Network Working Group
Internet-Draft
Updates: 1034, 1035 (if approved)
Intended status: Informational
Expires: 28 September 2026

T. Tian, Ed.
CoCa. Foundation

March 2026

UTXO Domain Name System (UTXO-DNS): A Distributed Domain Name System Based on the Blockchain UTXO Model
draft-guorong-utxo-dns-00

Abstract

This document defines the UTXO Domain Name System (UTXO-DNS), a distributed domain name system based on the blockchain Unspent Transaction Output (UTXO) model. UTXO-DNS provides a decentralized domain name resolution mechanism supporting the registration, resolution, and management of both global and region-specific domain names. The system adopts a hierarchical naming structure compatible with the existing DNS while ensuring domain name ownership proof and tamper-proof characteristics through blockchain technology.

This protocol extends the traditional DNS protocol by introducing a blockchain-based domain name ownership verification mechanism, supporting internationalized domain names, digital currency address records, and decentralized identity records, among other new features.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 2 September 2026.

Table of Contents

1. Introduction

1.1. Background and Motivation

With the development of distributed systems and blockchain technology, the traditional centralized domain name system faces challenges in ownership transparency, censorship resistance, and decentralized control. The existing DNS system has the following limitations:

* Centralized control: the management of top-level domains is concentrated in ICANN and a few registries.

* Non-transparent ownership: domain name ownership records are opaque and vulnerable to single points of failure.

* Security dependencies: relies on centralized roots of trust and certificate authorities.

* Limited internationalization: support for internationalized domain names is limited.

UTXO-DNS aims to provide an alternative solution based on the UTXO model, combining the naming hierarchy of DNS with the immutability of blockchain to achieve a truly decentralized domain name system.

1.2. Design Principles

UTXO-DNS follows these core design principles:

* Backward Compatibility: maintain compatibility with existing DNS protocols (RFC 1034, RFC 1035) as much as possible.

* Decentralization: eliminate single points of failure and single points of control, enabling distributed governance.

* Verifiability: all domain name records are verifiable on-chain, providing cryptographic proofs.

* Internationalization: full support for internationalized domain names (IDN) in accordance with RFC 5890.

* Extensibility: support for multiple record types and extended features, including digital currency addresses and decentralized identities.

* Privacy Protection: built-in privacy protection mechanisms supporting selective disclosure.

1.3. Terminology and Definitions

1.3.1. Key Terms

This document uses the following key terms:

Term	Definition
UTXO	Unspent Transaction Output, representing ownership of assets on a blockchain.
Domain NFT	Non-Fungible Token representing ownership of a domain name.
Resolver Contract	Smart contract responsible for mapping domain names to resource records.
JUPC	JMBC Unified Communication Protocol.
Character Byte	UTF-8 encoded byte sequence with a maximum length of 16 bytes.
JMBC	JMBC digital currency based on the UTXO model.
CBDC	Central Bank Digital Currency.

Table 1

1.3.2. Protocol Terms

This protocol uses the following ABNF syntax to define domain name formats:

```
domain-label      = 1*16(ALPHA / DIGIT / UTF8-char)
domain-name       = domain-label *("." domain-label)
utxo-domain       = domain-name ".utxo"
regional-domain   = domain-name ".utxo" "." region-code
region-code       = 2ALPHA  ; ISO 3166-1 alpha-2
```

Where UTF8-char refers to UTF-8 encoded characters conforming to RFC 3629.

2. Protocol Overview

2.1. System Architecture

UTXO-DNS adopts a layered architecture as shown below:

