



# STATE OF ENS DOMAINS

Part 1: IPFS, ICANN, DNS, ðApps, and identities



Attribution-ShareAlike 4.0  
International (CC BY-SA 4.0)



Presented by Steve Huguenin at Geneva DevChain Meetup  
which takes place in Lausanne, CH on 6 december 2022





# Contents

Domain Name System (DNS)

IANA, ICANN: Internet central authority

Ethereum

Evolution of the state of Blockchain address encoding

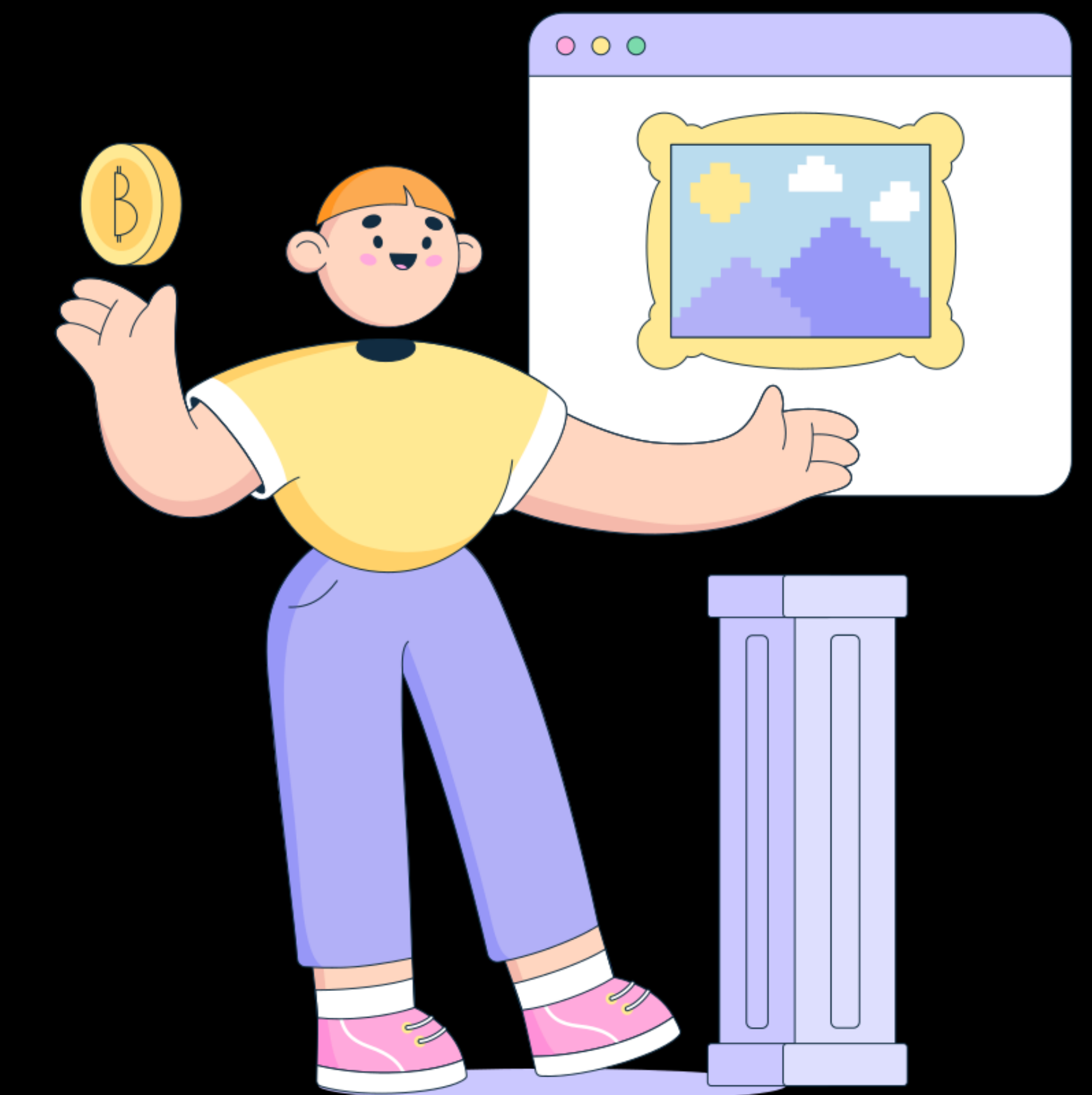
An open, permissionless DNS

Ethereum Name Service

DApp: Decentralised Application

Discussion with IANA

Scalability



# Domain Name System (DNS) 🌐

In both OSI and TCP/IP reference models, name service refer to the application Layer.

**A name service is an internet protocol for translation (resolution) of network identifiers (= addresses) with human readable names (= domain names).**



Name service primarily resolves **domain names** into **adresses**, but could also translates **adresses** into **domain names**.



