Blockchain Interoperability Specification

Version 0.5 rev 0.1

ABSTRACT: Blockchain Data & Storage Network Interoperability specification

Publication of this Working Draft for review and comment has been approved by the Blockchain Storage TWG. This draft represents a “best effort” attempt by the Blockchain Storage TWG to reach preliminary consensus, and it may be updated, replaced, or made obsolete at any time. This document should not be used as reference material or cited as other than a “work in progress.” Suggestions for revisions should be directed to http://www.snia.org/feedback/.

Working Draft

July 26, 2021

USAGE

DISCLAIMER

The information contained in this publication is subject to change without notice. The SNIA makes no warranty of any kind with regard to this specification, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The SNIA shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this specification.

Revision History

Revision	Date	Sections	Originator:	Comments
0.1	04/28/2021		Parmeshwr Prasad Olga Buchonina Andrey Verbitsky Ke Du Rafal Szczesniak	First draft of the interoperability specification
0.2	05/12/2021		Olga	Block Diagrams, notes
0.3	06/16/2021		Olga	Proposed Registers
0.4	07/19/2021	`	Olga	Additional Registers, Definitions, Diagrams
0.5	07/23/2021		Parmeshwr Prasad	review and added NVDIMM Spec

1. Objective of the Specification

This specification describes the Data Storage Centric Blockchain Interoperability architecture, interconnect attributes, blockchain management, and the programming interface required to design and build systems and peripherals that are compliant with the SNIA Blockchain Interoperability Specification

The goal is to enable such devices from different vendors to inter-operate in an open architecture. The specification allows Blockchain enabled systems and protocols to develop products and solutions which uninterruptible and secure data exchange as well creating market differentiation without the burden of carrying obsolete interfaces or losing compatibility.

Why Blockchain Interoperability?

Blockchain ecosystem is a heterogeneous landscape, consisting of different types of blockchain infrastructures. Blockchain interoperability is the ability to transfer data or assets and to execute smart contracts between two or more heterogeneous blockchains.

The interoperability breaks information silos, creates synergies, and allows new blockchain applications.

2. Introduction

2.1. Overview

2.1.1.

2.1.2. *What is the Difference Between a Blockchain and a Database?*

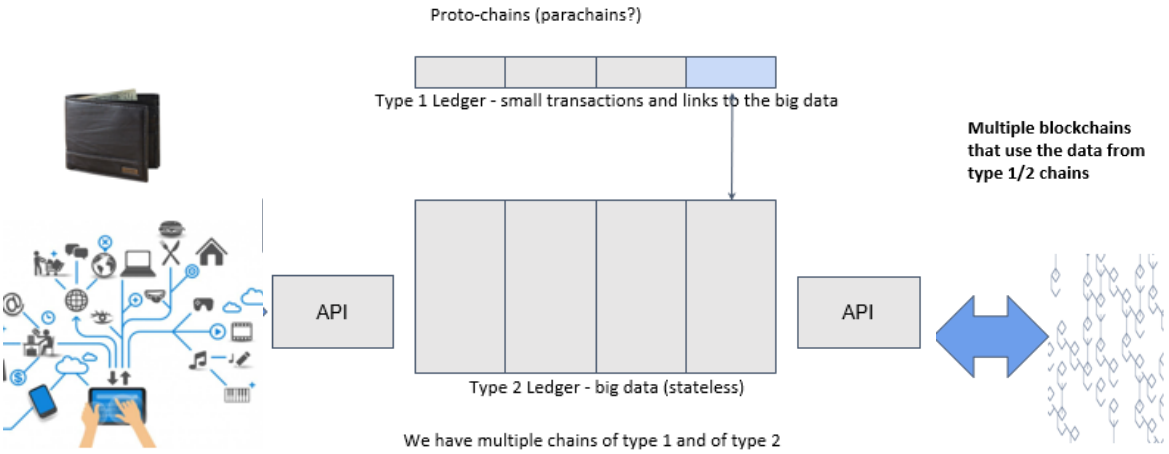
There is one significant difference between database and blockchain, i.e., decentralization. The blockchain is also a type of database, but it offers decentralization. The traditional database also helps to store and retrieve data but is centralized in nature. Blockchain also provides integrity of data which means that data once written cannot be modified or altered by anyone. This implies blockchain doesn't offer the data manipulations option. Validations are also more accurate on blockchain compared to the database due to data integrity.

