Internet Engineering Task Force V. Ramakrishna

Internet-Draft IBM Research

Intended status: Informational T. Hardjono

Expires: 24 January 2024 MIT

23 July 2023

Secure Asset Transfer (SAT) Use Cases

draft-ietf-satp-usecases-01

Abstract

This document describes prominent scenarios where enterprise systems and

networks maintaining digital assets require the ability to securely

transfer assets or data to each other.

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 24 January 2024.

Copyright Notice

Copyright (c) 2022 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.

1. Introduction

Business networks, built on both centralized and decentralized models,

have emerged to manage cross-organization assets and workflows. The scope

of such workflows and the assets they govern, as well as the set of

participating organizations within a network, have been quite limited,

partly for security, privacy, and scalability reasons, and partly because

organizations have been reticent to moving large portions of their pre

existing workflows to such networks. We see this especially in the areas

of trade, finance, supply chain logistics, and property management. Yet

the workflows managed by these networks are naturally interlinked in the

real world, and therefore cannot afford to remain isolated from each

other technologically, which would diminish the value of their assets. At

the same time, a network, once built, has institutional staying power,

and it is therefore impractical to assume that they will expand or merge.

Interoperability is therefore an imperative in this fragmented business

network ecosystem. This comes in different flavors, namely the ability to

move an asset from one network to another, interlinking workflows to

share asset state with proof of authenticity from one network to another,

and swapping assets in different networks as part of a business

transaction, as listed in the SAT Architecture Specification [SATA]. The

purpose of this document is to describe prominent examples of these modes

that have been encountered by enterprises and business consortiums and

identified as challenges to be overcome. In particular, this document

describes scenarios where the Secure Asset Transfer Protocol (SATP)

[SATP] can be directly applied to solve the problem of moving digital

assets across networks, for which no other canonical protocol exists in

the literature.

2. Terminology

There following are some terminology used in the current document.

We borrow terminology from NIST and ISO as much as possible,

introducing new terms only when needed:

o Asset network (system): The network or system where a digital

asset is utilized.

o Asset Transfer Protocol: The protocol used to transfer (move) a

digital asset from one network to another using gateways.

o Origin network: The current network where the digital asset is

located.

o Destination network: The network to which a digital asset is to be

transferred.

o Data sharing: The process, using the Asset Transfer Protocol, by which

one or more units of verifiably authentic data are communicated from

an Origin network to a Destination network, either voluntarily or upon

request.

o Asset Transfer: A fail-safe process of moving an asset from one

network to another, with the destruction of the asset in the Origin

network and its recreation in the Destination network occurring as a

single atomic action.

o Asset Exchange: A fail-safe process of exchanging (or swapping) assets

held by a pair of owners, each asset being maintained in a different

network, with the two in-network transfers occurring as a single

atomic action.

Further terminology definitions can be found in [NIST] and [ISO].

3. International Trade and Supply Chains

3.1. Trade Finance and Logistics

There are several real-world examples of consortium networks managing

different aspects of international trade. Networks like We.Trade [WET],

built on Hyperledger Fabric [HLF], and Marco Polo [MP], built on R3 Corda

[R3C], manage trade finance workflows by connecting exporters, importers,

and financial institutions (primarily banks). Other networks like

TradeLens [TL], built on Hyperledger Fabric, manage trade shipping and

documentation logistics, by connecting exporters and shipping carriers.

As an example, consider a system of two networks as illustrated in Figure

1: (a) a trade finance network managing letters of credit business

lifecycles from application to fulfilment, and (b) a trade logistics

network managing shipping consignment creation and dispatch documents

like bills of lading.

