Report of the Task Force

Global Implementation of Travel Rule Standards

November 23rd, 2021

Preface

Task Force Global Implementation of Travel Rule Standards (GI-TRUST) collaborates with global and local organizations to refine the standards of the *travel rule*, which requires financial institutions and virtual asset service providers (VASPs) to identify originators and beneficiaries of virtual assets (VAs).

The Group of 20 (G20) declared in 2018 that countries should regulate VAs and VASPs in line with Financial Action Task Force's (FATF) regulatory standards. Responding to their declaration, in 2019, FATF extended its Recommendation 15 (i.e., New Technologies) and Recommendation 16 (i.e., the Travel Rule), suggesting that countries apply their financial regulations to VAs and VASPs. Finally, the G20 declared in 2019 that countries should adopt the amendment of FATF's recommendations.

However, the FATF expressed concern that progress in adopting the travel rule has been slow. FATF's recommendations might fail if the world allows an extended grace period, allowing VASPs to move from strict countries to lenient countries. It is called a *sunrise* issue. Therefore, FATF announced its Updated Guidance for a Risk-Based Approach on October 28th, 2021, to shorten the sunrise by clarifying its regulatory standards.

Jung Hweon Jeon (Committee Chairperson, KBCA) and some experts hailed the more explicit standards of FATF yet reached a consensus that a genuine challenge is implementing the travel rule. They consider that technology cannot embody a regulation framework unless it fits relevant technological architecture, and the market hardly adopts the technology unless it leaves the conflict between regulations and economic principles. As a result, they concluded that G20, FATF, and countries need practical guidance implementing the travel rule standards in the market worldwide.

Task Force GI-TRUST aims at designing the practical guideline for the global implementation of travel rule standards in voluntary collaboration with virtual asset and AML/CFT experts: i.e., Jung Hweon Jeon (Committee Chairperson, KBCA) as the Task Force Team's Chairperson; Anson Zeall (Chairperson, IDAXA), Sandra Ro (CEO, GBBC), So Young Kim (Director of KPC4IR, KAIST), Jong Goo Yi (Lawyer, Kim & Chang), and Jeong Ha Lee (Former Director, KoFIU) as Vice-Chairpersons. GI-TRUST also invite experts from various domains as the Task Force Team Members: i.e., Kibae Kim (Principal Researcher of KPC4IR, KAIST), Joel Chung (President, KCAMS), Min Seob Lee (Senior Consultant, Lawfirm Yulchon), and Seok Hae HWANG (President, Datamation Co. Ltd.).

Task Force GI-TRUST approaches a comprehensive solution by listening to the opinions of various stakeholders surrounding the travel rule. The Task Force expects its practical recommendations will support G20, FATF, countries' regulatory bodies, and their markets to plan seamless and harmonious regulations for VAs and VASPs. Furthermore, the Task Force will pilot the interoperation of travel rule solutions on Korean VASPs and extend its collaboration to FATF, G20, and the countries leading the virtual assets and their regulations to prove the feasibility of their recommendations.

Participating Organizations:
Korea Blockchain Association
KAIST's Korea Policy Center for the Fourth Industrial Revolution
International Digital Asset Exchange Association
Global Blockchain Business Council
Lawfirm Kim & Chang
Korea Certified Anti-Money Laundering Specialist
Lawfirm Yulchon
Datamation Co. Ltd.

Citing Reference:

GI-TRUST, KBCA (2021), Report of the Task Force Global Implementation of Travel Rule Standards, Seoul
https://kblockchain.org/upload_data/download_file/[KBCA]GITRUST_REPORT_2021_final_v.2.pdf

Table of Contents

Executive Summary

The report discusses the global implementation of travel rule standards to find the challenges and solutions to those travel rule standards. The travel rule is the Financial Action Task Force's (FATF) regulatory recommendation requiring financial institutions and virtual asset service providers (VASPs) to identify originators and beneficiaries of virtual assets (VAs) for regulators to trace the travel of assets. The report focuses on the inherent properties of travel rule standards and VASPs' managerial behavior and recommends the cooperation of various stakeholders to elaborate the travel rule message format and make the standards compatible and interoperable.

The report consists of four parts. The first two parts analyze financial regulations, virtual asset service architecture, and commercial travel rule standards. Financial regulations have supervised stable financial markets, relying on the payment messages transferring among financial institutions built and governed by jurisdictions. On the other hand, VAs and VASPs fade in and out of the market liberally (dynamicity) and cover their services across jurisdictions (cross-borderness) without exchanging payment messages (messagelessness). Therefore, travel rule service providers (TRSPs) suggested various standards supporting the exchange of payment messages for financial regulations to apply to VAs and VASPs.

However, FATF (2021.07: Paragraph 129) warns on the "sunrise" issue, as the market adoption has been stretching for two years, although the market launched several travel rule standards. Therefore, in the third part, Task Force Global Implementation of Travel Rule Standards (GI-TRUST) shapes four problems and derives solutions to untie the two years of the travel rule's stalemate:

- (Problem) The market is challenging to select a few travel rule standards because their inseparable workflow constrains the choices of pairs of VASPs.
  - » (Solution) GI-TRUST recommends that regulatory standards guide travel rule standards to be compatible by inserting multi-channel integration (MCI).

- (Problem) The travel rule should interoperate with customer due diligence (CDD), risk assessment (RA), and suspicious transaction report (STR) processes for the AML/CFT mission.
  - » (Solution) GI-TRUST recommends adding interoperability to regulatory standards and designing a modular architecture to reduce the complexity in the interoperation.

- (Problem) A flexible message format standard obstructs mapping between message formats and discourages the innovation for the compatibility and interoperability of travel rule standards.
  - » (Solution) GI-TRUST recommends applying ISO 15022 (SWIFT message) to sophisticate the message format, and managing VASP and TRSP registries to support their trust.

- (Problem) Regulations evolve following fast-advancing technologies, and the existing regulatory framework might not fit VAs and VASPs' architecture in the end.
  - » (Solution) GI-TRUST introduces a trusted third party as a temporary solution to non-obliged entities but recommends stakeholders to discuss the future of regulations in the long view.

GI-TRUST provides both theoretical and practical implications. From an academic perspective, the report suggests a standardization framework harmonizing financial regulations with blockchain governance. In addition, the report provides regulators, entrepreneurs, and associations with a comprehensive approach to implementing the travel rule from a practical perspective. The report does not contribute a reference architecture of the travel rule to the blockchain society but recommends the society cooperate to shape a reference architecture opening the opportunities to VASPs, TRSPs, and any service providers of artificial intelligence and financial big data.

1. Introduction

The Financial Action Task Force (FATF) revised its recommendations to include virtual assets (VAs) virtual asset service providers (VASPs) in financial regulations in June 2019. The recommendations guide VASPs to implement the travel rule and know-your-customer (KYC) processes, defining what and how to aggregate and share when virtual assets transfer between customers.

Countries have applied a package of regulations, which FATF recommends, to financial institutions. They require financial institutions to the risk-based approach (RBA), the customer due diligence (CDD), the travel rule, the competent authority's supervision, and the international cooperation between the authorities. The authorities can then identify the actual ownership of assets (CDD) and trace the assets' transfer from person to person (Travel Rule) for anti-money laundering (AML) and watch risk filtering (WLF) in an efficient manual according to the risks (RBA), even when the assets travel across countries.

Centralization is a prerequisite for implementing financial regulations. A financial institution installs a hierarchical organization with clear responsibilities to collect, record, and report specific financial information of their customers, requiring privacy protection. Information systems support the organization in securely processing a large size of financial data. A competent authority then efficiently licenses, monitors, and supervises the centralized organizations. The centralized organization and the regulation by institutions reassure customers and governments.

On the other hand, the decentralized architecture of blockchain takes the opposite approach. Blockchain distributes the ledgers into a peer-to-peer network after pseudonymizing its customers' information and dilutes the responsibilities of each machine for RBA, CDD, and the travel rule in the decentralized architecture. FATF underlined VASPs to apply their standards in 2019 because, at the moment, most operate in a centralized organization like financial institutions. However, a VASP had to consider its customers' trust relying on pseudonymity, and the regulations face the market dynamics of VASPs.

Authorities can trace VAs with high cross-border mobility only if they identify genuine VASPs and real names of customers, i.e., an originator and a beneficiary of a transaction. Therefore, FATF's recommended that VASPs exchange payment messages off-chain when their customers transact on-chain to support tracing pseudonymized transactions. However, it recently expressed concerns about the unsatisfactory progress of travel rule implementation.

FATF listened to the market's requests to clarify the regulatory standards and responded to them with its Updated Guidance for a Risk-Based Approach (FATF, 2021.10). For example, it suggests VASPs should apply the cross-border standard to virtual asset transfers (FATF, 2021.10: Paragraph 169) and use their CDD process to verify their customers for implementing the travel rule (FATF, 2021.10: Paragraph 182). Furthermore, the guidance extends the scope of subjects from only centralized VASPs to decentralized VASPs and non-obliged entities (FATF, 2021.10: Paragraphs 179, 203-204).

However, the task force Global Implementation of Travel Rule Standards (GI-TRUST) is concerned about the economic complexity in the travel rule's implementation remaining even after the regulatory clarification. VAs and VASPs emerged in the market, sometimes conflicting with regulations, while financial institutions have evolved according to economic context for several centuries (Goldsmith, 1973). Therefore, enforcing the standard by the government would be likely to face resistance from the market (Alpen, 2021; Marquez, 2021).

Furthermore, the market should address their adoption in two constraints. First, there have already launched several travel rule standards, and they rely on various technologies in various architectures, e.g., OpenVASP, TRISA, Travel Rule Protocol (TRP), Sygna, VerifyVasp. Second, countries implement the travel rule in the timeline of institutionalizing VASPs, e.g., for Korea, by March 25th, 2022, so the

deadline of the travel rule is inflexible because it should accompany other regulations, e.g., taxation (Park, 2021). Therefore, the market should either select one of the incompatible standards or seek a technological solution to interoperate those standards.

GI-TRUST highlights the workflow of travel rule standards and the managerial behavior of VASPs adopting the standards. According to our architecture analysis, a travel rule standard mixes encryption, decryption, and verification inseparably. Moreover, it is hard for a travel rule service provider (TRSP) to adopt its competitor's standard because inseparability means replacing its standard with a competitor's one in the entire workflow. Therefore, the flooding standards for the travel rule constrain VASPs' choice and delay implementing the travel rule.

The solution to the travel rule's slow implementation is re-arranging the standards across their workflow:

- First, implementing the travel rule requires a pair of VASPs in the transaction to adopt a common standard. However, Because of the inseparable adoption by pairs, travel rule standards hardly share or dominate the market by network externalities (Katz and Shapiro, 1985; Katz and Shapiro, 1994). The guidance of FATF (2021.10: Paragraph 284-285) for technological standards such as TLS/SSL and X.509 do not resolve the inseparability issue as the inseparable workflow includes X.509 atop the transmission layer of TLS/SSL. Therefore, GI-TRUST recommends compatibility among standards by inserting multi-channel integration (MCI) (Figure 12).

- Second, the travel rule is a core of financial regulation's missions for Anti-Money Laundering and the Countering the Financing of Terrorism (AML/CFT). Therefore, the travel rule process should seamlessly interoperate with the processes for customer due diligence (CDD), risk assessment (RA), and suspicious transaction report (STR). Otherwise, cyber-attacks might target the junction of the travel rule with other AML/CFT processes. Thus, GI-TRUST recommends the guidance for interoperability (Table 5) and designs a modular architecture to reduce the complexity in the interoperation among AML processes (Figure 14).

- Third, GI-TRUST underlines the message format. The architecture analysis results suggest that commercial standards for the travel rule mainly synchronized their variables by the Inter-VASP Message Standard 101 (IVMS101), allowing a flexible message format implementation for the variables' values. However, the message format's diversity obstructs the translation and modification of travel rule messages, discouraging the innovation for compatible and interoperable standards. Therefore, GI-TRUST suggests extending the travel rule message according to VA's context (Table 6) and applying ISO 15022 (SWIFT message) to virtual assets (Table 8 and Table 9).

- Fourth, regulations evolve following fast-advancing technologies. For example, FATF (2021.10: Paragraph 202-204) embraces non-obliged entities such as private wallets, while FATF (2020) highlighted VASPs registering at Financial Intelligence Units (FIUs). GI-TRUST trust introduces a trusted third party (e.g., telecommunication providers) to support the travel rule for non-obliged entities (e.g., unhosted wallets) as a near-term solution (Figure 16). However, it urges planning a longer-view solution to the fast-growing VA market, where decentralized applications (DApps) and non-fungible tokens (NFT) might dominate the financial market (Figure 17).

GI-TRUST casts practical and academic implications. From a practical perspective, the solutions assist in designing virtual asset services complying with financial regulations and blockchain principles. They will mitigate the "sunrise problem" that leaves VASPs hiding in a darker country in a gray period of the travel rule implementation (FATF, 2021.07: Paragraph 129). Academically, the travel rule needs the co-production approach from technologies, businesses, and regulations (Jasanoff, 2006). Implementing the travel rule suggests in-depth conversations among stakeholders to shape a comprehensive regulation, business, and technology framework. Global organizations should lead the cooperation.

2. Financial Institutions and Virtual Asset Service Providers

2.1. Payment Among Conventional Financial Institutions

The Conventional Payment Method Spontaneously Satisfies the Travel Rule.

The travel rule was designed for conventional payment methods based on centralized and intermediary-based processes. Let us consider the simplest example of payment in South Korea (Figure 1). The service consists of three processes: payment, clearings, and settlement. The ordering bank sends the payment message to the beneficiary bank through the Korea Telecommunication and Clearings Institute (KTCI). The payment is concluded after the clearings by the KTCI and the settlement by the Bank of Korea (BOK). The payment message contains the customers' identity and account, and the value of transferred assets as the travel rule requires.

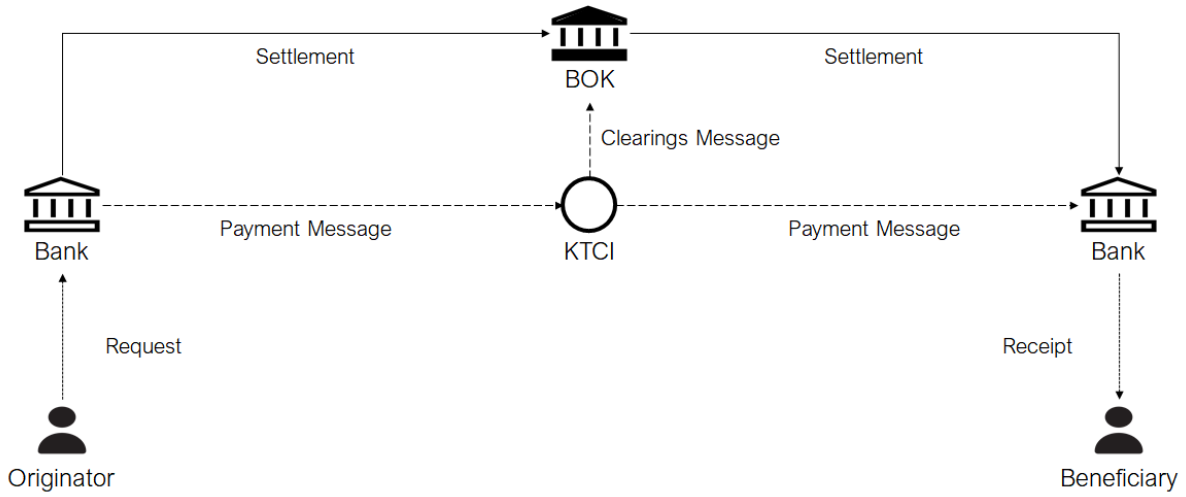

Figure 1. The Workflow of the Simplest Conventional Retail Payment (Icons sourced from the WEB).

The Conventional Payment Method Requires Trusted Third Parties for International Services.

The extension of conventional payment services needs more costs to trusted third parties. Moreover, the intervention of trusted-third parties stretches the transfer process to settle the payment that existing trusted third parties do not cover. As a result, the conventional payment system involves inefficiency increasing as the service coverage widens—Figures 2 to 4 show three scenarios of the conventional payment relying on trusted third parties.

The first scenario is a cross-border remittance (Figure 2). Because the payment-clearings-settlement system is engaged in an individual jurisdiction, the originator's and beneficiary's banks need intermediary banks. Each intermediary bank at the originator's and beneficiary's sides exchanges the payment message with house banks according to the process of domestic transfer (Figure 1). Moreover, the two intermediary banks exchange the payment messages through the platform and message standard of the Society for Worldwide Interbank Financial Telecommunication (SWIFT). Finally, they conclude their payment by the intervention of an international trusted third party, i.e., the Bank for International Settlements (BIS).

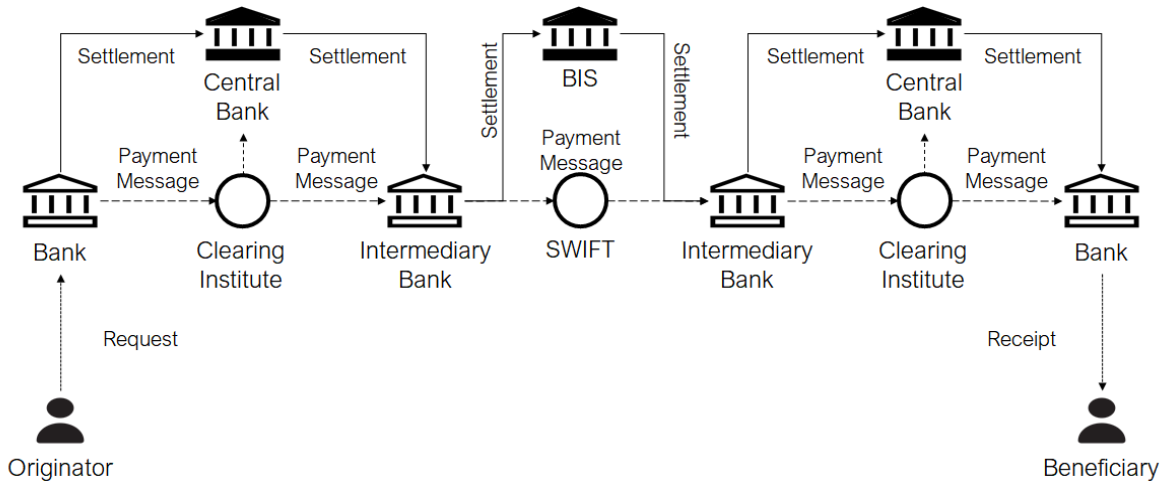

Figure 2. The Workflow of the Conventional Retail Payment Across Jurisdictions (Icons sourced from the WEB).

The second scenario is that a conventional payment market is adopting new information systems for payment. For example, a debit card inserts a value-added network (VAN) between a device for authentication and banks (Figure 3). If the debit card and its reader authenticate, an originator can pay for a beneficiary, and a beneficiary can receive it; respectively, the device sends their payment message to the originator's and beneficiary's banks and the clearing institute through a value-added network (VAN). The remaining process is the same as the most straightforward payment workflow in Figure 1.

