Internet Engineering Task Force
Internet-Draft
Intended status: Informational
Expires: April 5, 2021

T. Hardjono
MIT
M. Hargreaves
Quant Network
N. Smith
Intel

October 2, 2020

An Interoperability Architecture for Blockchain Gateways
draft-hardjono-blockchain-interop-arch-00

Abstract

With the increasing interest in the potential use of blockchain systems for virtual assets, there is a need for virtual assets to have mobility across blockchain systems. An interoperability architecture is needed to permit the flow of virtual assets between blockchain systems. The architecture must recognize that there are different blockchain systems, and that the interior constructs in these blockchains maybe incompatible with one another. Gateway nodes perform the transfer of virtual assets between blockchain systems while masking the complexity of the interior constructs of the blockchain that they represent.

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 April 5, 2021.

Table of Contents

1. Introduction

Currently there is little technical interoperability between blockchain systems. This results in the difficulty in transferring or migrating virtual assets associated with a public-key (address) in one blockchain system to another blockchain system.

The existing solutions involve a third party that mediates the transfer. This mediating third party is typically an asset-exchange entity (i.e. crypto-exchange) operating in a centralized hub-spoke fashion. This reliance on a third party results not only delays in

transfers, but also in the need for key-holders to open accounts at the third party entity.

This document describes an architecture for blockchain gateways that perform the unidirectional transfer of virtual assets between two autonomous blockchain systems which employ the gateways.

The purpose of this architecture document is to provide technical framework within which to discuss the various aspects of a transfer between two gateways, including security aspects and transfer commitment aspects.

2. Terminology

There following are some terminology used in the current document:

- Blockchain Domain: The collection of resources and entities participating within a blockchain system.
- Interior Resources: The various interior protocols, data structures and cryptographic constructs that are a core part of a blockchain system. Examples of interior resources include the ledger, consensus protocol, incentive mechanisms, transaction propagation networks, etc.
- Exterior Resources: The various resources that are outside a blockchain system, and are not part of the operations of a blockchain. Examples include data located at third parties such as asset registries, ledgers of other blockchains, PKI infrastructures, etc.
- Blockchain nodes: The nodes of the blockchain system which form the peer-to-peer network, which collectively maintain the shared ledger in the blockchain by following a consensus algorithm
- Blockchain address: This is the public-key of an entity as known within a blockchain system, employed to transact on the blockchain network and recorded on the ledger of the blockchain. Also refered to as transaction signing key pair.
- Entity public-key: This the private-public key pairs of an entity used for interactions outside the blockchain system (e.g. TL1.2 key-pairs). We use this term to distinguish this key pair from the blockchain address.
- Gateway node: This is the node that implements the asset transfer protocol for the purpose of transferring or migrating assets

across blockchain systems. Depending on the blockchain system implementation, some or all of the nodes may be gateway-capable.

- Asset transfer protocol: The technical protocol used by two gateway nodes to transfer a virtual asset.

- Virtual Asset: A virtual asset is a digital representation of value that can be digitally traded, or transferred as defined by the FATF [REF].

- Virtual Asset Service Provider (VASP): Legal entity handling virtual assets as defined by the FATF [FATF].

- Originator: Person or entity seeking the transmittal of virtual asset to a beneficiary.

- Beneficiary: Person or entity receiving the transmitted virtual asset from an originator.

Further terminology definitions can be found in [NIST].

3. Assumptions and Principles

The following assumptions and principles underlie the design of the current interoperability architecture, and correspond to the design principles of the Internet architecture.

3.1. Design Principles

- Opaque blockchain resources: The interior resources of each blockchain system is assumed to be opaque to (hidden from) external entities. Any resources to be made accessible to an external entity must be made explicitly accessible by a gateway node with proper authorization.

- Externalization of value: The gateway protocol is agnostic (oblivious) to the economic or monetary value of the virtual asset being transferred.