+------------+

| Exporter’s | +----------+ +---------------------+

| Bank | | Exporter | | Exporter |

+------------+ +----------+ +---------------------+

| | | | | |

3 | | 5 | 4 1 | | 2 | 4

Approve | | Request | Upload Book | | Create | Accept

L/C | | Payment | B/L Consignment | | Consignment | B/L

| | | | | |

V V V V V V

+-------------------------------+ +-------------------------------+

| Trade Finance Network | | Trade Logistics Network |

+-------------------------------+ +-------------------------------+

˄ ˄ ˄ ˄

2 | | 1 5 | | 3

Propose | | Request Dispatch | | Upload

L/C | | L/C Consignment | | B/L

| | | |

+------------+ +----------+ +-------------+

| Importer’s | | Importer | | Carrier |

| Bank | +----------+ +-------------+

+------------+

(a) (b)

Figure 1

An exporter who belongs to both systems must produce a valid bill of

lading in the trade finance network to enforce a payment from the buyer

to fulfil the terms of the letter of credit. But this bill, which serves

as evidence of a shipping consignment’s dispatch via a carrier, lies in

the other, i.e., trade logistics, network. The two networks must

therefore be interoperable in such a way that the logistics network can

share a bill with the finance network along with independently verifiable

proof of authenticity. Otherwise, the trade finance network’s workflow

must trust that the exporter is acting in good faith and supplying

genuine bills of lading, which adds insecurity. This interoperation,

which involves sharing of network data, can be extrapolated to other

scenarios involving the two networks. The trade logistics network can

require an exporter to produce a valid letter of credit from the trade

finance network before permitting a consignment record creation. Both

these cross-network data sharing instances are illustrated in Figure 2.

+----------+ 1 Agree on +----------+

| Exporter |<------------------>| Importer |

+----------+ Purchase Order +----------+

+------------+

| Exporter’s | +----------+ +---------------------+

| Bank | | Exporter | | Exporter |

+------------+ +----------+ +---------------------+

| | | | |

4 | | 12 5 | | 7 | 9

Approve | | Request Book | | Create | Accept

L/C | | L/C Consignment | | Consignment | B/L

| | | | |

| | | | |

| | |¯¯¯¯¯¯¯¯¯¯¯¯¯¯¯¯¯¯¯¯| | | |

| | | 11 Share B/L | | | |

V V V | V V V

+-------------------------------+ +-------------------------------+

| Trade Finance Network | | Trade Logistics Network |

+-------------------------------+ +-------------------------------+

˄ ˄ | ˄ ˄ ˄

| | | 6 Share L/C | | |

| | |\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_| | |

| | | |

3 | | 2 10 | | 8

Propose | | Request Dispatch | | Upload

L/C | | L/C Consignment | | B/L

| | | |

+------------+ +----------+ +-------------+

| Importer’s | | Importer | | Carrier |

| Bank | +----------+ +-------------+

+------------+

Figure 2

Asset transfers among trade networks: In the preceding example, letters

of credit and bills of lading represent portions of state of the larger

export-import workflow. But these documents are also digital assets in

their own rights.

A bill of lading can serve as title to the consignment of goods being

shipped, and hence can be traded as a security or used as collateral

against debt obligations in the financial market. Hence, Step 11 in

Figure 2 may well be embodied by the transfer rather than the sharing of

state of a bill so that it ceases to remain on the Trade Logistics

Network ledger and instead belongs to the Seller’s Bank on the Trade

Finance Network’s ledger.

A letter of credit may also assume the properties of a digital asset in

certain situations. Consider the case of an importer who wishes to move

their business to a different trade finance network and maintain their

records on that network’s ledger. We can assume that the banks and the

exporter participate in the second trade finance network as well, which

exists to serve a different clientele. The importer needs to be able to

move its letter of credit state to the other network and resume the trade

workflow after migration. This requires the ability to transfer the

letter in the form of a digital asset from one trade finance network to

another.

3.2. Tracking Food Shipments

The use case linking a trade finance network with a trade logistics

network can be augmented by adding a food tracking network like the IBM

Food Trust [IFT] to the mix. Such a network connects producers,

suppliers, manufactures, and retailers, who participate in food supply

chains. Purchase orders, like those negotiated between producers and

retailers, and which are illustrated as negotiated between exporter and

importers in Figure 2, are recorded in this network’s ledger. For quality

control, its business workflow will track at periodic intervals the state

(e.g., temperature and humidity) of containers carrying, for example,

produce from farm to source port and from destination port to warehouse.