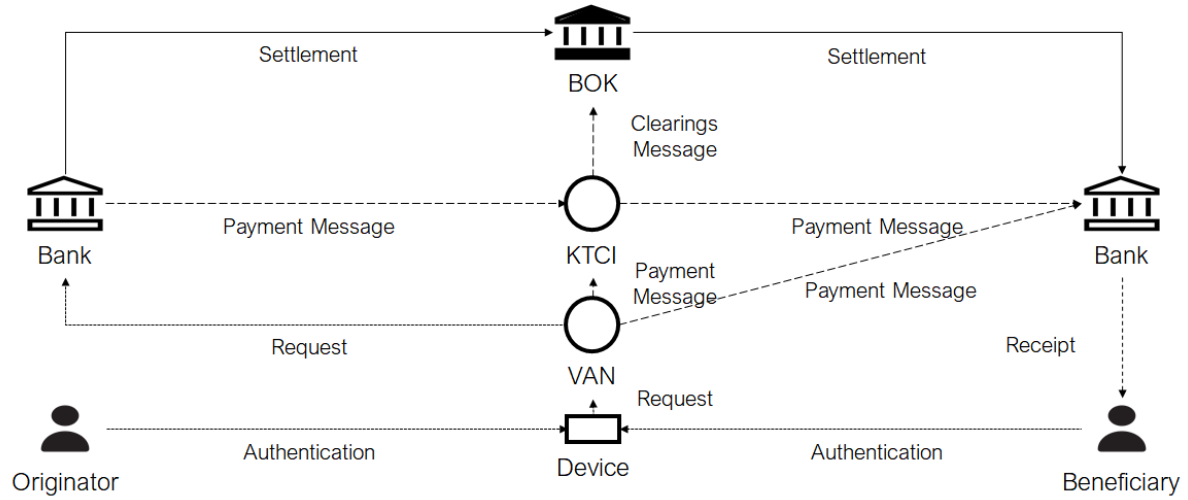

Figure 3. The Workflow of the Conventional Retail Payment by a Debit Card (Icons sourced from the WEB).

The third scenario simplifies the payment process by replacing a clearing institute and a central bank with a private trusted third party. For example, a credit card company clears the payment to send it to its partner bank when it receives the payment message from an originator and the request message from a beneficiary (Figure 4). The partner bank then transfers the payment to the beneficiary's bank according to a large-value payment system (e.g., Korea's BOK-Wire+, US Federal Reserve System's Fedwire, European Central Bank's TRAGET2).

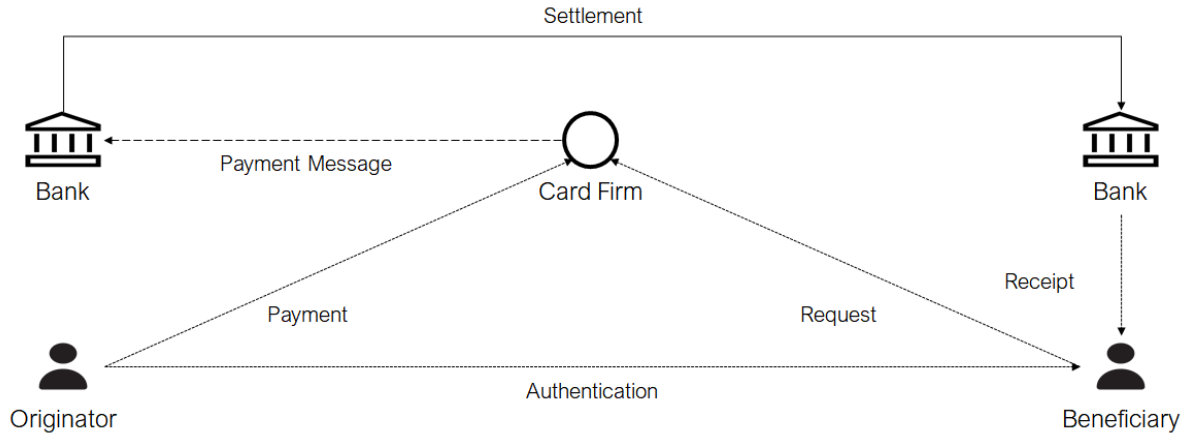

Figure 4. The Workflow of the Conventional Retail Payment by a Credit Card (Icons sourced from the WEB).

2.2. Blockchain-Based Payment Among Virtual Asset Service Providers

Blockchain-Based Payment Compresses Payment, Clearings, and Settlement in Algorithms.

Blockchain compresses payment, clearings, and settlement into its decentralized architecture. A blockchain's peer-to-peer network settles the payment irreversibly by containing their transactions in distributed ledgers. If an originator just dispatches a payment request to a blockchain system, it concludes as the transaction between an originator and a beneficiary is securely and immutably stored in the blockchain. The architecture does not need additional trusted-third parties but just requires those customers to access the Internet.

However, the actual workflow of the blockchain-based payment is more complicated than the ideal process. An originator needs the intervention of a virtual asset service provider (VASP) to transform her/his asset in a type (e.g., fiat money, or a virtual asset other than the requesting one) to the blockchain's virtual asset before transferring it to a beneficiary (Figure 5). The beneficiary also transforms the received virtual asset to another type through its house VASP. If the VASPs transform fiat money into a virtual asset and vice versa, they also need to cooperate with financial institutions.

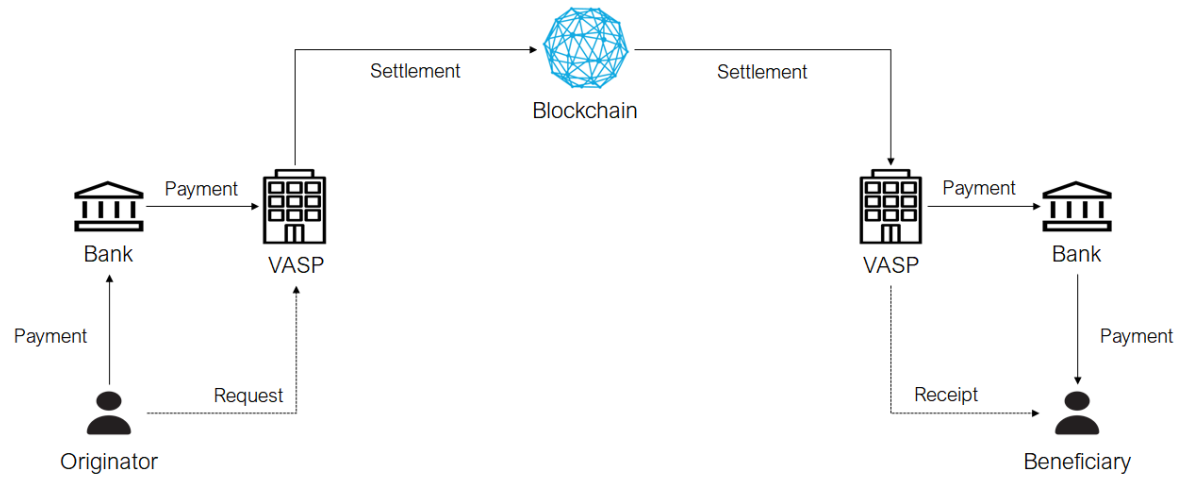

Figure 5. The Workflow of the Blockchain-Based Payment through VASPs (Icons sourced from the WEB).

The intricate architecture results from the existing financial regulation's focus on fiat money. Customers should exchange fiat money with virtual assets through VASPs before their VA transactions. Moreover, the government entrusts financial institutions with fiat money services and requires VASPs a license for their fiat money services, providing business advantages. For example, thirty-eight VASPs granting permission only for VA are at the cross-road of life, while four big VASPs maintain market dominance as the Korean Financial Intelligence Unit (KoFIU) admits their fiat money services complying with Korea's ARUSFI (Im, 2021). Korea's ARUSFI (2020) requires the information security management system (ISMS) and a real-name verification deposit and withdrawal account to register their businesses by October 25th, 2021.

Blockchain Stresses Regulations with Messagelessness, Cross-Borderness, and Dynamicity.

Blockchain stresses financial regulations with its three properties:

- First, payment messages disappear in the blockchain-based payment architecture. It is because blockchain does not need the intervention of trusted third parties (e.g., clearing institutes, central banks, and international financial institutions). Blockchain's distributed ledgers and consensus algorithms do not create payment messages to transfer among VASPs. Instead, the blockchain system returns to the public the history of the transfer of virtual assets among its clients. Therefore, it pseudonymizes the clients to protect their privacy from the public seeing the distributed ledgers.

- Second, blockchain supports efficient cross-border payment. Conventional payment across jurisdictions requires the intervention of trusted third parties to resolve the problems emerging from the regulatory difference (Figure 2). However, the blockchain-based payment architecture does not leave room for the intervention of trusted third parties (Figure 5). Instead, the architecture requires access to an originator and a beneficiary to the blockchain by their VASPs through the Internet. Therefore, a competent authority cannot trace the source of assets nor supervise suspicious transactions when the transaction passes out its jurisdiction.

- Third, the market gives birth to VASPs, while regulations build a financial institution. Financial institutions rely on relevant regulations. For example, the legal basis of the Korea Development Bank (KDB) is the Korea Development Bank Act accompanying the Banking Act, the Act on Real Name Financial Transactions and Confidentiality, and other financial regulations. However, GOPAX, a Korean crypto-exchange, is a service of Streami, a small enterprise of computer programming, which the Framework Act on Small and Medium Enterprises might apply to, for example. Therefore, Korea lacked the basis to apply financial regulations to the VASP before adopting FATF's recommendations.

In conclusion, the governance of blockchain is the opposite of financial regulations. On the one hand, conventional financial regulations impose duties to know their customers and protect their privacy on financial institutions. For example, a bank aggregates a customer's real name and postal address when s/he opens an account and requests a financial service. On the other hand, blockchain pseudonymizes its customers' accounts to protect their privacy in the data distributed across a peer-to-peer network.

The conventional audit system is hard to be implemented in blockchain-based virtual assets. Blockchain can not collect, record, and share its clients' real names because they violate blockchain's principle for decentralizing pseudonyms. Financial regulations rely on real names and transparent transactions to trace the virtual assets across real natural and legal persons. Domestic and international financial institutions are concerned that they might fail to govern the financial security on the virtual assets with the architecture opposite to their long-history regulations. FATF's amendment of recommendations responds to the worries of those regulatory limitations.

3. The Architecture of the Travel Rule Standards

3.1. Designing the Framework of Financial Regulations

The FATF Recommends VASPs to Comply with the Regulations for AML/CFT.

The Financial Action Task Force (FATF)'s amended recommendations embrace virtual assets (VAs) and virtual asset service providers (VASPs) (FATF, 2012-2020). Each jurisdiction should prepare measures proportional to the risks of VAs and VASPs, i.e., in a risk-based approach (RBA) (FATF, 2012-2020: Recommendation 1). The measures should accompany the domestic collaboration of a Financial Intelligence Unit (FIU) with national agencies enforcing laws and the international collaboration with other jurisdictions' FIUs (FATF, 2012-2020: Recommendation 2, 36-40).

The first step of institutionalization is that VASPs are licensed by or register at the Financial Intelligence Unit for their money or value transfer services (MVTS) (FATF, 2012-2020: Recommendation 14-15). VASPs are built by the market, so likely to be out of regulations, while financial institutions start from regulations (FATF, 2012-2020: Recommendation 26). Therefore, the FIU should identify VASPs to be ready to apply its Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) actions to those identified VASPs.

The next step is identifying customers by Customer Due Diligence (CDD) (FATF, 2012-2020: Recommendation 10). Like financial institutions, a VASP should collect the information of customers' identity, beneficial owner, and the purpose of a business relationship when it establishes the relationship and receives an occasional transaction request not less than 1,000 USD (FATF, 2012-2020: Recommendation 10, Interpretive Note 15). The VASP may collect the information from its customer and rely on trusted third parties (e.g., banks) (FATF, 2012-2020: Recommendation 17). Afterward, the VASP can report FIU a suspicious transaction by watch list filtering (WLF) and risk assessment (RA).

The Travel Rule Completes the AML/CFT Regulation for VAs and VASPs.

The final step is identifying the source of the asset, i.e., the so-called *travel rule.* FATF's Updated Guidance clarifies the travel rule from authorities' and VASPs' perspectives (FATF, 2021.10). At the authorities' side, FATF's Updated Guidance suggests the details of the travel rule (Table 1). For example, a country should add non-obliged entities (e.g., unhosted wallets) to the travel rule's coverage (FATF 2021.10: Paragraphs 179, 203), while FATF (2012-2020: Recommendation 15) focuses on the VASPs with centralized governance. A country should also apply the rules for cross-border wire transfers to all VA transfers (FATF, 2021.10: Paragraphs 169, 179) and require a VASP to verify its customer relying on its CDD process on the travel rule process, which FATF (2012-2020) did not comment.

At the VASPs' side, FATF's Updated Guidance suggests a technology-neutral approach to the travel rule (Table 2). Thus, for example, a VASP can adopt any technology such as application programming interface (API), transport layer security and secure sockets layer (TLS/SSL) connections, X.509 protocols, and asymmetric cryptography using private and public keys, either atop a DLT platform, a non-DLT platform, or through APIs (FATF, 2021.10: 202, 285). What counts is that those technologies for VASP's compliance with AML/CFT regulations should satisfy the accuracy, security, stability, and follow-up requirements (FATF, 2021.10: 283, 284).

Table 1. Significant Changes in the Travel Rule at the Authorities' Side between FATF Updated Guidance (2021.10) and FATF Recommendations (2012-2020).

Category	FATF Updated Guidance	FATF Recommendation
Regulation Coverage	The travel rule applies to VA transfers between VASPs, between a VASP and an obliged entity (e.g., a bank), and between a VASP and a non-obliged entity (e.g., an unhosted wallet) (FATF, 2021.10: 179).	The travel rule applies to ordering and beneficiary VASPs, and according to the context, they are the VASPs with a centralized organization licensed by or registered at the FIU (FATF, 2012-2020: INR 15 7. b).
Regulation Level	The rules for cross-border wire transfers apply to all VA transfers (FATF, 2021.10: 179).	FATF (2012-2020) does not explicitly comment on it.
CDD Duties	An ordering VASP verifies the originator's identity by its CDD process (FATF, 2021.10: 182), while a beneficiary VASP verifies the beneficiary's identity by its CDD process (FATF, 2021.10: 183). In addition, both ordering and beneficiary VASPs should filter the watchlist in sanctions and report suspicious transactions (FATF, 2021.10: Table 1).	FATF (2012-2020) does not explicitly comment on it.
Transmission Duties	An ordering VASP must submit the required information to the beneficiary institution immediately and securely (FATF, 2021.10: 184)., where 'immediately' means prior to or simultaneously with the VA transfer (FATF, 2021.10: 185) and 'securely' means encouraging authorized readability and impeding unauthorized disclosure (FATF, 2021.10: 186).	An ordering VASP must submit the required information to the beneficiary institution immediately and securely (FATF, 2012-2020: INR 15. 7. B). However, the paragraph does not define what 'immediately' and 'securely' mean.

Table 2. Significant Changes in the Travel Rule at the VASPs' Side between FATF Updated Guidance (2021.10) and FATF Recommendations (2012-2020).

Category	FATF Updated Guidance	FATF Recommendation
Technology Neutral Approach	A VASP can and should choose any technologies for the travel rule: either the DLT platform, an independent non-DLT platform, or an application programming interface (FATF, 2021.10: 282). They can also harness existing technologies: e.g., public and private keys, TLS/SSL connections, X.509 certificates, and API technology (FATF, 2021.10: 285).	FATF (2012-2020) does not explicitly comment on it.
Performance Requirement	A technological solution should support identifying a counterparty VASP accurately, securely, and stably submitting travel rule messages, sometimes to multiple entities, and maintaining a follow-up channel (FATF, 2021.10: 283). In addition, the technological solution should also "ensure effective scrutiny of transactions to identify" suspicious transactions (FATF, 2021.10: 284).	FATF (2012-2020) does not explicitly comment on it.

† Submitting: The information can be submitted directly or indirectly, with optional attachment to VA transfers.

Jurisdictions Legislate the FATF's Standards Abiding by their Regulatory Frameworks.

Most worldwide jurisdictions have immediately responded to the FATF's amendment of recommendations since 2019 (Table 3). They set the information share threshold at 1,000 USD/EUR and require VASPs to immediately obtain and retain personal information. For example, Switzerland and South Korea amended their regulations: Anti-Money Laundering Ordinance of the Financial Market Supervisory Authority (AMLO-FINMA) and the Act on Reporting and Using the Specific Financial Information (ARUSFI), respectively. In addition, Singapore and the USA proposed regulations: i.e., the Notice to Holders of Payment Service Licence (PSN02) and the Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies (FinCEN, 2019).

Table 3. Examples of Jurisdictions' Response to FATF's Amendment of Recommendations †

	FATF's Travel Rule	Switzerland's AMLO-FINMA	U.S. 31CFR	Singapore's PSN02	South Korea's ARUSFI
Threshold to Share the Information	• Threshold should be less than 1,000 EUR, 1,000 USD, or their corresponding values.	• 1,000 CHF	• 3,000 USD (for beneficiary VASP locating in the USA; FinCEN should reduce the threshold to 250 USD.)	• 1,500 SGD (for beneficiary VASP locating in Singapore)	• 1,000,000 KRW, or its corresponding value (complying with the threshold of beneficiary's jurisdiction)
Originator's Information	• Person Name • Account Number (wallet address) • Person Identifier (geographic address, national ID number, or date and place of birth for natural persons; and legal entity identifier for legal persons)	• Person Name • Account Number (wallet address) • Personal Identifier (geographic address; otherwise, either customer number or national identity number)	• Person Name • Account Number • Personal Identifier (physical address) • Ordering VASP's Identity • Additional Information (amount of transfer, execution date)	• Person Name • Account Number (wallet address) • Personal Identifier (either geographic address, identity card number, birth certificate number, passport, or date and place of birth)	• Person Name • Wallet Address • Personal Identifier (resident registration number for natural persons; corporate registration number for legal persons; and passport number or foreigner regist. number for foreigners) in the Condition of Request.
Beneficiary's Information	• Person Name • Account Number (wallet address)	• Person Name • Account Number (otherwise, transaction-related reference number)	• Person Name • Account Number • Beneficiary VASP's Identity • Any Unique Identifier	• Person Name • Account Number (wallet address)	• Person Name • Wallet Address
Time to Share the Information	• Ordering VASP shares the information 'immediately,' i.e., prior, simultaneously, or concurrently with the transfer.	• AMLO-FINMA does not express the time to share explicitly, but a VASP should submit it immediately or at least three business days after the request, according to the context of Article 10. 2.	• Ordering VASP shares the information 'immediately,' i.e., at the time of the transmittal of virtual assets.	• Ordering VASP shares the originator and beneficiary's names and wallet addresses immediately. • Ordering VASP submit originator's identifier within three biz. days after the request.	• Ordering VASP shares the originator and beneficiary's names and wallet addresses immediately. • Ordering VASP submit originator's identifier within three biz. days after the request.
Actions Required	• Ordering VASP verifies the accuracy of the originator's information, and beneficiary VASP the accuracy of the beneficiary's information. • Each VASP filters the watch list in sanction and reports suspicious transactions in 3 business days. • Each VASP retains the records at least for five years.	• AMLO-FINMA does not express the responsibility for accuracy verification. • Each VASP filters the watch list in sanction and reports suspicious transactions (no comment on deadline). • Each VASP retains the records at least for ten years.	• Ordering VASP verifies the accuracy of the originator's information and beneficiary VSP of beneficiary's information. • Each VASP filters the watch list in sanction and reports suspicious transactions immediately if necessary. • Each VASP retains the records at least for five years.	• Ordering VASP submits both customers' information to beneficiary VASP, which examines the payment information for STR. • Each VASP filters the watch list in sanction and reports suspicious transactions in 3 business days. • Each VASP retains the records at least for five years.	• Ordering VASP submits both customers' information to beneficiary VASP, but the Act does not express accuracy verification. • Each VASP filters the watch list in sanction and reports suspicious transactions immediately. • Each VASP retains the records at least for five years.

