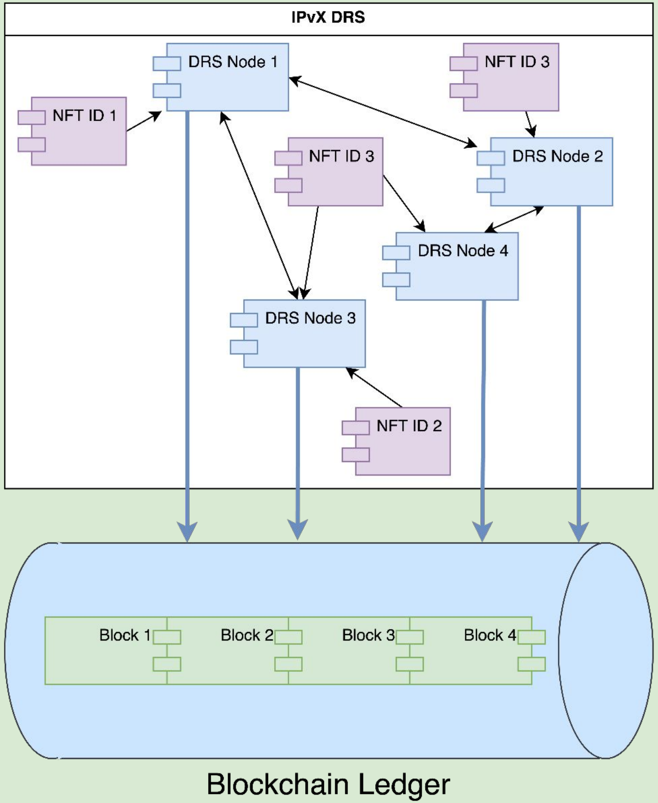
Along with traditional fields like *Timestamp, TTL, Checksum* and so on, there are new core fields in IPvX Data Packet:

- **Source IPX Address** - a variable during packet transfer, the source of a current packet
- **Destination IPX Address** - a variable during packet transfer, the address of a next hop
- **NFT Packet Identifier** - a constant during packet transfer, the identity of a source
- **Smart Contract Reference** - a constant during packet transfer, SC address to activate

We are still working on a packet structure.

Traditional Model vs. IPvX Model





Navigating a Distributed Network

All nodes are equal on IPvX Network, they are peer-to peer.

A node can be a regular user, or a specific one - a **Distributed Resolver Service (DRS)** node.

The user queries the desired **IPX address alias**, provides user's **NFT** identity, and point our which **SC** to activate if any required for this type of query.

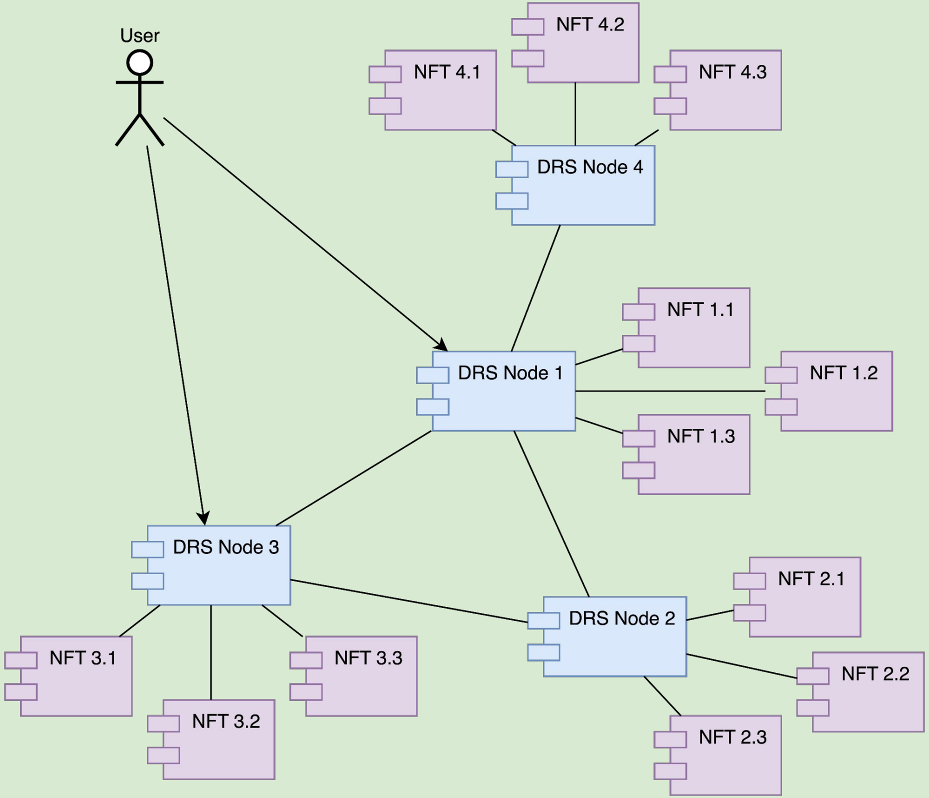
The **DRS** replies with an **IPX blockchain address**, and provides details on possible routes. According to user's query, this can be a fastest route, a cheapest route, or whatever criteria.

This is one basic scenario to use **DRS** as an alternative to classical DNS system.

With the power of **blockchain**, **NFT** and **Smart Contracts**, we can build a flexible network with numerous complex rules.

Decentralized System with DRS

IEDN



Security in IPvX

CIAAN:

- **Confidentiality** - data transmission is enciphered
- **Integrity** - transactions are digitally signed
- **Availability** - databases are distributed by design, numerous entry points
- **Authenticity** - origins are validated
- **Non-repudiation** - origins cannot refuse their transactions

Conclusion

IPvX Transition: The transition from DNS to IPvX with NFT identifiers marks a significant shift towards a more secure, decentralized network management system.

Technological Advancements: IPvX addresses critical limitations of DNS through enhanced security, scalability, and efficiency, using blockchain technology and NFTs for improved resource identification and management.

Future Outlook: The adoption of IPvX is poised to redefine Internet architecture, paving the way for a more resilient and user-empowered digital future.

Project X Contributors

Alexey Shkittin

Nikolay Labaznikov

Alexey Blagirev

Sergey Mukhortov

Alexander Timokhin

Questions & Answers