The opaque resources principle permits the interoperability architecture to be applied in cases where one (or both) blockchain systems are permissioned (private). It is the analog of the autonomous systems principle in IP networking [Clar88], where interior routes in local subnets are not visible to other external autonomous systems

The value-externalization principle permits asset transfer protocols to be designed for efficiency, speed and reliability - independent of

the changes in the perceived economic value of the virtual asset. It is the analog of the end-to-end principle in the Internet architecture [SRC84], where contextual information (economic value) is placed at the endpoints of the transaction. In the case of virtual asset transfers, the originator and beneficiary at the respective blockchain systems are assumed to have a common agreement regarding the economic value of the asset.

3.2. Operational Assumptions

The following conditions are assumed to have occurred, leading to the invocation of the asset transfer protocol between two gateway nodes:

- Application layer transfer request: The transfer request from an originator in the origin blockchain is assumed to have occurred prior to the execution of the asset transfer protocol.

- Identification of originator and beneficiary: The originator and beneficiary are assumed to have been identified and that consent has been obtained from both parties regarding the asset transfer.

- Identification of origin and destination blockchain: The origin and destination blockchain systems is assumed to have been identified.

- Selection of gateway nodes: The two gateway nodes at the origin and destination blockchain systems respectively is assumed to have been selected.

- Owners of gateway nodes are known: The legal entity operating the gateway nodes are assumed to be known.

4. Architecture

4.1. Goal of Architecture

The goal of the interoperability architecture is to permit two (2) gateway nodes belonging to distinct blockchain systems to conduct a virtual asset transfer between them, in a secure and non-repudiable manner while ensuring the asset does not exist simultaneously on both blockchains (double-spend problem).

The virtual asset as understood by the two gateway nodes is a digital representation of value, expressed in an standard digital format in a way meaningful to the gateway nodes syntactically and semantically.

The syntactic representation of the virtual asset between the two gateways need not bear any resemblance to the syntactic asset representation within their respective blockchain systems.

The architecture recognizes that there different blockchain systems currently in operation and evolving, and that in many cases the interior technical constructs in these blockchains maybe incompatible with one another.

The architecture therefore assumes that certain types of nodes (gateway nodes) will be equipped with an asset transfer protocol and other relevant resources that permits greater interoperability across these incompatible blockchain systems.

The resources within a blockchain system (e.g. ledgers, public-keys, consensus protocols, etc.) are assumed to be opaque to external entities in order to permit a resilient and scalable protocol design that is not dependent on the interior constructs of particular blockchain systems. This ensures that the virtual asset transfer protocol between gateways is not conditioned or dependent on these local technical constructs. The role of a gateway therefore is also to mask (hide) the complexity of the interior constructs of the blockchain system that it represents. Overall this approach ensures that a given blockchain system operates as a true autonomous system.

The current architecture focuses on unidirectional asset transfers, although the building blocks in this architecture can be used to support protocols for bidirectional transfers (conditional two unidirectional transfers).

For simplicity the current architecture employs two (2) gateway nodes in the respective blockchains, but collective multi-node transfers (i.e. multiple nodes at each side) may be developed based on the building blocks and constructs identified in the current architecture.

4.2. Overview of Asset Transfer

An asset transfer between two blockchain systems is carried out by two (2) gateway nodes that represent the two respective blockchain systems.

A successful transfer results in the asset being extinguished or marked on the origin ledger by the origin-gateway, and for the asset to be introduced by the destination-gateway into the destination ledger. The mechanism to extinguish or introduce an asset from/into a ledger is dependent on the specific blockchain system.

4.3. Phases in Asset Transfer

The interaction between two gateways in an asset transfer is summarized in Figure 1, where the origin blockchain is B1 and the destination blockchain is B2. The gateways are denoted as G1 and G2 respectively.