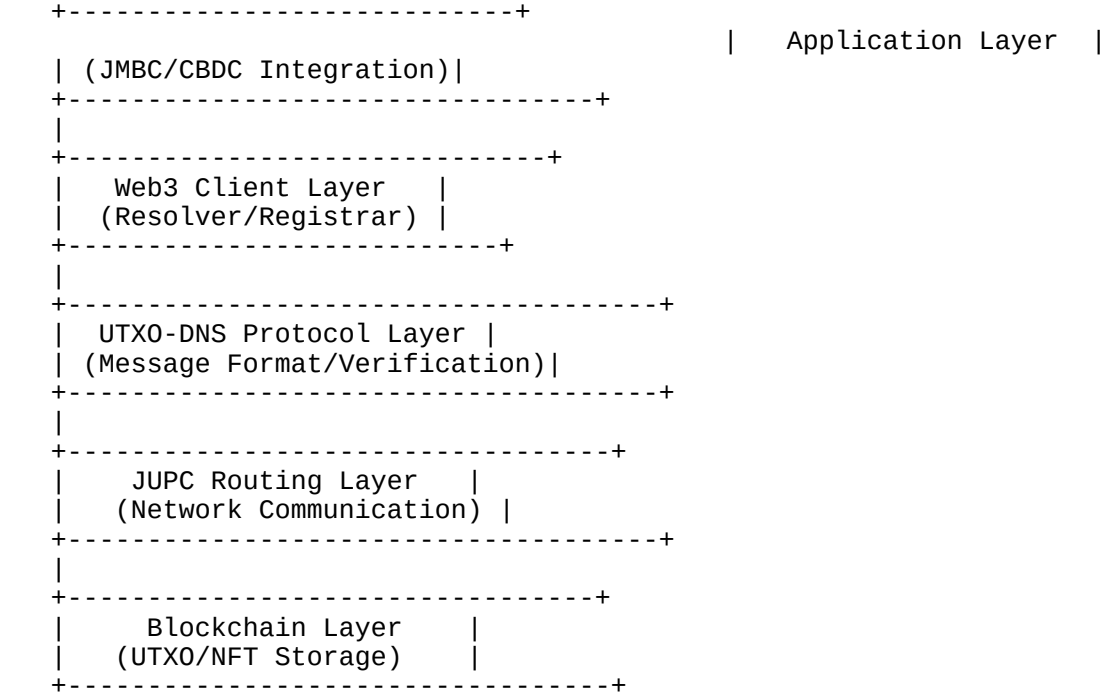


Figure 1

2.1.1. Protocol Stack

The UTXO-DNS protocol stack is as follows:

```
Application:   HTTP/HTTPS, SMTP, other application protocols
               |
UTXO-DNS:      Domain Name Resolution Protocol
               |
Transport:     JUPC/TCP, JUPC/UDP
               |
Network:       JUPC/IP
               |
Data Link:     Ethernet, Wi-Fi, 5G, etc.
```

2.2. Domain Name Format Specification

2.2.1. Syntax Definition

2.2.1.1. ABNF Syntax

UTXO-DNS domain names follow this ABNF syntax:

```
UTXO-DNS-name = global-domain / regional-domain

global-domain = label *("." label) ".utxo"
regional-domain = label *("." label) ".utxo" "." region-label
region-label = 2*63(ALPHA)

label = let-dig [*61(let-dig-hyp) let-dig]
let-dig = ALPHA / DIGIT
let-dig-hyp = ALPHA / DIGIT / "-"
```

Each label’s UTF-8 encoding must not exceed 16 bytes, and the total domain name length (including separators) must not exceed 253 bytes.

2.2.1.2. Internationalized Domain Name Processing

Internationalized domain names follow the IDNA2008 standards (RFC 5890-5894):

```
idn-label = *(ALPHA / DIGIT / other-utf8)
other-utf8 = UTF8-char  ; Unicode characters conforming to IDNA2008
```

The processing flow is as follows:

1. User input: "Example.Test.utxo"

2. Normalization: NFC normalization

3. Encoding: Convert to A-label (Punycode): "xn--fsq.xn--0zwm56d.utxo"

4. Storage: A-label form is stored on-chain

2.2.2. Domain Classification

2.2.2.1. Global Top-Level Domains

The format for global top-level domains is:

```
Example: jmbc.user.utxo
Structure: [organization].[namespace].utxo
```

Characteristics: universally applicable, no geographical restrictions, governed by a common set of rules.

2.2.2.2. Regional Domains

The format for regional domains is:

Example: jmbc.user.utxo.hk
Structure: [organization].[namespace].utxo.[region-code]
Region code: follows ISO 3166-1 alpha-2 standard

Characteristics: subject to region-specific regulations and must comply with local requirements.

3. Message Formats

3.1. Common Message Header

All UTXO-DNS messages share the following header structure:

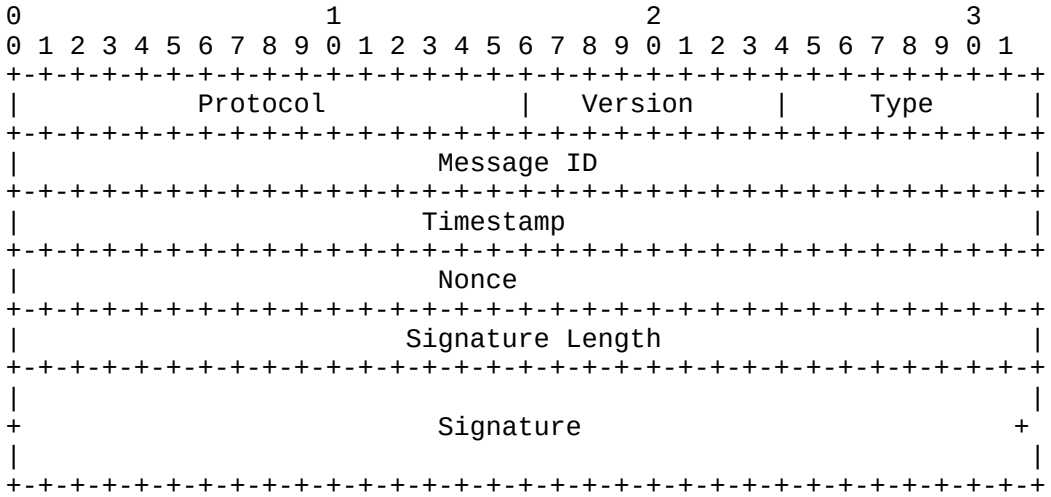


Figure 2

Field	Description
Protocol	Protocol identifier, fixed to 0x5544 (’UD’)
Version	Protocol version, currently 1
Type	Message type (1=Query, 2=Response, 3=Update, 4=Notification)
Message ID	Message identifier, used for request-response matching
Timestamp	Unix timestamp, second precision
Nonce	Random number to prevent replay attacks
Signature Length	Length of the signature in bytes
Signature	Sender’s signature over the message content

Table 2

3.2. Domain Name Resolution Query Message

The domain name resolution query message format is as follows:

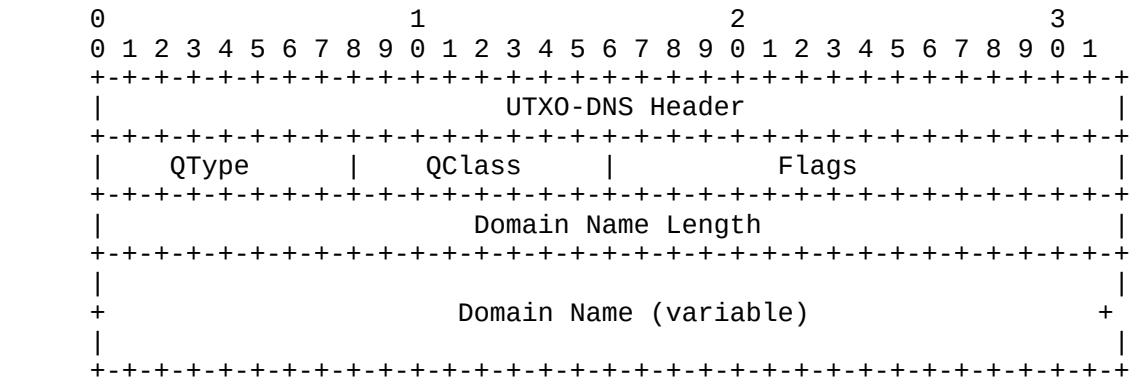


Figure 3

Field	Description
QType	Query type (1=A, 28=AAAA, 5=CNAME, 16=TXT, 257=JMBC, 258=CBDC)
QClass	Query class (1=IN, 255=ANY)
Flags	Flags - Bit 0: Recursion Desired (RD) - Bit 1: Checking Disabled (CD) - Bit 2: Authentic Data requested (AD) - Bits 3-15: Reserved
Domain Name Length	Length of the domain name in bytes
Domain Name	Domain name being queried, using DNS name compression format

Table 3

3.3. Domain Name Resolution Response Message

The domain name resolution response message format is as follows:

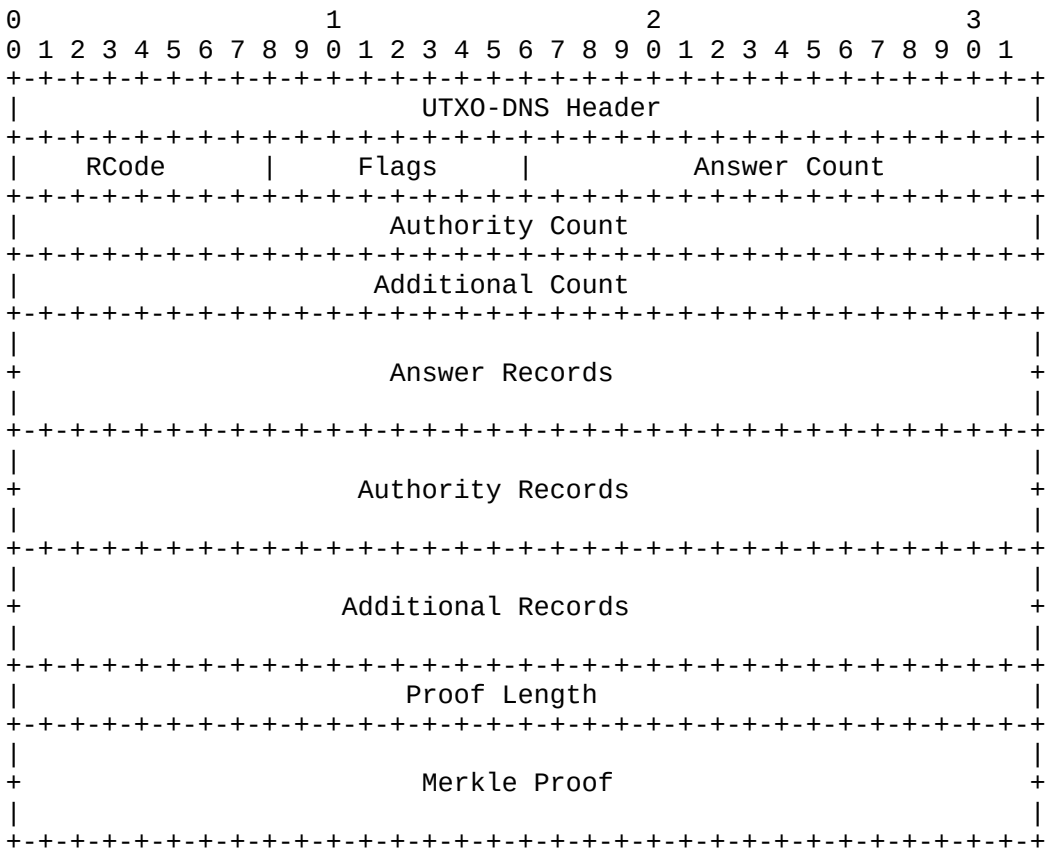

0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
UTXO-DNS Header
RCode
Flags
Answer Count
Authority Count
Additional Count
Answer Records
Authority Records
Additional Records
Proof Length
Merkle Proof

Figure 4

Field	Description
RCode	Response code (0=NOERROR, 3=NXDOMAIN, etc.)
Flags	Response flags - Bit 0: Authoritative Answer (AA) - Bit 1: Truncation (TC) - Bit 2: Recursion Available (RA) - Bit 3: Authentic Data (AD) - Bit 4: Checking Disabled (CD) - Bits 5-15: Reserved
Answer Count	Number of resource records in the answer section
Authority Count	Number of resource records in the authority section
Additional Count	Number of resource records in the additional section
Answer Records	Resource records for the answer section
Authority Records	Resource records for the authority section
Additional Records	Resource records for the additional section
Proof Length	Length of the proof data in bytes
Merkle Proof	Merkle proof used to verify the validity of the record

Table 4

3.4. Resource Record Format

The UTXO-DNS resource record format is as follows:

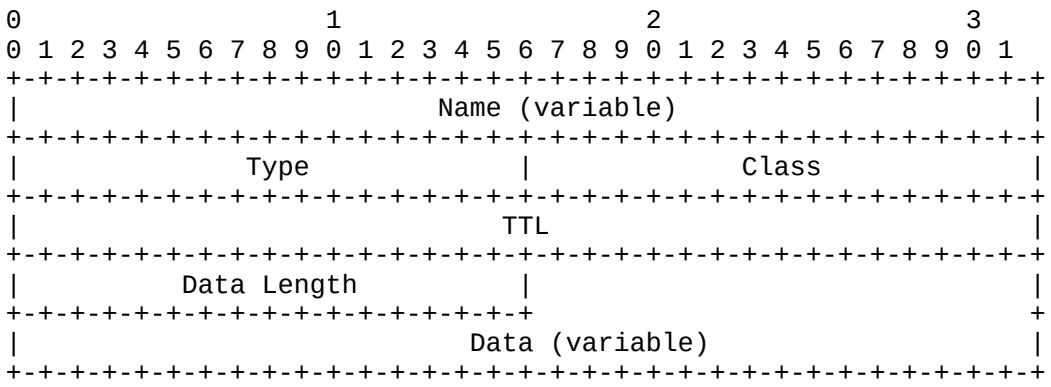


Figure 5

4. Record Type Definitions

4.1. Standard Record Types

4.1.1. A Record (IPv4 Address)

Type value: 1

Data format: 32-bit IPv4 address in network byte order

Example: 192.0.2.1

4.1.2. AAAA Record (IPv6 Address)

Type value: 28

Data format: 128-bit IPv6 address in network byte order

Example: 2001:0db8:85a3:0000:0000:8a2e:0370:7334

4.1.3. CNAME Record (Canonical Name)

Type value: 5

Data format: Canonical domain name using DNS name compression

Example: www.jmbc.user.utxo

4.1.4. TXT Record (Text Information)

Type value: 16

Data format: One or more character strings, each up to 255 characters

Example: "v=spf1 include:_spf.jmbc.utxo ~all"

4.2. Extended Record Types

4.2.1. JMBC Record (Digital Currency Address)

Type value: 257 (experimental)

Data format:

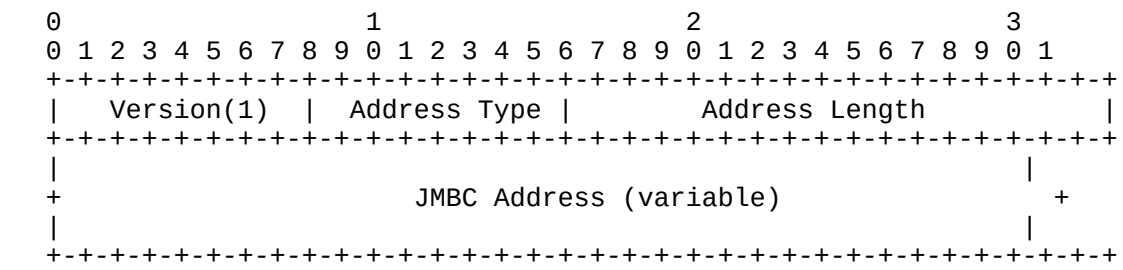


Figure 6

Field	Description
Version	Address format version, currently 1
Address Type	Address type (1=P2PKH, 2=P2SH, 3=Bech32)
Address Length	Length of the address data in bytes
JMBC Address	JMBC digital currency address

Table 5

4.2.2. CBDC Record (Central Bank Digital Currency Address)

Type value: 258 (experimental)

Data format:

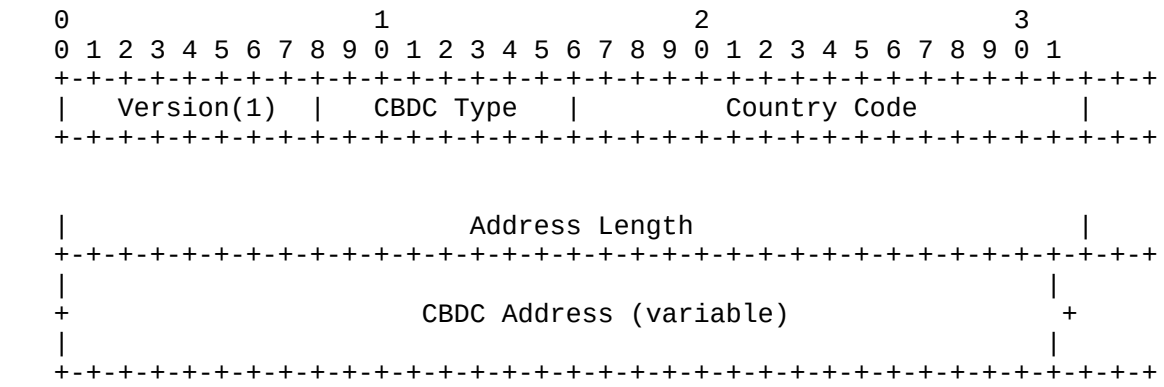


Figure 7

Field	Description
Version	Address format version, currently 1
CBDC Type	CBDC type (1=retail, 2=wholesale)
Country Code	ISO 3166-1 numeric country code
Address Length	Length of the address data in bytes
CBDC Address	Central Bank Digital Currency address

Table 6

4.2.3. DID Record (Decentralized Identifier)

Type value: 259 (experimental)