The trade logistics network handles documentation and dispatch but does

not track the location or condition of a consignment outside of a

carrier’s purview. Clearly, these networks play complementary roles in a

supply chain. The logistics network should be able to get the state and

history of a container before dispatch from the food tracking network, as

should the latter from the former after the carrier has delivered a

consignment. End-to-end supply chain visibility and effectiveness relies

on the interoperability of these two networks, or to be precise, their

ability to share verifiably authentic data with each other. Further, such

interoperation also enables the trade finance network to allow the

creation of a letter of credit only after verifying the existence of a

valid purchase order in the food tracking network. Figure 3 illustrates

the links between these networks.

+-------------------------------+

|¯¯¯¯| Food Tracking Network |¯¯¯¯¯¯¯¯¯¯|

| +-------------------------------+ |

Share | ˄ | Share

Purchase | | Share | Shipment

Order | |¯¯¯¯¯¯¯¯¯¯¯¯¯¯¯¯| | Shipment | State

| | Share B/L | | State |

V V | | V

+-------------------------------+ +-------------------------------+

| Trade Finance Network | | Trade Logistics Network |

+-------------------------------+ +-------------------------------+

| ˄

| Share L/C |

|\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_|

Figure 3

3.3. Supply Chain Management

To complete the picture, we can add a payments network to the mix, which

maintains currency accounts for clients in different countries and

enables cross-border payments, an example being the Stellar network

[STN]. After goods have been dispatched, and optionally after

verification of the delivery and proper condition of a shipment, payment

is due from an importer to an exporter. The trade finance network can

record a payment obligation on its ledger but it will rely on the

payments network to process and confirm the actual transfer of funds. The

former shares data about the obligation to the latter, which shares data

about a successful (or otherwise) payment in return, as illustrated in

Figure 4.

+-------------------------------+

|¯¯¯¯| Food Tracking Network |¯¯¯¯¯¯¯¯¯¯|

| +-------------------------------+ |

Share | ˄ | Share

Purchase | | Share | Shipment

Order | |¯¯¯¯¯¯¯¯¯¯¯¯¯¯¯¯| | Shipment | State

| | Share B/L | | State |

V V | | V

+-------------------------------+ +-------------------------------+

| Trade Finance Network | | Trade Logistics Network |

+-------------------------------+ +-------------------------------+

| ˄ | ˄

Share | | Share | Share L/C |

Payment | | Payment |\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_|

Obligation | | Fulfilment

| |

V |

+----------------------+

| Payments Network |

+----------------------+

Figure 4

Addendum: we can add yet another network to the mix, one that manages

regulatory compliance. (E.g., proof-of-concept systems have been built to

bring banks and corporations on a single distributed ledger and smart

contract platform to share KYC information in privacy-preserving ways

[BKYC] [SKYC].) Now issuances of letters of credit in the trade finance

system will be dependent on valid KYC records being maintained as assets

in the regulatory compliance system.

4. Currency and Finance

The emerging paradigm of Decentralized Finance (DeFi) and the emerging

application of Central Bank Digital Currency (CBDC) have opened up a

spectrum of scenarios that require management of financial digital assets

across multiple systems, typically built on distributed ledgers.

DeFi is a “new financial paradigm that leverages distributed ledger

technologies to offer services such as lending, investing, or exchanging

cryptoassets without relying on a traditional centralized intermediary”

[BISDeFi]. Following the Web3 philosophy, scoped for the world of

finance, DeFi offers architecture and protocols built on smart contracts

deployed on blockchain or other distributed ledger technology. It thereby

obviates the need for centralized management and orchestration of

financial processes (e.g., currency transfers, exchanges, securities

settlements) by trusted authorities who can gain undue leverage.