† Sourced from: FATF, 2021.10; GWP, 2020; AMLO-FINMA, 2021; 31CFR, no date; PSN02, 2019; ARUSFI, 2020.

The USA shows a unique response to FATF's recommendations. The U.S. Treasury's Financial Crimes Enforcement Network (FinCEN) provided guidance clarifying that it applies the regulation for Records to be Made and Retained by Financial Institutions (31CFR1010.410) to hosted wallets for the transactions of 3,000 USD or more (FinCEN, 2019). Therefore, its travel rule defines only the originator's physical address as her/his identifier and requires ordering and beneficiary VASPs' identity same as for the wire transfer between banks. FinCEN is supposed to reduce the threshold from $3,000 to $250 to fit FATF's standard at $1,000. However, unhosted wallets remain conflicting between FATF's recommendation to cover it and FinCEN's guidance excluding unhosted wallets from its regulations.

South Korea Implements the Travel Rule on Two Information Systems.

South Korea shows another unique response. Its amendment of ARUSFI adds VAs and VASPs to the information systems that it regulates (Figure 6). On the one hand, a VASP should build its Information Security Management System (ISMS) operated by its Chief Information Security Officer (CISO) with its manual because a VASP deals with customers' personal information. The government regulates the system through certification by the Korea Internet & Security Agency (KISA).

On the other hand, the VASP should also install its financial information reporting system at which the chief and the session staff manage the personal information of its customers and partner VASP's customers, complying with the customer due diligence (CDD) and the travel rule, respectively. They also achieve watch list filtering (WLF), risk assessment (RA), and suspicious transaction report (STR). The Korea Financial Intelligence Unit (KoFIU) then supervises the VASPs in its registry and shares the information with competent authorities, such as Supreme Prosecutors' Office (SPO), Financial Services Commission (FSC), National Intelligence Service (NIS), and Korea Customs Service (KCS).

A VASP should open its real name verification deposit and withdrawal account service at a commercial bank regarding fiat money. However, the banks rejected the request to open the accounts of thirty-eight VASPs among forty-two VASPs certified ISMS by KISA due to VAs and VASPs' uncertainty. Therefore, those thirty-eight VASPs cannot provide fiat-money services, according to Korea's ARUSFI (2020).

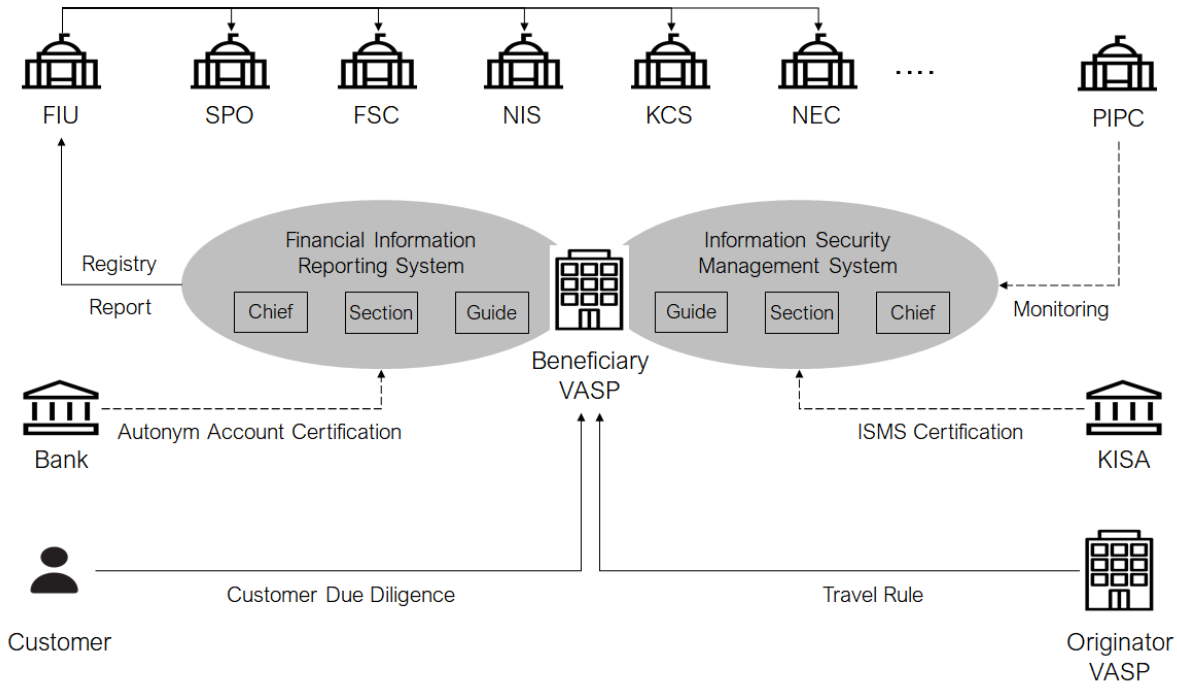

Figure 6. South Korea's Regulatory Framework for VASPs (Icons sourced from the WEB).

3.2. The Workflow and Specifications of Travel Rule Standards

The Travel Rule Inserts a Message Layer Between Virtual Asset Service Providers.

The market introduces travel rule protocols to support the virtual asset services complying with financial regulations. They insert a travel rule medium exchanging the payment messages, separated from the blockchain (Hardjono et al., 2021; Figure 7). If an originator and a beneficiary agree on their payment, the beneficiary sends the originator her/his name, account, and VASP (Steps 1-3). After receiving the originator's request, the originator and beneficiary VASPs open the session transferring their messages and verify their authenticity (Steps 4-9). If the messages are faultless, the ordering VASP concludes the payment by dispatching it on a designated blockchain (Step 10).

Encrypted Messages Transfer Through the Travel Rule Medium to Verify the Payment.

The VASPs' message exchange segment (Steps 4-9) consists of two parts. One is encrypting the travel rule message to send the counterpart. An ordering VASP collects the travel rule information and verifies its customer (Step 5). Moreover, it encrypts the message to request the beneficiary VASP the verification of its customer with attaching the originator's and beneficiary's information (Step 6). Once the beneficiary VASP decrypts and verifies the travel rule message from the ordering VASP, the beneficiary VASP encrypts the message containing its decision and more requested information to send it to the ordering VASP (Step 8). The ordering VASP then decrypts and verifies the message before dispatching the transfer on a blockchain.

The other part of the segment verifies the messages in two facets (Steps 5, 6, and 9). First, a VASP verifies the authenticity of the message when it receives the counterpart's encrypted message. For example, the originator and beneficiary VASPs share a public key to test if the message is invariant and sent by the proper partner. Second, a VASP also verifies the truth of the contents of the message. The VASP should decrypt and analyze the information, relying on its customers' databases in its financial information reporting system. Travel rule standards cover the former verification, and individual VASPs are responsible for the latter one.

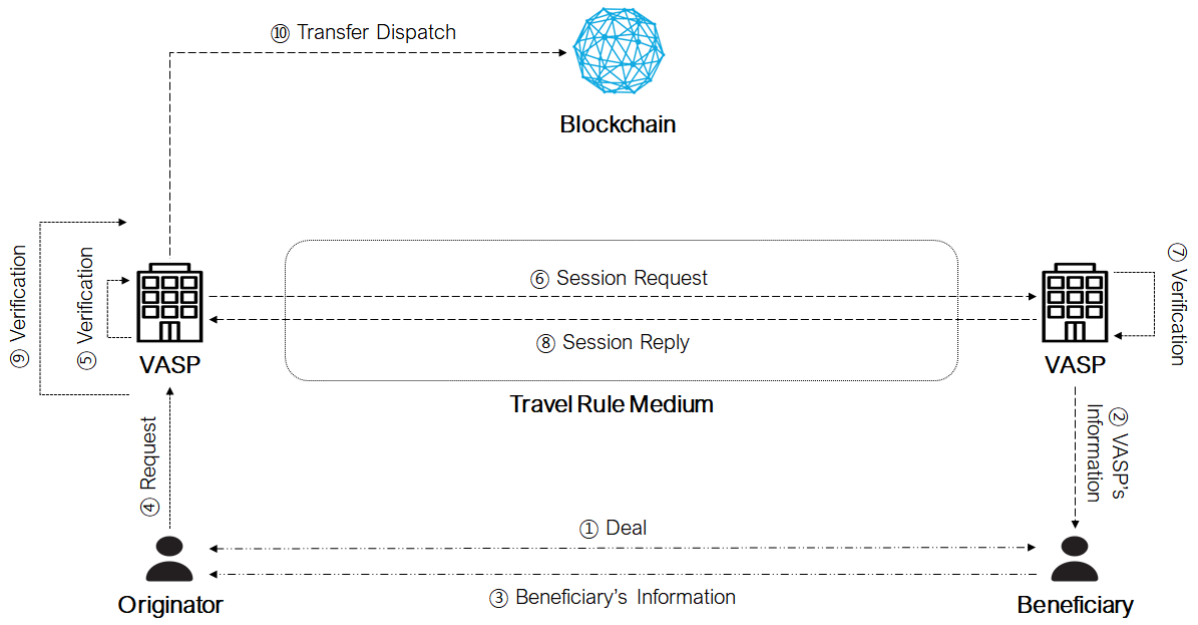

Figure 7. Workflow of a Travel Rule Service (Icons from the WEB).

The Implementation of the Travel Rule Includes the Relationships Between Banks and VASPs.

The travel rule works in a more complex situation than the description of Figure 7 because regulations also define the relationship between financial institutions and VASPs (Figure 5). On the one hand, for example, Korea binds a customer and a VASP by a bank (ARUSFI, 2020: Article 7.3.2). Therefore, the bank is responsible for evaluating the VASP's business before opening a VASP's real-name verification deposit and withdrawal account. The account helps KoFIU traces the virtual asset transfer (Figure 8).

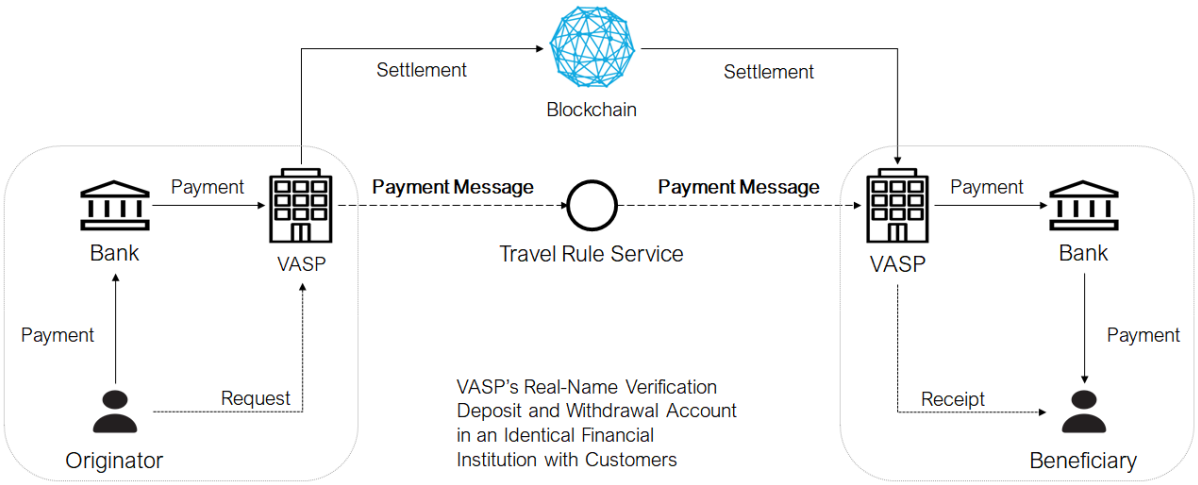

Figure 8. The Real Workflow of the Blockchain-Based Payment for Integrated Banks and VASPs.

On the other hand, multiple banks can also participate in blockchain-based payment (Figure 9). An originator transfers the fiat money from its bank to a VASP's bank before deploying blockchain-based payment if VASPs are separated from commercial banks, and the originator's bank is different from the VASP's bank. After the virtual asset transaction, the beneficiary can also receive the fiat money through her/his bank and the VASP's bank. Then the travel rule should continue to the pairs of banks and VASPs. FinCEN (2019), for example, does not ban the scenario despite the administrative complexity.

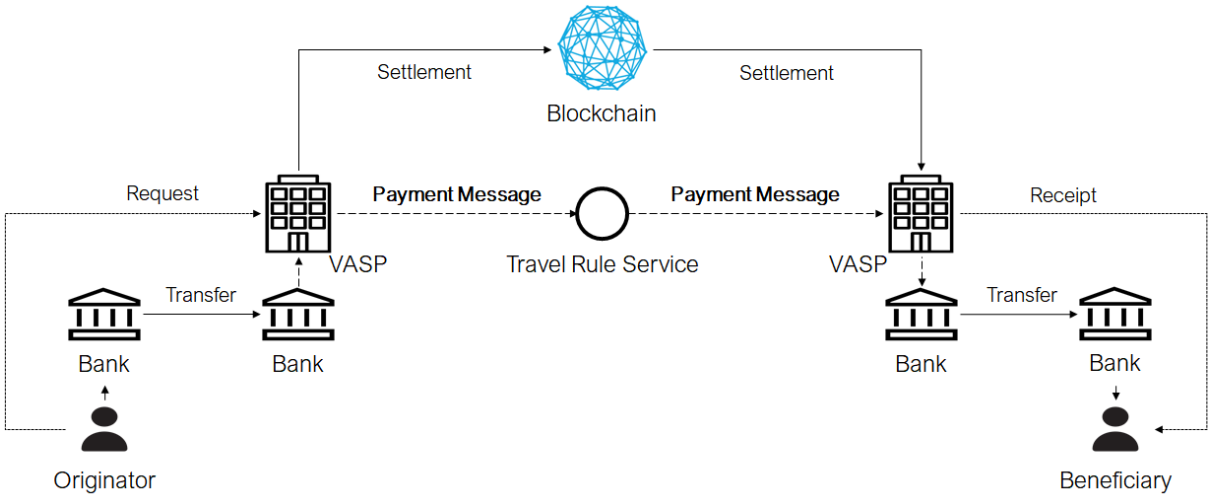

Figure 9. The Real Workflow of the Blockchain-Based Payment for Separated Banks and VASPs.

Travel Rule Standards Adopt Existing Standards for Message and Transmission.

GI-TRUST analyzed five existing travel rule standards: OpenVASP, Travel Rule Protocol (TRP), Travel Rule Information Sharing Architecture (TRISA), Sygna, VerifyVasp (Table 4). The analysis results in both universality and locality of those travel rule standards. On the one hand, they universally adopt existing technological standards for message and transmission according to FATF's (2021.10) technology-neutral approach.

First, existing travel rule standards mainly adopt Inter-VASP Message Standard 101 (IVMS101, https://intervasp.org/). FATF's travel rule recommends that VASPs obtain and retain originator and beneficiary's information (name, account number, and identifier such as geographic address). In addition, implementing the travel rule needs the information of VASPs in a transaction (name and address; and identity in the case of 31CFR1010.410). IVMS 101 defines the data structure and the variables involved in a blockchain-based payment message, complying with the International Organization for Standardization (ISO); e.g., ISO 8601 for dates, and ISO 3166-1 alpha-2 for countries.

Second, the travel rule standards mainly comply with FATF's (2021.10: Paragraphs 282-285) guidance on using existing technologies. For example, TRISA, OpenVASP, Sygna, and VerifyVASP encrypt and decrypt the payment message in an asymmetric cryptographic algorithm using pairs of public and private keys. Moreover, TRISA, TRP, Sygna, and VerifyVASP open the session at a transport layer of secure sockets layer and transport layer security (SSL/TLS) or hypertext transport protocol secure and transport layer security (HTTPS/TLS) for addressing and routing. As a result, VASPs transmit the payment message on the Internet, separated from the blockchain.

Verification Algorithms are Inseparable from Encryption and Identification Methods.

On the other hand, the inseparable procedure of encryption, identification, and verification localizes the travel rule standards, as a pair of VASPs should share a travel rule standard. First, the detail of the encryption algorithms is various across the travel rule standards. For example, Sygna encrypts the IVMS101 message with the elliptic curve integrated encryption scheme and the elliptic curve digital signature algorithm (ECIES/ECDSA). On the other hand, TRISA envelops the metadata, signature, and encrypted transaction data by hash-based message authentication code (HMAC).

The second feature is about certifying and verifying VASPs. Some of the protocols centralize managing the alliance server. For example, TRISA, Sygna Bridge, and VerifyVasp provide the alliance information with the certification of member VASPs to reassure a VASP that its counterpart VASP is reliable. The member VASPs can also update the counterpart VASPs' reliability in their enclave servers. On the other hand, TRP relies on enclave servers only, and OpenVASP uses smart contracts between VASPs for certification. Moreover, TRISA provides VASPs with centrally authorized certificates, while the other standards adopt mutual certification.

The workflow of travel rule standards suggests that verification is inseparable from the encryption, identification, and certification methods. A VASP can verify the counterpart VASP and its customer only once it decrypts the travel rule message. Therefore, the originator and beneficiary VASPs need to share a single protocol for the entire encryption, decryption, and verification process, as the verification process depends on the decryption of the encrypted message. The inseparability of procedures constrains a VASP to customize a segment of the travel rule workflow even if the message formats are translatable and share identical transmission protocols.

