Accountable Wallet

A wallet that can prove its legitimacy in a verifiable form

bg in

blockchain
governance
initiative
network

The Global Network for Blockchain Stakeholders™

This study is a work product of IAM, Key Management and Privacy Working Group of BGIN.

1. Abstract

The proposed framework for establishing the legitimacy of transactions in decentralized finance (DeFi) is a crucial step towards creating a more secure, transparent, and compliant ecosystem. By defining clear criteria for legitimacy and considering the unique characteristics of DeFi, this paper aims to provide a comprehensive approach to addressing the challenges posed by the anonymity and immutability of crypto assets.

At the core of the proposed framework is the principle that transactions should only be considered legitimate in cases of good faith and absence of negligence. This stance emphasizes the importance of due diligence and responsible behavior on the part of investors, as even well-intentioned actions can facilitate illicit activities if proper precautions are not taken. By penalizing negligence, regardless of intent, the framework seeks to encourage a culture of caution and vigilance among DeFi participants.

The paper identifies three key aspects of legitimacy that must be considered when evaluating the validity of transactions: the legitimacy of the wallet holder, the legitimacy of the wallet's past actions, and the legitimacy of the Crypto Asset Provenances. These aspects are designed to address the unique challenges posed by the anonymity of wallet holders, the anonymity of transactions, the inviolability of assets, and the inviolability of transactions in DeFi.

In particular, the paper highlights the significance of verifying the legitimacy of the Crypto Asset Provenances, an aspect that is often overlooked in traditional finance. By requiring investors to ensure that the funds they receive have not been obtained through illegal means, the framework aims to disrupt the money laundering process and make it more difficult for illicit actors to integrate their proceeds into the legitimate economy.

The proposed framework also acknowledges the complexity of defining universal transaction legitimacy, given the variations in legal frameworks across jurisdictions. Rather than focusing on specific legal regulations, the paper emphasizes the need for a flexible approach that can adapt to the decisions of judicial and administrative authorities in each jurisdiction. This adaptability is achieved through the use of compliance modules, which can be established in advance with digital signatures and timestamps, and selected based on the specific details of each transaction.

Moreover, the paper recognizes that compliance rules are not solely dependent on jurisdiction but also on factors such as the assets being traded, the transaction conditions, and the individual preferences of investors. By considering these variables and allowing for customizable compliance modules, the framework ensures that

legitimacy can be assessed in a context-specific manner, enhancing the overall effectiveness of the system.

The proposed criteria for legitimacy in DeFi transactions represent a thoughtful and nuanced approach to addressing the unique challenges posed by this emerging ecosystem. By emphasizing the importance of good faith, penalizing negligence, and considering the multiple aspects of legitimacy, the framework lays the foundation for a more secure, transparent, and compliant DeFi environment. As the DeFi space continues to evolve, this paper's contributions will serve as a valuable starting point for further research and development in the field of decentralized finance compliance.

Table of contents

2. Scope

3. Normative Reference

This document has no normative reference.

4. Terms and Definitions

This document uses the following terms as the shortcut for more complete wording provided as the definition. When the term appears within this document, it should be read as being replaced by the definition.

crypto asset

crypto watch list (originally defined in this paper?)

> a list of wallet addresses that have been confirmed to be managed as destinations for criminal proceeds, etc. Generally managed by jurisdictional authorities. It is sometimes called a sanctions list. However, in this paper, the term sanctions list is used to manage antisocial individuals and terrorist organizations to distinguish it from a list of wallet addresses.

decentralized autonomous organization (DAO)

> a voluntary association with the operating principles of digital cooperativism. As voluntary associations, they are a cross-jurisdictional way for strangers, friends, or unlikely allies to pseudonymously come together toward common goals, supported by a token model, incentives, and governance. Members of a DAO can have representative ownership of its digital assets through a token, which often simultaneously acts as a governance right and network utility.

[Source: Kei (2021)]

decentralized finance (DeFi)

financial application that could consist of a part of a decentralized financial system

[Source: Ushida and James (2021)]

CEXs

DApps

decentralized financial services, the associated smart contract addresses facilitating these services, such as decentralized vertical asset exchanges (DEXs). It is also called a DeFi protocol, but we will call it this to distinguish it from DeFi in the broader sense.

DEX

soulbound token (SBT)

publicly visible, non-transferable (but possibly revocable-by-the-issuer) token held by the soul

[Source: Weyl et al. (2022)]

self sovereign identity (SSI)

digital movement that recognizes an individual should own and control their identity without the intervening administrative authorities

[Source: Sovrin Foundation (2018)]

verifiable credential (VC)

tamper-evident credential that has authorship that can be cryptographically verified

[Source: World Wide Web Consortium (2022 a)]

decentralized identifier DID

identifier that enables verifiable, decentralized digital identity

[Source: World Wide Web Consortium (2022 b)]

Zero Knowledge Proof (ZKP)

5. Abbreviations and Symbols

In this document, the following abbreviations and symbols are used.

AML: Anti-Money Laundering

BGIN: Blockchain Governance Initiative Network

CTF: Counter Terrorism Financing

FATF: Financial Action Task Force

KYC: Know-Your-Customer

ML: Money Laundering

TF: Terrorist Financing

VASP: Virtual Asset Service Provider

PII: Personally Identifiable Information

6. Introduction

6.1. Characteristics of Decentralized Finance in Contrast to Traditional Finance

DeFi has often been criticized for its susceptibility to illicit activities such as money laundering and unfair trading practices[1]. If this assertion holds true when compared to traditional finance, it implies that certain inherent characteristics of DeFi, absent in traditional finance, facilitate these malicious activities. This chapter delves into the unique features of DeFi that potentially enable such misconduct, setting the stage for the proposed countermeasures discussed in the subsequent chapters.

6.1.1. Anonymity of Wallet holders

- Lack of Credit Assessment

1

Self-custodial wallets in the realm of crypto assets can effectively function as financial asset accounts without the need for KYC procedures or other forms of personal identification. This anonymity allows wallet holders to engage in transactions without disclosing their PII to any party, a distinctive feature in contrast to traditional finance that assessing counterparty risk is an essential process to transactions in traditional finance.

This confluence of factors—the anonymity of Crypto Asset and the trustless nature of DeFi—has inadvertently fostered an environment conducive to money laundering and other illicit activities by circumventing the need for due diligence on transaction counterparties. The unintentional complacency of well-intentioned investors further exacerbates the ease with which malicious actors can exploit these systems for nefarious purposes.

- Crypto Asset Travel Rule

  VASPs play a crucial role in converting crypto assets to fiat currencies. With the introduction of Travel Rule[2], a certain screening process was introduced for the transfer of crypto assets between VASPs. Still, many jurisdictions virtually permit VASPs to accept crypto assets from external self-custodial wallets[3] without imposing stringent sender verification[4]. In such cases, as long as crypto assets pass through a self-custodial wallet, it is possible to deposit crypto assets with untraceable origins into VASPs. It technically means that crypto assets from any illicit source could be deposited into VASPs, rendering the strict travel rules among VASPs ineffective.

- Ineffectiveness of Crypto Watch Lists

  Various regulatory authorities across jurisdictions have designated wallets associated with illicit activities on Crypto Watch Lists, mandating regulated VASPs to reject Crypto Asset deposits from these wallets. However, when these listed wallets attempt to deposit funds into VASPs after complex obfuscation through various methods, detecting the illicit origins of the crypto assets becomes exceedingly challenging.

  Moreover, maintaining an up-to-date crypto watch list poses significant difficulties. For instance, although the United States has banned the use of the Tornado Cash protocol[5], simply adding the contract addresses of such banned DApps to the crypto watch list is an ineffective measure. Malicious actors can

---

2

3 To be defined in chapter 8.

4

5

easily deploy new contract addresses, perpetuating a cat-and-mouse game.

- Compliance-Privacy Trade-off

  If the root cause of this problem lies in the anonymity of wallets, a straightforward solution would be to associate wallets with personal information verified by a trusted third party and exchange this information during transactions, enabling parties to assess the legitimacy of the transaction based on the provided information. However, this approach raises privacy concerns.

  Recent developments in technologies such as DIDs and VCs have focused on enabling individuals to prove their eligibility for transactions without disclosing excessive personal information. This paper explores the applicability of these technologies.

- Need for Technology to Prove the Legitimacy of Wallet Holders While Protecting Their Privacy

  The inherent anonymity and trustless nature of crypto assets, coupled with the lack of effective sanction enforcement, have inadvertently created an environment conducive to illicit activities in the DeFi space. Addressing these challenges requires a delicate balance between preserving user privacy and ensuring regulatory compliance.

  This paper explores the potential of existing technologies, such as DIDs, VCs, SBTs, ZKPs and so on to demonstrate legitimacy and transaction eligibility with minimal disclosure of personal information. It also examines the democratic and self-sovereign aspects of the credential issuance and verification processes.

  The subsequent chapters propose a novel framework that leverages advanced cryptographic techniques to enable the provable legitimacy of wallet holders without compromising their privacy, paving the way for a more secure and compliant DeFi ecosystem.