CBDC is a form of tokenized cryptocurrency that various central banks

around the world are experimenting with as the digital equivalent of

traditional central bank-issued money used by banks and other financial

institutions as well as end users for commercial transactions and

settlements. Central banks possess exclusive authority to mint and issue

money in physical cash form and in the form of electronic reserves. They

also support commercial bank money used in retail transactions by banks

and other users in their private capacities. Central banks have

traditionally used their control over these different forms of money to

enforce monetary policy in a way that promotes financial stability and

provides broad access to safe and efficient payments [BISCBDC]. CBDCs

would form a new, or alternative, type of central bank money, typically

(but not always) built on blockchain or other distributed ledger

technology. They have recently garnered significant interest in

government circles by promising increased access and inclusion, better

resilience, and increased scale and efficiency of currency transfers,

compared to traditional forms of central bank-issued or central bank-

backed currency.

CBDCs can broadly be classified into “wholesale” and “retail”. Wholesale

CBDC, which facilitates inter-bank and cross-border settlements, is

currency that is available only to banks and other financial

institutions. Retail CBDC is available to the public and can be used as a

digital form of cash, enabling fast transparent payments for goods and

services at high scale and volume; in effect, it can be used as a

substitute for legacy payment mechanisms.

Different system architectures exist to manage CBDC for banks and end

users, from issuance to transfers to redemptions. A 2-tier model as

illustrated in Figure 5 has recently gained popularity, where wholesale

CBDC networks manage interactions between central and commercial banks,

and retail CBDC networks manage interactions between commercial banks and

end users. If we consider the role of the central bank as the defining

characteristic of a system architecture, this model can be referred to as

“indirect”, because commercial banks mediate claims between the central

bank and end users and also facilitate payments. Other architectures also

exist, including “direct CBDC”, where the central bank issues CBDC

directly to end users and facilitates payments, and “hybrid CBDC”, which

provides users the facility to make direct claims on the central bank

while allowing intermediaries to facilitate payments [BISRCBDC].

4.1. Currency Transfers

The 2-tier “indirect CBDC” model illustrated in Figure 5 presents unique

interoperability challenges that require protocols for asset transfers

and which SATP is well-suited to handle. In the higher tier lie

wholesale CBDC networks, bringing together central or reserve banks and

various commercial banks. Following the DeFi logic, these networks are

typically built on distributed ledger and smart contract technologies.

Commercial banks hold reserve currency deposits with the reserve bank,

which has the special power to mint currency and issue CBDC and also

enforce regulatory compliance. In the lower tier lie retail CBDC networks

for commercial banks and their customers, built on similar technologies,

enabling seamless, efficient, and transparent payments using CBDCs. A

retail CBDC network may involve a single commercial bank or multiple

commercial banks, depending on the market caps of those banks and their

purposes for joining such a network.

+----------------------------------------+

| |

| Wholesale CBDC Network |

| |

| +----------------+ |

| | Central Bank | |

| +----------------+ |

| |

| +------------+ +------------+ |

| | Commercial | | Commercial | |

| | Bank A’s | | Bank B’s | ...... |

| | Account | | Account | |

| +------------+ +------------+ |

| |

+----------------------------------------+

˄ ˄

| |

| |

V V

+----------------------------+ +----------------------------+

| | | |

| Retail CBDC Network | | Retail CBDC Network |

| | | |

| +------------+ +---------+ | | +------------+ +---------+ |

| | Commercial | | Central | | | | Commercial | | Central | |

| | Bank A’s | | Bank | | | | Bank B’s | | Bank | |

| | Account | +---------+ | | | Account | +---------+ |

| +------------+ | | +------------+ |

| | | | .......

| +----------------+ | | +------------+ |

| | Client Account | ....... | | | Commercial | |

| +----------------+ | | | Bank C’s | |

| | | | Account | |

+----------------------------+ | +------------+ |

| |

| +----------------+ |

| | Client Account | ....... |

| +----------------+ |

| |

+----------------------------+

Figure 5

Here we will encounter scenarios where a given commercial bank maintains

digital currency accounts in a wholesale CBDC network as well as one or

more retail CBDC networks. To inject liquidity into a retail CBDC

network, this bank will need to transfer currency from its reserve

account in the wholesale CBDC network. Or it may need to approve (or at

least audit) the transfer of currency from one retail CBDC network to

another bank in another retail CBDC network. In the world of

decentralized finance, or DeFi for short, currency cannot afford to

remain siloed in any single CBDC network. Hence, these networks must be

interoperable in order to facilitate secure transfers of currency among

themselves, as illustrated in Figure 5.