Table 4. Overview of the Travel Rule Standards

		TRISA	TRP	OpenVASP	Sygna	VerifyVASP
Authentication	Identity	KYV Certificate	IP Address	Ethereum Address	VAAI	VASP Code
	Certification	Central Authority	Mutual Certification	Mutual Certification	Mutual Certification	Mutual Certification
	Verification	Alliance and Enclave Server	Enclave Server	Smart Contract between VASPs	Alliance and Enclave Server	Alliance and Enclave Server
Transmission	Addressing	SSL/TLS	HTTPS/TLS	VAAN	SSL/TLS	HTTPS/TLS
	Routing	SSL/TLS	HTTPS/TLS	--	SSL/TLS	HTTPS/TLS
	Transport	Encrypted Message Envelope	API	Whisper	API	API
Message	Message Format	IVMS101	IVMS101	--	IVMS101	IVMS101
	Encryption and Decryption	HMAC with Public and Private Key Pairs	BECH32	SECP256K1/AESGCM 96BitNonce with Public and Private Key Pairs	ECIES/ECDSA with Public and Private Key Pairs	Public and Private Key Pairs
Platform Type (DLT, Non-DLT)		Non-DLT	Non-DLT	DLT	Non-DLT	Non-DLT
Decentralization (Very Decentral, Decentral, Mid, Central, Very Central)		Central	Very Decentral	Decentral	Mid	Mid
Complexity (Very Complex, Complex, Mid, Simple, Very Simple)		Mid	Simple	Complex	Simple	Simple

† Sourced from: GWP, 2020; Jevans, et al., 2020; TRP, no date; Riegelnig, 2019; CoolBitX, 2020; VerifyVasp, no date.

4. Solutions to the Global Implementation of Travel Rule Standards

4.1. Standard Translation for Compatibility

The Inseparable Architecture Requires the Consensus of VASP Pairs for Adopting a Protocol.

Adopting a travel rule standard needs the consensus between originator and beneficiary VASPs as it supports their communication. Moreover, they should rely on a single protocol as encryption, decryption, identification, certification, and verification are inseparable. Therefore, a pair of VASPs are more likely to be locked in one standard than usual *de facto* standardization scenarios that depend on individuals' standard adoption by a market mechanism, such as network externalities (Katz and Shapiro, 1985; Katz and Shapiro, 1994).

Let us refer to basic scenarios of standardization (Figure 10) to compare them with the adoption by pairs in the condition of inseparable workflow. On the one hand, a standardization body (e.g., ISO, ITU-T, and IEEE Standard Association) can define the standard (Top Left in Figure 10). In the case of travel rule standards, an authority selects standard α instead of standard β. A political consideration might interfere with that process of standardization. It is called the *de-jure* standardization.

On the other hand, the market can select the standard instead of a central authority. It is called *de-facto* standardization. Network externalities work for that process (Katz and Shapiro, 1985; Katz and Shapiro, 1994). First, the market selects the travel rule standard α according to the number of VASPs adopting it because accessing VASPs through a travel rule standard is more beneficial for a VASP (Bottom Left in Figure 10). It is called a *direct* network externality. Second, the market selects the travel rule standard β that supports more blockchains, *so to speak*, if a VASP earns more benefit from more blockchains. It is called an *indirect* network externality.

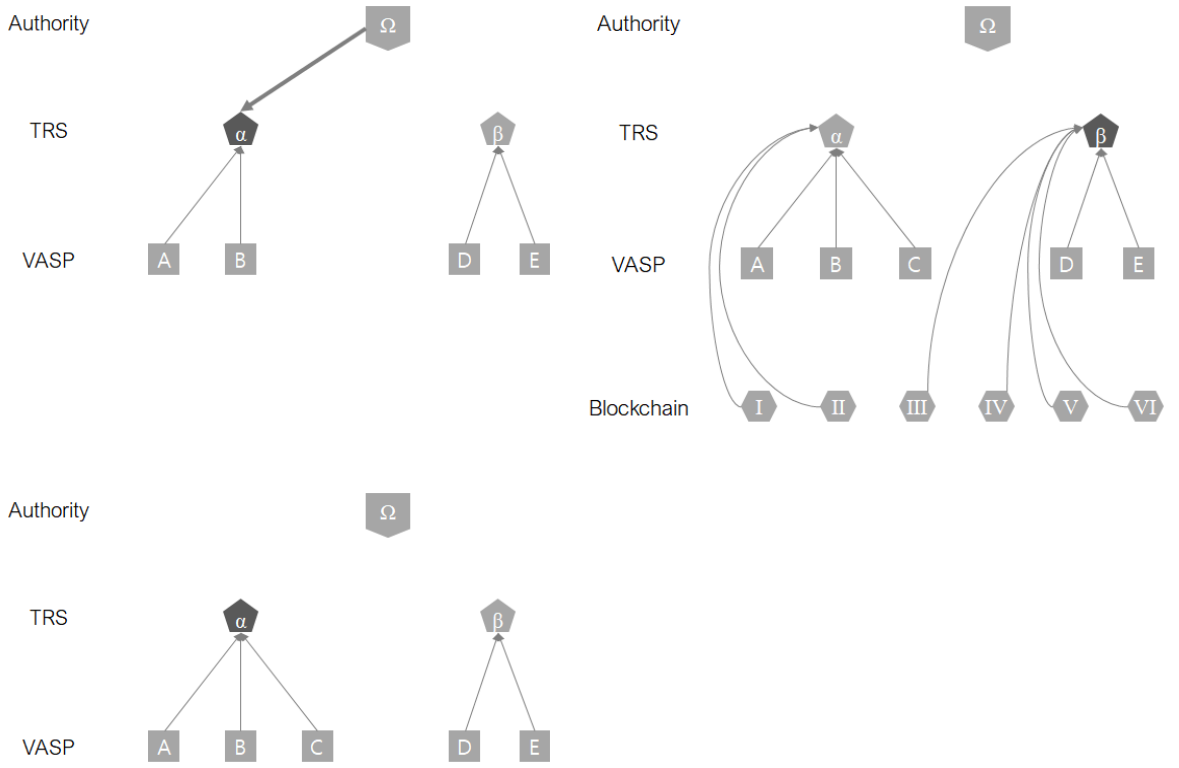

Figure 10. Existing Standardization Models: De-Jure Standardization (Top Left), De-Facto Standardization by a Direct Network Externality (Bottom Left), and an Indirect Network Externality (Right).

The Adoption by Pairs Might Result in the Economic Inefficiency.

The adoption by pairs might result in economic inefficiency. Let us start with a fictional scenario of standardization in layered architecture. In the scenario, Coinbase provides its service by HTTPS and authenticates its clients by the Terminal Access Controller Access Control System Plus (TACACS+). Moreover, Binance uses Secure Shell (SSH) at the application layer and Remote Authentication Dial-In User Service (RADIUS) for authentication. Let us also assume that Firefox supports HTTPS, SSH, and TACACS+, and Chrome does SSH, TACACS+, and RADIUS. Although only Firefox users can access Coinbase and only Chrome users Binance, Binance can easily extend its market to Chrome by adopting RADIUS and Coinone to Firefox by adopting HTTPS.

However, the layered model does not work for travel rule standards. Let us imagine TRISA and Sygna's scenario, both of which work by SSL/TLS. TRISA provides a central certificate authority to verify the payment message encrypted by HMAC before sealing it by a public key. On the other hand, in the Sygna standard, an originator VASP sends the payment message encrypted by ECIES/ECDSA before sealing it by a public key. If Coinbase and Binance adopt TRISA and Sygna, respectively, they cannot provide a compliant service at the moment. Furthermore, Coinbase cannot extend the market to Binance simply by adopting ECIES/ECDSA at the encryption layer as long as TRISA adheres to the primary certification method.

The market can provide four alternative scenarios. First, the market yields separated groups of travel rule standards (Top Left in Figure 11). For example, if VASP pair A and B use the travel rule standard α and a VASP pair B and C uses it too, another VASP pair A and C can exchange their travel rule messages by standard α. However, a VASP pair D and E adopting standard β will hardly join the alliance of standard α unless the benefit of the membership covers the installment cost enough. Thus, it separates the market and limits the benefit from the global service of virtual assets.

Second, an intermediary VASP might connect the separated market (Top Right in Figure 11). Let us consider that VASP C adopts standard β to extend its service to VASP D in the previous scenario. Then VASP E can also access the market of VASP C through the shared standard β. VASPs A and B can also link to VASPs D and E through the intermediation of VASP C, where VASPs A and B exchange the travel rule message with VASP C through standard α and VASPs D and E through standard β.

The intermediation by a few hubs reaching a majority of ends connects the entire system efficiently, shown in the previous examples: the Internet (Tu, 2000), airlines after deregulation (Pels, 2021), and even social networks (Albert et al., 1999). However, centralization is the opposite of blockchain's principle. For example, the top right side in Figure 11 shows that payment messages should pass by VASP C. It means that attacks will focus on VASP C to destroy the entire system (Albert et al., 2000), and VASP C is likely to be motivated to manipulate the blockchain societies through harnessing its political power.

Third, each VASP should adopt all travel rule standards (Bottom Left in Figure 11). For example, VASP E should adopt standard α if it needs to extend its service to VASP A, but VASP A adheres to it, and VASP C rejects their intermediation. VASP A might have to adopt standard β for the same reason, even if adopting standard β is less efficient for VASP A than passing by VASP C or VASPs B and E sharing standards. The scenario will ultimately connect all VASPs.

However, adopting all standards increases the cost of implementing the travel rule. Small VASPs occupying the majority of the market lacks the financial and organizational margins to embody the travel rule standards in their systems and can hardly suffer from the broken integrity of their services by accident. Therefore, small VASPs cannot rely on commercial travel rule services that have already proven performance, so consider the cost of installation and failure risks.

An alternative is that each VASP adopts the travel rule standard necessary to expand its service to a certain counterpart VASP. For example, the Bank of Korea could lead the standardization if it cooperates with five Korean financial institutions (i.e., Woori Bank, KB Bank, NH Bank, Hana Bank, Shinhan Bank) by harnessing its issuing power and their market share (Lim, 2020). Remaining financial institutions such as Kakao Bank and Deutche Bank would better follow their policy. Moreover, the financial regulations impose the cost for the global market on a few intermediary and correspondence banks. However, the domestic market-oriented policy does not work for VASPs free in cross-border services with more than three hundred VASPs (https://coinmarketcap.com). Each VASP will have to install all commercial travel rule services at worst.

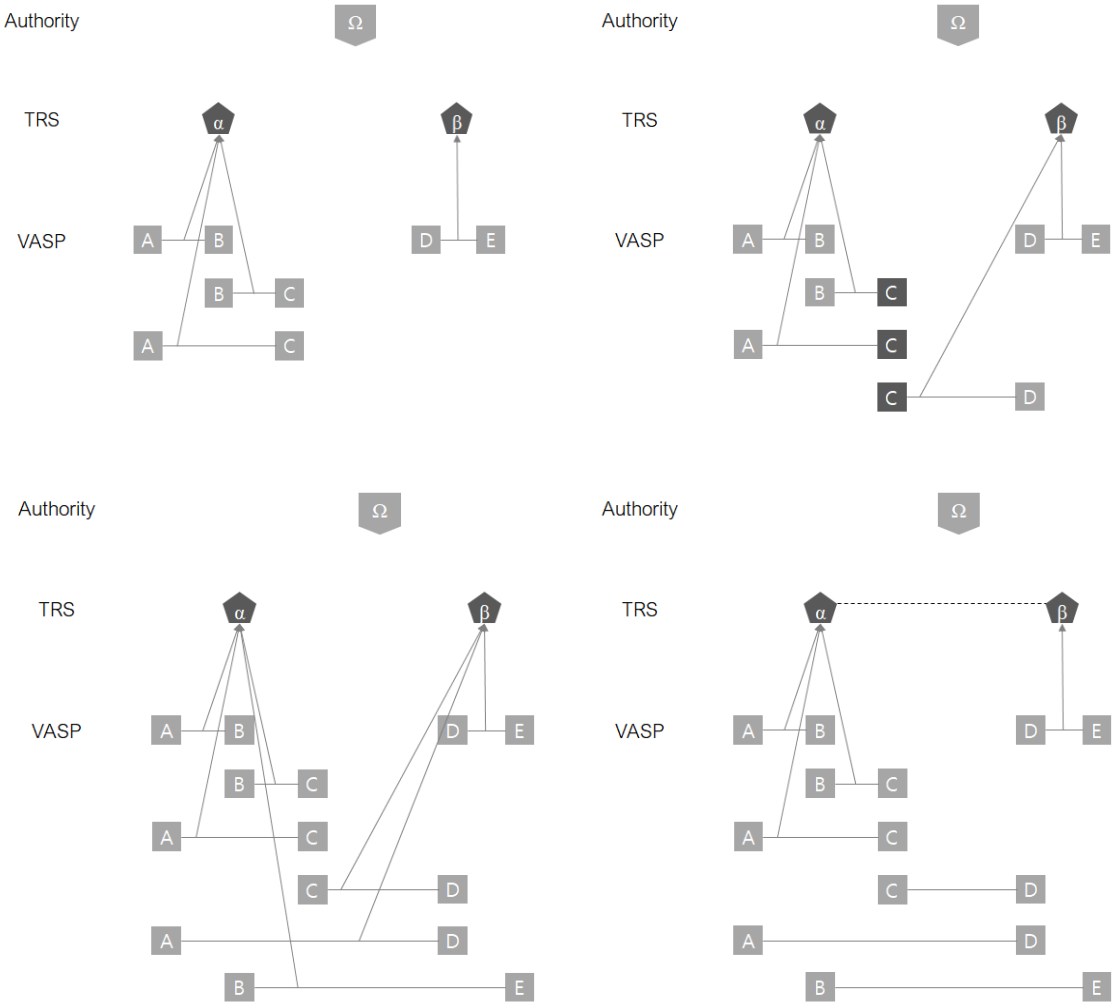

Figure 11. Standardization Scenarios: The Separation of MarketS (Top Left), the Rise of an Intermediary (Top Right), the Total Installment (Bottom Left), and the Loose Coupling of Federations (Bottom Right).

The Compatibility among Travel Rule Standards Will Bind the Worldwide Markets.

GI-TRUST suggests that compatibility among travel rule standards is a solution to the economic inefficiency due to the inseparable adoption by pairs. Let us turn back to the third scenario at the Bottom Left in Figure 11. If standard α is compatible with standard β, VASPs can exchange the travel rule message through the standards they have already installed. VASPs *A*, *B*, and *C* do not need to adopt standard β to extend its service to VASPs *D* and *E*, nor do VASPs *D* and *E* need to adopt protocol α.

Therefore, the compatibility makes VASPs' travel rule implementation efficient and prepares a fair competition environment for travel rule service providers (TRSPs).

An approach is that a central standardization such as FATF and ISO settles down the standard competition. However, early intervention might reduce the market's innovation motivation when a dominant design does not emerge. Furthermore, a travel rule standard covers all encryption, decryption, and verification procedures in the inseparable architecture. Therefore, it is infeasible that multiple standards take parts of the procedures, e.g., using standard α for encryption at VASP *C*'s side and standard β for decryption and verification at VASP *D*'s side. Thus, early centralized standardization deprives a technology for segment from advancing the entire workflow of the travel rule.

The alternative is that the market adjusts one standard to be compatible with the other (Haile and Altmann, 2018; Kang et al., no date). A compatible standard enhances the utility of its users as it extends the scope of its services (Kang et al., no date). Moreover, the second mover is incentivized to be compatible with the first mover's standard (Haile and Altmann, 2018). However, it is significant to remind that travel rule standards are inseparable. The compatibility means that a second-mover adopts the first-mover's standard, or the second-mover's standard replaces the first-mover's.

A solution to the compatibility in the inseparable architecture is translating one standard to another one at a software layer. In other words, let us consider two VASPs *C* and *D,* adopting travel rule standards α and β, respectively. VASP *C* sends a travel rule message to VASP *D* through its standard α. The standard α translates its message format and encryption-decryption-verification procedures to standard β. Then VASP *D* receives the travel rule message that is read with its standard β. As a result, each VASP seamlessly exchanges the travel rule message with keeping their standards. The approach imposes the innovation cost on a travel rule standard provider, willing to pay for providing a better service.

Two questions follow if the translation is a compatibility solution. First, who translates it between ordering and beneficiary VASPs? Among ordering and beneficiary VASPs, travel rule service providers, and public agencies, GI-TRUST recommends that an ordering VASP would better be responsible for the standard translation. A beneficiary VASP risks mistranslating the standard if the beneficiary VASP does not obtain enough information about the originator's travel rule standard. An ordering VASP might let the beneficiary VASP know wrong information intentionally or by mistake. On the other hand, the ordering VASP can translate its travel rule standard when it receives the beneficiary VASP's travel rule standard with the beneficiary's information.

Second, what technologies support the translation in the inseparable workflow of the travel rule? Translating travel rule standards mean switching the communication protocol on the one hand and mapping the message format on the other hand. Although the protocol switch is technologically trivial, the format mapping might weaken the security of the travel rule's workflow if the translation needs decrypting an encrypted message. Third parties can read the plain text by accident or intentional attack. Otherwise, the translation without decryption should wait for technological advances in cryptography, such as homomorphic encryption (Dijk et al., 2010).

Therefore, GI-TRUST suggests that the market inserts an open multi-channel integration (MCI) between travel rule standards (Figure 12). An MCI consists of multiple channels accessing their corresponding standards and an MCI agent managing those channels. The MCI agent switches the session channel to transmit an encrypted payment message between different travel rule standards.

For example, let us consider that an ordering VASP is about to transmit a message to a beneficiary VASP by ordering VASP's travel rule standard through Channel 1 in Figure 12. A legacy system processes and encrypts a travel rule message before it transmits it to the MCI agent through its corresponding channel (Channel 1 in Figure 12). The MCI agent attaches a header depicting VASP *B*'s travel rule standard and sends the headered secure message to VASP *B* through its corresponding channel (Channel 2 in Figure

12). VASP *B*'s legacy system receives the encrypted message by the MCI Agent's guidance to process and retain after decryption according to the header's information.

The MCI architecture works when at least one side of a VASPs' pair installs it as the MCI switches to the counterpart's channel. For example, VASP *C*'s legacy system directly accesses VASP *A*'s legacy system through Channel 3 in Figure 12, and receives the secure message with the header corresponding to VASP *C*'s encryption/decryption method.

A prerequisite of the workflow is that VASP *A* knows VASP *B*'s standard and encryption/decryption methods. GI-TRUST suggests that a repository of VASPs and TRSPs can support the information. Figure 14 and Table 6 will explain the detail.