6.1.2. Anonymity of Transactions

- Identification Risks of Actual Wallet holder from Transaction Data

  The anonymity of wallet holders and the anonymity of transactions are distinct concepts. Even if the information about the wallet holder is encrypted using proper technology, if the transaction history of the wallet is recorded on a public blockchain and can be seen by anyone, advanced analysis of on-chain data can often reveal the approximate identity of the wallet holder. In this sense, Satoshi Nakamoto's notion that privacy can be ensured through the anonymity of wallet

holders has been largely refuted today.

- Application of ZKP Technology

  The above issue has been pointed out for over a decade, leading to the emergence of blockchains and DApps that utilize ZKP techniques, such as Zcash[6], and mixing protocols like Tornado Cash[7]. These technologies enable the sending and receiving of crypto assets while obfuscating information such as the wallet addresses and the transaction amounts on the blockchain.

  However, they often inadvertently make it difficult to detect illegal transactions. It has been pointed out that these solutions to privacy risks are being misused for ML/TF[8].

- Money Laundering Using DEXs

  Moreover, DApps also provide a degree of transaction anonymity. In addition to the aforementioned Tornado Cash, even DEXs, which do not inherently aim to provide anonymity function, offer a certain degree of anonymity and commingle crypto assets. Many DEXs provide Crypto Asset trading functionality through a liquidity pool mechanism. Most DEXs do not require authentication for usage, allowing anyone holding crypto assets to become a liquidity provider. Due to the liquidity pool mechanism, DEXs do not strictly facilitate peer-to-peer transactions. The liquidity pool itself has an address and momentarily becomes the owner of the crypto assets. Consequently, the pool may contain crypto assets sourced from illegal proceeds, and given the large number of users, tracing the destination of the pooled crypto assets becomes extremely challenging. Strictly speaking, from a legal perspective, if even a single liquidity provider in a DEX has supplied liquidity from an illegal source, all users of that DEX become counterparties to illegal transactions, indirectly assisting in money laundering or other illicit activities.

- Need for Technology to Prevent Illegal Transactions While Protecting Transaction Privacy

  The anonymity of transactions in DeFi ecosystem presents both opportunities and challenges. While advanced cryptographic techniques like zero-knowledge proofs and mixing protocols have enabled users to transact without revealing their identities or transaction details, these same technologies have inadvertently facilitated illicit activities such as money laundering.

6

7

8

In light of these challenges, this paper seeks to develop a methodology that strikes a balance between protecting transaction secrecy and preventing illegal transactions. By leveraging advanced cryptographic techniques, such as zero-knowledge proofs, the proposed framework aims to enable users to demonstrate their legitimacy without revealing sensitive information.

The subsequent sections of this paper delve into the technical and conceptual aspects of this proposed methodology, exploring how it can be applied to various blockchain architectures and transaction models. By providing a means for users to prove their compliance without compromising their privacy, this framework aims to mitigate the trade-off between anonymity and regulatory oversight, fostering a more secure and transparent DeFi ecosystem.

6.1.3. Asset Inviolability

- Difficulty in Asset Seizure

  Even if regulatory authorities successfully identify self-custodial wallets involved in illicit transactions on the blockchain, they cannot confiscate the associated assets in the same manner as in traditional finance unless they can identify the actual wallet holder and compel them to reveal their private keys through legal means. This process becomes impossible if the assets are managed in self-custodial wallets anonymously, or if are managed by terrorist organizations where there is no legal means of confiscation.

  One of the proposed potential conceivable methods for seizing or invalidating crypto assets is for validators to arbitrarily invalidate the tokens of the offending wallets or exclude their transactions from being included on the blockchain. This was actually done in one of the biggest Bitcoin mining pools, but it was rewound after facing a lot of opposition from pool participants[9]. Permitting such actions would grant excessive power to validators, undermining one of the core value propositions of public blockchains—the self-sovereignty of assets, leading it could make it pointless to use DeFi. Therefore, this paper does not recommend such an approach. It means that the legitimacy of a wallet should be self-proven, not by validators.

- Building an Economy Formed by Legitimate Users

  Given the premise that illegally obtained Crypto Asset assets held by external parties cannot be confiscated or invalidated, the imperative for all participants acting in good faith is to rigorously avoid transacting with wallets holding such

9

illicit assets. This approach effectively severs the means for converting these illicit assets into other forms of monetary value.

- Establishing a Method to Verify the Legitimacy of Counterparties

  The inviolability of assets in DeFi ecosystem poses significant challenges for regulatory authorities seeking to combat illicit activities. The anonymity of self-custodial wallets and the decentralized nature of public blockchains render traditional methods of asset seizure and invalidation largely ineffective. In light of these limitations, the onus falls on the participants themselves to maintain the integrity of the ecosystem by rigorously avoiding interactions with wallets associated with illicit activities.

  However, the problem lies in the immense difficulty of determining the legitimacy of counterparties and verifying that their current holdings were obtained through legitimate means.

  This paper proposes a novel approach to address this challenge by introducing a framework that enables wallets to establish and prove their legitimacy to their transaction counterparties. By equipping wallets with additional credibility proofs and providing techniques for investors to verify the trustworthiness of their counterparties, this framework aims to create an economy formed by legitimate transactions. This self-proofing-verifying ecosystem would effectively isolate wallets engaging in illicit activities, severing their access to other forms of monetary value.

  However, the success of this approach hinges on the ability to reliably determine the legitimacy of transaction counterparties, verify the legal provenance of their asset holdings and incentives to stay away from fraudulent wallets. The following chapters delve into the technical and conceptual aspects of this proposed framework, exploring how advanced cryptographic techniques and decentralized attestation mechanisms can be leveraged to enable the provable legitimacy of wallets and their holdings while preserving user privacy.

  By empowering participants to make informed decisions about their transaction counterparties and incentivizing compliant behavior, this framework aims to create a more secure and transparent DeFi ecosystem that upholds the principles of asset self-sovereignty while deterring illicit activities.

6.1.4. Inviolability of Transactions

- Difficulty in Preventing Illicit Transactions

  In public blockchain transactions, as long as the transaction fee paid by the

transaction creator to the validator is sufficient, no one can, basically, externally stop the creation and inclusion of transactions on the blockchain. This property makes it fundamentally impossible to prevent crypto asset transfers between wallets managed by investors who lack the intention to act legitimately. Moreover, it is challenging to stop the illegal conversion of illicit crypto assets into goods or fiat currencies in jurisdictions that do not comply with global anti-money laundering regulations such as those set by the FATF. As mentioned in the previous section, the only conceivable method to stop illegal transactions would be for validator to arbitrarily refuse to validate certain transactions. However, it is impossible for validators to verify the legality of all transactions submitted to them. Previous research[10] has also explored this possibility but concluded that it would be extremely difficult to implement.

- Issues Arising from the Inability to Reject Crypto Asset Receipts

  Another significant problem arising from this property is that even legitimate investors cannot refuse to receive illicit crypto assets sent to them. Since the receipt of illicit crypto assets cannot be rejected, wallets that have received such crypto assets cannot be immediately considered illegitimate. This complicates the judgment of the legitimacy of any given wallet.

  It is not only difficult but also fundamentally impossible to definitively determine whether a wallet that has received illicit crypto assets has actively participated in illegal activities based solely on on-chain data. Furthermore, if wallets that have received illicit crypto assets are not penalized in any way, it becomes impossible to deter money laundering using crypto assets. Therefore, it is crucial to design a system that incentivizes each wallet to avoid receiving illicit crypto assets, as a countermeasure against the ease of creating and holding multiple wallets.

- Giving incentives for maintaining one's legitimacy

  The inviolability of transactions in the DeFi ecosystem presents significant challenges for preventing illicit activities and enforcing regulatory compliance. The fundamental properties of public blockchains, such as the inability to censor transactions and the immutability of recorded transactions, make it extremely difficult for authorities to intervene and stop illegal transactions from being processed. Moreover, the inability of legitimate investors to reject the receipt of illicit crypto assets further complicates the issue, as wallets that have inadvertently received such funds cannot be immediately considered illegitimate based solely on this fact. In other words, the problem lies in the difficulty of determining whether a wallet that has received illicit crypto assets has actively

10

participated in illegal activities based solely on on-chain data. This ambiguity creates a significant obstacle for deterring money laundering and other illicit activities in the DeFi ecosystem.

To address these challenges, the paper proposes a novel approach that focuses on incentivizing each wallet to avoid receiving illicit crypto assets, rather than relying on external authorities to police transactions. By creating a system that rewards compliant behavior and penalizes the receipt of illicit funds, this framework aims to create a self-regulating ecosystem that deters malicious actors from exploiting the inherent properties of public blockchains for nefarious purposes.

The subsequent sections of this paper delve into the technical and conceptual aspects of this proposed incentive structure, exploring how advanced cryptographic techniques and decentralized attestation mechanisms can be leveraged to create a more secure and compliant DeFi ecosystem. By aligning the incentives of participants with the goals of regulatory compliance and the prevention of illicit activities, this framework seeks to strike a balance between the benefits of decentralization and the need for effective oversight and enforcement.