Data format: JSON-LD representation of a W3C DID document

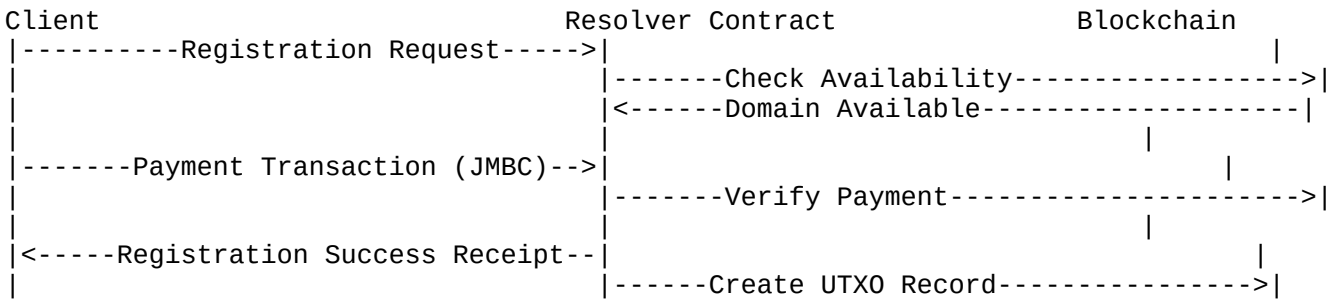
Example:

```
{
  "@context": "https://www.w3.org/ns/did/v1",
  "id": "did:utxo:jmbc.user.utxo",
  "verificationMethod": [...],
  "authentication": [...]
}
```

5. Protocol Operations

5.1. Domain Name Registration Flow

Domain name registration follows this flow:



5.1.1. Detailed Registration Steps

1. The client sends a domain registration request to the resolver contract, containing the desired domain name and registration period.

2. The resolver contract checks whether the domain name is available (not registered and not on the reserved list).

3. If available, the resolver contract returns the registration fee and payment address.

4. The client sends a transaction containing JMBC payment to the specified address.

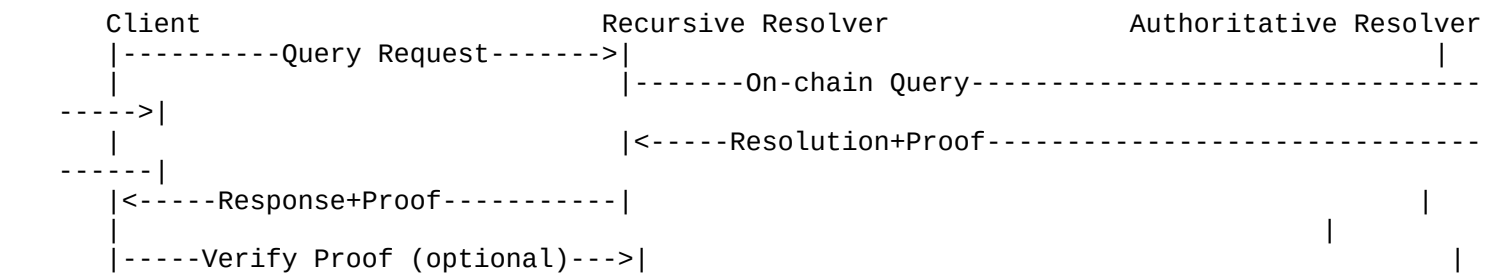
5. After verifying the payment, the resolver contract creates a domain UTXO record on the blockchain.

6. The client receives the transaction hash of the successful registration as a receipt.

5.2. Domain Name Resolution Flow

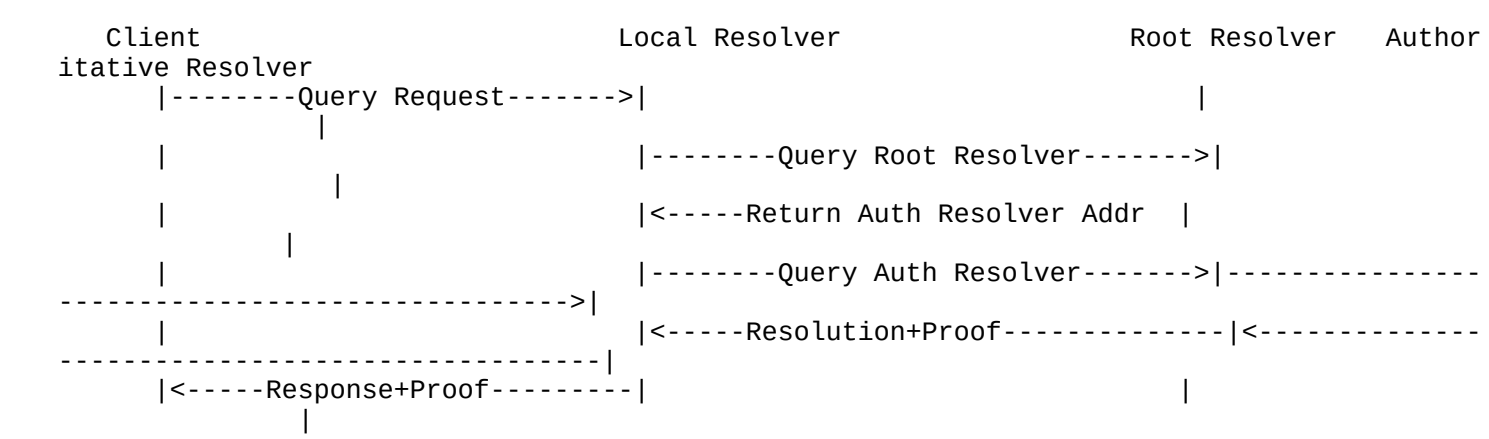
5.2.1. Recursive Resolution Flow

The recursive resolution flow is as follows:



