

Internet Engineering Task Force
Internet-Draft
Intended status: Informational
Expires: December 10, 2021

S. Chen
Data61
T. Hardjono
MIT
June 8, 2021

Gateway Identification and Discovery for Decentralized Ledger Networks
draft-chen-dlt-gateway-identification-00

Abstract

Today there is a growth in the number of blockchain and decentralized ledger networks (DLN) around the world, and interoperability across different networks represents a challenge for the value proposition of these networks.

One approach for blockchain interoperability to be achieved is to employ gateways that permit assets to flow across the relevant networks of blockchains.

However, a core requirement for interoperability is the correct identification of computer systems that act as gateways and the correct validation of the ownership of the gateway. A secondary requirement is for a gateway to inquire as to the existence of an entity address (public key) within a given decentralized ledger network.

This memo discusses options with regards gateway identification and verification strategies. It looks at addressing the problem from the application layer and from the network layer. It also discusses other options, such as relying on a third-party blockchain-registered identifiers and resolver services

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 December 10, 2021.

Copyright Notice

Copyright (c) 2021 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](https://trustee.ietf.org/bcp78) and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	2
2.	Conventions used in this document	3
3.	Terminology	4
4.	Gateway Registration, Discovery and Validation	5
4.1.	Overview	5
4.2.	Gateway Declaration and Registration	5
4.3.	Gateway Discovery and Validation	6
4.4.	Verification of Identities and Addresses	6
5.	Network Layer Gateway Discovery and Verification	7
5.1.	Prerequisites	7
5.2.	DNS-based Gateway Discovery	8
6.	Application Layer Gateway Discovery and Verification	9
7.	Security Consideration	11
8.	IANA Consideration	11
9.	References	11
9.1.	Normative References	11
9.2.	Informative References	12
	Authors' Addresses	12

[1.](#) Introduction

Currently there is a growth in the number of blockchain and distributed ledger technology (DLT) systems being deployed worldwide for different areas of applications (e.g. finance, supply chains, IoT

devices, etc.). One notable application is in the area of digital assets (or virtual assets) [[FATF](#)].

As independent autonomous systems, each decentralized ledger network (DLN) employs its own interior protocols (e.g. consensus protocols)

that manages the resources (e.g. shared ledger) relevant to the assets and entities in that network. Key to the success of the blockchain and DLT paradigm is the interoperability between DLNs, permitting digital assets to be moved across DLNs in an efficient and secure manner.

For the purposes of asset transfers across DLNs, one or more nodes within a DLN can take-on the role of a gateway that peers with other gateways belonging to other DLNs [[ARCH](#)]. As a node participating in a blockchain, a gateway has access to the resources (e.g. ledger) located in the interior of that blockchain. Facing outbound, the gateway has the ability to peer with matching gateways to facilitate asset transfers.

A core requirement for the gateway-to-gateway protocol [[ODAP](#)] employed by peered gateways is the is the correct identification of the systems that act as gateways and the correct validation of the ownership of the gateway. Gateway ownership is notably important in cases where a digital asset bearing economic value is to be transferred cross-border (cross regulatory jurisdictions).

(a) Application layer: At the application layer a gateway identification scheme is needed that permits an organization who participate in a given DLN to declare (advertise) one or more gateways into that DLN. This permits organizations to establish peering agreements (contracts) based on the asset type, DLN and jurisdictions, identifying (specifying) the gateways that will be used to connect to the DLN.

(b) Network layer: In order for asset transfer services to scale-up, some degree of automation is needed for a gateway to discover peer gateways in remote DLN. This discovery must be efficient in order to minimize the time required for a digital asset from an originator in an origin DLN to be transferred cross-chain to the beneficiary in the destination DLN (see [[ODAP](#)]).

[2.](#) Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC 2119](#) [[RFC2119](#)].

In this document, these words will appear with that interpretation only when in ALL CAPS. Lower case uses of these words are not to be interpreted as carrying significance described in [RFC 2119](#).

[3.](#) Terminology

The following are some terminology used in the current document. Further terminology can be found in [[NIST](#)][OSI].

- o Decentralized ledger network (DLN): A blockchain system or an implementation of a decentralized ledger technology (DLT) consisting nodes that shares a common set of resources. This term is used generically to refer to the collection of nodes as an autonomous system.
- o DLN identification number: This is the unique network identification for a DLN. This is akin to the AS-number issued by ARIN in North America for autonomous systems operated by Internet Service Providers.
- o Device identity: This is the unique public-private key pair that is bound to the device (e.g. hardware) of the gateway. Examples include the IEEE 802.1AR Secure Device Identity [DevID] and the TPM EK/AIK key pair [TPM]. The device identity public key may be represented using an X.509 certificate.
- o Gateway service endpoint: The URL or URI at the gateway device that provides gateway related services, such as asset transfer/migration services. See [[ODAP](#)] for a definition of the ODAP protocol.
- o Service endpoint identity: This is the unique public-private key pair bound to the protocol service end-point of the gateway

function. This key-pair is used in the establishment of a secure channel with a peer gateway (e.g. TLS). The endpoint identity public key should be represented using an X.509 certificate, which unambiguously states the purpose of the endpoint.