6.2. Money Laundering and Terrorist Financing

6.2.1. Money laundering using crypto

Money laundering using crypto assets refers to the process of utilizing crypto assets to disguise the proceeds of crime as funds or assets obtained through legitimate means. The objective of money launderers, in this context, is to cleanse various types of illicit funds, including those derived from crypto asset-related crimes such as hacking, as well as proceeds from other illegal activities like drug sales, converting them into seemingly legitimate funds.

A typical money laundering process using crypto asset involves the following steps:

1. First, the criminal proceeds are converted into crypto assets. This is often done through VASPs that do not require decent KYC, Bitcoin ATMs, VASP accounts that have been illegally sold, mining, or transactions on the dark web.
2. Next, the crypto assets are routed through multiple self-custodial wallets, DApps, and cross-chain transactions to obfuscate the trail of funds.
3. Finally, the crypto assets are converted back into fiat currency through VASPs or dark web transactions. By declaring the fiat currency proceeds obtained through this

process as capital gains from legitimate crypto asset trading and paying taxes accordingly, the illicit funds can be disguised as legitimately earned income.

(Insert exiting definitions from FATF and other sources here)

On the other hand, terrorist financing using crypto assets refers to the process of sending or providing funds to plan, execute, or otherwise support terrorist activities using crypto assets. While there are many similarities between money laundering and terrorist financing, a crucial difference lies in the fact that the source of funds in terrorist financing may not necessarily be derived from criminal proceeds. This distinction significantly impacts the effectiveness of the proposed approach, making the prevention of terrorist financing particularly challenging. For example, if legally obtained funds are transferred through several wallets and eventually deposited into wallets or VASP accounts controlled by terrorist organizations, as long as the intermediary wallets are not designated on sanction lists or crypto watchlists, these transactions are technically legal. In such cases, it is not only technically infeasible but also fundamentally unjustifiable to stop these transactions. This underscores the fact that the only viable countermeasure is to prevent the conversion of crypto assets held by wallets controlled by these entities into other forms of monetary value.

It is important to note that crypto asset transactions between malicious actors who are aware of each other's illicit intentions cannot be stopped under any circumstances. Therefore, the primary objective of our approach is to create separate economies: one formed by transactions between legitimate investors, and another formed by transactions between illegitimate investors. This segregation will be discussed in more detail in the following sections.

Furthermore, it is not within the scope of this proposal to detect which wallets are controlled by terrorist organizations or other malicious entities. This is not a task that can be automated and requires investigation and legal procedures by relevant authorities. The role of this approach is to provide a means for individuals to prove that they do not fall into these categories and have not engaged, directly or indirectly, with wallets that do.

VASPs are already required to implement measures to avoid transacting with wallets that have accessed banned protocols, but other self-custodial wallets lack both the means and incentives to prevent transactions with such wallets. Self-custodial wallets need both a method to detect malicious users and a motivation to avoid transacting with them.

(Insert an overview here, clarifying the different roles. Detecting malicious wallets is not the purpose of this paper. That is the responsibility of governments. Illustrate the overall picture to demonstrate the differing roles here)

This paper provides a comprehensive overview of the money laundering and terrorist financing risks associated with crypto assets, detailing the typical processes employed by criminal actors to exploit the unique features of DeFi for illicit purposes. It underscores the limitations of existing approaches in detecting and preventing illicit transactions.

This paper argues that the primary objective should be to create separate economies—one for legitimate actors and another for illegitimate actors—by providing a means for individuals to prove their compliance and incentivizing them to avoid transacting with malicious entities.

The proposed approach focuses on empowering legitimate actors to demonstrate their compliance and avoid engaging with illicit entities, thereby creating a self-regulating ecosystem that deters money laundering and terrorist financing.

The subsequent sections of this paper delve into the technical and conceptual aspects of this proposed framework, exploring how advanced cryptographic techniques and decentralized attestation mechanisms can be leveraged to enable the provable legitimacy of wallets and their transactions while preserving user privacy. By aligning the incentives of participants with the goals of regulatory compliance and the prevention of illicit activities, this approach seeks to strike a balance between the benefits of decentralization and the need for effective oversight and enforcement in the fight against money laundering and terrorist financing.

6.2.2. Significant loophole for self-custodial wallets.

The FATF has already proposed a crypto asset version of the Travel Rule for AML/CFT purposes, which has been implemented in several jurisdictions. In these jurisdictions, investor's information is exchanged between VASPs through Travel Rule protocols[11], and screening checks are performed from the perspective of preventing money laundering and terrorist financing at the time of remittance.

The FATF guidelines recommends VASPs to conduct appropriate due diligence not only for transfers between VASPs but also for transfers with self-custodial wallets. However, as mentioned earlier, VASPs are still struggling to establish effective screening methods for transactions involving self-custodial wallets, and screening checks between VASPs and self-custodial wallets remain inadequate in many jurisdictions. As a result, screening checks between VASPs and self-custodial wallets remain inadequate in many jurisdictions, creating a significant loophole for illicit actors to exploit.

Prior researches have attempted to detect and crack down on money laundering and

---

11

terrorist financing by analyzing on-chain data, but while these methods are effective, it is believed that such an approach alone would be extremely difficult to detect all illegal transactions without overlooking[12].

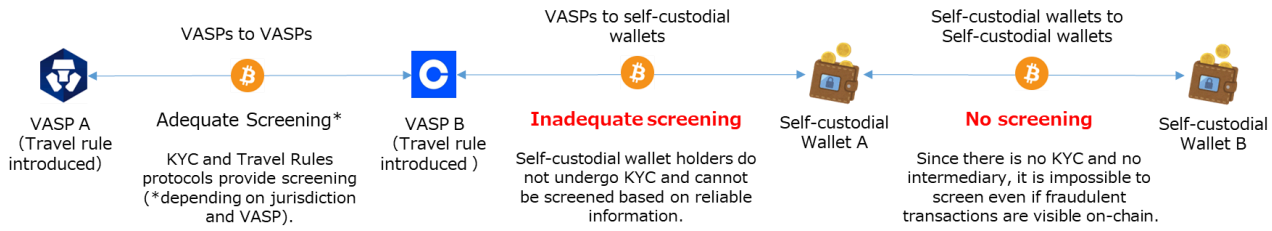


Figure 1：

The challenges faced by regulators and VASPs in implementing effective AML/CFT measures in the crypto asset space underscore the need for innovative solutions that can bridge the gap between the decentralized nature of crypto assets and the requirements of regulatory compliance. The inadequacy of current screening checks, particularly in the context of self-custodial wallets, highlights the importance of developing new frameworks that can enable the provable legitimacy of wallets and their transactions while preserving user privacy.

The subsequent sections of this paper delve into the technical and conceptual aspects of a proposed framework that aims to address these challenges by leveraging advanced cryptographic techniques and decentralized attestation mechanisms. By empowering legitimate actors to demonstrate their compliance and incentivizing them to avoid engaging with illicit entities, this approach seeks to create a self-regulating ecosystem that deters money laundering and terrorist financing in the Crypto Asset space.

To illustrate the challenges in cracking down on money laundering using crypto assets, this section will explain the methods employed using the Tornado Cash protocol and discuss the difficulties in their enforcement.

6.2.3. Typical Process of Money Laundering Using Crypto

- Tornado Cash Protocol

  Tornado Cash is a DApps operating on Ethereum, commonly referred to as a "Crypto Asset Mixer[13]". This protocol allows users to deposit and withdraw crypto assets. Upon deposit, the depositor receives secret data as proof of the deposit.

12

13

Using this secret data, the depositor can withdraw the deposited crypto assets at any time. The withdrawal wallet does not need to be the same as the deposit wallet. The deposited crypto assets are pooled together, making it impossible to link the deposit wallet to the withdrawal wallet[14]. This property allows users to send crypto assets without revealing the recipient wallet address on the blockchain.

The U.S. Office of Foreign Assets Control (OFAC) designated Tornado Cash as a sanctioned DApps in August 2022, alleging that it was used by North Korean-affiliated organizations and others for money laundering purposes. U.S. citizens were prohibited from using it, and VASPs were requested to reject deposits from addresses that had used the protocol[15]. USDC held in addresses with a history of using Tornado Cash was frozen by Circle who is the issuer of USDC[16].

However, after the sanctions, Tornado Cash randomly sent small amounts of crypto assets to innocent wallets, resulting in the USDC in those wallets being frozen. It highlights the difficulty in cracking down on anonymous transactions and illustrating that wallets receiving crypto assets from sanctioned DeFi or wallets should not necessarily be considered malicious.

In August 2023, some of the developers of Tornado Cash were arrested[17]. This arrest sparked a significant debate regarding the legitimacy of arresting individuals for writing code that provides a means for privacy protection. It is important to note that Tornado Cash operates autonomously and can be copied indefinitely, making it impossible to shut down and allowing money laundering to continue unabated.

- Process of Money Laundering

  If the funds that money launderers wish to launder are not in the form of crypto assets but fiat currencies, they first convert these funds into crypto assets. This is often done by purchasing crypto assets along with wallets on the dark web at inflated prices, using KYC-free Bitcoin ATMs, or engaging in mining using the illicit funds as operating capital, thereby converting the illicit funds into crypto assets. To avoid detection when depositing these crypto assets directly into VASPs, money launderers use Tornado Cash or similar services to obfuscate the origin of the funds.