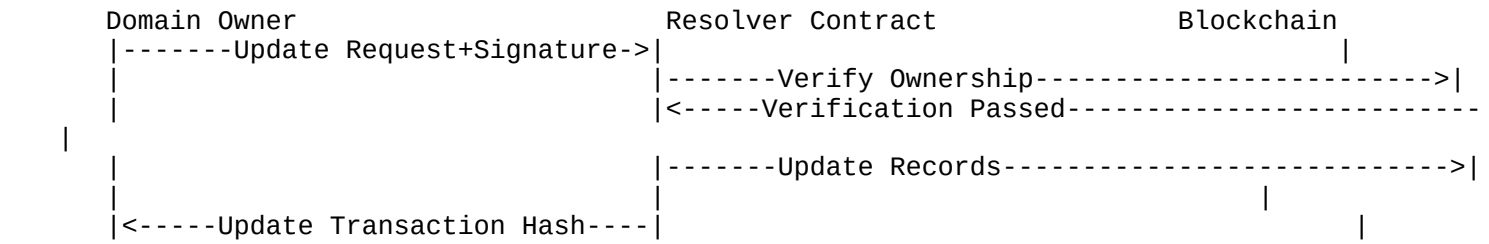
5.2.2. Iterative Resolution Flow

The iterative resolution flow is as follows:



5.3. Domain Name Update Flow

The domain name update flow is as follows:



Domain updates include the following operations:

* Modifying resource records (e.g., A, AAAA, TXT records).

* Changing the resolver contract address.

* Setting sub?domain delegation.

* Renewing domain registration.

* Transferring domain ownership.

6. Security Considerations

6.1. Threat Model

6.1.1. Attack Types

UTXO-DNS faces the following types of attacks:

* Domain Hijacking: an attacker attempts to illegitimately gain control of a domain.
* Cache Poisoning: polluting resolver caches to return false records.
* Man?in?the?Middle Attacks: intercepting and modifying DNS queries/responses.
* DDoS Attacks: denial?of?service attacks against resolution services.
* Sybil Attacks: creating many fake nodes to influence the network.
* Private Key Leakage: theft of a domain owner?s private key leading to domain theft.
* Smart Contract Vulnerabilities: security flaws in resolver contracts.

6.2. Security Mechanisms

6.2.1. Cryptographic Guarantees

UTXO-DNS employs the following cryptographic mechanisms:

1. Digital Signatures: all domain operations require the owner?s signature, using ECDSA (secp256k1) or EdDSA (Ed25519).
2. Merkle Proofs: on?chain proofs of record existence and validity.
3. Zero?Knowledge Proofs: optional identity privacy protection using zk?SNARKs or zk?STARKs.
4. Post?Quantum Algorithms: support for migration to post?quantum cryptography (PQC), including lattice?based signature schemes.

6.2.2. Operational Security

Operational security mechanisms include:

1. Timelocks: delays for sensitive operations (e.g., ownership transfer), default 24 hours.

2. Multi?signature: important domains can be configured with multi?sig control, requiring m?of?n signatures.

3. Emergency Recovery: recovery mechanism for lost private keys via social recovery or custodial services.

4. Sybil Attack Mitigation: registration limits and staking requirements; new registrations must stake JMBC.

5. Rate Limiting: rate limiting on frequent operations to prevent abuse.

6.3. Privacy Considerations

6.3.1. Privacy Threats

Privacy threats in UTXO-DNS include:

* Query Monitoring: attackers monitoring DNS queries to analyze user behaviour.

* Ownership Correlation: linking real identities to users via domain ownership.

* Transaction Graph Analysis: analysing blockchain transaction graphs to infer user relationships.

* Metadata Leakage: metadata exposed during resolution leaking user information.

6.3.2. Privacy?Enhancing Technologies

UTXO-DNS adopts the following privacy?enhancing technologies:

1. Encrypted Queries: support for Oblivious DNS over JUPC (ODoJ) using HPKE for end?to?end encryption.

2. Differential Privacy: adding Laplace noise to query statistics to protect aggregate privacy.

3. Ephemeral Identifiers: support for short?lived domains with automatic expiration for privacy.

4. Anonymous Credentials: anonymous proof of domain ownership using CL signatures or BBS+ signatures.

5. CoinJoin Techniques: transactions using CoinJoin or similar techniques to enhance privacy.

7. IANA Considerations

7.1. Protocol Number Assignment

This specification requests IANA to assign new values in the following registries:

7.1.1. DNS Parameters Registry

Assign the following values in the "Resource Record (RR) TYPEs" sub?registry of the "DNS Parameters" registry:

Type Value	Mnemonic	Description	Reference
257	JMBC	JMBC digital currency address	[This document]
258	CBDC	Central Bank Digital Currency address	[This document]
259	DID	Decentralized Identifier document	[This document]

Table 7

7.1.2. Port Numbers Registry

Assign the following ports in the "Service Name and Transport Protocol Port Number" registry:

Port	Protocol	Description	Status
5353	tcp/udp	UTXO-DNS service port	Suggested
5354	tcp/udp	UTXO-DNS over TLS service port	Suggested

Table 8

7.2. Creation of New Registries

This specification requests IANA to create the following new registries:

7.2.1. UTXO-DNS Error Codes Registry

Create a "UTXO-DNS Error Codes" registry with the following initial values:

Code	Name	Description
100	BLOCKCHAIN_ERROR	Blockchain interaction error
101	PROOF_INVALID	Proof is invalid
102	DOMAIN_EXPIRED	Domain name has expired
103	INSUFFICIENT_FUNDS	Insufficient funds
104	SIGNATURE_INVALID	Signature is invalid
105	CONTRACT_ERROR	Smart contract error

Table 9

The registration policy for this registry shall be "Standards Action".