We can identify two specific instances of currency transfer across

networks in this example: one from a wholesale CBDC network to a retail

CBDC network, and another from one retail CBDC network to another. Since

currency in tokenized form is a digital asset, these scenarios require

the direct application of a secure protocol for asset transfer. SATP

[SATP] fits the bill, is agnostic of the types of distributed ledger

technologies on which the respective networks are built, and simply

requires the networks to use SATP gateways. This is not just a

theoretical proposition; a candidate design for a bridge between

Hyperledger Fabric [HLF] and Hyperledger Besu [HLB] networks using SATP

and the Hyperledger Cacti interoperability platform [HLC] has been

proposed by distributed ledger researchers [Aug23].

4.2. Multi-CBDC Economy

Several governments, banks and financial communities have explored the

use of a shared ledger containing multiple CBDCs as way to potentially

obtain an economy of scale in the development and maintenance of their

own respective CBDCs. Such a Multi-CBDC approach has the potential

benefit to improve cross-border payments and protect monetary

sovereignty, without necessarily becoming a monetary union [BISMCBDC].

However, even within a Multi-CBDC configuration, there must be a

mechanism to interconnect each respective national (sovereign) bank

network with the shared Multi-CBDC network. Gateways appear to be an

attractive means to permit the transfer of a CBDC from one national

network/ledger into the shared Multi-CBDC ledger, and vice versa. One

major requirement is the assurance that consistency is maintained between

the CBDC counts on the national network with that on the Multi-CBDC

network (i.e. no counterfeiting; no double-spend).

With or without a Multi-CBDC ledger, the existence of different national

networks managing different wholesale CBDC assets will necessitate inter-

network transfers for cross-border payments and settlements [BISCBP]

[WBGCBP] [PUbin]. Whether directly between two wholesale CBDC networks or

between a wholesale CBDC network and the Multi-CBDC network, transfer of

currency assets is a problem for which SATP appears to be the most

suitable solution.

4.3. Delivery vs Payment (DvP) of Securities

In Decentralized Finance, or DeFi for short, investors and financial

institutions will form networks to manage the creation and purchase of

securities. As a simple example, we can consider a network consisting of

the Treasury, which issues bonds, and commercial banks, which purchase

and trade bonds. We can also consider a payments network of the kind we

saw in Section 3.3 (or a retail CBDC network of the kind we saw in

Section 4.1), which allows CBDC transfers between commercial banks’

accounts. In the securities network, banks may wish to transfer bonds to

each other but only in exchange for compensation. But such compensation

can be made only on a payments network where the two maintain currency

accounts (e.g., in CBDC). Therefore, the securities and payment networks

must be able to interoperate in such a way that two banks can carry out a

delivery-vs-payment transaction spanning these two independent networks.

Such a transaction must be atomic, i.e., either both bond and CBDC tokens

get transferred in their respective networks or neither gets transferred.

Figure 6 illustrates this exchange.