14

15

16

17

VASPs, such as those located in the United States, are required by OFAC regulations to reject Crypto Asset deposits from self-custodial wallets that have directly used Tornado Cash. However, money launderers are well aware of this and are unlikely to send the funds directly to VASPs. If money launderers route the funds through multiple self-custodial wallets in a complex manner before sending them, it becomes difficult for VASPs to detect that the wallet attempting to deposit the crypto assets has used Tornado Cash. In this case, for VASPs to detect the use of Tornado Cash, they need to examine not only the transaction history of the wallet directly depositing the crypto assets but also the transaction history of indirectly related wallets. However, there is a limit to the extent of this examination. For example, if a VASP checks up to five wallets back, with each wallet having an average of 20 addresses in its transaction history, the VASP would need to examine 20 to the power of 5, or 3.2 million addresses, considering the country of residence and transaction details for each address. This may not be practical. Moreover, even if it were possible, if money launderers knew that the VASP's compliance policy was to check up to five wallets back, they would simply route the funds through six wallets. This is a recursively valid argument, demonstrating that this approach cannot, in principle, make VASP's compliance measures perfect. As a result, VASPs are constantly exposed to the risk of being penalized by authorities for failing to prevent money laundering, and there is no perfect cost-benefit point no matter how much they invest in compliance measures.

Through this process, money launderers can deposit the crypto assets into VASPs, convert them into fiat currencies, declare the fiat currency proceeds as capital gains earned through legitimate Crypto Asset investment activities using self-custodial wallets, and pay taxes accordingly, effectively laundering the funds.

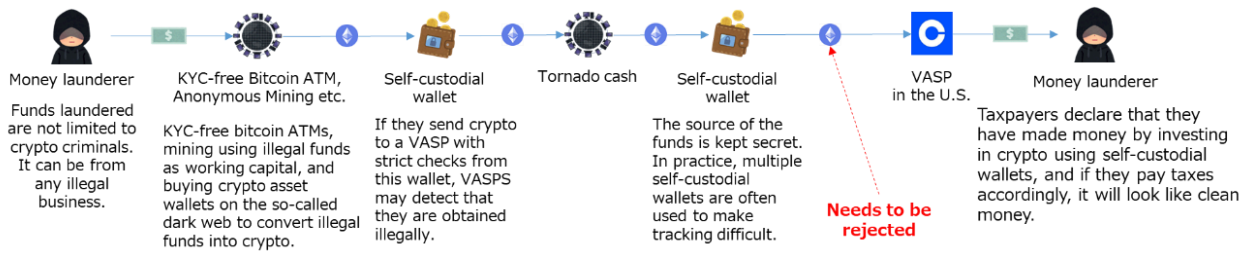


Figure 2

- VASPs' Dilemma

The problem for VASPs is not only the difficulty of detecting whether a self-custodial wallet attempting to deposit crypto assets into the VASP has used a

designated DApps like Tornado Cash. Even if the VASP could detect the indirect history of using designated DApps by the self-custodial wallet, the VASP has dilemma in that they cannot determine illegitimacy of the deposit, as the VASP cannot confirm whether the indirect usage history of the designated DApps was done by the self-custodial wallet user of their own volition or it simply accidentally received the crypto assets from other wallets that had used the designated DApps. Even if the wallet holder themselves did not use Tornado Cash, it is possible that a well-intentioned self-custodial wallet received illicit crypto assets from a malicious self-custodial wallet as payment for legitimate business transactions and is attempting to convert them into fiat currency through a VASP. Conversely, it could simply be that a Tornado Cash user routed the funds through intermediaries before depositing them into the VASP. In both cases, the on-chain appearance is identical, making it impossible for VASPs to determine whether the deposit is in good faith or bad faith based on the intention of the depositor. As a result, VASPs find themselves in a dilemma where they can neither accept nor reject crypto assets from wallets indirectly involved in fraud.

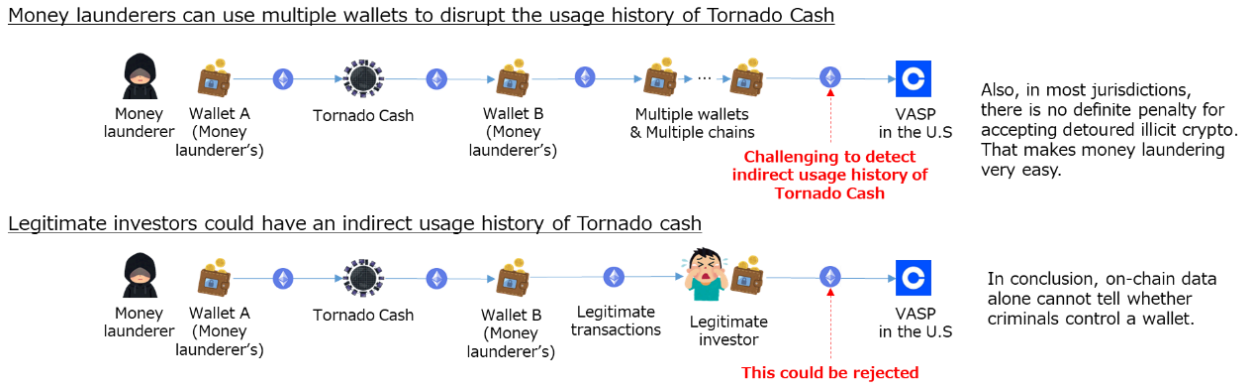


Figure 3

- Limitation of Regulatory Approaches

When introducing legal regulations, it is important to be aware that excessively strict laws may, conversely, expose a country's citizens to risk. Even with the introduction of such strict AML regulations, VASPs have yet to establish methods to detect illegal activities by customers using self-custodial wallets with a high degree of accuracy as illustrated above. Applying laws that harshly penalize VASPs for failing to detect illegal activities in such a context would make it impossible for VASPs to sustain their businesses. In the case of DApps, there is a possibility that developers and governance token holders may be unfairly prosecuted for illegal activities by malicious DApps users.

As a result, jurisdictions that introduce stricter regulations lose competitiveness compared to the others that do not since it is technically impossible to introduce uniform regulations worldwide[18]. Consequently, citizens end up using DApps or VASPs in inadequately regulated jurisdictions, exposing them to unnecessary risks.

Therefore, this paper, while assuming that the world cannot unify regulations, discusses measures to reduce the incentives for each economy participant to engage in illicit transactions.

- Our approach

  The paper takes the stance that the only solution to the above problem is for well-intentioned investors to be cautious not to unintentionally receive illicit crypto assets from malicious wallets in the first place.

  If a legitimate investor inadvertently receives crypto assets with a money launderer, the crypto assets obtained through that transaction may become undepositable into VASPs. However, if VASPs were to accept the deposit of these crypto assets, the money launderer would ultimately succeed in laundering the funds. This makes it difficult to determine, based solely on on-chain data, whether an investor's acquisition of illicit crypto assets was in good faith or bad faith. Therefore, this paper takes the position that, in principle, wallets that have received crypto assets from sanctioned wallets should not be allowed to convert those crypto assets into fiat currency or other assets through VASPs or other means, regardless of whether the receipt was in good faith or bad faith.

  However, a crucial point to consider in the design is that if VASPs do not accept these crypto assets, it may encourage the affected investor to use illegal VASPs that unconditionally accept illicit crypto assets. To prevent this, when conducting transactions using the proposing accountable wallets, the system should be designed to allow users to know the impact on future transactions deterministically prior to executing a transaction. In other words, when a user is notified that a transaction counterparty is safe to transact with, there should be a guarantee that the user will not be unreasonably rejected by any subsequent transaction counterparty after conducting the transaction. While this may seem like an obvious design requirement, providing this information with certainty is not straightforward due to the following reasons:

  1. The need to assess the credibility of the transaction counterparty without violating their privacy in any way

---

18

2. The need to verify the legality of all past transactions of the counterparty, including indirect transactions
3. The possibility that each counterparty may have different legality criteria

To realize these requirements, each investor using a self-custodial wallet must carefully verify various aspects of their counterparty's trustworthiness, necessitating the development of highly robust methods. The subsequent chapters will discuss these methods in detail, along with various possible scenarios and their solutions.

This approach does not directly propose methods to prevent unfair exploitation attacks that exploit vulnerabilities in smart contracts or other systems. Rather, it aims to ensure that even if such exploitation occurs, all legitimate investors refuse to convert the exploited assets into other forms of monetary value. For example, in the NEM incident[19], the stolen NEMs were sold on the dark web at low prices. Even if these were purchased for arbitrage purposes at prices significantly lower than the market price, the investor would fail in their arbitrage attempt as they would be unable to prove the legitimacy of the acquisition route of those crypto assets to other investors. The aim is to reduce the incentive to engage in hacking by designing a mechanism where crypto assets with unknown acquisition routes are discounted.

6.3. Unfair Trading

6.3.1. Unfair Trading

Unfair trading practices in the realm of crypto assets are diverse, and several prior studies have made significant contributions to their classification and analysis[20]. In this paper, rather than delving into these classifications, we focus on the challenges of applying securities laws to crypto asset crimes in various jurisdictions and proposes potential countermeasures.

