Secure Asset Transfer Protocol
Internet-Draft
Intended status: Informational
Expires: 6 May 2026

T. Hardjono
MIT
D. Avrillionis
Compellio Inc.

2 November 2025

Secure Asset Transfer Protocol (SATP) Terminology
draft-hardjono-satp-terminology-00

Abstract

This memo collates existing terminology related to digital assets, asset networks and distributed ledger technology (DLT) that are relevant to the secure asset transfer protocol (SATP) and the IETF more broadly. Existing terms are borrowed as much as possible, and new terms are introduced only when necessary and with emphasis on technology neutrality.

About This Document

This note is to be removed before publishing as an RFC.

The latest revision of this draft can be found at https://ietf-satp.github.io/draft-hardjono-satp-terminology/draft-hardjono-satp-terminology.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-hardjono-satp-terminology/.

Discussion of this document takes place on the Secure Asset Transfer Protocol Working Group mailing list (mailto:sat@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/sat/. Subscribe at https://www.ietf.org/mailman/listinfo/sat/.

Source for this draft and an issue tracker can be found at https://github.com/ietf-satp/draft-hardjono-satp-terminology.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction 2
2. Asset Networks Related Terminology 3
3. Gateway Related Terminology 5
4. Digitized Assets and Registries Terminology 5
5. References 6
5.1. Normative References 6
5.2. Informative References 7
Authors' Addresses 7

1. Introduction

The SAT protocol for interoperability utilizes peered gateways to perform a unidirectional transfer of a digital assets, from an origin asset network to a destination asset network [ARCH]. As stated in [CORE] the SAT protocol is agnostic to the type of network or system behind the gateways, and the protocol focuses on the interactions between the two gateways.

While the SAT protocol defines the interaction between two gateways such that certain properties of the transfer is achieved (atomicity, consistency, isolation, durability), the protocol specification does not define how each gateway interfaces and interacts with their respective asset network. Furthermore, the SAT protocol employs an abstraction of the functions present in these asset network. Examples of such abstraction include the functions of locking (disabling) the asset on a network, burning (destroying) an asset, minting (creating) and so on. However, in order to achieve a higher degree of precision in describing the utilization of the SAT protocol and its impact on asset networks, a definition of these terms is required.

The goal of this document is to provide a terminology definition of the entities, constructs and on-chain functions that are relevant within the context of a SAT protocol deployment with gateways. A layered approach is adopted to describe these constructs and on-chain functions, in order to minimize confusion with regards to which entities are utilizing these.

As far as possible, this document will borrow existing terminology from other published standards. The sources of this existing terminology will be cited. When needed, the document will be verbose in providing definitions in order to remove any ambiguity in the use of the constructs (e.g. smart contract invoked by a gateway, versus that invoked by a client).

2. Asset Networks Related Terminology

* Address: A short, alphanumeric string derived from a user’s public key using a hash function, with additional data to detect errors. Addresses are used to send and receive digital assets. [NISTIR8202] Account: An entity in a blockchain that is identified with an address and can send transactions to the blockchain. [NISTIR8301] Atomic swap: An exchange of tokens that does not involve the intervention of any trusted intermediary and automatically reverts if all of the provisions are not met. [NISTIR8301]

* Blockchain: Blockchains are distributed digital ledgers of cryptographically signed transactions that are grouped into blocks. Each block is cryptographically linked to the previous one (making it tamper evident) after validation and undergoing a consensus decision. As new blocks are added, older blocks become more difficult to modify (creating tamper resistance). New blocks are replicated across copies of the ledger within the network, and any conflicts are resolved automatically using established rules. [NISTIR8202]

* Custodian: A third-party entity that holds and safeguards a user’s private keys or digital assets on their behalf. Depending on the system, a custodian may act as an exchange and provide additional services, such as staking, lending, account recovery, or security features. [NISTIR8301]

* Consensus: A process to achieve agreement within a distributed system on the valid Cryptocurrency state. Also known as a consensus algorithm, consensus mechanism, consensus method. [NISTIR8202]

* Double Spend: Transacting with the same set of digital assets more than once. [NISTIR8202]

* Off-chain: Refers to data that is stored or a process that is implemented and executed outside of any blockchain system. [NISTIR8301]

* Oracle: A source of data from outside a blockchain that serves as input for a smart contract. [NISTIR8301]

* Permissioned blockchain: A system where every node, and every user must be granted permissions to utilize the system (generally assigned by an administrator or consortium). [NISTIR8202]

* Permissionless blockchain: A system where all users’ permissions are equal and not set by any administrator or consortium. [NISTIR8202]

* Smart contract: A collection of code and data (sometimes referred to as functions and state) that is deployed using cryptographically signed transactions on the blockchain network. The smart contract is executed by nodes within the blockchain network; all nodes must derive the same results for the execution, and the results of execution are recorded on the blockchain. [NISTIR8202]

* Wallet: Software used to store and manage asymmetric-keys and addresses used for transactions. [NISTIR8202]

* Wallets, Custodial: Account custody -- and the custody of the associated tokens-- which is delegated to institutional third-party custodians who hold and safeguard private keys on behalf of users. They provide different degrees of custody services and risk management. Custodial wallets are also known as externally hosted wallets or managed wallets. [NISTIR8301]

3. Gateway Related Terminology

* Gateway smart contracts: The smart contracts invoked by SATP Gateways in course of completing an asset transfer from an origin asset network to a destination asset network. Some of the smart contracts invoked by a gateway may be generic to any type of asset (or asset class) on the asset networks, while other smart contracts may be designed specifically for gateways.