2.2. Scope

2.3. Outside of Scope

2.4. Theory of Operation

The idea is to create and enable ability for interactions between two or more chains for asset/block of data transfers



The interoperability can be done by connecting one or more external Cryptographic applications via API interface to SNIA proto-chain which is nothing more but a lookup table (ledger) keeping the track of transactions via headers or Hash functions. This is done via transferring snapshots of data at fixed periods of time.

2.5. Conventions

2.6. Definitions/Glossary

Asset

anything that has value to a stakeholder [ISO 22739 22739:2020(E)]

Block

structured data comprising **block data** and a **block header** [ISO 22739 22739:2020(E)]

Block data

structured data comprising zero or more **transaction records** or references to **transaction records** [ISO 22739 22739:2020(E)].

Block header

structured data that includes a **cryptographic link** to the previous block unless there is no previous block [ISO 22739 22739:2020(E)].

Note 1 to entry: A **block header** can also contain a **timestamp**, a **nonce**, and other **DLT platform** specific data, including a **hash value** of corresponding **transaction records.** [ISO 22739 22739:2020(E)].

Block reward

reward given to **miners** or **validators** after a **block** is **confirmed** in a **blockchain system**
Note 1 to entry: A reward can be in the form of a **token** or **cryptocurrency**. [ISO 22739 22739:2020(E)].

Blockchain
distributed ledger with **confirmed blocks** organized in an append-only, sequential chain using **cryptographic links** [ISO 22739 22739:2020(E)].

Note 1 to entry: Blockchains are designed to be tamper resistant and to create final, definitive and **immutable** **ledger records** . [ISO 22739 22739:2020(E)].

Blockchain system
system that implements a **blockchain**
Note 1 to entry: A blockchain system is a type of **DLT system**. [ISO 22739 22739:2020(E)].

Confirmed
accepted by **consensus** for inclusion in a **distributed ledger** [ISO 22739 22739:2020(E)].

Confirmed block
block that has been **confirmed** [ISO 22739 22739:2020(E)].

Confirmed transaction
transaction that has been **confirmed** [ISO 22739 22739:2020(E)].

Consensus
An agreement among **DLT nodes** that a **transaction** is **validated** and that the **distributed ledger** contains a consistent set and ordering of **validated transactions**
Note 1 to entry: Consensus does not necessarily mean that all **DLT nodes** agree. [ISO 22739 22739:2020(E)].
Note 2 to entry: The details regarding consensus differ among **DLT** designs and this is a distinguishing characteristic between one design and another.

Consensus mechanism
rules and procedures by which **consensus** is reached [ISO 22739 22739:2020(E)].

Crypto-asset
digital asset implemented using cryptographic techniques [ISO 22739 22739:2020(E)].

Cryptocurrency
crypto-asset designed to work as a medium of value exchange
Note 1 to entry: Cryptocurrency involves the use of decentralized control and **cryptography** to secure **transactions** , control the creation of additional **assets**, and verify the transfer of **assets**. [ISO 22739 22739:2020(E)].

Cryptographic hash function
function mapping binary strings of arbitrary length to binary strings of fixed length, such that it is computationally costly to find for a given output an input that maps to the output, it is computationally

infeasible to find for a given input a second input that maps to the same output, and it is computationally infeasible to find any two distinct inputs that map to the same output
Note 1 to entry: Computational feasibility depends on the specific security requirements and environment. [ISO 22739 22739:2020(E)].

Cryptographic link
reference, constructed using a **cryptographic hash function** technique, that points to data
Note 1 to entry: A cryptographic link is used in the **block header** to reference the previous **block** in order to create the append-only, sequential chain that forms a **blockchain** . [ISO 22739 22739:2020(E)].

Cryptography
discipline that embodies the principles, means, and methods for the transformation of data in order to hide their semantic content, prevent their unauthorized use, or prevent their undetected modification [ISO 22739 22739:2020(E)].

Decentralized application
DApp
application that runs on a **decentralized system** [ISO 22739 22739:2020(E)].

Decentralized system
distributed system wherein control is distributed among the persons or organizations participating in the operation of the system
Note 1 to entry: In a decentralized system, the distribution of control among persons or organizations participating in the system is determined by the system's design. [ISO 22739 22739:2020(E)].

Digital asset
asset that exists only in digital form or which is the digital representation of another **asset**. [ISO 22739 22739:2020(E)].