For instance, several U.S.-based CEXs, such as Coinbase, have been subject to enforcement actions for violating securities laws by listing certain crypto assets deemed to be securities. However, this issue seems more constructive by addressing by introducing some system that these potentially securities crypto assets could be held only by eligible wallets rather than banning selling it.

In addition, in the United States, the mainstream argument is that DEXs should also

19

20

comply with securities laws. If it can be achieved, then obviously CEXs can also comply with securities laws using same system. Therefore, in order to make a stricter assumption in this paper, we will focus on the premise that DEXs should be subject to the same regulations as securities dealers and explore how DEXs can comply with these regulations.

One approach could be to distribute credentials to users who have read and acknowledged important information about tokens, securities laws, and the handling of personal information. Even if a token claims to be a non-security utility token, it is often considered to have security-like properties. In such cases, token issuers are required to register the securities with regulatory authorities in most jurisdictions. Both investors and securities dealers (could be DEXs) must be able to determine whether a token has undergone this registration process.

It is important to note that the applicability of securities laws to crypto assets varies by jurisdiction and the specific Crypto Asset in question. In jurisdictions where a Crypto Asset is not considered a security, the securities laws designed to ensure fair securities transactions (such as the Securities Act in the United States) may not apply. However, many jurisdictions have separate regulations prohibiting unfair trading practices in crypto assets, even when they are not considered securities. For example, insider trading (e.g., front-running by VASP insiders before the listing of a Crypto Asset) and market manipulation (e.g., manipulating spot prices to generate significant profits in futures trading) are often prohibited even when the Crypto Asset in question is not considered a security. This research aims to address the prevention of such unfair trading practices, regardless of the security status of the crypto assets involved. One of the reasons cited for the prevalence of unfair trading practices in Crypto Asset transactions is that, unlike stocks and other securities, crypto assets are traded on multiple exchanges and can be traded anonymously through decentralized exchanges.

Moreover, the issuance of security tokens—the tokenization of traditional securities such as stocks, bonds, and trust beneficiary rights on the blockchain—has become increasingly popular in recent years. These tokens clearly fall under the purview of securities laws, and establishing technologies that enable the compliant circulation of security tokens on permissionless blockchains is in high demand.

6.3.2. Market Manipulation

- Example: Collateral Value Manipulation in Mango Markets

  An example of market manipulation is the case of collateral value manipulation in Mango Markets[21]. The attacker established a large position in the perpetual

[21]

futures of the illiquid MNGO token, artificially inflating the price of the MNGO token from $0.30 to $0.91. They then borrowed over $114 million in USDC from the protocol using the unrealized gains as collateral.

While it is extremely challenging to prevent such activities, one potential approach is to issue credentials to investors with multiple wallets, allowing the service provider to identify when those wallets are managed by the same investor. This means that when purchasing a token A, an investor would need to provide a zero-knowledge proof that all wallets holding token A are not under their control. It could be possible within the scope of the self-certification technology envisioned by accountable wallets.

6.3.3. Unregistered Securities Dealing

- Example: The Ooki DAO Case

  The Ooki DAO offers leveraged trading as DApps. The CFTC (U.S. Commodity Futures Trading Commission) sued the founders of Ooki DAO for violating U.S. commodity trading laws and other regulations by providing leveraged trading to investors without proper registration. This case raised questions about the nature of DAOs. A key issue was whether program developers or token holders should be held liable if a DeFi provided by a DAO violates securities laws. This presents a dilemma in either case. When considering the responsibility of program developers, in this case, the program developers merely provided development and technology in accordance with the DAO's decision-making. Moreover, given that the development was carried out openly by multiple individuals, many questioned the appropriateness of holding the developers liable[22]. The governance issue also arises regarding the operational responsibility of organizations like DAOs in such cases.

  When considering the responsibility of token holders, in most cases, they have not entered into formal investment agreements when purchasing governance tokens and may not be involved in all of the DAO's decision-making processes. This seems insufficient as a basis for pursuing their responsibility for the DeFi's securities law violations. While participating in the DAO's governance voting could be viewed as involvement in the DAO's decision-making, this theory would result in token holders who did not participate in the voting not being held liable, potentially raising further concerns about the DAO's governance and disincentivizing participation in governance voting.

  Furthermore, in this case, the provision of leveraged trading in violation of U.S.

22

commodity trading laws and other regulations was cited as the offense. However, the operation was not necessarily intended to target U.S. residents. The U.S. government pointed out that adequate measures were not taken to prevent U.S. residents from accessing the DeFi.

The key takeaway from this case is that developers involved in DeFi development must not only ensure compliance with securities laws and other regulations but also implement technical measures to restrict access from residents of jurisdictions where the DeFi is not compliant with the securities laws. It could also be possible within the scope of the self-certification technology envisioned by accountable wallets.

6.3.4. Insider Trading

- Example: Insider Trading by Coinbase Employees and Others

  In Japan, the Securities and Exchange Surveillance Commission monitors for insider trading. Detecting insider trading requires information about investors' employers, but VASPs do not possess such information, posing a challenge.

  To prevent VASP insiders from engaging in front-running of pre-listed crypto assets, one straightforward solution would be to prohibit VASP employees from buying and selling crypto assets altogether. However, this would be akin to prohibiting bank employees from engaging in foreign exchange transactions, which lacks legitimacy. Therefore, VASPs that allow participation only by those who can prove, without revealing their actual occupation or employer, that they are not employed by a VASP-related company may be necessary. A possible concrete method could involve VASPs sharing the hash values of their employees' PIIs among themselves. Individuals not employed by VASPs can generate a zero-knowledge proof, using the hash value database of VASP employees' PIIs and their own digitally signed PII, to prove that they are not employed by a VASP. This approach could be used to prevent VASP employees from engaging in front-running using DEXs. Such technology will also be essential for the circulation of security tokens. In most jurisdictions, individuals who have access to non-public information about their employer or other companies due to their position are generally prohibited from freely buying and selling the stocks of those companies (insider trading). To prevent this, DEXs would need to mandate users to provide a zero-knowledge proof that they are not insiders of the security token they are attempting to purchase when dealing with security tokens.

(It is necessary to illustrate how these problems can be prevented by the introduction of

accountable wallets.

There are two approaches: by making insider trading impossible, or by making insider trading easily detectable even if it is occurring.)

6.4. The Compliance Trilemma

All of the issues discussed in this chapter can be summarized briefly in what we call the “compliance trilemma”.

6.4.1. Privacy vs Enforceability

Public blockchains like Bitcoin are designed to make all transactions visible to anyone since methods like chain analysis risk violating privacy, raising serious privacy concerns for users. To enhance privacy, technologies such as zero-knowledge proof compatible blockchains and mixing protocols have emerged. While they improve privacy, they may make it difficult to detect illegal activities when used for such purposes. Also, compliance-enhancing initiatives like the Travel Rule Protocol may violate investor privacy.

Therefore, there is a trade-off between ensuring privacy and the enforceability of laws and regulations.

6.4.2. Enforceability vs Efficiency

Although the travel rule has already been introduced in various jurisdictions, it requires for users to manually prove the source of funds, but these measures require VASPs to verify the information, which incurs significant costs. Also, many jurisdictions still do not require strict identity verification nor verification processes for the legitimacy of the source of funds for deposits of crypto assets from self-custodial wallets, which creates a loophole that negates the effort put in by regulated VASPs and legitimate users. Also, as mentioned earlier, part of the problem is that legitimate users may unintentionally become involved in money laundering by illegitimate users in the process of trading on DEXs, etc. It is not realistic for legitimate users to completely avoid this through their own efforts.

Therefore, there is a trade-off between the enforceability of laws and regulations and the efficiency of decentralized finance.

6.4.3. Privacy vs Efficiency

Protecting user privacy is essential when conducting financial transactions on a

blockchain. However, verifying a user's legitimacy while safeguarding their privacy tends to be more costly compared to situations where privacy is not a concern. This increased cost manifests in various aspects of financial transactions.

For instance, in general, when seeking to raise funds, individuals with lower creditworthiness often face higher costs. Maintaining privacy implies that various pieces of information, including personal asset and transaction details, cannot be disclosed. Consequently, parties interested in assessing an individual's creditworthiness find it challenging to obtain sufficient information, making it difficult to establish trust. As a result, if a lender wishes to extend credit to such an individual, they have no choice but to set higher interest rates. In essence, the individual's decision to protect their privacy leads to an increase in their cost of borrowing.

Furthermore, it is not only the privacy-conscious individual who bears the increased costs; those seeking to transact with privacy-oriented users may also incur higher expenses. For instance, before engaging in a transaction, it is often necessary to verify that the counterparty has not been involved in any criminal activities. However, when dealing with users who prioritize privacy, confirming such information can be exceedingly difficult and costly. This implies that VASPs and regulatory authorities may face significant expenses when attempting to ascertain whether a particular cryptocurrency user has been involved in illicit activities.

Therefore, there is a trade-off between the ensuring privacy and the efficiency of decentralized finance.

In conclusion, a solution is needed to ensure a balanced harmony between transaction legitimacy, investor privacy, and compliance without incurring excessive costs. This paper is an attempt to solve this problem.