# IANA, ICANN: Internet central authority 👑

ICANN stands for **Internet Corporation for Assigned Names and Numbers**

ICANN is a nonprofit policymaker for the IP addresses and top level domains (TLD).

IANA owns three name service computers (servers) known as the **Domain Name System** (DNS) Root which makes the internet working.

When the DNS root breaks down, the entire internet does not respond.

The reference top level domain is in fact .arpa which originates from the legacy **ARPANET**.

The internet was designed to be without any central authority before **Tim Berners-Lee** came up with the **World Wide Web (WWW)**.





# Ethereum

The decentralized supercomputer = ledger + smart contract platform

Based on Ethereum Virtual Machine (EVM)

The first public Layer-1 Turing complete blockchain:  
Endless possibilities

People crowdfund Vitalik Buterin to develop this protocol. 

Smart contracts are composed of routines and events which are **fully interoperable**.

Many use cases are presented in the proposal among them is a decentralised name service protocol.



*Vitalik Buterin pitches his idea for a decentralised supercomputer named Ethereum*



# Evolution of the state of Blockchain address encoding

Bitcoin: Base 58 (2009)

- Developed by Satoshi Nakamoto
- Replaced by BECH32 in SegWit

Ethereum: 0x + Keccak-256 hash (2013)

- Derive from SHA-3
- Still used today and should remain in Eth2
- Used in Layer-2 protocols (side-chains, Zk rollups, etc.)

Cardano: blake2b-256 (2015)

- BLAKE2 is currently the strongest encoding method which ever exists.
- Cardano also delegates to Layer-2 protocols but already implements PoS validation.

**All these encodings are subject to human errors.**



# An open, permissionless DNS

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.1;

// This is a smart contract - a program that can be deployed to the Ethereum blockchain.
contract SimpleDomainRegistry {

    address public owner;
    // Hypothetical cost to register a domain name
    uint constant public DOMAIN_NAME_COST = 1 ether;

    // A `mapping` is essentially a hash table data structure.
    // This `mapping` assigns an address (the domain holder) to a string (the domain name).
    mapping (string => address) public domainNames;

    // When 'SimpleDomainRegistry' contract is deployed,
    // set the deploying address as the owner of the contract.
    constructor() {
        owner = msg.sender;
    }

    // Registers a domain name (if not already registered)
    function register(string memory domainName) public payable {
        require(msg.value >= DOMAIN_NAME_COST, "Insufficient amount.");
        require(domainNames[domainName] == address(0), "Domain name already registered.");
        domainNames[domainName] = msg.sender;
    }

    // Transfers a domain name to another address
    function transfer(address receiver, string memory domainName) public {
        require(domainNames[domainName] == msg.sender, "Only the domain name owner can transfer.");
        domainNames[domainName] = receiver;
    }