Digital signature
data which, when appended to a digital object, enable the user of the digital object to authenticate its origin and integrity [ISO 22739 22739:2020(E)].

Distributed ledger
ledger that is shared across a set of **DLT nodes** and synchronized between the DLT nodes using a **consensus mechanism**
Note 1 to entry: A distributed ledger is designed to be tamper resistant, append-only and **immutable** containing **confirmed** and **validated** **transactions** . [ISO 22739 22739:2020(E)].

DLT
distributed ledger technology
technology that enables the operation and use of **distributed ledgers** [ISO 22739 22739:2020(E)].

DLT account
distributed ledger technology account
representation of an **entity** participating in a **transaction**

Note 1 to entry: A **smart contract** , **digital asset** , or one or more **private keys** , for example, can be associated with a DLT account. [ISO 22739 22739:2020(E)].

DLT address
distributed ledger technology address
value that identifies a **DLT account** participating in a **transaction** [ISO 22739 22739:2020(E)].

DLT network
distributed ledger technology network
network of **DLT nodes** which make up a **DLT system** [ISO 22739 22739:2020(E)].

DLT node
distributed ledger technology node
node
<distributed ledger technology> device or process that participates in a network and stores a complete or partial replica of the *ledger* **records** [ISO 22739 22739:2020(E)].

DLT oracle
distributed ledger technology oracle
oracle
service that updates a **distributed ledger** using data from outside of a **DLT system**
Note 1 to entry: DLT oracles are useful for **smart contracts** that cannot access sources of data external to the **DLT system** . [ISO 22739 22739:2020(E)].

DLT platform
distributed ledger technology platform
set of processing, storage and communication **entities** which together provide the capabilities of the **DLT system** on each **DLT node** [ISO 22739 22739:2020(E)].

DLT system
distributed ledger system
distributed ledger technology system
system that implements a **distributed ledger** [ISO 22739 22739:2020(E)].

DLT user
distributed ledger technology user
entity that uses services provided by a **DLT system** [ISO 22739 22739:2020(E)].

distributed system
system in which components located on networked computers communicate and coordinate their actions by interacting with each other [ISO 22739 22739:2020(E)].

double spending
failure of a **DLT platform** where the control of a **token** or **crypto-asset** is incorrectly transferred more than once

Note 1 to entry: Double-spending is most often associated with **cryptocurrency** . [ISO 22739 22739:2020(E)].

entity
item inside or outside an information and communication technology system, such as a person, an organization, a device, a subsystem, or a group of such items that has recognizably distinct existence [ISO 22739 22739:2020(E)].

failure
loss of ability to perform as required [ISO 22739 22739:2020(E)].

fault tolerance
ability of a functional unit to continue to perform a required function in the presence of faults or errors [ISO 22739 22739:2020(E)].

genesis block
first **block** in a **blockchain**
Note 1 to entry: A genesis block has no previous **block** and serves to initialize the **blockchain** . [ISO 22739 22739:2020(E)].

hard fork
change to a **DLT platform** in which new **ledger records** or **blocks** created by the **DLT nodes** using the new version of the **DLT platform** are not accepted as valid by **DLT nodes** using old versions of the **DLT platform**
Note 1 to entry: If not adopted by all **DLT nodes** , a hard fork can result in a **ledger split** .
Note 2 to entry: In some contexts, the terms "hard fork" and **"fork"** are sometimes used for a **ledger split** that results from a hard fork of a **DLT platform** . [ISO 22739 22739:2020(E)].

hash value
string of bits which is the output of **a cryptographic hash function** [ISO 22739 22739:2020(E)].

immutability
property wherein **ledger records** cannot be modified or removed once added to a **distributed ledger**
Note 1 to entry: Where appropriate, immutability also presumes keeping intact the order of **ledger records** and the links between the **ledger records** [ISO 22739 22739:2020(E)].

interoperability
ability of two or more systems or applications to exchange information and to mutually use the information that has been exchanged [ISO 22739 22739:2020(E)].

leaf node
node that has no child **nodes** [ISO 22739 22739:2020(E)].

ledger
information store that keeps **records** of **transactions** that are intended to be final, definitive and **immutable** [ISO 22739 22739:2020(E)].

ledger record
record containing **transaction records**, **hash values** of **transaction records**, or references to **transaction records** recorded on a **distributed ledger**
Note 1 to entry: A reference can be implemented as a **cryptographic link**. [ISO 22739 22739:2020(E)].

ledger split
fork
creation of two or more different versions of a **distributed ledger** originating from a common starting point with a single history [ISO 22739 22739:2020(E)].