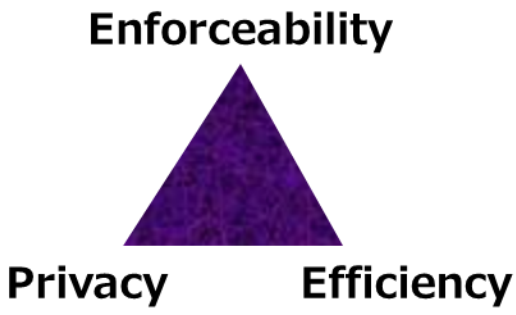


Figure 4: Blockchain ‘s Compliance Trilemma

7. Proposals

7.1. Accountable Wallets

7.1.1. A proof of own legitimacy

As illustrated in the previous chapters, directly stopping illegal crypto asset transactions is difficult. Even if authorities identify illegal wallets, they cannot seize or invalidate the crypto assets in those wallets.

Given these realistic preconditions, this paper focuses on how legitimate crypto asset users can avoid transacting with illegal counterparties. However, as demonstrated in the previous chapters, it is extremely difficult for the receiver to judge the originator's wallet's legitimacy, including investigating indirect past transactions.

Therefore, in this paper, we propose to change the approach from the conventional one in which the receiver verifies the legitimacy of the originator with limited information to one in which the originator submits a proof of its own legitimacy to the receiver, and the receiver verifies that proof.

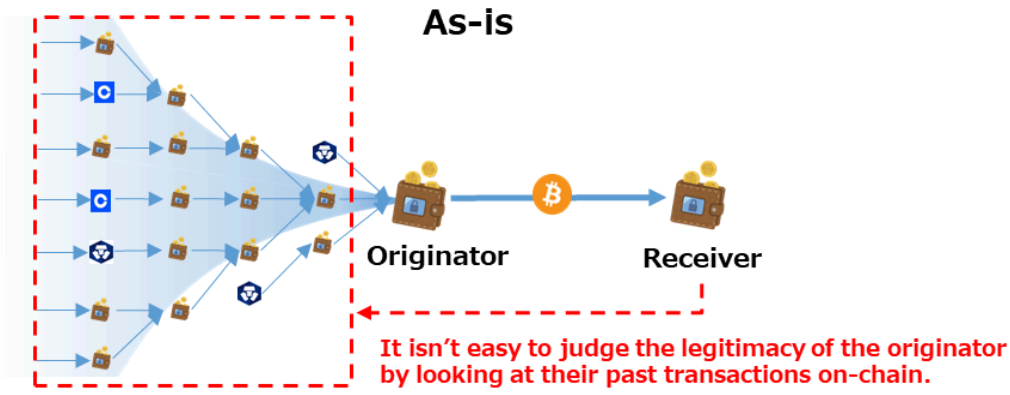


Figure 5

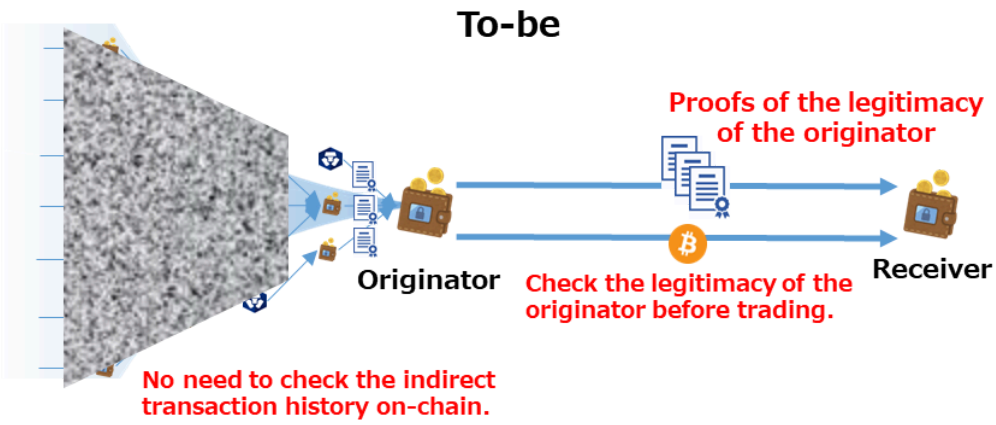


Figure 6

7.1.2. Mechanism

The definition of an accountable wallet is a wallet that can prove its own legitimacy to counterparties in a verifiable form. The legitimacy proven by wallets can be broadly divided into three categories: the legitimacy of the Wallet Holder, the legitimacy of the wallet's past actions (conducts), and the legitimacy of the origin of the crypto assets held. These will be explained in detail in the subsequent chapters.

Even if a wallet is actually legitimate, it is not considered an accountable wallet if it cannot prove these in a verifiable form (a non-accountable wallet). This requires technology that allows the prover to demonstrate legitimacy without revealing privacy, a mechanism for any verifier to cryptographically verify the integrity and authenticity[23] of the proofs issued by the prover. To achieve this goal, advanced cryptographic techniques, such as zero-knowledge proofs, to enable wallets to prove their legitimacy without compromising user privacy. This privacy-preserving approach is crucial for ensuring widespread adoption, as users are more likely to embrace a system that protects their sensitive information. Moreover, the framework emphasizes the importance of developing a robust verification mechanism that allows any verifier to cryptographically confirm the integrity and authenticity of the proofs issued by the prover. This ensures the integrity of the system and prevents malicious actors from circumventing the legitimacy requirements.

The subsequent chapters delve into the technical and conceptual aspects of the proposed framework, providing a detailed examination of the three key dimensions of legitimacy and the mechanisms for proving and verifying compliance. By offering a

23

comprehensive solution to the challenges posed by the anonymity and immutability of crypto assets, the Accountable Wallets framework represents a significant step towards reconciling the goals of privacy, decentralization, and regulatory compliance in the DeFi space.

7.2. Accountable Economy

7.2.1. Formation of an Accountable Economy

- Incentive Mechanism

  The success of the Accountable Wallets framework hinges on the establishment of effective incentive mechanisms that encourage investors to conduct proper verification before engaging in transactions. Simply put, this mechanism is that your credibility will be damaged if you fail to verify the legitimacy of your counterparty and leading to disadvantages in future transactions. By aligning the incentives of participants with the goals of regulatory compliance and the prevention of illicit activities, the system aims to foster a more secure and transparent DeFi ecosystem.

- Accountable Economy and Non-Accountable Economy

  No matter how much we aim to provide measures to minimize privacy intrusions, it is unlikely that all wallets will hold credentials due to privacy concerns and other reasons. Even if KYC to wallets is mandated by regulations, the stateless nature of crypto asset wallets makes it impossible to enforce. Many prior studies describe the process of building a clean economy based on the assumption that all wallets are KYC'd, but this is not a realistic assumption.

  In this paper, therefore, as a realistic assumption, we assume that even with our best efforts, KYC'd and non-KYC'd wallets will coexist within the economy. The important thing is to consider how to provide economic incentives for wallets to be KYC certified and what economic disadvantages to bring to those who do not adopt it.

  This strategy aims to effectively form a legitimate economic sphere by enabling investors to verify the legitimacy of their counterparties before conducting crypto asset transactions, thereby excluding illicit investors and effectively reducing the market value of illicit crypto assets held by such wallets.

  If the proposed system of self-proving legitimacy and Trust Scores (explained later) is successfully implemented, it is expected that wallets that can prove their own legitimacy (Accountable Wallets) will be incentivized to transact only with

other Accountable Wallets to maintain own Trust Score higher, leading to the formation of an economy where active transactions occur primarily among Accountable Wallets. This economy will be referred to as the "Accountable Economy."

Conversely, those who cannot prove their legitimacy (Non-Accountable Wallets) are expected to be avoided by Accountable Wallets (legitimate investors and regulated VASPs), forcing them to transact only with other Non-Accountable Wallets, resulting in the formation of an economy where transactions occur primarily among Non-Accountable Wallets. This economy will be referred to as the "Non-Accountable Economy."

This exclusion is expected to effectively eliminate wallets that has illicitly acquired crypto asset and hinder the ability to trade illicit crypto assets with legitimate one.

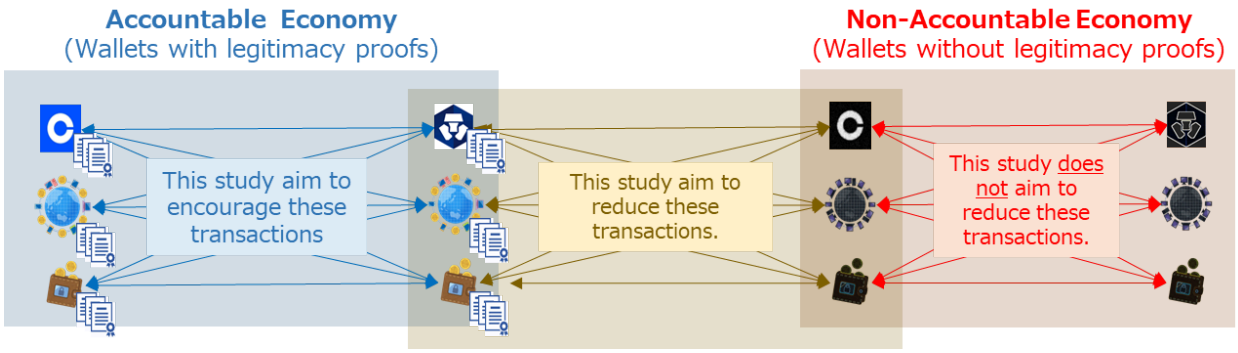


Figure 7

7.2.2. Sanctions Mechanism for Illegal Assets

- Realistic Penalty Approach for Illegal Wallets

The introduction of a credit model where the credit of a wallet is impaired and negatively affects future transactions if a certified wallet transacts with a low-creditworthy counterparty is expected to promote transactions between high-creditworthy wallets in the decentralized financial economy, which may ultimately result in the exclusion of fraudulent transactions from the decentralized financial economy.