- o Owner identity: This is the unique public-private key pair of the entity who legally owns and operates the gateway. For clarity this entity is referred to as a virtual asset service provider (VASP). The VASP identity public key should be represented using an X.509 certificate, possibly including extended fields such as those found in Extended Validation (EV) X.509 certificates [CAB].
- o Blockchain gateway service provider (BGSP): The virtual asset service provider that owns and operates the gateway service. The term provides distinction from a technical/protocol perspective, since a BGSP entity is a virtual asset service provider in the business and regulatory sense.

[4. Gateway Registration, Discovery and Validation](#)

[4.1. Overview](#)

In the context of a digital asset transfer, a gateway identification, discovery and verification solution consists of mechanisms that permit a local gateway to obtain assurance that a given remote device is a gateway with verifiable identity and ownership. That is, it need to obtain assurance that (a) the device is operating as a gateway for a designated blockchain or decentralized ledger network and (b) is owned by an entity operating under the relevant jurisdiction in the context of the digital asset in question.

(i) gateway identity authentication: verification that the device with a given identification truly functions as a gateway (and not a rouge server masquerading as a gateway);

(ii) gateway ownership validation: verification that a remote gateway is owned by the organization (e.g. VASP) that is operating within a given jurisdiction;

(iii) asset type transferability: verification that a remote gateway

for a destination DLN is mechanically capable to receive the type of asset and that legally permitted to receive the type of asset.

[4.2.](#) Gateway Declaration and Registration

A given asset service provider may possess multiple nodes within one or more DLNs globally. Depending on the specific technical constraints of a given DLN (e.g. consensus model), not every node within the DLN may be designated to be a gateway capable of participating in an asset transfer between two DLNs. As such, the service provider must nominate its nodes or systems specifically as gateways. As such, there must be some mechanism that permits the asset service provider to declare that a given device or system serves as a gateway into a given DLN.

One possible approach is for the service provider to publish a signed list of the gateways and the endpoints that implement the cross-chain asset transfer protocol for a given asset type. Extending this notion, a directory of gateways may be established by a group or consortium of asset service providers as a means to share a common location where gateway information can be found.

This directory approach is currently already being developed by some asset service providers in the context originator/beneficiary data for compliance to the Travel Rule regulations [[FATF](#)] dealing with anti-money laundering (AML). An example is the TRISA directory

[[TRISA](#)], which lists business information of virtual asset service providers (VASP) claiming compliance to the AML regulations. Such a directory could be extended to include the gateways owned and operated by the VASPs.

[4.3.](#) Gateway Discovery and Validation

When an originator (sender) in an origin DLN1 seeks to transfer digital assets to a beneficiary (recipient) located in a remote destination DLN2, a gateway G1 in DLN1 must be able to locate and validate one (or more) gateways G2 serving DLN2.

This discovery process must be automated as far as possible, and discovery should not require human intervention. If a directory of gateways is available, then it should be utilized by both gateways G1

and G2.

Discovery, therefore, covers a number of layers and functions:

- o Gateway network device discovery: There must be a mechanism to discover the gateway at the IP network layer (e.g. IP address, port number) and obtain the device identity of the gateway (e.g. LDevID or device public key).
- o Gateway service endpoint discovery and validation: Following the device discovery, there must be a mechanism to discover and verify the endpoint at the gateway that provide services related to its role as a gateway. These include the endpoint for asset transfers and the endpoint for crash recovery [Crash].

[4.4.](#) Verification of Identities and Addresses

In many cases, an originator (sender) in an origin DLN1 may be in possession only of the beneficiary's name and blockchain-address. This means that the gateway G1 in DLN1 must ensure that the beneficiary's address exists in the DLN2 and that it is bound to the beneficiary entity or user in DLN2.

Although out scope for the current work, it is perhaps worth noting that the responsibility of verifying the identity and legal status of originators and beneficiaries lies with the virtual asset service providers who employ technical mechanism (including gateways and nodes) to transact the digital assets [[FATF](#)].

[5.](#) Network Layer Gateway Discovery and Verification

Gateway discovery and verification at the network layer takes a bottom-up strategy, where a gateway discovers a peer remote gateway and initiates verifications. This is part of Phase-1 of the gateway architecture [[ARCH](#)]. This approach mimics the client to MTA (Message Transfer Agent) interaction pattern in the classic SMTP mail transfer protocol [[RFC2821](#)].