The three phases of an asset transfer between gateways

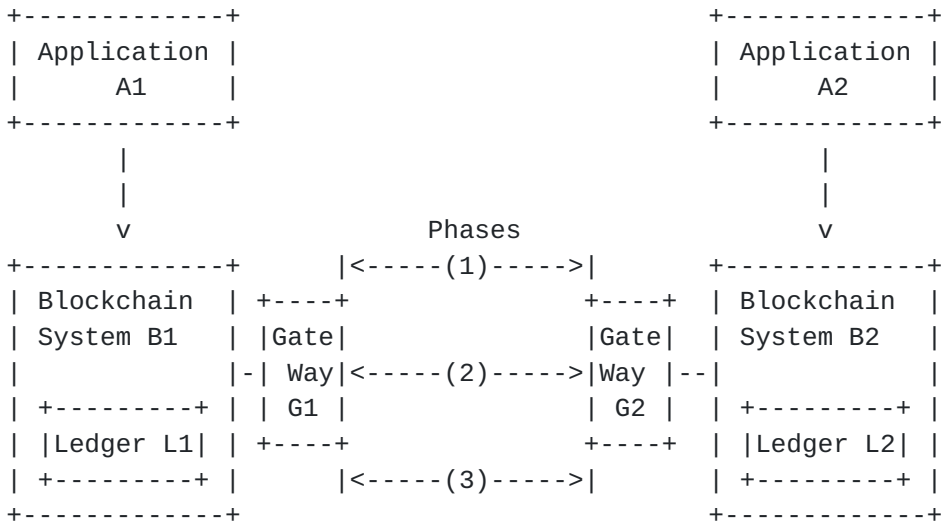

Figure 1

4.3.1. Phase 1: Exchange of security parameters and asset information

In this phase the gateways G1 and G2 initiate a connection to each other in order to perform a number of functions. Some of these are as follows:

- Exchange of parameters for secure channel establishment between G1 and G2.
- Delivery of asset-related information and asset-holder information, including originator and beneficiary identities and public keys, and the node-owner (VASP) identities and public keys.
- Exchange of parameters related to commitment mechanism employed within the flows of the asset transfer protocol.

4.3.2. Phase 2: Evidence of asset locking

In this phase, gateway G1 must provide gateway G2 with sufficient evidence that the asset on blockchain B1 is in a locked state on ledger L1 and safe from double-spend on the part of its current owner (the originator).

The precise form of the evidence is dependent on the blockchain system in B1, and must be previously agreed upon in Phase 1.

The purpose of this evidence is for dispute resolution between G1 and G2 (i.e. entities who own and operate G1 and G2 respectively) in the case that double-spend is later detected.

The gateway G2 must return a signed receipt to G1 of this evidence in order to cover G1 in the case of later denial by G2.

4.3.3. Phase 3: Final commitment of transfer

In this phase gateway G1 indicates to G2 its readiness to finally commit to the transfer, and vice versa. Both messages must be signed by G1 and G2 respectively in case of later (post-transfer) disputes.

Gateway G1 marks the ledger L1 that the virtual asset is no longer associated with the public-key of previous owner (originator) and that the asset no longer exists on the blockchain system B1.

Similarly, gateway G1 marks the ledger L2 in blockchain system B2 to indicate that henceforth the asset is associated with the public-key of the new owner (beneficiary).

Optionally, both G1 and G2 may exchange the local ledger marking information (e.g. block number and transaction number) with each other. This information may aid in future audit and accountability purposes from a legal perspective.

5. Related Open Issues

There are a number of open issues that are related to the asset transfer protocol between gateway nodes. Some of the issues are due to the fact that blockchain technology is relatively new, and that technical constructs designed for interoperability have yet to be addressed. Some of the issues are due to the nascency of the virtual asset industry and lack of conventions, and therefore require industry collaboration to determine these.

5.1. Global identification of blockchain systems and public-keys

There is currently no standard nomenclature to identify blockchain systems in a globally unique manner. The analog to this is the AS-numbers associated with IP routing autonomous systems.

Furthermore, an address (public-key) may not be unique to one blockchain system. An entity (e.g. user) may in fact employ the same public-key at multiple distinct blockchain systems simultaneously.

However, in order to perform an asset transfer from one blockchain system to another, there needs to be mechanism that resolves the beneficiary identifier (as known to the originator) to the correct public-key and blockchain system as intended by the originator.

5.2. Selection of gateways nodes within a blockchain system

A given blockchain system must possess the capability to select or designate gateway nodes that will perform an asset transfer across blockchain systems.

A number of blockchain systems already employ consensus mechanisms that elect a node to perform the transaction processing (e.g. proof of stake in Ethereum). The same consensus mechanisms may be used to elect the gateway node.