* Views: A projection of the state of an asset on a blockchain or asset network intended for an audience external to the network. This state information may pertain to a single element, a subset of the state, or a function over a subset. For private (permissioned) asset networks, a gateway may provide an interface to access the view from the internal private ledger, and to return the relevant cryptographic proof regarding the truthfulness of the claim regarding then reported state of the asset. [SATP-VIEWS]

* View Address: A unique identifier or locator for a view into the state of an asset on a blockchain or asset network. [SATP-VIEWS]

4. Digitized Assets and Registries Terminology

* Artifacts: The set of metadata information that supports the verification of a tokenized asset recorded on an asset network or specific blockchain. The artifact information may be recorded within the body of a value-bearing token, or it may be recorded in a separate utility token (bearing no value) that is referenced by the value-bearing token. Other The artifact information may be recorded off-chain in artifacts registries and other proprietary databases (e.g. in Central Securities Depositories (CSD)).

* Central Securities Depositories: A central securities depository (CSD) is a specialized financial market infrastructure (FMI) organization holding securities such as shares or bonds, either in certificated or uncertificated (dematerialized) form, allowing ownership to be easily transferred through a book entry rather than by a transfer of physical certificates. This allows brokers and financial companies to hold their securities at one location where they can be available for clearing and settlement. [Wikipedia]

* Asset Schema (Asset Definition Schema): The semantic definition of the tokenizable real-world assets in a computer-readable format (e.g. expressed in JSON-LD syntax, Common Domain Model (CDM) syntax, and others). Certain industry verticals or asset-specific trading communities (e.g. Bonds) may define a subset of a larger asset definition schema. These derived schemas are called schema-profiles (or simply "profile").

* Digital Asset Record (DAR): The set of artifact information and attributes of a real-world asset (RWA) that have been digitized into a standard format. The DAR is a standalone digital record that either carries the artifact information itself or carries links/pointers (URLs) to, or hash-values of other artifacts information located elsewhere on the internet. The DAR is expressed in a machine-readable format (e.g. JSON-LD) and is therefore blockchain-independent.

* Tokenized Asset Record (TAR): The on-chain representation of a Digital Asset Record (DAR) that is formatted according to the specific record/block structure of the ledger of the blockchain. The TAR must carry a cryptographic hash of the DAR from which it was derived.

* Decentralized Registry: The decentralized and persistent storage of the artifacts, schemas and DARs pertaining to a tokenized real-world asset (RWA) that enables the legal status of the token to be verified.

5. References

5.1. Normative References

[BASE64] Josefsson, S., "The Base16, Base32, and Base64 Data Encodings", RFC 4648, DOI 10.17487/RFC4648, October 2006, <https://www.rfc-editor.org/rfc/rfc4648>.

[DATETIME] Klyne, G. and C. Newman, "Date and Time on the Internet: Timestamps", RFC 3339, DOI 10.17487/RFC3339, July 2002, <https://www.rfc-editor.org/rfc/rfc3339>.

[JSON] Bray, T., Ed., "The JavaScript Object Notation (JSON) Data Interchange Format", STD 90, RFC 8259, DOI 10.17487/RFC8259, December 2017, <https://www.rfc-editor.org/rfc/rfc8259>.

[JWA] Jones, M., "JSON Web Algorithms (JWA)", RFC 7518, DOI 10.17487/RFC7518, May 2015, <https://www.rfc-editor.org/rfc/rfc7518>.

[JWS] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Signature (JWS)", RFC 7515, DOI 10.17487/RFC7515, May 2015, <https://www.rfc-editor.org/rfc/rfc7515>.

[JWT] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Token (JWT)", RFC 7519, DOI 10.17487/RFC7519, May 2015, <https://www.rfc-editor.org/rfc/rfc7519>.

[REQ-LEVEL] 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/rfc/rfc2119>.

[RFC2616] Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., and T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1", RFC 2616, DOI 10.17487/RFC2616, June 1999, <https://www.rfc-editor.org/rfc/rfc2616>.

5.2. Informative References

[NISTCSWP] "NIST A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems", January 2020, <https://doi.org/10.6028/NIST.CSWP.9>.

[NISTIR8202] 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>.

[NISTIR8301] "NIST Blockchain Networks Token Design and Management Overview (NISTR-8301)", February 2021, <https://doi.org/10.6028/NIST.IR.8301>.

Authors’ Addresses

Thomas Hardjono
MIT
Email: hardjono@mit.edu

Denis Avrillionis
Compellio Inc.
Email: denis@compellio.com