5.1. Prerequisites

To ensure the safety of the transferred digital assets, blockchain gateway service providers (BGSP) must be trustworthy to clients who use the services. As a result, they must meet a high standard to ensure security and trust at different levels, ranging from business to networking, from hardware device to software protocol. In particular, the following basic prerequisites (but not limited to) must be met:

- o They must be a legal business entity registered with local authority. The registration should be certified in form of a verifiable digital certificate.
- o They must apply for an Autonomous System (AS) number [[RFC6996](#)] from ARIN, or other region networking authorities (such as RIPE NCC for Europe and APNIC for East and South Asia), dedicated to their gateway IP addresses, e.g., 888.10.10.10
- o The IP address should be bound to a meaningful domain name by registering in DNS [[RFC1034](#), [RFC1035](#)], e.g., G1.DLT1.com.
- o To be better discovered, a number of canonical names are registered in DNS as CNAME record as shown in Table 1.
- o In addition, BGSP(s) should also be issued with a license/certificate as authorized approval to provide blockchain gateway services from the corresponding blockchain foundation/authority, and register their services with well-known business directories and publish on the Internet.

Based on the above prerequisites, blockchain gateways can discover each other to establish trust step by step for digital asset transfer using either bottom-up or top-down approach.

G1.DLT1.com	A	888.10.10.10
DLT1	CNAME	G1.DLT1.com
G2.DLT2.com	A	999.10.10.10
DLT2	CNAME	G2.DLT1.com

Figure 1

5.2. DNS-based Gateway Discovery

This is a bottom-up approach to blockchain gateway discovery as shown in the Figure below.

(Figure TBD - DNS-based Gateway Discovery)

Figure 2

Client (Alice) wants to transfer a certain value of digital assets (v) from one blockchain (DLT1) to another client (Bob) on another blockchain (DLT2), which can be represented in ERC20 as follows:

```
transfer(Bob_PublicKey@DLT2, v)
```

The following MTA-Style protocol is specified for gateway networking device discovery:

- o Alice can send the transfer request to G1 directly if Alice trusts G1 and G1 is pre-configured in Alice wallet; Or Alice can discover G1 and establish trust with G1 by following the same protocol as described below.
- o As a result of receiving Alice's request, G1 lookup a gateway for DLT2 via DNS and DNS returns G2's IP address, e.g., 999.10.10.10
- o (Optional) G1 can verify the ownership of the received IP address with 3rd party service to ensure if G2 is trustworthy.
- o G1 sends a request for exchanging business certificate (BC) by embedding its business certificate in the request, which can be specified in the json format (see Figure).

- o If G1's certificate is valid, G2 will reply by sending its business certificate as specified (see Figure).
- o (Optional) G1 may request for verification of Bob's blockchain address (public key) and (optional) his living location (for tax purpose) with DLT2.

```
{
  "Request": {
    "CMD": "ExchangeBC",
    "Certificate": {
      . . .
    }
  }
}
```

Figure 3

```
{
  "Response": {
    "Certificate": {
      . . .
    }
  }
}
```

Figure 4

Up to this point, G1 and G2 establish trust at both business and network levels enough and ready to start the transfer digital asset (v) via the asset transfer protocol [[ODAP](#)].

[6.](#) Application Layer Gateway Discovery and Verification

Another approach that is commonly adopted by a community of service providers is for the community to share information regarding standardized service endpoints (e.g. REST APIs). There are multiple ways for a community of consortium of entries to share endpoints information, including a centralized signed-list or database, a replicated distributed database and more recently listing mechanisms based on blockchains (e.g. DIDs). In the following, the term business directory is used generically to represent the list. An example of this approach is the TRISA directory currently being developed for Travel Rule sharing [[TRISA](#)]. Depending on the

community of consortium, the information in the directory may be

publicly readable or it may be accessible only to members of the community.

Applying this approach to gateways, a business entities who participate in the directory must proactively register (publish) its gateways and the DLN for which each gateway speaks. The information must include minimally the following: (a) the gateway device identity, (b) one of more blockchains (DLNs) served by the gateway, (c) the identity of the business entity (e.g. asset service provider), (d) expiration of the information in the directory. This information must be source authentic (i.e. digitally signed) by entity registering it.

(Figure TBD - Application Layer Gateway Discovery and Verification)

Figure 5

Suppose that BGSP-1 and BGSP-2 provide blockchain gateway services for DLT1 and DLT2 with G1 and G2, respectively and both register with business directories and publish their services on the Internet. As a result, they should easily discover each other.