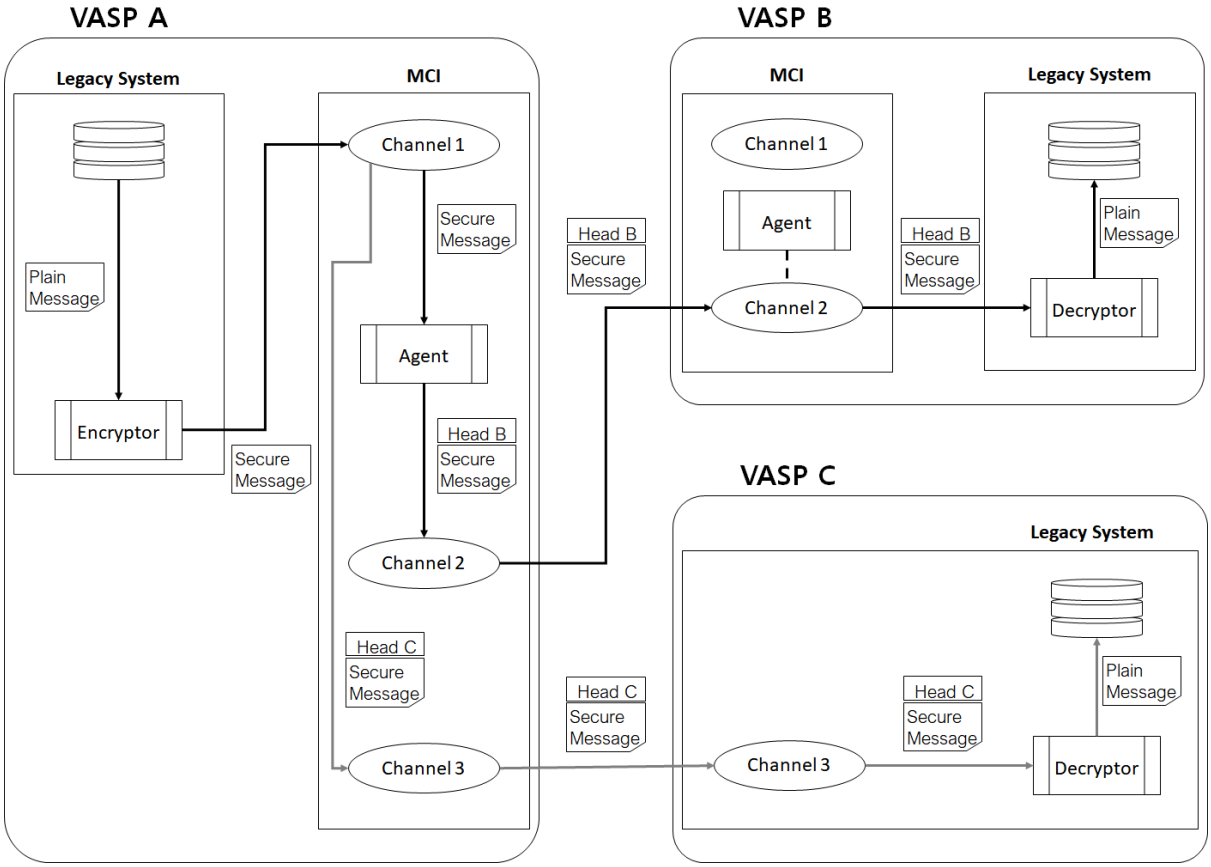

Figure 12. The Workflow of the Multi-Channel Integration (Sourced from Datamation, Co., Ltd., 2021).

4.2. Modular Architecture of an AML-KYVC System for Interoperability

The Travel Rule Process Should Interoperate with RA, CDD, and STR Processes for AML/CFT.

The travel rule is a component of the regulatory system for Anti-Money Laundering and the Counter-Financing of Terrorism (AML/CFT). Achieving the goal of AML/CFT, the travel rule output should work for the risk analysis (RA) process in support of its customer due diligence (CDD) process (Figure 13). In addition, the travel rule outputs should also reach the counterpart VASP through the transaction status tracking (TST) process and the Financial Intelligence Unit (FIU) through the suspicious transaction report (STR) process. The entire system then will achieve the AML/CFT mission in collaboration with the competent authorities and partner VASPs.

First, interoperating the travel rule with the CDD process is what FATF recommends in its updated guidance (FATF, 2021.10: Paragraphs 182-183). According to the guidance, an ordering VASP is responsible for verifying the originator's information through its CDD process (FATF, 2021.10: Paragraph 182), and a beneficiary VASP the beneficiary's information through its CDD process (FATF, 2021.10: Paragraph 183). South Korea's VASPs work with their host bank for the CDD process because the ARUSFI (2020: Article 7.3.2) binds a VASP and its customers with a bank.

Next, the travel rule process should also interact with the RA process connecting to the STR process (Chung and Kang, 2020). FATF (2012-2020: INR 1) requires a VASP to assess the risk of its customer's transaction in a risk-based approach before the VASP dispatches the virtual asset transfer on the blockchain (FATF, 2012-2020: Recommendation 15; FATF, 2021.10: Paragraphs 68, 82, 87, 92). VASPs can use the watch list that the government or international bodies share (FATF, 2021.10: Paragraph 257).

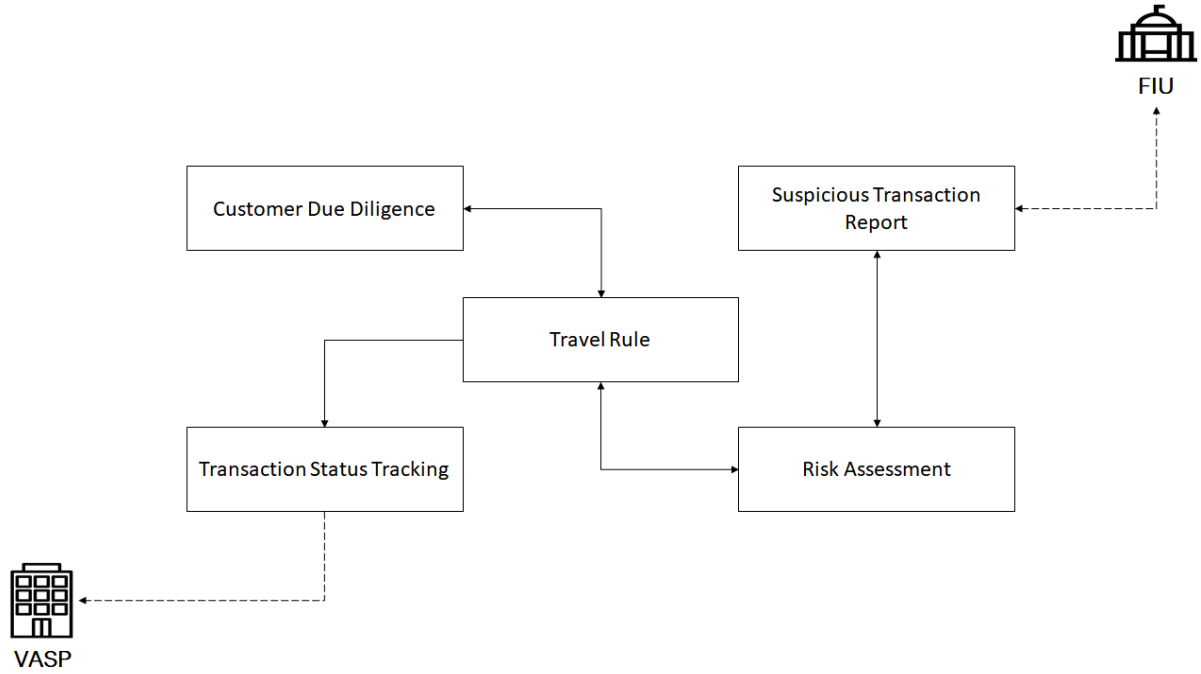

Figure 13. The Interoperation of the Travel Rule in an AML/CFT System (Icon sourced from the WEB).

From a technological perspective, the RA process should also interoperate with CDD and STR processes. The RA process needs the customer's information (i.e., name, account number, and an identifier such as geographic address), which the CDD process supplies, to infer her/his nationality, residence, and financial activities by a fuzzy algorithm. Furthermore, the STR process supplies the customer's history of suspicious transactions and the watch list that an FIU shares. According to the RA results, a VASP reports suspicious transactions to the FIU through its STR process. Recording the RA results on a database of CDD and RA processes will help the next round of CDD and RA processes.

Finally, GI-TRUST proposes adding the transaction status tracking (TST) process to the AML/CFT system. The travel rule ends with dispatching the virtual asset transfer on the blockchain in existing travel rule standards (Figure 8). However, the payment information retained in a VASP's database might deviate from the settlement information recorded on the blockchain if the dispatch fails or drops or intentional or accidental intervention affect the blockchain. FATF (2021.10) omitted the process, but it is necessary to maintain the travel rule records identical to the blockchain's records.

The Interoperation Needs the Extension of FATF's Recommendations on CDD, RA, STR.

Table 5 proposes the guidelines for the interoperation among the travel rule, CDD, RA, STR, and TST processes. On the one hand, the interoperation of the travel rule with CDD, RA, and STR is consistent with the existing recommendations of FATF. GI-TRUST proposes that a travel rule process should be interoperable with the CDD process to verify the accuracy of a VASP's customer in line with FATF (2021.10: Paragraphs 182-183). Moreover, its recommendations on the risk assessment (FATF, 2012-2020: Recommendation 15, INR 1; FATF, 2021.10: Paragraphs 68, 82, 87, 92) are extensible to clarify the interoperation between the travel rule and RA processes. The RA process should also be interoperable with the STR process to update the watch list and report suspicious transactions.

Table 5. Proposed Additional Regulatory and Technological Guidelines to FATF Updated Guidance (2021.10) and FATF Recommendations (2012-2020).

Category	Proposed Regulatory and Technological Guideline	FATF Recommendation and Updated Guidance
Interoperation with CDD	For accuracy, a travel rule process should reach the CDD process to verify a customer's name and identifier (e.g., geographical address, date, and place of birth, national ID number).	FATF (2021.10: Paragraphs 182-183) has already expressed the interoperation of the travel rule process with the CDD process, either independently or relying on trusted third parties.
Interoperation with RA and STR	A travel rule process should reach the RA process to filter a customer from the watchlist shared by competent authorities and assess the risk of the transaction. If the RA process returns a suspicious transaction, the travel rule process stops the transaction, and the STR process submits the suspicious transaction to FIU. It means the RA process should also be interoperable with the STR process.	The proposed guideline on the interoperation with RA and STR suggests FATF add the interoperation features to its guidelines on the risk assessment (2012-2020: Recommendation 15, INR 1; 2021.10: Paragraphs 68, 82, 87, 92).
Interoperation with TST	A travel rule process should receive the transaction status from the TST process to maintain the payment information recorded in the travel rule process in line with the settlement information recorded on the blockchain.	FATF (2012-2020; 2021.10) do not explicitly comment it. FATF(2021.10: Paragraph 283.f) comments that technologies should "provide a VASP with a communication channel to support further follow-up," but it aims at CDD and RA.
Technology Neutral Approach	The interoperation among the travel rule, CDD, RA, STR, TST processes should abide by FATF's technology-neutral approach so that each process can access any other processes without technological obstruction. For example, the RA process can harness a fuzzy algorithm to infer the identity of a customer and the characteristic of her/his transaction. The processes can also rely on existing protocols such as APIs for their communication.	The proposed guideline is in line with FATF (2021.10: Paragraph 285).
Performance Requirement	Each process of the AML/CFT system should be able to interoperate with the CDD, RA, STR, and TST processes securely*, massively ⁑, and unobstructedly ⁂. * The 'secure' interoperation means that the interoperation should be protected from personal information leaks and intentional or accidental intervention. ⁑ The 'massive' interoperation means that the interoperation should be capable of carrying out the transmission of an amount of data among TR, CDD, RA, STR, and TST processes without latency. ⁂ The unobstructed interoperation means that each process should always be accessible to any other process through a standardized communication protocol.	FATF (2012-2020; 2021.10) do not explicitly comment it.

On the other hand, FATF's recommendations miss the travel rule's interoperation with the TST process. Financial regulations stay at conventional payment systems, where they adjust an error through the procedures of payment, clearing, and settlement by financial institutions. However, blockchain omits those procedures, and the records on the payment message layer might deviate from the blockchain's record. The deviation impedes the traceability of virtual assets. Therefore, GI-TRUST proposes that FATF adds a guideline on the TST process and its interoperation with the travel rule process.

Furthermore, it is notable to consider that "[c]ountries should treat all VA transfers as cross-border wire transfers" (FATF, 2021.10: 179). It means that a VASP's travel rule process has to manage faster, much more messages containing flexible data on customers' identifiers (e.g., geographical address, date, and place of birth, national ID number) than conventional financial institutions. Therefore, the interoperation of travel rule, CDD, RA, STR, TST processes needs technological supports to process the 'massive' data within components and the communication between components.

The problem is that the junction between processes is the weak point of an AML/CFT system. For example, a readable message might leak if the plain text transmits between components after its decryption. Otherwise, an intentional attack is likely to target the unsecured niche between secured processes. Therefore, GI-TRUST proposes a performance standard saying that the interoperation should be 'secure.' A technology neutral approach applies to embodying the 'security standard through either decrypting after transmitting an encrypted message, physically sealing the path transferring plain texts, or analyzing the encrypted message without decryption (Rivest et al., 1978).

Finally, GI-TRUST suggests that 'unobstructedness' should be a performance standard for interoperation. Any obstruction to a process (e.g., a travel rule process provided by company α) excludes the access from the other process (e.g., an RA process provided by company $\neg\alpha$). It leads a VASP to lock in the standards provided by company α for all AML/CFT processes. Let us remind that a blockchain-based system should avoid centralization, as it might impact its decision-making.

Therefore, a technology-neutral approach applies again to the unobstructed interoperation. Any standard must not lock a process. Standardized communication protocols will help the unobstructed interoperation among the travel rule, CDD, RA, STR, and TST processes. For example, VASPs and AML/CFT segment providers can cooperate in designing and verifying the protocols, such as the application programming interfaces (APIs) supporting a TST process to monitor and approve the transactions transferring from a travel rule process.

Cloud provides an efficient environment to support the functions of the travel rule, CDD, RA, STR, and TST. A VASP can rely entirely or partly on Cloud and integrate the Cloud services into an AML/CFT system. Using Cloud is outsourcing information systems, which is different outsourcing from the outsourcing/agency model that FATF (2012-2020: Recommendation 17) excludes from relying on trusted third parties. Using the Cloud requires examining the security and responsibility according to each jurisdiction's regulations despite its efficiency. For example, South Korea's financial institutions could start using Amazon Web Services and Google Cloud Platform as the government certificates their information security management system (ISMS) in December 2020 and April 2021, respectively.

The Modular Architecture of AML-KYVC Makes the Travel Rule's Interoperation Flexible.

Modular architecture reduces the complexity in the innovation of a vast system (Cusumano, 2002). In a modular architecture, a moduled process provides its function to the system and requests the other processes to provide it with its function through an open interface. A process developer can focus on designing, implementing, and modifying its process without considering the interaction with other processes. A system user can integrate multiple processes on her/his demand without understanding the entire configuration.

GI-TRUST suggests extending financial institutions' Know Your Customer (KYC) system by applying the modular architecture to the travel rule (Figure 14). A VASP needs an information system's support to identify its partner VASP and its customer because the virtual asset market lacks supervision by regulations like financial institutions. Therefore, the proposed system includes identifying counterpart VASPs and their customers. It also involves identifying and assessing its customers and their transactions. GI-TRUST calls it an Anti-Money Laundering Know Your VASP and Customer (AML-KYVC) system.

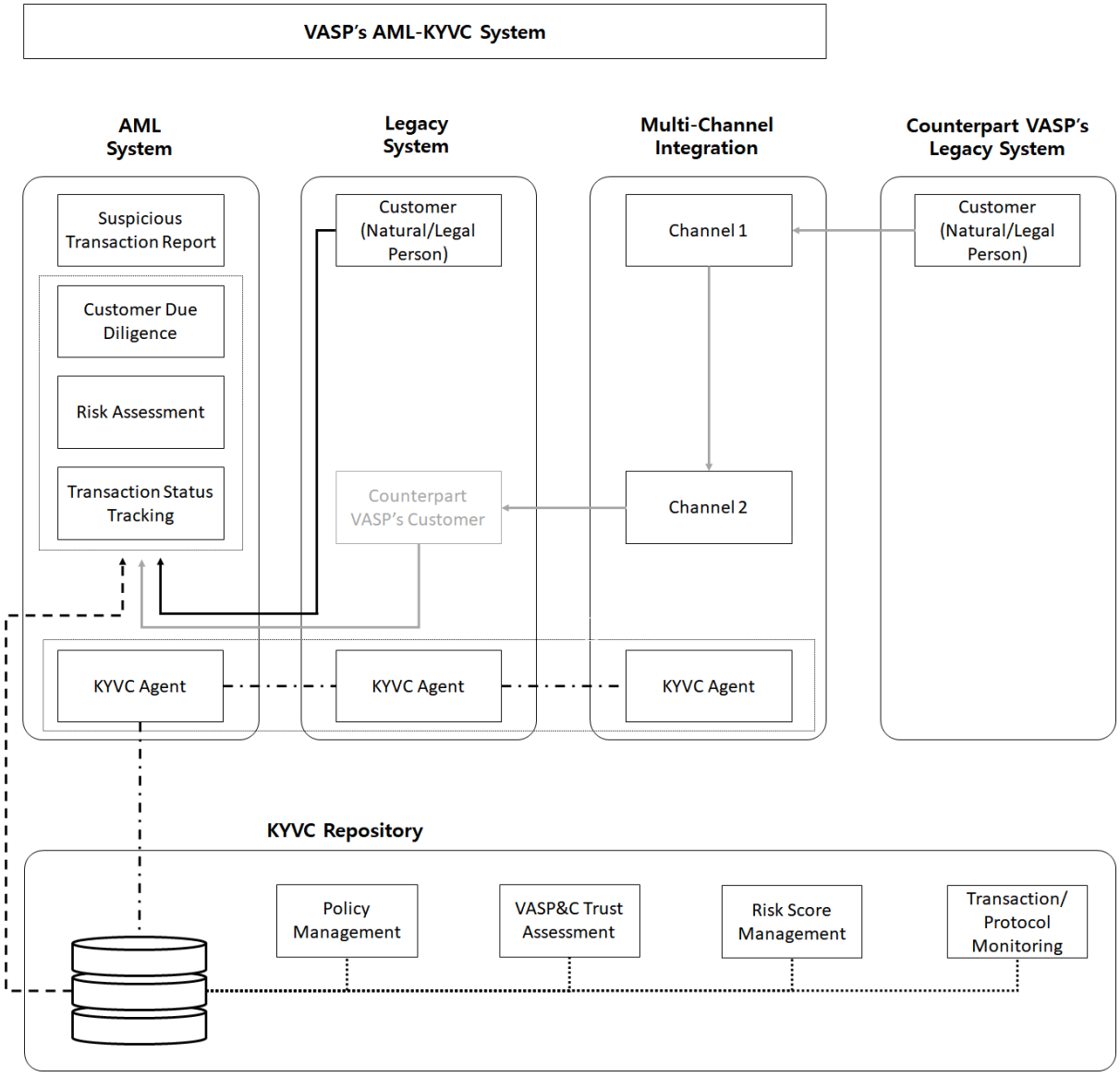

Figure 14. The Architecture of the Interoperation of the Travel Rule through Multi-Channel Integration (Sourced from Datamation, Co., Ltd., 2021)

The AML-KYVC system has four subsystems in a modular architecture. The first part is an AML system consisting of CDD, RA, STR, and TST processes to support the conventional AML/CFT missions. The second subsystem is the legacy system that manages the accounts of its customers (i.e., natural persons and legal persons) and its partner VASP's customers (i.e., natural persons and legal persons). The third subsystem is the multi-channel integration (MCI) module, supporting the exchange of travel rule messages between different standards as Figure 12 introduced. The last part is the KYVC Repository

listing and assessing VASPs and TRSPs.