7.2.2. UTXO-DNS Flags Registry

Create a "UTXO-DNS Flags" registry to record flag definitions in UTXO-DNS messages.

The registration policy for this registry shall be "Expert Review".

8. Intellectual Property Statement

8.1. Patent Policy

This specification follows the IETF patent policy[RFC8179].

8.1.1. Patent Disclosure Obligations

According to RFC 8179, all entities participating in the development of this standard must:

1. Early Disclosure: disclose known essential patents in a timely manner during the standardisation process.

2. Licensing Commitment: commit to license essential patents on reasonable and non?discriminatory (RAND) terms.

3. Transparency: publicly disclose patent holdings to avoid patent ambush.

8.1.2. CoCa. Foundation Patent Commitment

The CoCa. Foundation hereby declares that:

For any patented technology essential to the implementation of this specification, the CoCa. Foundation commits to grant royalty?free licenses to all implementers, with licensing terms conforming to the IETF RAND principles.

8.2. Copyright

This specification document follows the IETF copyright policy[RFC5378].

The text of this specification itself may not be copyrighted; it may be copied, distributed, and derived from, provided that the copyright notice is retained.

8.3. Trademarks

The following terms may be trademarks or registered trademarks of their respective owners:

* UTXO-DNS
* .utxo
* JMBC
* JUPC

All other trademarks mentioned in this document are the property of their respective owners.

9. Implementation Considerations

9.1. Compatibility Considerations

9.1.1. Compatibility with Legacy DNS

UTXO-DNS is designed with compatibility with legacy DNS in mind:

1. Protocol Compatibility: uses a query?response model similar to traditional DNS.

2. Record Type Compatibility: supports traditional DNS record types (A, AAAA, CNAME, TXT, etc.).

3. Extension Mechanism: uses EDNS(0) extension mechanisms for compatibility.

4. Proxy Gateway: provides a proxy gateway from legacy DNS to UTXO-DNS.

9.1.2. Compatibility with ENS

Differences between UTXO-DNS and the Ethereum Name Service (ENS):

Feature	UTXO-DNS	ENS
Base Model	UTXO/NFT model	Account model
Naming Hierarchy	Fixed .utxo TLD	Arbitrary TLDs
Regional Support	Built?in regional domains	No built?in support
Payment Integration	Native JMBC/CBDC	ETH/ERC-20

Table 10

UTXO-DNS plans to provide a bidirectional bridge with ENS, allowing domain migration between the two systems.

9.2. Performance Considerations

9.2.1. Blockchain Performance

UTXO-DNS adopts the following strategies to mitigate blockchain performance limitations:

1. Layered Storage: only ownership proofs and critical metadata are stored on?chain; resolution records are stored off?chain.

2. State Channels: high?frequency updates are handled via state channels and settled periodically on the main chain.

3. Batch Processing: multiple operations are packed into a single transaction to reduce on?chain load.

4. Cache Optimisation: extensive use of caching to reduce on?chain queries.

5. Sidechain Scaling: sidechains handle resolution queries while the main chain handles ownership transfers.

9.2.2. Resolution Performance

Domain name resolution performance optimisations:

1. Local Caching: clients and resolvers implement multi?level caching.

2. Prefetching: intelligent prefetching based on access patterns.

3. Parallel Queries: query multiple resolvers in parallel, using the fastest response.

4. Proof Batching: batch verification of Merkle proofs.

10. Standardisation Roadmap

10.1. Standardisation Phases

The UTXO-DNS standardisation plan consists of four phases:

Phase	Name	Timing	Main Objective
Phase 1	Experimental Draft	2024 Q4	Publish initial Internet?Draft, establish test network
Phase 2	Proposed Standard	2025 Q2	Complete interoperability testing, request IANA assignments
Phase 3	Draft Standard	2026 Q1	Stable version, at least two independent implementations
Phase 4	Internet Standard	2027 Q1	IESG approval, published as RFC

Table 11

10.2. IETF Standardisation Process

UTXO-DNS standardisation follows the IETF standards process:

Initial Draft ? IETF Review ? Working Group Formation ? Working Group Draft ? Multiple Reviews ? Working Group Last Call ? IESG Review ? RFC Publication

A request for working group formation is expected to be submitted to the IETF in Q1 2025.

11. Appendix A: Full List of Error Codes

Code	Name	Description
0	NOERROR	Successful completion
1	FORMERR	Format error
2	SERVFAIL	Server failure
3	NXDOMAIN	Domain name does not exist
4	NOTIMP	Function not implemented
5	REFUSED	Query refused
6	YXDOMAIN	Domain name already exists
7	YXRRSET	Resource record set already exists
8	NXRRSET	Resource record set does not exist
9	NOTAUTH	Server not authoritative
10	NOTZONE	Domain name not in zone
100	BLOCKCHAIN_ERROR	Blockchain interaction error
101	PROOF_INVALID	Proof invalid
102	DOMAIN_EXPIRED	Domain name expired
103	INSUFFICIENT_FUNDS	Insufficient funds
104	SIGNATURE_INVALID	Signature invalid
105	CONTRACT_ERROR	Smart contract error