- o BGSP-1 finds BGSP-2 via one of global business directories (or even Google), or vice versa. Then, they negotiate each other with aim to establish a business collaboration via providing cross-chain asset transfer services between DLT1 and DLT2 offline. As a result of successful negotiation, BGSP-1 and BGSP-2 both signs a legal business contract for the collaboration, including agreements about (but not limited to) the network configuration, security setting, and transfer protocols to be used.
- o Up to the agreement signed, BGSP-1 and BGSP-2 can configure each network and gateway servers according to the agreed settings.

- o At runtime, when receiving a transfer request from a client (Alice), G1 can send a handshaking request to G2 directly for establishing secure channel for transferring digital asset (v) via the asset transfer protocol [[ODAP](#)].

[7.](#) Security Consideration

In addition to the basic security setting mentioned above, the following technologies can also be considered as either enhancement or alternatives of security settings:

HTTPS/TLS: Whenever using HTTP [[RFC2616](#)] for the protocol execution, HTTPS/TLS [[RFC2821](#)] must be enabled by default against eavesdropping attack.

DNSSEC: is a set of extensions to DNS that uses asymmetric cryptography to provide origin authentication and integrity checking for DNS data [[RFC 2535](#)]. DNSSEC ensures not just the origin of the DNS record, but also its integrity, which thus enhances the security and trust of the blockchain gateway queries if adopting DNSSEC.

Trusted hardware and attestations: Gateways may be implemented in computer systems possessing a secure processor (e.g. TPM)[ISO/IEC 11889] or secure enclave (e.g. SGX). For example, server machines can store security keys and conducts common security operations for hardware authentication and authorization. The use of device-unique public key pairs boiund to these types of trusted hardware, copled with their attestations capabilities, may significantly enhance the security and trust between the gateways to conduct blockchain asset transfer services collaboratively.

[8.](#) IANA Consideration

(TBD)

[9.](#) References

9.1. Normative References

- [FATF] FATF, "International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation – FATF Revision of Recommendation 15", October 2018, <<http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html>>.
- [ISO] ISO, "Blockchain and distributed ledger technologies- Vocabulary (ISO:22739:2020)", July 2020, <<https://www.iso.org>>.
- [NIST] Yaga, D., Mell, P., Roby, N., and K. Scarfone, "NIST Blockchain Technology Overview (NISTR-8202)", October 2018, <<https://doi.org/10.6028/NIST.IR.8202>>.

Chen & Hardjono Expires December 10, 2021 [Page 11]

Internet-Draft DLT Gateway Identification June 2021

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), DOI 10.17487/RFC2119, March 1997, <<https://www.rfc-editor.org/info/rfc2119>>.
- [RFC2234] Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", [RFC 2234](#), DOI 10.17487/RFC2234, November 1997, <<https://www.rfc-editor.org/info/rfc2234>>.
- [RFC7519] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Token (JWT)", [RFC 7519](#), DOI 10.17487/RFC7519, May 2015, <<https://www.rfc-editor.org/info/rfc7519>>.

9.2. Informative References

- [ARCH] Hardjono, T., Hargreaves, M., and N. Smith, "An Interoperability Architecture for Blockchain Gateways. [draft-hardjono-blockchain-interop-arch-02](#)", April 2021, <<https://datatracker.ietf.org/doc/draft-hardjono-blockchain-interop-arch/>>.
- [BCH21] Belchior, R., Correia, M., and T. Hardjono, "DLT Gateway Crash Recovery Mechanism, IETF, [draft-belchior-gateway-recovery-01](#).", March 2021, <<https://datatracker.ietf.org/doc/draft-belchior-gateway-recovery-01>>.

[recovery/](#)>.

- [ODAP] Hargreaves, M. and T. Hardjono, "Open Digital Asset Protocol, IETF, [draft-hargreaves-odap-01](#).", November 2020, <<https://datatracker.ietf.org/doc/draft-hargreaves-odap/>>.
- [RFC5939] Andreasen, F., "Session Description Protocol (SDP) Capability Negotiation", [RFC 5939](#), DOI 10.17487/RFC5939, September 2010, <<https://www.rfc-editor.org/info/rfc5939>>.
- [TRISA] TRISA, "Travel Rule Information Sharing Architecture for Virtual Asset Service Providers", August 2020, <<https://trisa.io/trisa-whitepaper/>>.

Authors' Addresses

Shiping Chen
Data61

Email: shipping.chen@data61.csiro.au

Chen & Hardjono	Expires December 10, 2021	[Page 12]
-----------------	---------------------------	-----------

Internet-Draft	DLT Gateway Identification	June 2021
----------------	----------------------------	-----------

Thomas Hardjono
MIT

Email: hardjono@mit.edu