Merkle root
root node of a **Merkle tree** [ISO 22739 22739:2020(E)].

Merkle tree
tree data structure in which every **leaf node** is labelled with the **hash value** of a data element and every non-leaf node is labelled with the **hash value** of the labels of its child **nodes** [ISO 22739 22739:2020(E)].

miner
DLT node which engages in **mining** [ISO 22739 22739:2020(E)].

mining
activity, in some **consensus mechanisms**, that creates and **validates** **blocks** or **validates** **ledger records**
Note 1 to entry: Participation in mining is often incentivized by **block rewards** and **transaction fees**. [ISO 22739 22739:2020(E)].

node
<organization of data> elementary component from which a data structure is built

nonce
number or bit string used once in a set of cryptographic operations
Note 1 to entry: A nonce is often random or pseudo-random. It is commonly used to guard against replay attacks, where a message is captured and re-sent by a malicious actor. In some **blockchain systems** it is used to modulate **mining** during the generation of a new **block** and is stored in the **block header** [ISO 22739 22739:2020(E)].

off-chain
related to a **blockchain system**, but located, performed, or run outside that **blockchain system** [ISO 22739 22739:2020(E)].

off-ledger
related to a **DLT system**, but located, performed, or run outside that **DLT system** [ISO 22739 22739:2020(E)].

on-chain
located, performed, or run inside a **blockchain system** [ISO 22739 22739:2020(E)].

on-ledger
located, performed, or run inside a **DLT system** [ISO 22739 22739:2020(E)].

peer-to-peer
relating to, using, or being a network of equal peers that share information and resources with each other directly without relying on a central **entity** [ISO 22739 22739:2020(E)].

permissioned
requiring authorization to perform a particular activity or activities [ISO 22739 22739:2020(E)].

permissioned DLT system
permissioned distributed ledger system
permissioned distributed ledger technology system
DLT system in which permissions are required [ISO 22739 22739:2020(E)].

permissionless
not requiring authorization to perform any particular activity [ISO 22739 22739:2020(E)].

permissionless DLT system
permissionless distributed ledger system
permissionless distributed ledger technology system
DLT system that is **permissionless** [ISO 22739 22739:2020(E)].

private DLT system
private distributed ledger system
private distributed ledger technology system
DLT system that is accessible for use only to a limited group of **DLT users**
Note 1 to entry: Public and private categories apply to **DLT users**,
and **permissioned** and **permissionless** categories apply to **DLT users** and those **entities** that administer or operate the **DLT system**. [ISO 22739 22739:2020(E)].

private key
key of an **entity's** asymmetric key pair that is kept secret and which should only be used by that **entity** [ISO 22739 22739:2020(E)].

prune
produce a smaller replica of a **distributed ledger** by removing all **transaction records** meeting specified criteria while ensuring that those **transactions** can be restored with integrity if needed [ISO 22739 22739:2020(E)].

public DLT system
public distributed ledger system
public distributed ledger technology system
DLT system which is accessible to the public for use [ISO 22739 22739:2020(E)].

public key
key of an **entity's** asymmetric key pair which can be made public [ISO 22739 22739:2020(E)].

public-key cryptography
cryptography in which a **public key** and a corresponding **private key** are used for encryption and decryption, or are used for verifying digital signatures and digitally signing, respectively [ISO 22739 22739:2020(E)].

record
information created, received and maintained as evidence and as an **asset** by an organization or person, in pursuit of legal obligations or in the **transaction** of business
Note 1 to entry: This term applies to information in any medium, form or format. [ISO 22739 22739:2020(E)].

reward system
incentive mechanism
method of offering reward for some activities concerned with the operation of a **DLT system**
Note 1 to entry: An example of a reward is a **block reward**. [ISO 22739 22739:2020(E)].

root node
node that has no parent **node** [ISO 22739 22739:2020(E)].

Shared ledger
distributed ledger in which the content of **ledger records** is accessible by multiple **entities** [ISO 22739 22739:2020(E)].

Sidechain
blockchain system that **interoperates** with a separate associated **blockchain system** to perform a specific function in relation to the associated **blockchain system**
Note 1 to entry: By convention the original chain is normally referred to as the "main chain", while any additional **blockchains** which allow **DLT users** to transact on the main chain are referred to as "sidechains". [ISO 22739 22739:2020(E)].