    // Withdraw funds from contract
    function withdraw() public {
        require(msg.sender == owner, "Only the contract owner can withdraw.");
        payable(msg.sender).transfer(address(this).balance);
    }
}
```

example taken on 6/12/2022 from <https://ethereum.org/en/>

# Ethereum Name Service

Based on the current proposal

Delegates domain name registration for the whole Ethereum network

Feature configurable routes for all kind of services (**ETH, BTC, Twitter, website, etc.**)

Requires some fees for minting (**ERC1155**)

Compatible with **MetaMask, WalletConnect** and **Gnosis Safe**

Interoperable with **Layer-2** protocols

Feature multiple **Ethereum Improvement Proposal (EIP)** standards

Tradable as an **Non Fungible Token (NFT)**



# Interplanetary File System (IPFS)

IPFS is based on a technology stack named **libp2p**.

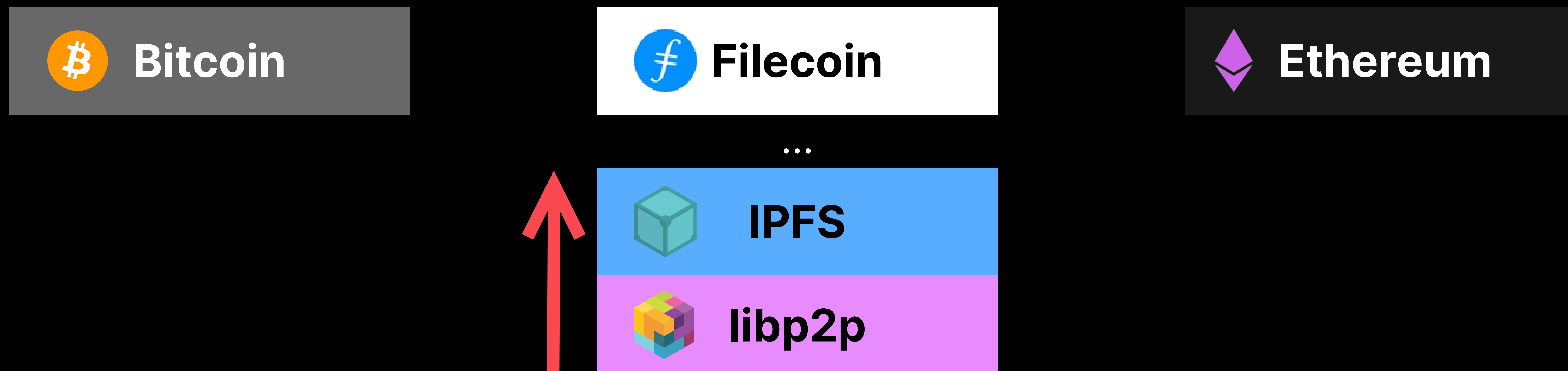
It implements libp2p initially to serve as the decentralised storage of **Filecoin** but it is interoperable with any protocol.

It could replace **HTTP** and can be encrypted with **Tor**.

It is peer **distributed** and **fault tolerant** (replication, splitting, etc.).

It belongs to the family of **graph databases** (Merkle DAG).

It experienced incredible growth in 2021 with **NFT** popularity.






# DApp: Decentralised Application + =

ethereum.eth


PARENT

eth


REGISTRANT




0x899FcB1437DE65DC6315f5a69C017dd3F2837557



CONTROLLER




0xAd2e180019FCa9e55CAdE76E4487F126Fd08DA34



EXPIRATION DATE

2034.05.04 at 11:28 (UTC+02:00)




Remind Me

RECORDS

ADDRESSES

ETH

0xde0B295669a9FD93d5F28D9Ec85E40f4cb697BAe



BTC

Not set


LTC

Not set

DOGE

Not set

ipfs://bafybeidoodypolrlzuffnng5swfpotyhu7cdjh5vs6sc6jbuz47lprw6wfi




(https://ethereum.eth.limo)

TEXT RECORD

url

ethereum.org



email

Not set

avatar

Not set

description

Not set

notice

Not set

keywords

Not set

com.discord

Not set

com.github

Not set

com.reddit

Not set

com.twitter

Not set

org.telegram

Not set

eth.ens.delegate

Not set

ENS recordings contain two main sections:

- Addresses feature ETH, BTC, LTC and DOGE.
- Text record feature different media information and a possible ENS delegate (redirection).

ENS text record works a the DNS route settings but has no compatibility with DNS records whatsoever (CNAME, A, AAAA, etc. are not implemented in ENS).

ENS is able to route any request to IPFS.

MetaMask has a complete support for ENS routing through an IPFS node (often [dweb.link](https://dweb.link)).

DApps are a major step for a true decentralised web.