However, there are some blockchain systems that do not elect a single node and which employ a race-to-process strategy (e.g. proof of work in Bitcoin). Since the winner of the proof of work can be any node in the blockchain system, this implies that all the nodes in these types of blockchains must be gateway-capable.

5.3. Commitment protocols and forms of commitment evidence

Within Phase 2, the gateway nodes must implement one (or more) transactional commitment protocols that permit the coordination between two gateways, and the final commitment of the asset transfer.

The choice of the commitment protocol (type/version) and the corresponding commitment evidence must be negotiated between the gateways during Phase 1.

For example, in Phase 2 and Phase 3 discussed above the gateways G1 and G2 may implement the classic 2 Phase Commit (2PC) protocol [Gray81] as a means to ensure efficient and non-disputable commitments to the asset transfer.

Historically, transactional commitment protocols employ locking mechanisms to prevent update conflicts on the data item in question. When used within the context of virtual asset transfers across blockchain systems, the fact that an asset has been locked by G1 (as the 2PC coordinator) must be communicated to G2 (as the 2PC participant) in an indisputable manner.

The exact form of this evidence of asset-locking must be standardized (for the given transactional commitment protocol) to eliminate any ambiguity.

6. Security Considerations

Although the current interoperability architecture for blockchain gateways assumes the externalization of the value of assets, as a blockchain system holds an increasing number of virtual assets it becomes attractive to attackers seeking to obtain cryptographic keys of its nodes and its end-users.

Gateway nodes are of particular interest to attackers because they enable the transferal of virtual assets to external blockchain systems, which may or may not be regulated. As such, hardening technologies and tamper-resistant crypto-processors (e.g. TPM, SGX) should be used for implementations of gateways [HS19].

7. Policy Considerations

Virtual asset transfers must be policy-driven in the sense that it must observe and enforce the policies defined for the blockchain domain. Resources that make-up a blockchain systems are owned and operated by entities (e.g. legal persons or organizations), and these entities typically operate within regulatory jurisdictions [FATF]. It is the responsibility of these entities to translate regulatory policies into functions on blockchain systems that comply to the relevant regulatory policies.

At the application layer, asset transfers must take into consideration the legal status of assets and incorporate relevant asset-related policies into their business logic. These policies must permeate down to the nodes that implement the functions of asset transaction processing.

The smart contract abstraction, based on replicated shared code/state on the ledger [Herl19], must additionally incorporate the notion of policy into the abstraction.

8. References

8.1. 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>.

[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>.

8.2. Informative References

[Clar88] Clark, D., "The Design Philosophy of the DARPA Internet Protocols, ACM Computer Communication Review, Proc SIGCOMM 88, vol. 18, no. 4, pp. 106-114", August 1988.

[Gray81] Gray, J., "The Transaction Concept: Virtues and Limitations, in VLDB Proceedings of the 7th International Conference, Cannes, France, September 1981, pp. 144-154", September 1981.

[Herl19] Herlihy, M., "Blockchains From a Distributed Computing Perspective, Communications of the ACM, vol. 62, no. 2, pp. 78-85", February 2019, <https://doi.org/10.1145/3209623>.

[HLP19] Hardjono, T., Lipton, A., and A. Pentland, "Towards and Interoperability Architecture for Blockchain Autonomous Systems, IEEE Transactions on Engineering Management", June 2019, <https://doi:10.1109/TEM.2019.2920154>.

[HS2019] Hardjono, T. and N. Smith, "Decentralized Trusted Computing Base for Blockchain Infrastructure Security, Frontiers Journal, Sepcial Issue on Blockchain Technology, Vol. 2, No. 24", December 2019, <https://doi.org/10.3389/fbloc.2019.00024>.

[SRC84] Saltzer, J., Reed, D., and D. Clark, "End-to-End Arguments in System Design, ACM Transactions on Computer Systems, vol. 2, no. 4, pp. 277-288", November 1984.

Authors' Addresses

Thomas Hardjono
MIT

Email: hardjono@mit.edu

Martin Hargreaves
Quant Network

Email: martin.hargreaves@quant.network

Ned Smith
Intel

Email: ned.smith@intel.com