Legitimate investors and VASPs are expected to become reluctant to accept crypto assets from Non-Accountable Wallets in order to maintain their own legitimacy, leading to a decrease in demand for crypto assets with non-accountable wallets. As a result, the value of crypto assets with the

non-accountable wallets will be lower than the one with the accountable wallets due to low demands. Consequently, crypto assets in the Non-Accountable Economy are expected to have a lower value compared to those in the Accountable Economy.

This will function as a penalty for becoming the non-accountable wallets. This mechanism implies that when an Accountable Wallet becomes a Non-Accountable Wallet, the value of the crypto assets it holds diminishes, serving as a penalty for transacting with wallets that cannot prove their legitimacy. This approach is expected to function as a practical and realistic penalty for illegal wallets, which have previously been unable to receive any form of penalty under traditional approaches.

- Impossibility of Arbitrage between the Two Economies

  If a wallet in the Accountable Economy obtains BTC at a discounted price from the Non-Accountable Economy for arbitrage purposes, that wallet will be considered non-accountable. That wallet can no longer transact with anyone in the Accountable Economy resulting the arbitrage failed.

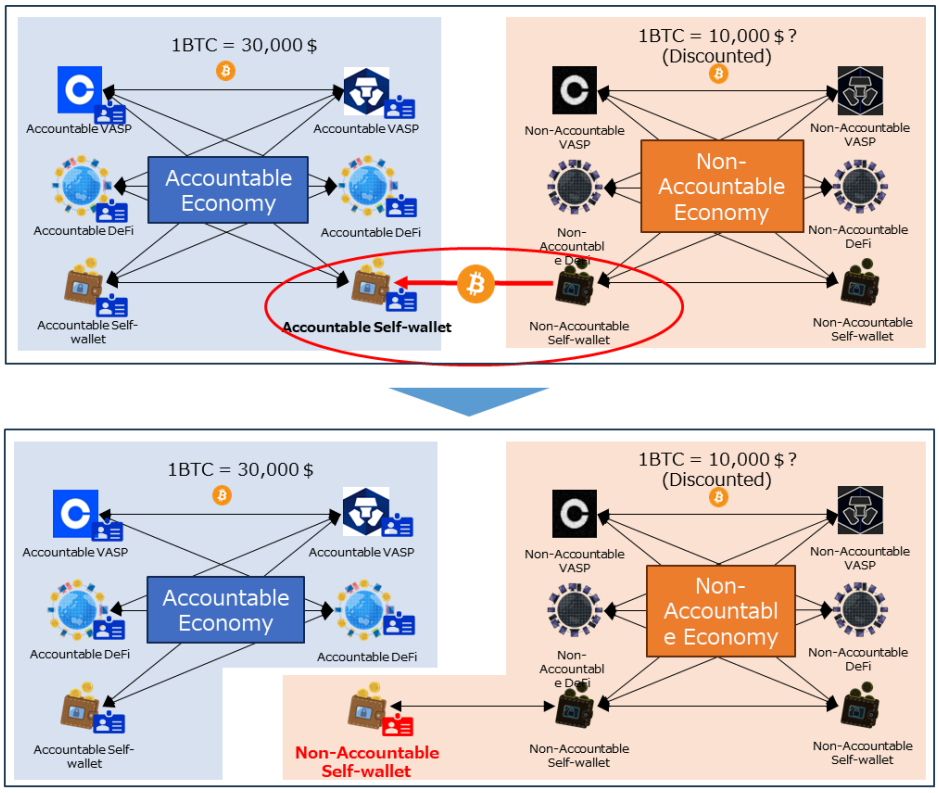


Figure 8

- Regarding Concerns about Crypto Asset's Fungibility

It has been brought to our attention that the proposed Accountable Wallet framework may potentially impact the fungibility of crypto asset, as it could lead to a price divergence between the Accountable Economy and the Non-Accountable Economy. While this concern is understandable, it is essential to recognize that the primary goal of our approach is not to create a divide but rather to provide users with the freedom to choose the level of compliance they wish to adhere to while engaging in cryptocurrency transactions.

We acknowledge that there exists an inherent trade-off between the principles of decentralization, which crypto asset embodies, and the compliance requirements often sought by traditional financial systems. The proposed framework does not aim to impose a singular compliance standard upon all users but instead seeks to empower individuals to define and uphold their own compliance rules based on their specific needs and preferences.

Censorship resistance and ability to protect assets from undue influence or seizure by governments or other centralized authorities. However, this characteristic also creates a challenge when seeking to balance privacy with the need for compliance, particularly regarding Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT). In traditional finance, compliance measures are mandatory and often enforced through centralized intermediaries, but in decentralized ecosystems, these requirements are harder to enforce.

The current lack of tools for crypto asset users who desire to maintain a certain level of compliance poses a significant challenge. These users have no means to verify whether the crypto assets they receive originate from illicit sources or to prove the legitimacy of their own transactions to counterparties. This gap creates a compliance blind spot that forces well-intentioned users into a dilemma: they either participate in the crypto asset economy with increased legal and reputational risk, or they avoid using crypto asset altogether due to compliance concerns.

The Accountable Wallet framework addresses this issue by providing the necessary technologies for users to verify the legitimacy of their transaction partners according to their self-defined rules. It introduces the necessary tools for users to self-regulate and verify their counterparties based on their own definitions of compliance.

It is crucial to recognize that the definition of "legitimacy" may vary across jurisdictions and among individual users. Therefore, the compliance rules within this framework should be viewed as a matter of personal choice. For instance, the FBI publishes a list of sanctioned crypto asset addresses. It is up to each user to decide whether to transact with wallets included in this list or with wallets

that have previously interacted with sanctioned addresses. The key is to have the ability to detect such interactions prior to engaging in a transaction.

If all users collectively agree to exclude addresses on the FBI's list from their transactions, crypto asset from those addresses would effectively become unacceptable. This consensus forms the core of compliance in a decentralized system.

The notion that crypto asset's fungibility is at risk because of compliance-based price differentiation between the Accountable and Non-Accountable Economies misses the broader point about market consensus. If enough users and institutions choose to prioritize compliance, the value of crypto assets circulating in the Non-Accountable Economy will likely decrease. This is not because crypto asset itself is losing its fungibility by design, but because market participants—both individuals and institutions—are exercising their preference for clean and legitimate assets.

While we believe that the Accountable Wallet approach offers a valuable solution, we recognize that it is unrealistic to expect universal adoption of this framework. Consequently, a divide may emerge between the Accountable Economy, formed by users of Accountable Wallets, and the Non-Accountable Economy, comprised of users who choose not to adhere to these principles.

One of the significant hurdles in combating money laundering and terrorist financing with cryptocurrencies is the inability to seize crypto assets from illegal addresses, even when they are identified as holding criminal proceeds. However, our approach enables the most legitimate users to collectively refuse transactions with these addresses, effectively hindering the conversion of the illicit proceeds held by these addresses into other forms of monetary value. By creating a mechanism that allows compliant users to self-select their counterparties, this framework significantly reduces the avenues available for laundering criminal proceeds.

It is important to emphasize that the resulting distinction between the Accountable and Non-Accountable Economies does not constitute an attack on crypto asset's fungibility. Instead, it is a consequence of market behavior, driven by users' preferences for compliance and legitimacy. The potential loss of fungibility is not the primary objective but rather a consequence of users striving to maintain compliance according to their own standards.

- Lowering KYC costs across the VASP industry

  Currently, VASPs are forced to incur significant compliance costs due to the

implementation of the Travel Rule. In particular, verifying that crypto assets sent from external self-custodial wallets to VASPs are not illegally obtained is far more difficult than the same verification for crypto assets sent from VASPs.

Looking ahead, the successful implementation of the Accountable Economy has the potential to significantly reduce compliance costs for VASPs and other regulated entities. By enabling self-custodial wallets to prove their legitimacy through cryptographic credentials, the burden of verifying the provenance of incoming crypto assets can be greatly streamlined, allowing VASPs to focus their resources on more complex compliance challenges.

8. Definition of legitimacy

8.1. Three Factors of Transaction Legitimacy

This paper aims to establish a mechanism for proving and verifying the legitimacy of transactions in decentralized finance. To achieve this goal, it is essential first to define what constitutes a legitimate transaction. While defining universal transaction legitimacy is challenging due to variations in laws across jurisdictions, establishing these conditions is crucial for designing protocols and consensus mechanisms. As this paper does not focus on the legal regulations of specific jurisdictions, it is necessary to define a universal standard of legitimacy that serves as a more stringent criterion.