## Discussion with IANA 🕌

Users can register their internet domain names in ENS:

- DNS cannot solve .eth names.
- ENS organisation need recognition from IANA to lease domain names and receive a .arpa domain name.

ENS domains are currently the only registrar for domain names

- Registrars could interact with ENS smart contract.
- Customers would pay either in **ETH** or **FIAT** (in a staking pool).

Ethereum Foundation has no governance on ENS:

- ENS is #1 solution for decentralised domain names.

ENS domains is run by a profit organisation.

It is difficult to measure the difficulty for implementing a domain name server between DNS and ENS.



# Scalability

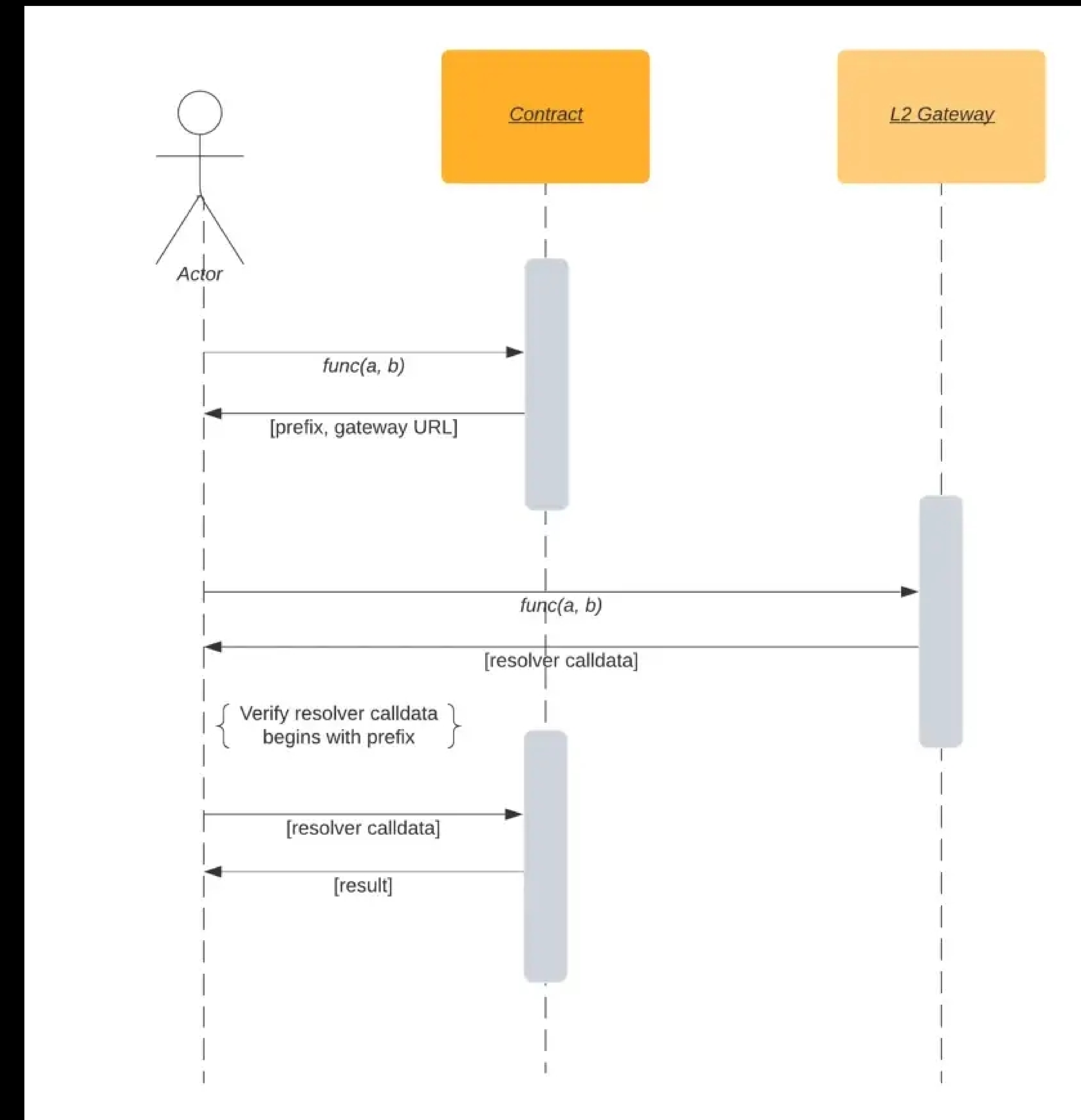
ENS are looking into delegating ENS records to **Layer-2 solutions**.

ENS are currently working with **Optimism** to solve scalability issues regarding **minting ERC1151 tokens**.

Minting a **single domain** and **transferring your assets back and forth** might be **the most expensive way** to mint an ERC1151 token.

Working with Optimism requires some bridge to transfer your assets.

Optimism has a native Ethereum bridge <https://app.optimism.io/bridge/deposit>





# References

How ENS is taking Ethereum to the rest of the Internet by Brantly Millegan (Devcon5) <https://archive.devcon.org/archive/watch/5/how-ens-is-taking-ethereum-to-the-rest-of-the-internet/>

Wikipedia - Ethereum <https://en.wikipedia.org/wiki/Ethereum>

Wikipedia - Bitcoin <https://en.wikipedia.org/wiki/Bitcoin>

Wikipedia - Cardano <https://en.wikipedia.org/wiki/Cardano>

Wikipedia - Domain Name System [https://en.wikipedia.org/wiki/Domain\\_Name\\_System](https://en.wikipedia.org/wiki/Domain_Name_System)

Wikipedia - ICANN <https://en.wikipedia.org/wiki/ICANN>

Wikipedia - IANA <https://en.wikipedia.org/wiki/IANA>

What is ETH.LIMO? (Medium) <https://medium.com/@ethdotlimo/what-is-eth-limo-faf18dcaa36d>

MVP of ENS on L2 with Optimism: Demo Video + How to Try It Yourself (Medium) <https://medium.com/the-ethereum-name-service/mvp-of-ens-on-l2-with-optimism-demo-video-how-to-try-it-yourself-b44c390cbd67>



## Contact us



**Steve Huguenin**  
[steve@brotherday.one](mailto:steve@brotherday.one)

**Frank Medjo'o**  
[frank@brotherday.one](mailto:frank@brotherday.one)



# Legal terms

## You are free to:



**Share** — copy and redistribute the material in any medium or format

**Adapt** — remix, transform, and build upon the material for any purpose, even commercially.

This license is acceptable for Free Cultural Works.

The licensor cannot revoke these freedoms as long as you follow the license terms.