+-----------------------------------------------------------------------+

| Bond Network |

| |

| +----------+ Issue +---------------------------+ |

| | Treasury |------------------>| Commercial Bank A’s | |

| +----------+ Bond | Portfolio | |

| +---------------------------+ |

| | |

| | Transfer |

| | Bond |

| V |

| +---------------------------+ |

| | Commercial Bank B’s | |

| | Portfolio | |

| +---------------------------+ |

+-----------------------------------------------------------------------+

˄

∥

∥

V

+-----------------------------------------------------------------------+

| Payment Network / Retail CBDC Network |

| |

| +-----------+ +---------------------------+ |

| | Central | | Commercial Bank A’s | |

| | Bank | | Account | |

| +-----------+ +---------------------------+ |

| | |

| | Transfer |

| | Currency |

| V |

| +---------------------------+ |

| | Commercial Bank B’s | |

| | Account | |

| +---------------------------+ |

+-----------------------------------------------------------------------+

Figure 6

In a variation of this example, the two commercial banks may hold CBDC

accounts in two different Payment Networks. In that case, fulfilment of

the DvP would require transfer of CBDC from one network to another. An

instance of SATP between gateways representing those two networks would

handle that problem.

5. Transferal of Digital Art and Payments across National Borders

There is currently growing interest within many artist communities of

developing and selling digital-only artwork, in which the artwork

consists of a file in a well-known (e.g. JPEG, MPEG) format that is

created by an artist. The artists seek to sell copies of the digital-only

artwork on the global marketplace, allowing anyone in the world to

purchase a copy and consume (e.g. display offline) the artwork at the

buyer’s discretion. Currently, the most popular technological vehicle to

achieve this goal is through the tokenization of the copies of the

artwork coupled with digital encryption/signature technologies to

transfer control (and thereby legal ownership) of the digital-only

artwork to the buyer.

Although there are a number of technical and legal challenges (e.g.

copyright enforcement) to completing such a sale, one key issue pertains

to the sale and payment for digital-only artwork across national borders.

Many nations enforce taxation upon the sale of any asset, including that

of artwork generally both domestically and internationally. Thus, when

the control/ownership of a tokenized digital-only artwork is transferred

to a new owner in a foreign nation and payment is received, taxation must

be obtained at the point-of-sale (which could be an online platform) and

proof of delivery must be traceable to ensure that no taxation-avoidance

occurs. A secure asset transfer protocol between systems that can be

built on distributed or shared ledgers via gateways with designated legal

authority is necessary to enforce governmental regulations and provide

accountability.

6. Interoperation Protocol Considerations

The use cases provided as examples serve to illustrate instances of

general phenomena that the Secure Asset Transfer Protocol [SATP],

with a limited number of variations, is designed to handle. The data

sharing examples in Section 3 can be extrapolated to any kinds of data

that need to be shared between networks running arbitrary workflows. The

asset transfer example in Section 4.1 and the asset exchange example in

Section 4.2 similarly can be extrapolated to any kinds of digital assets

lying within any kind of network. Considerations for the interoperability

protocol, or SATP, can therefore be limited to standard distributed

systems issues like integrity, fault tolerance, and liveness, while

completely disregarding the nature of the assets, networks, and

workflows, which can all remain opaque to the protocol.

7. References

7.1. Normative References

[Aug23] A. Augusto, R. Belchior, I. Kocsis, L. Gönczy, A. Vasconcelos,

and M. Correia, "CBDC Bridging between Hyperledger Fabric and

Permissioned EVM-based Blockchains." 2023 IEEE International

Conference on Blockchain and Cryptocurrency (ICBC), Dubai,

United Arab Emirates, 2023, pp. 1-9,

doi: 10.1109/ICBC56567.2023.10174953,

<https://www.techrxiv.org/articles/preprint/CBDC\_bridging\_

between\_Hyperledger\_Fabric\_and\_permissioned\_EVM-based\_

blockchains/21809430>.

[BISCBDC] Bank of Canada, European Central Bank, Bank of Japan, Sveriges

Riksbank, Swiss National Bank, Bank of England, Board of

Governors of the Federal Reserve, and Bank for International

Settlements, “Central bank digital currencies: foundational

principles and core features.” Bank for International

Settlements, BIS Report, October 2020,

<https://www.bis.org/publ/othp33.htm>.