KYVC agents coordinate the interaction among those subsystems in a VASP's AML-KYVC system and arrange the communication with its partners' systems. Each VASP's AML-KYVC system reaches its partner's AML-KYVC system through the MCIs by the KYVC agents' mediation. The information of a counterpart VASP's customer transfers by switching channels (from Channel 1 to Channel 2 in Figure 14) according to the workflow depicted in Figure 12.

The KYVC respository consists of VASP and cusomer assessment, policy management, risk score management, and transaction monitoring modules. The VASP and customer assessment module evaluates macro-level risks of VASPs and customers. The policy management module follows up recent guideline and regulations of FATF and worldwide jurisdictions' FIUs. The risk score management module evaluates the AML/CFT risks at a macro-level. And the transaction/protocol monitoring module watches transactions and protocols.

A VASP's CDD, RA, and TST modules receive its customer, its counterpart VASP's customer, and the KYVC repository's macro-level assessment. The CDD and RA modules determines a suspicious transaction with the information from its legacy system and counterpart VASP's legacy system, and the KYVC repository. They report it to the Financial Intelligence Unit through the STR module.

A combination of KYVC agents provides the travel rule service, integrating them with other modules. Let us consider that one VASP customer requests payment to the other VASP's customer. An ordering VASP transfers the originator's information from its legacy system to its CDD and RA processes. It also receives the information of the counterpart VASP's customer to send it to its CDD and RA processes after assessing the counterpart VASP's and TRSP's reliability. The MCI redirect the channels (e.g., Channel 1 to Channel 2 in Figure 14) to transfer the message of the counterpart VASP's customer adopting a standard different from the ordering VASP's.

A VASP can integrate the AML-KYVC processes in various ways. It can develop some of those processes and outsource the other processes and the system integration. A prerequisite of the flexible system design is standardizing the modules' interfaces and opening a module's functionality to other modules. TRSPs can specialize their services in the configuration and its quality of services in the modular architecture.

4.3. Elaborate Message Format for Compatibility and Interoperability

Extension of the FATF Standard Mitigates the Uncertainty in Payment Messages.

Standardizing the message format is a prerequisite for the compatibility and interoperability of travel rule standards. FATF (2012-2020; 2021.10) recommends the basic information that a travel rule message should contain: originator's name, account number and identifier, and beneficiary's name and account number (Table 3). However, VAs and VASPs are too dynamic for regulators to manage. Many VASPs fade in and out of the market, while financial institutions are built and supervised by law. Therefore, GI-TRUST proposes extending the message standard to catch up with the dynamicity.

The proposed message standard mainly complies with the guideline of FATF (2012-2020: INR 15; 2021.10: Paragraphs 182-183). GI-TRUST remarks two comments on the existing guidelines. First, the market would better build a convention on the beneficiary's jurisdiction threshold. Worldwide jurisdictions respond with various thresholds (e.g., Switzerland's 1,000 CHF, USA's 250 USD) to FATF's 1,000 EUR/USD threshold to share the information (Table 6). Setting the threshold at the beneficiary's jurisdiction as South Korea's ARUSFI defines will clarify implementing the travel rule and leave the decision on implementing the travel rule for the beneficiary's side.

Table 6. Extension of the FATF Standard for the Global Implementing of Travel Rule Standards

Category	Variable	Note
Threshold to Share	Threshold	An ordering VASP abides by the beneficiary's jurisdiction in the condition of FATF's recommendation.
Originator's Information	Person Name Account Number Person Identifier	The variables are the same as FATF (2021.10: Paragraphs 182-183).
Beneficiary's Information	Person Name Account Number	The variables are the same as FATF (2021.10: Paragraphs 182-183).
Virtual Asset's Information	Type of the Virtual Asset Amount of the Virtual Asset	The variables are based on 31CFR1010.410.
Ordering VASP's Information	VASP Identification Code Repository Identification Code	GI-TRUST proposes to add them to travel rule messages. A travel rule message remarks the VASP identification code and the repository identification code only. Moreover, a separate repository publishes the VASP's information: - VASP's Legal Name - VASP's Status (Reliable, Unreliable, Pending) - VASP's Identifier (e.g., Geographical Address, Legal Entity Identifier). A trusted third party (entitled the repository identification code) or federation verifies VASPs and manages the repository.
Beneficiary VASP's Information	VASP Identification Code Repository Identification Code	The note is the same as one of the beneficiary VASP's information categories.
TR Standard Information	Travel Rule Standard Identification Code Travel Rule Standard Version Number	GI-TRUST proposes adding the travel rule standard information to the travel rule message to translate between travel rule standards. The message contains the Travel Rule Standard Identification Code and the Travel Rule Standard Version Number only for the size burden reduction. Moreover, a separate repository publishes the travel rule standard's information: - Travel Rule Standard's Commercial Name - Travel Rule Standard Developer's Legal Name - Description of the Encryption Method - Description of the Verification Method - Description of Transmission Protocol

Second, GI-TRUST suggests that informing an originator's identifier needs careful considerations. FATF (2012-2020: INR 15; 2021.10: Paragraphs 182-183) and worldwide jurisdictions list the originator's geographical address, national ID number, or date and place of birth as her/his identifier. Thus, the specification fits domestic transfers, in which a beneficiary VASP can infer the originator by its jurisdiction's standard. However, various standards on identifiers leave the identity inference problem. For example, an American VASP can identify a Korean originator using the national ID number more quickly than a Korean VASP can for an American originator using the postal address.

Furthermore, GI-TRUST recommends adding VASP's information, travel rule standard's information, and virtual asset's information to the travel rule message. That information will help a VASP implement the travel rule in dynamic market conditions.

First, GI-TRUST proposes that a message contains the virtual asset information. FATF (2021.10: Paragraph 182-183) does not explicitly express that a travel rule message should contain the virtual asset's information. However, some jurisdictions (e.g., 31CFR1010.410) guide travel rule messages containing the amount of transferring the asset. Moreover, the travel rule standards already list the virtual asset information (i.e., type of virtual assets such as BTC, ETH, XRP, and the amount to transfer). Those variables support RA and SPR processes.

Second, the message should contain VASP's information. FATF (2021.10: 182-183) and any country (AMLO-FINMA, 2021; PSN02, 2019; 31CFR, no date; ARUSFI, 2020) do not include VASP's

information. A constraint is that adding more information to a message increases the burdens of the transmission and process of the message. GI-TRUST suggests managing a separate repository of the VASP information. A travel rule message remarks the VASP identification code and the repository identification code only. On the other hand, a separate repository publishes the VASP's legal name and the status of the VASP's reliability (i.e., reliable, unreliable, and pending). A trusted third party (entitled the repository identification code) or their federation verifies VASPs and manages the repository as some TRSPs publish their alliance directories.

Third, GI-TRUST proposes adding the travel rule standard information to the message. The standard's information will help a VASP or TRSP makes the standard compatible with the other standard or interoperable with other AML/CFT processes. However, the information does not appear in FATF guidelines and worldwide jurisdictions (Table 3). Therefore, to reduce the size burden, like in the VASPs' information, the message contains only the Travel Rule Standard Identification Code and the Travel Rule Standard Version Number. Moreover, a separate repository publishes the travel rule standard's information: i.e., standard's name, standard developer's name and identifier, encryption method, verification method, and transmission protocols.

Managing the VASP and TRSP registries needs centralized governance by trusted third parties. Some of TRSPs operate their VASP registries. The market can use those existing registries and evaluate their reliability. Otherwise, they can build independent VASP and TRSP registries. However, one organization cannot sufficiently reach all VASPs and TRSPs across jurisdictions; it would be costly even if it is possible. A federation of associations is a feasible way. A local association manages the VASPs and TRSPs registries in a jurisdiction and exchanges their information with the other jurisdiction's association through global organizations.

Elaborate Message Formats Like ISO 15022 Will Regularize the Irregular Data.

Various writing styles of a message will prevent building travel rule standards compatible and interoperable. There are various conventions for writing dates, names, amounts of money, and postal addresses. For example, Koreans are familiar with writing the eighth date of March in 2011 as of 11/03/08, while Americans and Europeans write it 03/08/11 and 08/03/11, respectively. Furthermore, the Korea Blockchain Association locates at Office #301 on the third floor of Teheran Office Building, 52-6 Teheran-ro, Gangnam-gu, Seoul 06211, Republic of Korea, while Koreans are more familiar with "(06211) Korea Seoul Gangnam-gu Teheran-ro 52gil 6 Teheran Office Building Number 301." Finally, Germans write $1.000,00 for one thousand dollars while Americans $1,000.00.

IVMS101 suggests the data structure and the formats of those variables. For example, IVMS101 defines the date format as a text value of a number of four ciphers – a number of two ciphers – a number of two ciphers according to ISO 8601 (JWG IVMS, no date: 36). Moreover, it defines the structure of a customer's data consisting of a person's name and geographic address allowing multiplicities, and unique identifiers such as national identification complying with the country codes of ISO 3166-1 alpha-2 (JWG IVMS, no date: 18). If it identifies a person with her/his geographical address, it specifies the address into the department, street name, postcode, and country, abiding by ISO 19160.

However, IVMS101 allowing the liberal implementation leaves it inefficient the compatible and interoperable implementation of travel rule standards. Let us compare two examples of travel rule standards (Table 7). CoolBitX (2020) assumes that David Beckham requesting the transfer of 0.347895 ETH writes his name, home address, and date of birth in the personal information category. In addition, he writes the ordering VASP's identifier and VA information in the transfer information category. On the other hand, in VerifyVASP, he writes VA information at the payload category while writing his name and identifiers in the originator's category at the payload category. The writing styles are also slightly different, e.g., "Switzerland" and "CH" for the country, "0x8000003c" and "ETH" for the type of virtual

asset, and including and excluding the ordering VASP's information.

The difference in various styles works as a barrier in translating the messages. It results in one or more of the three outputs: (1) A VASP using one travel rule standard fails to read the message written in the other standard by its counterpart VASP even if the two standards share the encryption and verification methods. (2) An AML/CFT system's CDD, RA, STR, and TST processes adjusted to one travel rule standard fail to read the message written in the other standard even if they share the standards for encryption and verification methods. (3) No new travel rule standard enters the market due to the cost of translating all message formats, despite a better quality of service.

GI-TRUST turned to conventional financial institutions that hey had the same issue. The Society for Worldwide Interbank Financial Telecommunication (SWIFT) introduced in 1973 a secured, reliable network for financial message communication to the international banking services. It resolved the issues on various writing conventions by standardizing the messages according to the service types. The International Organization for Standardization (ISO) designed the standard for SWIFT messages (ISO 15022). The message types define the tags, options, and formats of the message, e.g., for general transfer between financial institutions (SWIFT TM 202), selling securities (SWIFT TM 543), and buying securities (SWIFT TM 541).

Table 7. Comparison of the Originator Information between CoolBitX Sygna and Lambda256 VerifyVASPs

Category	CoolBitX Sygna	Lambda256 VerifyVASP
Originator Information: Person Name	"private_info" > "originator". - "name": "David Beckham."	"originator" > "originatorPersons" > "naturalPerson" > "name" > "nameIdentifier". - "primaryIdentifier" : "David", - "secondaryIdentifier" : Beckham"
Originator Information: Person Identifier (Date of Birth)	"private_info" > "originator". - "date_of_birth" : "1975-05-02"	"originator" > "originatorPersons" > "naturalPerson" > "dateAndPlaceOfBirth" > - "dateOfBirth" : "1975-05-02"
Originator Information: Person Identifier (Home Address)	"private_info" > "originator". - "physical_address" : "Bahnhofstrasse 665, 8001 Zurich, Switzerland"	"originator" > "originatorPersons" > "naturalPerson" > "geographicAddress". - "townName": "Zurich" - "addressLine": "Bahnhofstrasse 665" - "country": "CH"
Account Number (Wallet Address)	"transfer_info" > "private_info" > "transaction". - "originator_addr" : "0x05ECAf39376…"	"accountNumber" : "0x05ECAf39376…"
Originator VASP Info: VASP Identification Code	"transfer_info" > "private_info" > "transaction". - "originator_vasp_code" : "VASPJPJT"	∗ VerifyVASP provides the VASP's information that it has registered. The information is not called in the message
Virtual Asset Info: Type of the VA	"transfer_info" > "private_info" > "transaction". - "transaction_currency" : "0x8000003c"	"symbol" : "ETH"
Virtual Asset Info: Amount of the VA	"transfer_info" > "private_info" > "transaction". - "amount" : 0.347895	"amount" : "0.347895"

GI-TRUST suggests that a message standard will encourage innovation. VASPs and TRSPs can apply elaborate message formats like ISO 15022 to their travel rule messages. However, they are more severe in blockchain-based VASPs because of blockchain's automation of trust and cross-border services. A VASP faces an amount of travel rule messages for automated payments. Moreover, it has to enlarge its size to maintain the quality of service if it manages the travel rule messages in its organization and bylaws like conventional financial institutions. Furthermore, the VASP has to consider cultural diversity to manage the travel rule messages for cross-border payment. Paradoxically, a decentralized service needs centralized trusted third parties to support the travel rule messages besides a blockchain system.

Table 8 depicts an example of the travel rule message for a simple payment that slightly modifies ISO 15022. The example codes command to open a session of the travel rule message for transferring 0.005 BTC from Kibae Kim (a customer of VASP UPbit) to Jung Hweon Jeon (a customer of VASP Korbit). Two tags, 16R and 16S, open and close the session for virtual asset transfer (TRANSF), respectively. Tag 56A sets the VA type at BTC and its amount to transfer at 0.005. Tag 52V shows the VASPs participating in the transfer. The ordering VASP (ORGN) is Upbit (UPBT), an exchange business (EXC), and the beneficiary VASP (BNFC) Korbit (KORB), an exchange business (EXC), too. Tag 52H declares that Kibae Kim is the originator (ORGN) and Jung Hweon Jeon is the beneficiary (BNFC). The message format receives the memory space according to the specifying lexical format of ISO 15022.

Table 8. Example of the Travel Rule Message for a Simple Payment Relying on ISO 15022

Example Code	Format	Field Specification
:16R:TRANSF/1	:16a[“/”3n]	(Session Type) / (Modifier)
:56A::BTC0,00500000	:3!a256n[,16!n]	(VA Type) (Amount)
:52V::ORGN/EXC/UPBT	:4!a/3!a/4!a	(Originator or Beneficiary) / (Exchange, …) / (VASP)
:52V::BNFC/EXC/KORB	:4!a/3!a/4!a	(Originator or Beneficiary) / (Exchange, …) / (VASP)
:52H::ORGN/Kim/Kibae	:4!a/128a/128a	(Originator or Beneficiary) / (Surname) / (Name)
:52H::BNFC/Jeon/Jung Hweon	:4!a/128a/128a	(Originator or Beneficiary) / (Surname) / (Name)
:16S:TRANSF/1	:16a	(Session Type) / (Modifier)

Elaborate Message Formats Like ISO 15022 Should Extend to Embrace Smart Contracts.

The smart contract, a unique feature of virtual assets, will complicate the travel rule. A smart contract is contained in a blockchain as a transaction, but a value of a virtual asset does not transfer before a specific condition triggers the contract. Therefore, the value transfer lags considerably behind the payment request. Moreover, the beneficiary is unclear during the pending period. However, the FATF recommendation does not consider smart contracts’ scenarios so that financial regulations might miss covering the travel according to a smart contract.

GI-TRUST suggests that the travel rule messages should be extensible to embrace smart contracts. Table 9 depicts an example of a smart contract modifying the travel rule message described in Table 8. The codes open a session of the travel rule message for requesting the transfer of 0.005 BTC total in the condition described in the Ethereum-based smart contract {kb_cntr_v01}. Because the beneficiary is not determined, Tags 52V and 52H do not work for the example. Tags 53V replaces 52V to show that a beneficiary VASP (BNFC) is determined (TBD) according to the reference (REF2) {kb_cntr_v01}. Likewise, Tag 53H depicts that a beneficiary (BNFC) is determined (TBD) according to the reference (REF2) {kb_cntr_v01}. Tag 62S defines the smart contract in the reference (REF2) of {kb_cntr_v01} runs on the Ethereum platform (ETH).

The section does not describe the remaining procedure after the execution of the contract for compactness. It also omits the tags for postal addresses, dates, and other variables for simplicity.

Table 9. Example of the Travel Rule Message for a Smart Contract Relying on ISO 15022

Example Code	Format	Field Specification
:16R:TRANSF/1	:16a[“/”3n]	(Session Type) / (Modifier)
:56A::BTC0,00500000	:3!a256n[,16!n]	(VA Type) (Amount)
:52V::ORGN/EXC/UPBT	:4!a/3!a/4!a	(Originator or Beneficiary) / (Exchange, …) / (VASP)
:53V::BNFC/TBD/REF2{kb_cntr_v01}	:4!a/3!a/4!a[{64w}]	(Originator or Beneficiary) / (Exchange, …) / (Ref)
:52H::ORGN/Kim/Kibae	:4!a/3!a/4!a[{64w}]	(Originator or Beneficiary) / (Surname) / (Name)
:53H::BNFC/TBD/TBD	:4!a/128a/128a	(Originator or Beneficiary) / (Surname) / (Name)
:62S::ETH/REF2{kb_cntr_v01}	:4!a/128a/128a	(Platform) / (Ref)
:16S:TRANSF/1	:16a	(Session Type) / (Modifier)

4.4. Sync Up with Technologies in a Longer View

VA Technologies Advances Fast and Regulations Chases Wallets, NFT, and Supply Chains.

Virtual asset technologies advance fast, and regulations chase the advancing technologies fast. FATF 2012-2020: INR 15.3) recommended institutionalizing VASPs so that competent authorities could supervise them. However, non-obliged entities such as unhosted wallets are located at a vague region of the financial regulations, as it is "not a money transmitter" (FinCEN, 2019: 16). The existing financial regulations impose the travel rule on "centralized" virtual asset service providers. However, the travel rule fails in tracing the asset flow through non-obliged entities (e.g., unhosted wallets) between obliged entities (centralized exchanges, CEX) (Figure 15). Therefore, FATF (2021.10: Paragraph 179) added the transactions with non-obliged entities to the regulation scope.

