

Internet Engineering Task Force  
Internet-Draft  
Intended status: Informational  
Expires: 23 January 2026

W. Zhang  
Enterprise Ethereum Alliance  
T. Hardjono  
MIT  
22 July 2025

SATP Network Identification  
draft-zhang-satp-network-identification-01

## Abstract

There is currently a lack of a standard network identification or numbering for digital asset networks. This deficiency makes it difficult for the transfer of digital assets from one network to another, due among others, to the possibility in the collision in the numbering of the remote networks. This document proposes a globally unique 32-byte identifier for each asset network based on some unique inherent characteristics of each network.

## 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 23 January 2026.

## Copyright Notice

Copyright (c) 2025 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 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 Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

## Table of Contents

1. Introduction . . . . .	2
2. General Identification Requirements . . . . .	3
3. Identifier Specification . . . . .	3
3.1. Hash of genesis block (16 bytes) . . . . .	3
3.2. Custom subnetwork number (4 bytes) . . . . .	3
3.3. Subnetwork Type (2 bytes) . . . . .	4
3.4. Network Owner Identifier (2 bytes) . . . . .	4
3.5. Reserved (7 bytes) . . . . .	4
3.6. Checksum (1 bytes) . . . . .	4
4. Security Considerations . . . . .	4
5. References . . . . .	5
5.1. Normative References . . . . .	5
5.2. Informative References . . . . .	6
Authors' Addresses . . . . .	6

## 1. Introduction

In order to begin addressing the lack of a standard for network identification (numbering) for digital asset networks (e.g. based on shared ledgers), the current document proposes a 32-byte identifier scheme that permits each network to be uniquely identified at the network level, while at the same permitting each network to assign its own numbering to interior sub-networks (e.g. multiple shared ledgers within a network). This approach is based on the scheme proposed in [EIP3220].

A standard identifier scheme for asset networks is important for the interoperability among these networks, as it prevents misidentification of networks and provides a means for nodes and gateways in the network to assert (to external entities) which network or ledger they represent.

Additionally, a standard identifier scheme is crucial for the IETF secure asset transfer protocol (SATP), where gateways seeking to transfer digital assets from one network to another must be able to uniquely identify the origin network and destination network [SATP-ARCH].

## 2. General Identification Requirements

An asset network identification should satisfy the following general requirements:

- \* It should provide unique identification of each asset network in a way that facilitates cross-network transfers in the digital asset ecosystem.
- \* It should semantically carry some minimal information that supports the discovery of asset networks.
- \* When possible, it should semantically permit the network owner to subset (sub-net) the identifier string to indicate sub-networks (ledgers) within the asset network.
- \* It should permit the differentiation between an original (parent) network from a forked (child) network.

## 3. Identifier Specification

The following provides the specification for the 32-bytes for the network identification, including the field length and description or purpose of each field.

### 3.1. Hash of genesis block (16 bytes)

Within a network utilizing a shared ledger, this is the cryptographic hash of the genesis block of the ledger.

In the case of a network forked into two networks, the official network should still keep its original hash. The forked network should take the hash of the block immediately prior to the fork.

The 16 bytes is the 16 least significant bytes, assuming network byte order.

In other specifications [EIP3220] this is also called the Truncated Genesis Block Hash.

### 3.2. Custom subnetwork number (4 bytes)

This is the subnetwork identification number that can be used internally within a network or the legacy network number when signing transactions intended for the ledger in that subnetwork. The number can be used to identify subnetworks or be compatible with legacy network identifications.

For networks that do not support this feature, this value must be set zero.

In other specifications [EIP3220] this is also called the Native ChainID.

### 3.3. Subnetwork Type (2 bytes)

This is the portion that identifies the subnetwork within a network, if any exists.

Reserve is 0x00 as an undefined.

In other specifications [EIP3220] this is also called the Chain Type.

Examples: The value 0x01 is Ethereum mainnet. The value 0x1[0-A] is Ethereum testnet. The value 0x2[0-A] is Ethereum a private development network.

### 3.4. Network Owner Identifier (2 bytes)

This portion is optionally used by an owner of an original network in the case of forks of that network into separate independent networks.

For networks that do not support the notion of an owner, this value is set to zero.

In other specifications [EIP3220] this is also called the Governance Identifier.

### 3.5. Reserved (7 bytes)

Reserved for future use. Use 000000 for now.

### 3.6. Checksum (1 bytes)

Used to verify the integrity of the identifier. The value is calculated as the truncated SHA256 message digest of the rest of the identifier, using the least significant byte, assuming network byte order.

## 4. Security Considerations

Today there is no mechanism for network owners to register (or obtain) a unique network identifier for their networks. This raises the dilemma that two networks may choose the same identifiers, leading to collisions in the case of cross-network (cross-jurisdiction) asset transfers:

- \* Preventing identifier collision: With the use of the current proposed network identification scheme, the utilization of the hash of the genesis block of each network (ledger) provides a higher assurance that the chances for collisions in numbering will be low.
- \* Detecting replay attacks: The use of a standardized asset network identifier reduces the potential for replay attacks a network internally (locally) by virtue of the inclusion of the interior subnetwork number (ChainID) portion in the signed transaction.

In the case of gateways in SATP, the network identifier could be included in the digital certificate (e.g. X.509 certificate) that identifies the gateway device and gateway owner, signifying that the gateway serves the given network.

When two gateways G1 and G2 are participating in a cross-network asset transfer (SATP-core) each gateway can include their corresponding network identifier in the pre-transfer preparation stage (Stage-0).

## 5. References

### 5.1. Normative References

- [EIP3220] Zhang, W. and P. Robinson, "EIP-3220: Crosschain Identifier Specification", 21 October 2020, <<https://eips.ethereum.org/EIPS/eip-3220>>.
- [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>>.
- [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>>.
- [SATParch] Hardjono, T., Hargreaves, M., Smith, N., and V. Ramakrishna, "Secure Asset Transfer Protocol Architecture", 24 July 2023, <<https://datatracker.ietf.org/doc/draft-ietf-satp-architecture/>>.
- [SATPcore] Hargreaves, M., Hardjono, T., and R. Belchior, "IETF Secure Asset Transfer Protocol (SATP)", 9 July 2023, <<https://datatracker.ietf.org/doc/draft-ietf-satp-core/>>.>.

## 5.2. Informative References

[Chainlist]

Chainlist, "Chainlist  
(<https://github.com/dbarobin/networklist-org>)", 2020,  
<<https://chainlist.network>>.

[ISO20022] ISO, "Universal Financial Industry Message Scheme (ISO  
20022).", July 2023, <<https://www.iso20022.org>>.

## Authors' Addresses

Weijia Zhang  
Enterprise Ethereum Alliance  
Email: [weijiazhang@utexas.edu](mailto:weijiazhang@utexas.edu)

Thomas Hardjono  
MIT  
Email: [hardjono@mit.edu](mailto:hardjono@mit.edu)