[BISCBP] Bank for International Settlements, Committee on Payments and

Market Infrastructures, Innovation Hub, International Monetary

Fund, and World Bank Group, “Central bank digital currencies

for cross-border payments.” Bank for International

Settlements, Report to the G20, July 2021,

<https://www.bis.org/publ/othp38.htm>.

[BISDeFi] R. Auer, B. Haslhofer, S. Kitzler, P. Saggese, and F. Victor,

“The Technology of Decentralized Finance (DeFi).” Bank for

International Settlements, BIS Working Paper No. 1066,

<https://www.bis.org/publ/work1066.htm>.

[BISMCBDC] R. Auer, P. Haene, and H. Holden, “Multi-CBDC arrangements and

the future of cross-border payments.” Bank for International

Settlements, BIS Paper No. 115, March 2021,

<https://www.bis.org/publ/bppdf/bispap115.htm>.

[BISRCBDC] R. Auer and R. Boehme, “The technology of retail central bank

digital currency.” Bank for International Settlements, BIS

Quarterly Review, March 2020,

<https://www.bis.org/publ/qtrpdf/r\_qt2003j.htm>.

[BKYC] Kumar Bhaskaran, Peter Ilfrich, Dain Liffman, Christian

Vecchiola, Praveen Jayachandran, Apurva Kumar, Fabian Lim,

Karthik Nandakumar, Zhengquan Qin, Venkatraman Ramakrishna,

Ernie GS Teo, and Chun Hui Suen, "Double-Blind Consent-Driven

Data Sharing on Blockchain." First IEEE Workshop on Blockchain

Technologies and Applications (BTA) 2018, Co-located with 2018

IEEE International Conference on Cloud Engineering (IC2E),

Orlando, FL, April 17, 2018.

[HLB] “Hyperledger Besu”, <https://www.hyperledger.org/use/besu>.

[HLC] P. Somogyvari, J. S. Sasan, I. Sato, T. Takeuchi, V.

Ramakrishna, S. Nishad, K. Narayanam, and D. Vinayagamurthy,

“Introducing Hyperledger Cacti, a multi-faceted pluggable

interoperability framework.” Hyperledger Foundation Blog,

November 2022,

<https://www.hyperledger.org/blog/2022/11/07/introducing-

hyperledger-cacti-a-multi-faceted-pluggable-interoperability-

framework>.

[HLF] Elli Androulaki, Artem Barger, Vita Bortnikov, Christian

Cachin, Konstantinos Christidis, Angelo De Caro, David

Enyeart, Christopher Ferris, Gennady Laventman, Yacov

Manevich, Srinivasan Muralidharan, Chet Murthy, Binh Nguyen,

Manish Sethi, Gari Singh, Keith Smith, Alessandro Sorniotti,

Chrysoula Stathakopoulou, Marko Vukolic, Sharon Weed Cocco,

and Jason Yellick, "Hyperledger Fabric: A Distributed

Operating System for Permissioned Blockchains", EuroSys 2018,

<https://dl.acm.org/doi/pdf/10.1145/3190508.3190538>.

[IFT] IBM, "IBM Food Trust – Blockchain for the world’s food

supply", 2022,

<https://www.ibm.com/blockchain/solutions/food-trust>.

[ISO] ISO, "Blockchain and distributed ledger technologies-

Vocabulary (ISO:22739:2020)", July 2020,

<https://www.iso.org>.

[MP] Marco Polo Network Operations (Ireland) Limited, "Marco Polo

Network: Blockchain Enabled Supply Chain & Payment

Solutions.", 2022,

<https://marcopolonetwork.com/>.

[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>.

[PUbin] Bank of America Merrill Lynch, BCS Information Systems, Credit

Suisse, DBS Bank, HSBC, J.P. Morgan, Mitsubishi UFJ Financial

Group, OCBC Bank, R3, Singapore Exchange, and UOB Bank, “The

future is here: Project Ubin: SGD on Distributed Ledger.”

Deloitte and Monetary Authority of Singapore (MAS), Report,

2017,

<https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/

financial-services/sg-fsi-project-ubin-report.pdf>.