FATF's extension of the regulation scope leaves issues on the legitimacy and feasibility of law enforcement. The issue of legitimacy asks if the law can regulate personal devices such as unhosted wallets. Furthermore, it asks who is responsible for the financial regulations if it is legitimate. For example, let us assume that regulations apply to virtual assets seamlessly flowing across financial institutions, obliged VASPs, and non-obliged VASPs because they provide financial services. However, can an FIU supervise the non-fungible tokens and blockchain-based supply chains when a type of virtual assets transit to the other type after passing by works of art through NFT (Goodwin, 2021) and physical products through a blockchain-based supply chain (WEF, 2020.04; WEF, 2020.12)?

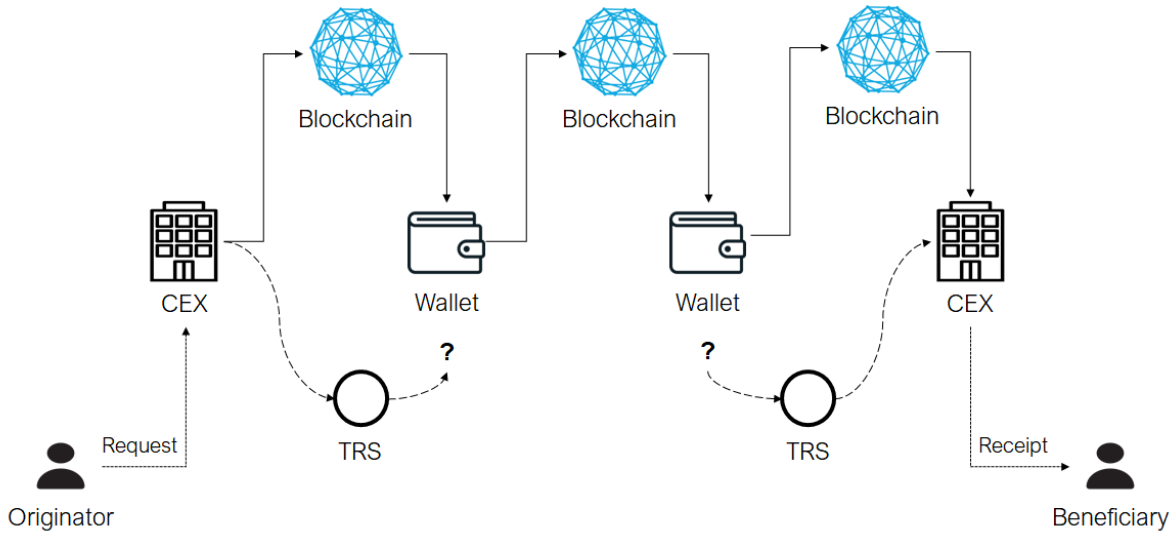

Figure 15. The Workflow of Blockchain-Based Payment through Private Wallets (Icons sourced from the WEB).

If regulations solve the legitimacy issue, they face a challenging problem on the technical feasibility of law enforcement. Questions are: How can a regulation incentivize the consumers using the unhosted wallets, NFTs, and blockchain-based supply chains to enter the scope of its regulation? Will a consumer voluntarily install the regulation-layer component to her/his device? Should the regulation require an unhosted wallet maker to plant a regulation-layer component so that competent authority can supervise consumers? Do the works of art, and intermediary products along the supply chain also comply with financial regulations? Those are out of the scope of GI-TRUST. Nevertheless, it shows two architectural solutions to approaching technologies and leaves the regulatory issues for further studies.

TTP Works for Approaching Scenarios, But Regulations Need to Reimagine its Framework.

The first scenario is about a transaction with an unhosted wallet. In the scenario, no travel rule alliances might detect an obliged VASP for the unhosted wallet. Therefore, its counterpart VASP needs an alternative to verify the unidentified VASP's customer. Figure 16 describes the verification through a trusted third party, such as a telecommunication service provider and a clearing institute that possess the customer's information (Chung and Kang, 2020). In the scenario, an ordering VASP is identified in a travel rule society, but a beneficiary VASP is not. If the ordering VASP sends the payment message to a trusted third party, it notifies its customer of the action and verifies its customer. The ordering VASP executes the payment on a blockchain after verifying the trusted third party's reply.

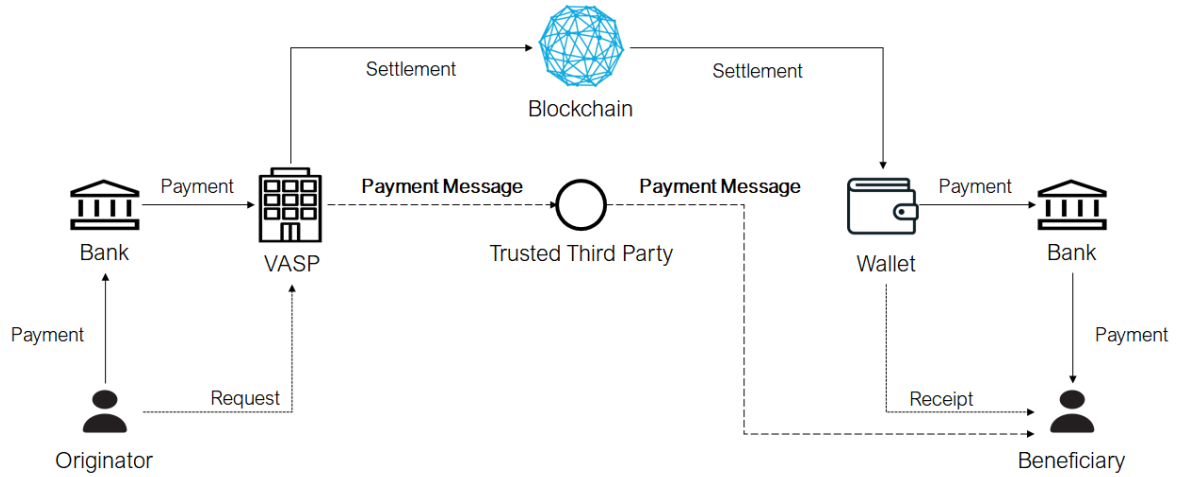

Figure 16. The intervention of a Trusted Third Party in the Payment by Virtual Assets.

The following scenario is when virtual assets dominate. Financial regulations could apply to the unhosted wallet when the fiat money dominates the market because the financial institutions reject the business relationship with the uncompliant virtual asset services (Figure 16). However, the next round of wallets, NFTs, and blockchain-based supply chains are that virtual assets permeate the payment market dominated by the USD, VISA, Mastercard, and Paypal. If the fiat money disappears at the market, a customer does not need to rely on centralized VASPs to exchange a virtual asset with fiat money and a financial institution to deposit and withdraw the fiat money. The payment workflow has a straightforward architecture consisting of only blockchain and wallets (Figure 17).

The workflow of the payment through wallets (Figure 17) looks like those of the most straightforward conventional retail payments (Figure 1). However, they have a fundamental difference. Blockchain does not have the payment message layer in its compressed payment, clearings, and settlement procedures, while the conventional payment runs on exchanging payment messages among banks, the clearing institute, and the central bank. Therefore, financial regulations should resolve the problems of the legitimacy and feasibility of law enforcement commented above. Telecommunication service providers, which have a centralized organization and reach almost all registered consumers, can offer a travel rule service layer to the blockchain-based payment workflow. Stakeholders need a discussion on inserting a travel rule service, mitigating the conflict with the philosophy of blockchain.

In conclusion, virtual assets should reimagine the regulations at a framework level. The questions are: How can regulations identify obliged entities and non-obliged entities when virtual assets dominate the payment market? Which are the scope of the principle of privacy protection, the scope of the global financial security, and industrialization if wallets, NFTs, and blockchain-based supply chains

interoperate with each other? Competent authorities need a longer view to design the regulations for VAs and VASPs. They should also consider the constraints of transforming their institutions and societies, taking an amount of cost (Fuentelsaz et al., 2012; Heiss et al., 2021).

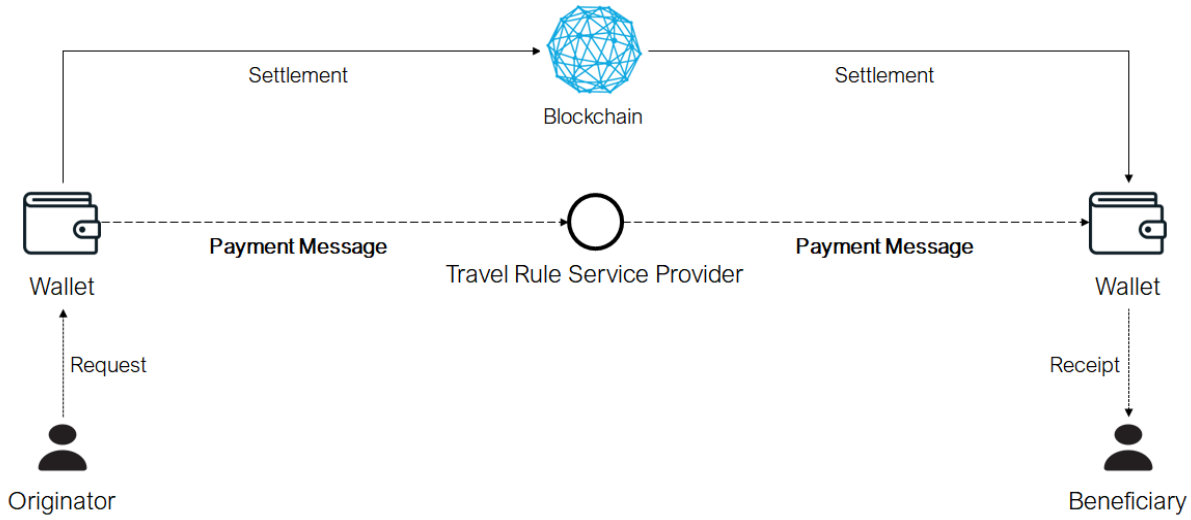

Figure 17. The Workflow of the Blockchain-Based Payment through Unhosted Wallets

5. Discussion

5.1. Summary of Findings

Architecture Analysis Results Shows Gaps Between Virtual Assets and Financial Regulations.

GI-TRUST analyzed the workflow of travel rule standards in the architecture of financial regulations and blockchain-based payment. The architecture analysis underlines three features of blockchain-based virtual assets (VAs). First, blockchain omits the payment message layer and compresses payment, clearings, and settlement into consensus algorithm and distributed ledgers (messagelessness). Second, VAs seamlessly flow across jurisdictions only if customers can access the Internet (cross-borderness). Third, the VA market changes fast as private sectors create VA business models and VASPs (dynamicity). Their architecture is the opposite of the financial institutions built by the legal foundation (stability), exchanging messages for payment, clearings, and settlement (messagefulness) focusing on local jurisdictions (borderness).

Those gaps between VAs and regulations challenge implementing the travel rule. Financial regulations insert the payment message layer among VASPs to trace the flow of VAs for the AML/CFT (FATF, 2012-2020). The FIU supervises them atop the suspicious transaction reports from VASPs analyzing the payment messages. However, the regulatory requirement means the conflict between financial regulations and blockchain governance. The market should adopt what their business model does not need (messagelessness vs. messagefulness). The regulations should adjust their jurisdictional enforcement to the cross-border payment of blockchains (cross-borderness vs. borderness) and apply those for financial institutions to the dynamic market of VAs and VASPs (dynamicity vs. stability). They result in FATF's (2021.07: 129) warning on the "sunrise" issue, as the market adoption has been stretching for two years although the market launched several travel rule standards.

GI-TRUST Suggests Four Solutions to Four Problems.

Responding to the recent clarification of FATF (2021.10), GI-TRUST proposes four solutions to the corresponding four problems in the global implementation of travel rule standards.

- The first problem is about the standardization by the market. The architecture analysis results show that the travel rule's procedures are inseparable, so choosing one standard replaces the other. Therefore, a VASP bears an immense burden of selecting a standard on a higher uncertainty than conventional *de-facto* standardization scenarios.
  - » GI-TRUST suggests that cooperation of travel rule service providers (TRSPs) can resolve the market adoption problem. In other words, a TRSP adopts a multi-channel integration (MCI) and develops its standard compatible with each other through the MCI (Figure 12). Then TRSPs can compete based on their quality of service in a bigger market.
- The second problem is the issue from the AML/CFT mission. The travel rule is one of the processes of an AML/CFT system, esp., an information system for the service of exchanging massive secure messages. Therefore, at a communication terminal among VASPs, the travel rule process should interoperate with the CDD, RA, STR, and TST processes for the system's mission (Figure 13).
  - » GI-TRUST suggests that FATF (2012-2020; 2021.10) extends its recommendations on the travel rule to accept the interoperation requirements: i.e., regulatory standards and technological guidelines for the interoperation of the travel rule with CDD, RA, STR, and TST (Table 5). It also suggests that a modular architecture extending financial institutions' KYC systems will help TRSPs adopt cutting-edge technologies and design the travel rule services according to VASPs' requirements (Figure 14).
- The third problem is pragmatic. The architecture analysis results suggest that standardizing the message format is a prerequisite of implementing the travel rule. First, travel rule standards contain the information of VAs and VASPs that have a much higher uncertainty than fiat money and conventional financial institutions. In addition, the lack of market dynamicity in the text might misunderstand or mistranslate the messages. Second, the standards need elaborate grammar and vocabulary to enhance the compatibility and interoperability of the travel rule standards.
  - » GI-TRUST suggests that FATF (2021.10: Paragraphs 182-183) extends the travel rule message items to ordering and beneficiary VASPs' information, the travel rule standard information, and VA information (Table 6). Furthermore, GI-TRUST proposes that a popular message standard IVMS101 adopts the elaborate message format of ISO 15022 (SWIFT message) (Table 8) and advances it to prepare a dynamic situation with smart contracts (Table 9).
- The fourth problem underlines fast-advancing technologies. The VA market changes fast, and the regulations also do their best to chase the advancing technologies. Especially, today's technical issue is re-connecting the payment message between centralized VASPs through decentralized VASPs and devices, out of the scope of regulations only two years ago (FATF, 2012-2020: INR 15; FinCEN, 2019).
  - » From a near-term view, GI-TRUST suggests that inviting a trusted third party to the payment message layer can impose the obligation on the non-obliged entities (Figure 16; Chung and Kang, 2020). However, it might be a temporary solution for a longer view. VAs connect services with NFT, supply chains, and decentralized identity. Therefore, GI-TRUST recommends that the market, regulators, and non-profit organizations redesign the regulation framework preparing for the time when VAs dominate the payment market (Figure 17).

5.2. Academic and Practical Implications

GI-TRUST Contributes a Standardization Model Harmonizing Regulations with Blockchain.

GI-TRUST's discussion contributes four points to the academy. First, GI-TRUST requests that academic societies prove the economic and technological feasibility of its solutions. The encryption, identification, and verification procedures are inseparable in a travel rule standard's workflow. Moreover, its adoption needs the consensus of a pair of VASPs. Therefore, a standard locks a VASPs pair and is likely to rely on the bargaining power of a VASP. The issue is different from usual standardization scenarios depending on network externalities, i.e., the membership size or the scope of services (Katz and Shapiro, 1985; Katz and Shapiro, 1994; Shapiro and Varian, 1999; Rysman, 2009). Therefore, the inseparable adoption by pairs requires rigorous economic analysis to prove the impact of the standardization model.

Second, GI-TRUST provides a guideline to design the reference architecture of the travel rule, extensively an AML/CFT system. In the knowledge of the task force team, multi-channel integration (Figure 12), modular architecture (Figure 14), elaborate message format (Tables 8-9), and centralized VASPs and TRSPs registries (Figure 14 and Table 6) are the best solutions to encourage the travel rule standards' compatibility and interoperability. Furthermore, they will mitigate the uncertainty of the standard adoption. GI-TRUST's recommendations encourage the academic societies to advance each of those components and integrate them into a reference architecture. Significant constraints in the design are re-balancing the governance between centralization and decentralization and real names and pseudonyms. For example, efficient decentralization of travel rule services among VASPs needs centralized governance of VASPs and TRSPs repositories in relevant mutual controls. If the market neglects the shared repository, the market might centralize by a few dominant TRSPs and VASPs.

Third, the travel rule issues stimulate the academy to study the governance of the VA market and the roles of regulations in a longer view. The travel rule weaves the real name principle of regulation with pseudonym principles of VAs and VASPs. Regulations assume that financial institutions have central organizations analyzing and reporting suspicious to competent authorities with keeping the privacy protection. However, customers assume that VAs and VASPs are reliable as long as they maintain pseudonymity and decentralization. Regulating VAs and VASPs addresses how the economy can harmonize decentralization with centralization. FATF (2012-2020; 2021.10) found that VASPs are centralized enough to impose the financial regulations, but soon concentrating on centralized VASPs leaves it void a majority of the VA market (*or* non-obliged entities *or* unhosted wallets). The conventional centralization approach of regulations will no longer work for VAs and VASPs if decentralized services dominate the market (Figure 17). The report leaves the issue of re-balancing between centralization and decentralization for further studies.

Fourth, GI-TRUST's recommendations orient the VA market to the convergence of blockchain with artificial intelligence (AI). The fourth industrial revolution suggests blockchain and AI as independent pillars, where blockchain replaces institutions for *trust* with consensus algorithms and AI human beings for thinking with machine learning algorithms (Schwab, 2017). Separating pillars was necessary at the initial stage but currently leaves a wide gap in compliant operation. Blockchain completes its mission of trust-building when it entrusts AI with diagnosing and supervising suspicious transactions as legitimate transactions reassure natural and legal persons. The solutions to compatibility (Figure 12), interoperability (Figure 14), and message standards (Tables 8-9) guide massive, secure, and unobstructed transmission of financial big data to AI (Table 5). Relevance of FIU's use of AI for supervision leaves for further studies. Inversely, AI also needs blockchain to feed big data on data marketplaces (WEF, 2021), but it is out of GI-TRUST's scope.

GI-TRUST Contributes a Comprehensive Approach to Multiple Stakeholders.

GI-TRUST highlights four points of cooperation in a comprehensive approach from a practical perspective. First, lawmakers and regulators need a broader scope of AML/CFT in a longer view. For example, the travel rule process interoperates with CDD, RA, STR, and TST processes to achieve the AML/CFT mission. Moreover, the AML/CFT system abides by broader financial regulations, e.g., the Act on Reporting and Using Specific Financial Information, the Banking Act, the Act on Real Name Financial Transactions and Confidentiality, and the Personal Information Protection Act in Korea. At the moment, VAs are provided mainly by VASPs but evolve into a more decentralized governance style (e.g., decentralized crypto exchanges and private wallets) through integrating with non-financial blockchains (e.g., NFT, blockchain-based supply chains, and DID services) (Figure 17). Understanding the regulatory framework and fast-advancing technologies will help to fill the regulation-technology gaps and avoid irreconcilable conflicts when VAs gets more popular in the market.