+------+--------------------+-----------------------------------+

Table 12

12. Appendix B: Example Messages

12.1. Example Query Message

Query for the A record of jmbc.user.utxo:

Raw message (hexadecimal):
5544 01 01 00000001 00000000 00000001 00000000
00000048 3045022100... 00 01 0001 0B 6A6D6263
2E757365722E7574786F 0001 0001

Decoded:
- Protocol: UTXO-DNS (0x5544)
- Version: 1
- Type: Query (1)
- Message ID: 1
- Timestamp: 0
- Nonce: 1
- Signature length: 72 bytes
- Signature: 3045022100...
- QType: A (1)
- QClass: IN (1)
- Domain name length: 11 bytes
- Domain name: "jmbc.user.utxo"

12.2. Example Response Message

Response containing A record 192.0.2.1:

```
Raw message (hexadecimal):
5544 01 02 00000001 00000000 00000001 00000000
00000048 3045022100... 00 0001 0001 0000 0000
00000020 0B6A6D62632E757365722E7574786F 0001
0001 0000012C 0004 C0000201 00000020 010203...

Decoded:
- Protocol: UTXO-DNS (0x5544)
- Version: 1
- Type: Response (2)
- RCode: NOERROR (0)
- Flags: Authoritative Answer (0x0001)
- Answer count: 1
- Authority count: 0
- Additional count: 0
- Proof length: 32 bytes
- Domain name: "jmbc.user.utxo"
- Type: A (1)
- Class: IN (1)
- TTL: 300 seconds
- Data length: 4 bytes
- Data: 192.0.2.1
- Proof: Merkle proof data
```

13. Appendix C: Configuration Examples

13.1. Resolver Configuration File Example

Example UTXO-DNS resolver configuration file (YAML format):

```
# utxo-dns-resolver.yaml
version: 1.0
network:
  chain_id: "jmbc-mainnet-1"
  rpc_endpoints:
    - "https://rpc.jmbc.utxo:8545"
    - "https://rpc2.jmbc.utxo:8545"
  ws_endpoints:
    - "wss://ws.jmbc.utxo:8546"

resolver:
  cache_size: 10000
  cache_ttl: 300
  max_recursion: 10
  enable_dnssec: true
  enable_privacy: true

security:
  require_proof: true
  proof_expiry: 3600
  allowed_algorithms:
    - "secp256k1"
    - "ed25519"
    - "sr25519"

logging:
  level: "info"
  format: "json"
  output: "/var/log/utxo-dns/resolver.log"
```

13.2. Client Configuration File Example

Example UTXO-DNS client configuration file (JSON format):

```
{
  "version": "1.0",
  "resolvers": [
    "https://dns1.jmbc.utxo:5353",
    "https://dns2.jmbc.utxo:5353"
  ],
  "fallback_resolvers": [
    "8.8.8.8",
    "1.1.1.1"
  ],
  "prefer_utxo": true,
  "enable_cache": true,
  "cache_size": 1000,
  "privacy": {
    "enable_encryption": true,
    "enable_oblivious": false,
    "query_minimization": true
  },
  "debug": false
}
```

14. Normative References

[RFC1034] "Domain names - concepts and facilities", STD 13, RFC 1034, DOI 10.17487/RFC1034, November 1987, <https://www.rfc-editor.org/info/rfc1034>.

[RFC1035] "Domain names - implementation and specification", STD 13, RFC 1035, DOI 10.17487/RFC1035, November 1987, <https://www.rfc-editor.org/info/rfc1035>.

[RFC5890] "Internationalized Domain Names for Applications (IDNA): Definitions and Document Framework", RFC 5890, DOI 10.17487/RFC5890, August 2010, <https://www.rfc-editor.org/info/rfc5890>.

[RFC6891] "Extension Mechanisms for DNS (EDNS(0))", RFC 6891, DOI 10.17487/RFC6891, April 2013, <https://www.rfc-editor.org/info/rfc6891>.

[RFC8179] "Intellectual Property Rights in IETF Technology", BCP 79, RFC 8179, DOI 10.17487/RFC8179, May 2017, <https://www.rfc-editor.org/info/rfc8179>.

[RFC5378] "Rights Contributors Provide to the IETF Trust", BCP 78, RFC 5378, DOI 10.17487/RFC5378, November 2008, <https://www.rfc-editor.org/info/rfc5378>.

[RFC8126] "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/info/rfc8126>.

15. Informative References

[Bitcoin] Nakamoto, S., "Bitcoin: A Peer-to-Peer Electronic Cash System", 2008, <https://bitcoin.org/bitcoin.pdf>.

[ENS] ENS Team, "Ethereum Name Service Documentation", <https://docs.ens.domains/>.

[JUPC] CoCa. Foundation, "JMBC Unified Protocol Communication Specification", Version 1.0, 2024, <https://jmbc.utxo/specs/jupc-v1.0>.

Appendix A. Author’s Address

12710 PLAZA SIMATUPANG LANTAI 6 UNIT 3, JALAN TB SIMATUPANG KAV.IS NOMOR 01 RT. 002 RW. 017, PONDOK PINANG, KEBAYORAN LAMA, KOTA ADM. JAKARTA SELATAN, DKI JAKARTA JAKARTA Indonesia +62-81320006570 cocapetroleum@gmail.com standards@jmbc.utxo

Author’s Address

Tian Guorong (editor)
CoCa. Foundation
Jakarta
12710
Indonesia
Phone: 62-8132000657+86-133X79841229
Email: cocapetroleum@gmail.com, standards@jmbc.utxo