[R3C] R3, "Corda: A Technical White Paper", August 2019,

<https://www.r3.com/reports/corda-technical-whitepaper/>.

[SATA] Hardjono, T., Hargreaves, M., Smith, N., and V. Ramakrishna,

"Secure Asset Transfer (SAT) Interoperability Architecture,

IETF, draft-ietf-satp-architecture-01.", July 2023,

<https://datatracker.ietf.org/doc/draft-ietf-satp-

architecture/>.

[SATP] Hargreaves, M., Hardjono, T., and R. Belchior,

"Secure Asset Transfer Protocol (SATP), IETF,

draft-ietf-satp-core-02.", July 2023,

<https://datatracker.ietf.org/doc/draft-ietf-satp-core/>.

[SKYC] Michael Curry, "Blockchain for KYC: Game-changing RegTech

innovation.", September 21, 2018,

<https://www.ibm.com/blogs/blockchain/2018/09/blockchain-for-

kyc-game-changing-regtech-innovation/>.

[STN] Stellar Development Foundation, "Stellar – Access your

universe of opportunities", 2022,

<https://www.stellar.org/>.

[TL] TradeLens, "TradeLens: Supply chain data and docs.", 2022,

<https://www.tradelens.com/>.

[WBGCBP] “Central Bank Digital Currencies for Cross-Border Payments: A

Review of Current Experiments and Ideas.” World Bank Group,

Other Financial Sector Study, November 2021,

<https://documents1.worldbank.org/curated/en/

369001638871862939/pdf/Central-Bank-Digital-Currencies-for-

Cross-border-Payments-A-Review-of-Current-Experiments-and-

Ideas.pdf>.

[WET] IBM, "we.trade.", 2019,

<https://www.ibm.com/case-studies/we-trade-blockchain>.

7.2. Informative References

[Abebe19] Ermyas Abebe, Dushyant Behl, Chander Govindarajan, Yining

Hu, Dileban Karunamoorthy, Petr Novotny, Vinayaka Pandit,

Venkatraman Ramakrishna, Christian Vecchiola, "Enabling

Enterprise Blockchain Interoperability with Trusted Data

Transfer", Middleware 2019 - Industry Track, December 2019,

<https://arxiv.org/abs/1911.01064>.

[Abebe21] Ermyas Abebe, Yining Hu, Allison Irvin, Dileban Karunamoorthy,

Vinayaka Pandit, Venkatraman Ramakrishna, Jiangshan Yu,

"Verifiable Observation of Permissioned Ledgers", ICBC 2021,

May 2021, <https://arxiv.org/abs/2012.07339>.

[ABCH20] Ankenbrand, T., Bieri, D., Cortivo, R., Hoehener, J., and

T. Hardjono, "Proposal for a Comprehensive Crypto Asset

Taxonomy", May 2020, <https://arxiv.org/abs/2007.11877>.

[BVGC20] Belchior, R., Vasconcelos, A., Guerreiro, S., and M.

Correia, "A Survey on Blockchain Interoperability: Past,

Present, and Future Trends", May 2020,

<https://arxiv.org/abs/2005.14282v2>.

[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, Special Issue on Blockchain Technology,

Vol. 2, No. 24", December 2019,

<https://doi.org/10.3389/fbloc.2019.00024>.

[HTLC21] "Hash Time Locked Contracts", Bitcoin Wiki

<https://en.bitcoin.it/wiki/Hash\_Time\_Locked\_Contracts>.

[IDevID] Richardson, M. and J. Yang, "A Taxonomy of operational

security of manufacturer installed keys and anchors. IETF

draft-richardson-t2trg-idevid-considerations-01", August

2020, <https://tools.ietf.org/html/draft-richardson-t2trg-

idevid-considerations-01>.

[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

Venkatraman Ramakrishna

IBM Research - India

Email: vramakr2@in.ibm.com

Thomas Hardjono

MIT

Email: hardjono@mit.edu