Second, VASPs' and TRSPs' participation is decisive to the success of implementing the travel rule. For example, a greedy strategy of a VASP or a TRSP might return most of the market share because of the lock-in by the pairs' inseparable adoption (Section 4.1). However, they should not neglect the *cross-borderness* of virtual assets (Section 2.2). The dominance in a local market by closing standards might trap a VASP or a TRSP in a local optimum trap as its partners choose a more beneficial standard with generous travel rule standards in the global market. In other words, even if a VASP has considerable bargaining power at a local jurisdiction, the VASP should keep in mind that there are much more VASPs in the global market. Therefore, GI-TRUST suggests that TRSPs open their standards to their rivals and VASPs cooperate with their competitors to implement the travel rule. An action point is that VASPs and TRSPs design a reference architecture according to GI-TRUST recommendations (Figures 12 and 14) and test the travel rule standards in local and global environments *together*.

Third, GI-TRUST recommends centralized governance in message format and VASPs and TRSPs registries for compatible and interoperable implementation of travel rule standards (Section 4.3). The centralized governance of trusted third parties prerequisites the trust of VASPs, TRSPs, customers, and competent authorities. The trusted third parties should represent the interest of VASPs and TRSPs to design practical message formats and registries. Concurrently, mutual control should work for them by transparent information publication, VASPs' and TRSPs' monitoring, and government supervision. Furthermore, the trusted third parties should be fully aware of jurisdictions' legal and market context to assess VASPs and TRSPs. At the moment, they should reach the information of the other jurisdictions to support the AML/CFT for cross-border virtual asset services. GI-TRUST recommends that local blockchain-related associations, societies, and communities lead their jurisdictions in their worldwide collaboration. They satisfy the constraints of interest representation, full awareness, and global access.

Fourth, GI-TRUST invites global non-profit organizations to lead the global cooperation of local associations, societies, and communities. Building global channels with multiple stakeholders consumes time, effort, and social capital, although it is timely implementing the travel rule. Non-profit organizations such as the World Economic Forum (WEF) and the Global Blockchain Business Council can use their social capital to rally those stakeholders from VASPs, TRSPs, competent authorities (e.g., the US FinCEN, Singapore's MAS, the Korean FIU), international financial institutions (e.g., FATF and BIS), standardization organizations (e.g., ISO, ITU-T, and IEEE SA), and civic organization. Their leadership will help design a sustainable, compliant, and virtual asset market atop a deep understanding of the local and global context, satisfying all stakeholders. For example, WEF has abundant experience in designing the future of the data economy (WEF, 2021.04), and GBBC leads the blockchain societies to plan the decentralized future (GBBC, 2021).

5.3. Limitations

GI-TRUST leaves two practical issues for further studies. First, GI-TRUST does not comment on the specificity of individual jurisdictions, while it focuses on the global features of VA services and their conflict with jurisdictions' diversity. For example, Korea's ARUSFI defines the national ID number as an originator's identifier and prescribes an ordering VASP sends the originator's identifier within three business days after the beneficiary VASP's request. On the other hand, FATF's (2021.10: 182-183) guidance lists the geographical address, date, and place of birth, or national ID number as an identifier option and suggests submitting the originator's identifier immediately. The discrepancy between jurisdictions might obstruct the global implementation of the travel rule.

Second, GI-TRUST does not provide a reference architecture but only recommendations to design it. Therefore, GI-TRUST's recommendations call for rigorous design of the reference architecture. The design should rely on sound economic analysis of the market's success and failure in implementing the travel rule. The analysis should also suggest the government's and standardization bodies' intervention. The evaluation could base on an analysis of empirical data obtained, for example, from interviews with experts or test implementations of the solutions. This evaluation would also result in more substantial support for the proposed solutions. Furthermore, GI-TRUST expects a pilot test of the global implementation of travel rule solutions to reveal practical issues and provide clues to the sophistication of the regulatory and technological standards.

6. Concluding Remarks

The travel rule separating traceability from the decentralization of pseudonyms weaves the regulatory framework with the technological architecture and business incentives. Thus, it is time to ask if traditional approaches from dividing a problem into simpler ones can work for the travel rule, where solving one problem makes another one. In short, the travel rule, a small component of financial regulation for blockchain, calls for a significant change in the approaches of regulators, policymakers, VASPs, TRSPs, associations, and civic organizations. GI-TRUST's In-depth conversations derived a comprehensive solution feasible economically, technologically, and regulatorily to the problems of implementing the travel rule in four practical points: compatibility, interoperability, message formats, and fast-advancing technologies. The sun of the travel rule will rise faster once the worldwide societies build adequate regulatory and technological standards in collaboration with all those stakeholders.

References

31 CFR (no date). *Title 31 – Money and Finance: Treasury in the Electronic Coe of Federal Regulations*. Legal Information Institute (https://www.law.cornell.edu/cfr/text/31).

Albert, R., Jeong, H., and Barabasi, A.-L. (1999). "Diameter of the World-Wide Web," *Nature*, 401: 130-131. (https://doi.org/10.1038/43601).

Albert, R., Jeong, H., and Barabasi, A.-L. (2000). "Error and attack tolerance of complex networks," *Nature*, 406 (6794): 378-382. (https://doi.org/10.1038/35019019).

Allison, I. (2020). "Inside the standards race for implementing FATF's travel rule," *CoinDesk*, Feb 5th, (https://www.coindesk.com/business/2020/02/04/inside-the-standards-race-for-implementing-fatfs-travel-rule/).

Alper, T. (2021). "FATF wants to 'gut' DeFi with 'vague' new guidelines, say crypto players," *Cryptonews*, Oct 29th, (https://cryptonews.com/news/fatf-wants-to-gut-defi-with-vague-new-guidelines-say-crypto-players.htm).

AMLO-FINMA (2021). *Regulation for the Swiss Financial Market Supervisory Authority on Anti-Money Laundering and Combating the Financing of Terrorism in the Financial Sector*. Ordinance of the Swiss Financial Market Supervisory Authority, Last Updated on Jan 1st, 2021. (https://www.fedlex.admin.ch/eli/cc/2015/390/de).

ARUSFI (2020). *Act on Reporting and Using the Specific Financial Information*. Act No. 17299 amended on May 19th, 2020, and enforced on May 20th, 2020. (https://law.go.kr/법령/특정금융거래정보의보고및이용등에관한법률).

Blind, K. (2004). The Economics of Standards: Theory, Evidence, Policy. Edard Elgar Publishing. (ISBN 978-1-84376-793-0).

BOK. (2014). *Payment and Settlement Institution of Korea*. Seoul, ISBN 979-11-5538-145-8 93320 (Written in Korean), (https://www.bok.or.kr/portal/bbs/P0000610/view.do?nttId=95839&menuNo=200466&pageIndex=1).

Chung, J. and Kang, H.-G. (2020). "Study of methodologies for compliance with the travel rules when trading virtual assets by virtual asset operators (VASPs): With a focus on the FATF's Interpretative Note to Recommendation 15 (INR 15), Paragraph 7(b)," *Korean Journal of Law and Economics*, 17 (1): 331-352 (Written in Korean).

CoolBitX. (2020). *Sygna Bridge Report: FATF Recommendation 16 Technical Solution for Virtual Asset Transactions*. (https://www.sygna.io/blog/types-of-fatf-r16-crypto-travel-rule-solutions/).

Cusuman., M. and Gawer, A. (2002). "The elements of platform leadership," *MIT Sloan Management Review*, 43 (3): 51-58. (https://www.proquest.com/docview/224971159?pq-origsite=gscholar&fromopenview=true).

Datamation, Co., Ltd. (2021). "Application of the Travel Rule to Implementing the AML (AML KYVC)," *Materials of Datamation, Co., Ltd.'s Intelligent Financial Engineering Laboratory*. (http://ec2-13-125-245-226.ap-northeast-2.compute.amazonaws.com:8080/main.do?changeLocale=en)

FATF (2012-2020), *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*, FATF, Paris, France, (www.fatf-gafi.org/recommendations.html).

FATF (2019), *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, FATF, Paris, (www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html).

FATF (2021.07). *Second 12-month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers*. FATF, Paris, France (http://www.fatf-gafi.org/publications/fatfrecommendations/documents/second-12-month-review-virtual-assets-vasps.html).

FATF (2021.10). *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, FATF, Paris, France, (www.fatf-gafi.org/publications/fatfrecommendations/documents/Updated-Guidance-RBA-VA-

VASP.html).

FinCEN (2019). Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies. FinCEN Guidance, FIN-2019-G001, (https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-certain-business-models).

FinCEN (2020). *Threshold for the Requirement to Collect, Retain, and Transmit Information on Funds Transfers and Transmittals of Funds that Begin or End Outside the United States, and Clarificaion of the Requirement to Collect, Retain, and Transmit Information on Transactions Involving Convertible Virtual Currencies and Digital Assets with Legal Tender Status*. Joint Notice of Proposed Rulemaking at Federal Register, 85 (208): 68005-68006, (https://www.federalregister.gov/documents/2020/10/27/2020-23756/threshold-for-the-requirement-to-collect-retain-and-transmit-information-on-funds-transfers-and).

Fuentelsaz, L., Maicas, J.P., and Polo, Y. (2012). "Switching costs, network effects, and competition in the European mobile telecommunications industry," Information Systems Research, 23 (1): 93-108, (https://doi.org/10.1287/isre.1100.0303).

Genkin, D., Papadopoulos, D. and Papadopoulos, C. (2018). "Privacy in decentralized cryptocurrencies," Communications of the ACM, 61 (6): 78-88.

GBBC (2021). *Global Standards Mapping Initiatives*. Insight Reports and Interactives of Global Map of the Global Blockchain Business Council in Collaboration with 131 Partners in 187 Jurisdictions. (https://gbbcouncil.org/gsmi/).

Goldsmith, R.W. (1973). "The historical background: Financial institutions as investors in corporate stock before 1952," *International Investors and Corporate Stock: A Background Study*. NBER, ISBN: 0-870-14237-2.

Goodwin, J. (2021). "What is an NFT? Non-fungible tokens explained," *CNN Business*, November 10th, 2021. (https://www.cnn.com/2021/03/17/business/what-is-nft-meaning-fe-series/index.html).

GWP (2020). *Travel Rule Report*. (https://www.gwp.ch/Downloads/Travel%20Rule%20Report/November%202020/gwp_Travel-Rule-Report_November-2020.pdf).

Haile, N. and Altmann, J. (2018). "Evaluating investments in portability and interoperability between software service platforms," *Future Generation Computer Systems*, 78: 224-241. (http://dx.doi.org/10.1016/j.future.2017.04.040).

Hardjono, T., Lipton, A. and Pentland, A. (2020). "Toward a public-key management framework for virtual assets and virtual asset service providers," *Journal of FinTech*, 1 (1): 2050001.

Heiss, F., McFadden, D., Winter, J., Wuppermann, A., and Zhou, B. (2021). "Inattention and switching costs as sources of inertia in medicare Part D," *American Economic Review*, 111 (9): 2737-2781. (https://doi.org/10.1257/aer.20170471).

Im, F. (2021). S. Korea's crypto rules might only help the 'big 4' exchanges. *Coindesk*, Apr. 1st, (https://www.coindesk.com/policy/2021/04/01/s-koreas-crypto-rules-might-only-help-the-big-4-exchanges/).

ISO. (1999). "Securities – Scheme for Messages (Data Field Dictionary)," *ISO 15022*.

Jasanoff, S. (2006). "Ordering knowledge, ordering society," *State of Knowledge: The Co-Production of Science and Social Order*. (S. Jasanoff, Ed.) Routledge, London.

Jevans, D., Hardjono, T., Vink, J. Steegmans, F., Jefferies, J. and Malhotra, A. (2020). *Travel Rule Information Sharing Architecture for Virtual Asset Service Providers*. TRISA Whitepaper vs. 8. (https://trisa.io/trisa-whitepaper/).

JWG IVMS. (no date). *InterVASP Messaging Standards: IVMS101 Universal common language for communication of required originator and beneficiary information between virtual asset service providers*. (http://34.64.107.172/~vasp/wp-content/uploads/2020/05/IVMS101-interVASP-data-model-standard-issue-1-FINAL.pdf).

Kang, S., Shim, D., and Altmann, J. (no date). "Consumer Adoption of Security Features of E-Payment Services and its Implications for Building Security into Internet Infrastructure," Under Review at *Electronic Commerce Research and Application*.

Katz, M.L. and Shapiro, C. (1985). "Network externalities, competition, and compatibility," *American Economic Review*, 75 (3): 424-440.

Katz, M.L. and Shapiro, C. (1994). "Systems competition and network effects," *Journal of Economic Perspectives*, 8 (2): 93-115.

Lim, Y. (2020). "Financial institution's market share: Woori Bank at the top in deposit and KB Bank in lending," *Daily Hankook*, 2020.03.20 (written in Korean) (http://daily.hankooki.com/lpage/column/202003/dh20200320080716145650.htm).

Marquez, R. (2021.10.29.). "FATF publishes crypto guidance, why the DeFi sector could be at risk," *Bitcoinist*, (https://bitcoinist.com/fatf-publishes-crypto-guidance-why-the-defi-sector-could-be-at-risk/).

Park, S.H. (2021). "Oligopoly, Taxation, Travel Rule: Challenges for Institutionalizing the Cryptoexchanges," *Hankyoreh*, 2021.10.13. (Written in Korean) (https://www.hani.co.kr/arti/economy/it/1014922.html).

Pels, E. (2021). "Optimality of the hub-spoke system: A review of the literature, and directions for future research," *Transport Policy*, 104: A1-A9. (https://doi.org/10.1016/j.transpol.2020.08.002).

PSN02 (2019). *Notice to Holders of Payment Service License (Digital Payment Token Service) for Monetary Authority of Singapore Act*, CAP. 186. MAS Notice PSN02. Last Revised on 28 June 2021, (https://www.mas.gov.sg/regulation/notices/psn02-aml-cft-notice---digital-payment-token-service).

Riegelnig, D. (2019). *OpenVASP: An Open Protocol to Implement FATF's Travel Rule for Virtual Assets*. OpenVASP, (https://www.openvasp.org/wp-content/uploads/2019/11/OpenVasp_Whitepaper.pdf).

Rivest, R., Adleman, L., and Dertouzos, M. (1978). "On data banks and privacy homomorphisms," *Foundations of Secure Computation*, 4 (11): 169-180. (https://www.semanticscholar.org/paper/ON-DATA-BANKS-AND-PRIVACY-HOMOMORPHISMS-Rivest-Dertouzos/c365f01d330b2211e74069120e88cff37eacbcf5).

Rysman, M. (2009). "The economics of two-sided markets," *American Economic Association*, 23 (3): 125-143. (https://doi.org/10.1257/jep.23.3.125).

Schwab, K. (2017). *The Fourth Industrial Revolution*. World Economic Forum.
(ISBN: 978-1524758868).

Shapiro, C. and Varian, H.R. (1999). *Information Rules: A Strategic Guide to the Network Economy*. Harvard Business School Press.
(ISBN: 0-87584-863-X).

TRP. (no date). *Travel Rule Protocol*. GitHub Project ID 18618478.
(https://gitlab.com/travelruleprotocol/travel-rule-protocol).

Tu, Y. (2000). "How robust is the Internet?" *Nature*, 406 (6794): 353-354.
(https://doi.org/10.1038/35019222).

Van Dijk, M., Gentry, C., Halevi, S., and Vaikuntanathan, V. (2010). "Fully homomorphic encryption over the integers," *Advances in Cryptology – EUROCRYPT 2010*, 24-23.
(https://doi.org/10.1007/978-3-642-13190-5_2).

VerifyVasp. (no date). *Key features and structure of VerifyVASP*.
(https://docs.verifyvasp.com/overview).

WEF (2020.04). *Inclusive Deployment of Blockchain for Supply Chains: Part 6 – Introduction*. White Paper of the World Economic Forum,
(https://www.weforum.org/whitepapers/inclusive-deployment-of-blockchain-for-supply-chains-part-6-a-framework-for-blockchain-interoperability).

WEF (2020.12). *Bridging the Governance Gap: Interoperability for Blockchain and Legacy Systems*. White Paper of the World Economic Forum,
(https://www.weforum.org/whitepapers/bridging-the-governance-gap-interoperability-for-blockchain-and-legacy-systems).

WEF (2021.04). *Data-Driven Economics: Foundations for Our Common Future*. White Paper of the World Economic Forum,
(https://www.weforum.org/whitepapers/data-driven-economies-foundations-for-our-common-future).

Whitaker, A. (2019). "Art on blockchain: A primer, history, and taxonomy of blockchain use cases in the arts," *Artivate*, 8 (2): 21-46.
(https://doi.org/10.34053/artivate.8.2.2).

Sources of Icons

: Logo of the Global Blockchain Business Council (https://gbbcouncil.org).

: https://www.flaticon.com/kr/authors/xnimrodx.

: https://icon-icons.com/ko/아이콘/사람이/110935.

: https://www.flaticon.com/kr/free-icon/goverment_1683953 (user50870304) .

: https://icon-icons.com/ko//아이콘/기관/80/144269.

: https://icons8.com/icons/set/bitcoin.

: https://freeicons.io/life-style-icons-14/wallet-icon-29345s.

Acknowledgment

Lead Authors

Kibae KIM (Principal Researcher, Korea Policy Center for the Fourth Industrial Revolution, KAIST)
Jung Hweon JEON (Chairman, Global Cooperation Committee, Korea Blockchain Association)
So Young KIM (Director of the Korea Policy Center for the Fourth Industrial Revolution, KAIST)

Content Contributors:

Jae Geun SEOL (Senior Vice President, Korea Blockchain Association)
Sandra RO (CEO, Global Blockchain Business Council)
Anson ZEALL (Chairman, International Digital Asset Exchange Association)
Jong-Goo YI (Lawyer, Lawfirm Kim & Chang)
Jeong Ha LEE (Former Director, Korea Financial Intelligence Unit)
Joel CHUNG (President, Association of Certified Anti-Money Laundering Specialist)
Seok Hae HWANG (President, Datamation Co. Ltd.)
Min Seob LEE (Senior Consultant, Lawfirm Yulchon)

Reviewers:

Jörn ALTMANN (Professor, Technology Management Economics and Policy Program, College of Engineering, Seoul National University)
Seunghyun KIM (Senior Research Fellow, Science and Technology Policy Institute)
Sheila WARREN (Deputy Head of the Centre for the 4th Industrial Revolution, World Economic Forum)
Ashley LANNQUIST (Lead, Digital Currency Governance Consortium, World Economic Forum)
Tanvi RATNA (CEO, Policy 4.0)
Suk Won Harold KIM (Director, Korea Blockchain Association)
Jeff Yoonchul KANG (Korea Country Manager, CoolBitX)
Wooju GWON (VerifyVasp Lead, Lambda256)
Myunghun CHA (CEO, Coinone)
James Won-Ki Hong (Director of CCBR, POSTECH)
Riyad CAREY (Senior Policy Analyst, Global Blockchain Business Council)
Kyung Geun LEE (Professor, Seoul School of Integrated Science and Technology)

Communication Lead:

Daseul Moon (Manager, Korea Blockchain Association)

Representative Contact:

Suk Won Harold Kim (Director, Korea Blockchain Association)
tel: 02-6412-4778~9
fax: +82-2-6412-4776
email: kbca@kblockchain.org