Smart contract
computer program stored in a **DLT system** **wherein** the outcome of any execution of the program is recorded on the **distributed ledger**
Note 1 to entry: A smart contract can represent terms in a contract in law and create a legally enforceable obligation under the legislation of an applicable jurisdiction. [ISO 22739 22739:2020(E)].

soft fork
change to a **DLT platform** that is not a **hard fork** and in which some **records** or **blocks** created by the **DLT nodes** using the old version of the **DLT platform** are not accepted as **valid** by **DLT nodes** using new versions of the **DLT platform** [ISO 22739 22739:2020(E)].

subchain
logically separate chain that can form part of a **blockchain system**
Note 1 to entry: A subchain allows for data isolation and confidentiality. [ISO 22739 22739:2020(E)].

timestamp
time variant parameter which denotes a point in time with respect to a common time reference [ISO 22739 22739:2020(E)].

token
digital asset that represents a collection of entitlements [ISO 22739 22739:2020(E)].

transaction
smallest unit of a work process, which is one or more sequences of actions required to produce an outcome that complies with governing rules
Note 1 to entry: Where appropriate, transaction is understood more narrowly, as the smallest unit of a work process related to interactions with **blockchains** or **distributed ledgers** . [ISO 22739 22739:2020(E)].

transaction fee
fee paid to **miners** or **validators** for inclusion of a **transaction** in a **distributed ledger** [ISO 22739 22739:2020(E)].

transaction record
record documenting a **transaction** of any type
Note 1 to entry: Transaction records can be included in, or referred to, in a **ledger record** . [ISO 22739 22739:2020(E)].
Note 2 to entry: Transaction records can include the result of a **transaction** .

trust
degree to which a user or other stakeholder has confidence that a product or system will behave as expected by that user or other stakeholder [ISO 22739 22739:2020(E)].

validated
status of an **entity** when its required integrity conditions have been checked
Note 1 to entry: For example, in a **DLT system** , a **transaction** , **ledger record** , or **block** can be validated. [ISO 22739 22739:2020(E)].

validation
function by which a **transaction** , **ledger record** , or **block** is **validated** [ISO 22739 22739:2020(E)].

validator
entity in a **DLT system** that participates in **validation**
Note 1 to entry: In some **DLT systems** the **DLT node** that has the role of validator can digitally sign a **ledger record** or **block** . [ISO 22739 22739:2020(E)].

wallet
application used to generate, manage, store or use **private** and **public keys**
Note 1 to entry: A wallet can be implemented as a software or hardware module. [ISO 22739 22739:2020(E)].

2.7. External References

2.7.1. SPDM Spec
https://www.dmtf.org/sites/default/files/standards/documents/DSP0274_0.99a.pdf

2.7.2. TCG Spec
https://trustedcomputinggroup.org/wp-content/uploads/TCG_Storage-Opal_SSC_v2.01_rev1.00.pdf

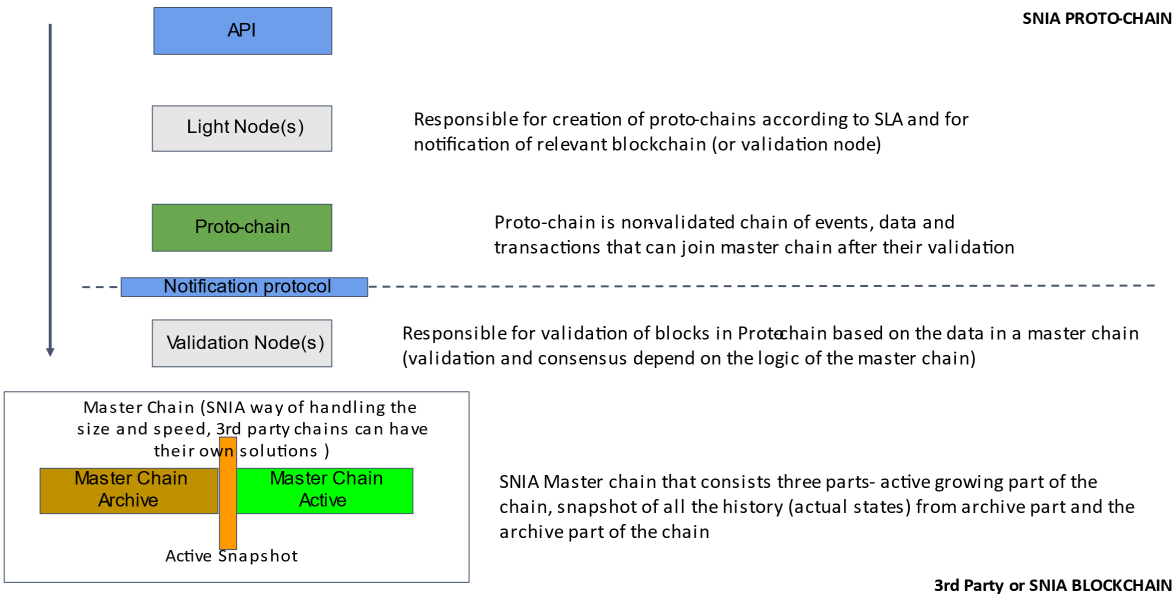
2.7.3. NVME Spec
https://nvmexpress.org/wp-content/uploads/NVM-Express-1_4a-2020.03.09-Ratified.pdf

2.7.4. NIST
https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf

2.7.5. ISO TC307, SC-7 Committee
https://www.iso.org/committee/6266604.html

1.7.6 NVDIMM Namespace spec
https://pmem.io/documents/NVDIMM_Namespace_Spec.pdf

3. High Level Block Architecture for Blockchain



How SNIA Protochain is built in device driver

- TBD

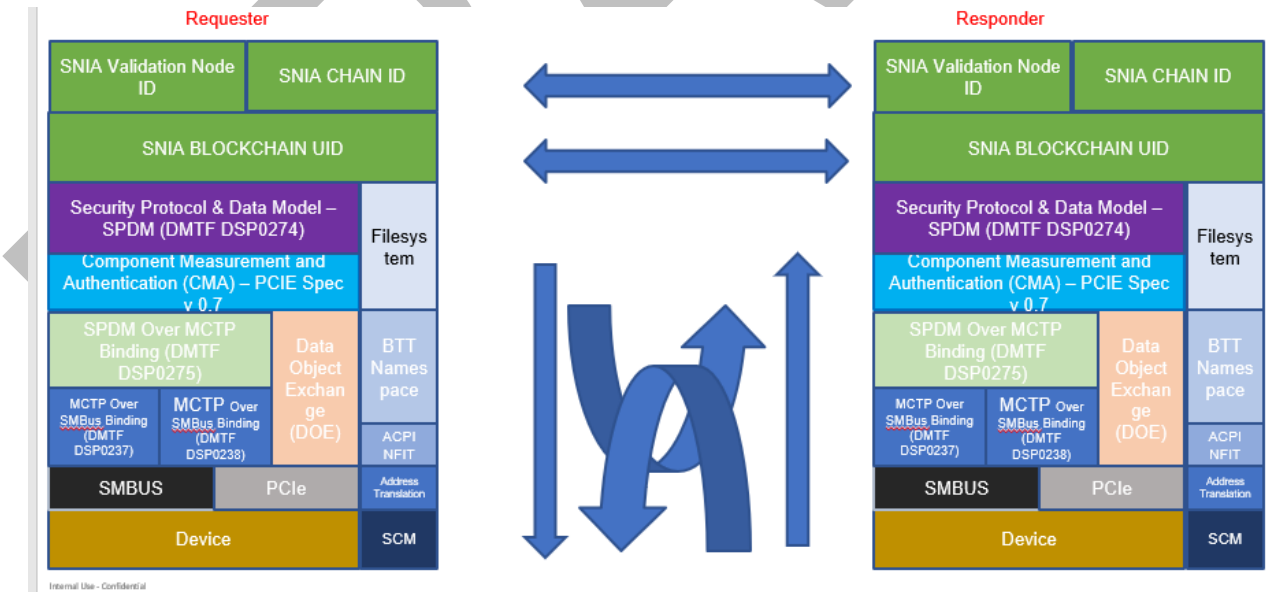
4. System Blocks - Layering Overview

4.1. SNIA Validation Node ID

4.2. SNIA Chain ID

4.3. SNIA Blockchain ID

4.4. Handshake between Requester and Responder UID



5. Blockchain Registers

Notes: need UID, control registers

Table 1: SNIA Blockchain UID Property Definitions

Offset	Size (in bytes	Name
0h	8	SNIA Blockchain ID
8h	4	SNIA Validation Node ID
Ch	4	SNIA Protochain ID
Fh	4	Requester ID
14h	4	Responder ID
18h	4	SPDM+Response Code
1Ch	4	SPDM + Capabilities
1Fh	4	SPDM + Algorithm
20h	4	SPDM + Vendor Defined Response

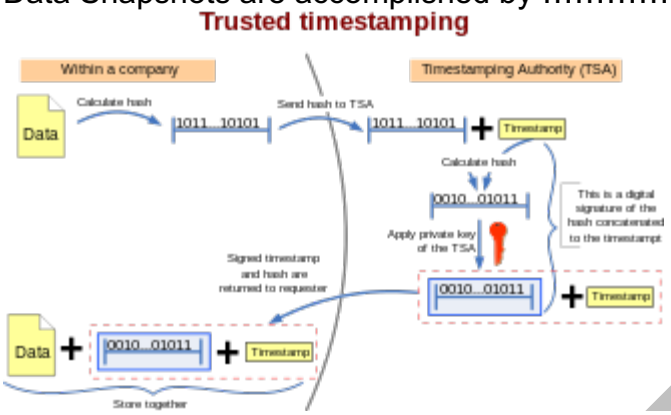
From SPDM specification registers used:

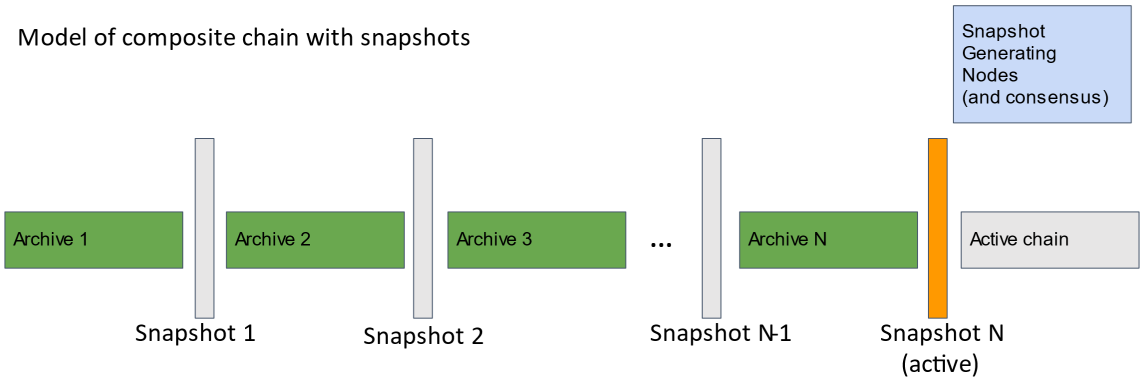
- SPDM Response code
    - Reserved – 0x64-0x7D – Use for Identification of Blockchains
- CAPABILITIES response message Register
        - Bit 6 – Status for UID Blockchain specific enabled
        - Flag Field Register Byte3 7:0 Responder supports Blockchain ID and Blockchain enabled protocol
- ALGORITHM response message
    - Bit 20 – Hash Blockchain enabled
- VENDOR_DEFINED_RESPONSE response message
    - SNIA BLOCKCHAIN INTEROP SPEC ID

6. Data Governance
  6.1. Data integrity
    6.1.1. Physical Data Integrity
    6.1.2. Logical Data Integrity
    6.1.3. File Systems

10.1. Data Snapshots

Data Snapshots are accomplished by ……..





11. API Requirements

12. Bibliography

12.1. There ar P3P Policy Usage Statistic https://trends.builtwith.com/docinfo/P3P-Policy

12.2. The Platform for Privacy Preferences 1.0 (P3P1.0) Specification https://www.w3.org/TR/P3P/#guiding_principles

12.3. https://www.ams.org/notices/201107/rtx110700905p.pdf

12.4. https://csrc.nist.gov/CSRC/media/Presentations/NIST-Block-Chain-Research-Project/images-media/ar-dy-blockchain-combined.pdf

12.5. https://csrc.nist.gov/News/2020/nist-publishes-cswp-on-emerging-blockchain-idms

12.6. https://en.wikipedia.org/wiki/Trusted_timestamping

12.7. https://datatracker.ietf.org/doc/html/draft-hardjono-blockchain-interop-arch-00

12.8.