This involves a thorough decomposition of the requirements for establishing transaction legitimacy into detailed factors. The process includes a comprehensive analysis of the criteria and evidence necessary to determine the legitimacy of a transaction.

Although it is difficult to define universal transaction legitimacy due to differences in laws across jurisdictions, as a universal principle, legitimacy can be defined as the absence of illegality. Therefore, the initial task is to compile a list of universally avoidable transactions. Our workshop team concluded that all scenarios in which legitimate investors should not make transactions can be classified into three scenarios:

1. when the owner of the counterparty's wallet is an antisocial force or other sanctioned party
2. when the counterparty's wallet has been involved in any exploit or designated by authorities as a wallet for exploited assets
3. when the counterparty's wallet has received crypto assets from any wallet falling

under either of the above two categories

An accountable wallet is defined as a wallet that can prove its own legitimacy to others. Therefore, from here on, an accountable wallet is defined as a wallet that does not fall into any of all three scenarios above. In other words, the legitimacy that one should prove to the counterparty at the time of a transaction can be categorized into three aspects. The above three proofs can be simply rephrased as "Legitimacy of the Wallet Holder," "Legitimacy of the Wallet's Past Actions (conducts)," and "Legitimacy of the Crypto Asset Provenances." In the following sections, we will take a closer look at these properties and how to prove them.

8.1.1. Legitimacy of Wallet Holders

This refers to a state in which the individual or organization managing any wallet has no issues that would hinder transactions with the counterparty. The legitimacy of such wallet holders is divided into the perspective of anti-money laundering laws and other financial regulations (such as securities laws).

From the former perspective, legitimate service providers and investors must avoid involvement with wallets associated with terrorists or other illegal organizations. Specifically, transactions should not be conducted if the wallet holder is an individual or organization designated by the authorities of each jurisdiction on sanction lists or other lists. This principle is same as existing finance.

The key point of this definition is that self-custodial addresses managed by illegitimate organizations or individuals should be avoided even if they have not engaged in any wrongdoing in crypto asset transactions. Wallets managed by individuals or organizations engaged in illegal activities outside the crypto asset economy should not be transacted with, even if the address has obtained crypto assets through legal means.

More conservatively, anonymous wallets with unidentified owners should be avoided if one does not want to risk being perceived as having transacted with an illegitimate counterparty, as they may be controlled by illegal organizations. This paper takes this stance.

However, revealing personal information such as names and addresses to prove the legitimacy of the Wallet Holder would lead to a serious breach of privacy. Therefore, a method is needed to prove and verify that an investor's attribute information complies with the counterparty's compliance standards without disclosing personal information.

This applies not only to self-custodial wallets but also to VASP custodial wallets and DEX contract addresses. For custodial wallets, if the VASP managing the custodial

wallet has not obtained the appropriate license in the jurisdiction where it is located, it will similarly be regarded as an illegitimate wallet holder.

Moreover, counterparties may have their own additional transaction conditions, which are rules from the perspective of securities laws and other regulations. For example, certain tokens may only be held by residents of specific countries, or investors may have personal preferences to only transact with residents of certain countries. These conditions must also be proven to comply with transaction rules without disclosing personal information.

The next chapter will discuss how to prove these to transaction counterparties.

8.1.2. Legitimacy of Wallet Conducts

Crimes related to organizations or individuals and crimes related to Wallet Conducts should be classified separately. This differs from the legitimacy of the wallet holder mentioned in the previous section. The previous section referred to a state in which the wallet holder is considered to be involved in illegal transactions, not limited to on-chain transactions, and is listed on sanction lists or other lists. In other words, the entities listed on such sanction lists are the individuals or organizations themselves. On the other hand, the subject of illegality in this section is the wallet. Moreover, this classification is necessary because there are many instances of criminal acts by wallets with unknown managers in highly anonymous decentralized finance. These are considered criminal acts with unidentified suspects. Legitimate users should avoid transacting with wallets that have committed crimes, even if the suspects are unknown.

In other words, illegitimacy related to Wallet Holders and illegitimacy related to Wallet Conducts are clearly distinguished. Illegitimacy related to Wallet Conducts in this context refers to Crypto Asset transactions that are deemed illegal under the laws and regulations of the jurisdiction to which the address manager belongs. In some jurisdictions, there are DApps and others that are prohibited from accessing, and accessing these may also be considered an illegal act in that jurisdiction. For example, as mentioned in the previous chapters, the United States has banned U.S. residents from using Tornado Cash. This means that Tornado Cash is listed on a Crypto Asset watchlist.

The problem here is that laws differ by jurisdiction. This methodology is not intended to automatically determine the legality of any action in decentralized finance. Only the judicial and administrative authorities of each jurisdiction can make such determinations. This is their job and an inviolable domain. Therefore, this paper takes the stance that this information is oracle data provided by the authorities. In other words, for this methodology to be established, the authorities need to designate addresses that have

engaged in wrongdoing as sanctioned through oracle data. This is not an unrealistic assumption, as the FBI and others have already designated some wallet addresses as sanctioned. What this paper emphasizes is not the divergent legal regulatory trends of each jurisdiction, but rather how authorities should disclose this information in specific data formats, how to aggregate that data into a single dataset, and how legitimate investors can prove their own legitimacy to others by not being listed on those datasets.

The next chapter will discuss how to prove these to transaction counterparties.

8.1.3. Legitimacy of Crypto Asset Provenances

As in the above two cases, even if the wallet that a legitimate investor is attempting to transact with is not managed by sanctioned individuals or organizations and the wallet itself has not engaged in illegal activities, if the wallet has received crypto assets from wallets designated as involved in illegal activities, it is a haven for illegal crypto assets, and transactions should not be conducted with that wallet.

In traditional finance, the payee is generally not required to confirm the legitimacy of the payer's source of funds during transactions, at least in cases of good faith. For example, if you were running a shop and received payment from money obtained through crime, you would not be held accountable if you were unaware of it. However, this paper takes the stance that any wallet should not receive crypto assets from wallets holding illegally obtained funds, regardless of whether the receipt was in good faith or bad faith. In many jurisdictions, receiving illegal funds may not be punishable if the receipt was in good faith, meaning that the recipient was unaware that the funds were proceeds of crime. However, as explained in a previous chapter, it is theoretically impossible to prove based solely on on-chain data and VCs whether the receipt of illegal funds was in good faith or bad faith. Therefore, if we allow investors who have received illegal funds to claim innocence simply by asserting good faith, i.e., without any penalty, it would effectively enable unlimited money laundering through P2P transactions. Consequently, this paper takes a very conservative stance for the sake of complete proof of legitimacy: any wallet should not receive crypto assets from wallets holding illegally obtained funds, regardless of whether the receipt was in good faith or bad faith.

To fully prove this, one must demonstrate that all past indirect transaction counterparties were also legitimate. For those transaction counterparties to prove this, they must also demonstrate that they have only transacted with legitimate counterparties. Without a reliable method to determine whether the counterparty's held crypto assets are illegitimate, even cautious investors may face unreasonable penalties, necessitating a robust determination method.

In other words, to fully prove that crypto assets were legally obtained, it is necessary to

design a "chained" proof. The idea is that at the time of a transaction, this proof is sent to the counterparty's wallet along with the crypto assets, and the receiving wallet can use it to prove its own legitimacy to other wallets in future transactions.

This proof must be designed in a way that allows the wallet that actually conducted the transaction to prove to others that the crypto assets were received from a legitimate party without disclosing the personal information of the counterparty, as the proof is intended to be used in P2P transactions as well. Ideally, the proof should be able to prove this while obfuscating even the past wallet address transaction history, and the following chapters propose a solution that incorporates the concept of privacy pools[24].

Furthermore, a problematic issue in issuing this proof is how to deal with cases where an attacker sends illegally obtained crypto assets to you against your will. This paper also discusses the concept and appropriate handling procedures for proving that such cases were handled appropriately.

8.2. Proofs Examples

8.2.1. Wallet Classification

The content that a wallet needs to prove to demonstrate its legitimacy varies depending on the entity managing the wallet. While there are various types of wallet holders in practice, for the sake of focusing the discussion, this paper categorizes wallets into three types based on the managing entity: custodial wallets, smart contract addresses, and self-custodial wallets.

- Custodial Wallets

  Custodial wallets are addresses owned by VASPs, such as crypto asset exchanges and custodians. The regulations applicable to these wallets vary depending on the jurisdiction in which they are located and the services they provide.

  The key point in this segment is that these addresses always have a legally responsible entity. Today, blockchain explorers commonly label these addresses with the name of the managing entity, and these addresses generally do not have anonymity. Consequently, when these addresses receive crypto assets from illegitimate wallets and this fact is brought to light through the proposed methodology, the information is likely to become public, and it is easier to impose penalties on the managing entities from a legal or reputational perspective. This is expected to play a crucial role in motivating all participants in the Accountable

24

Economy to act with integrity through the Trust Score mechanism. It is also important to note that VASPs are the primary entities responsible for converting crypto assets into fiat currencies. The differences in behavior will be discussed in more detail in following Chapters.

- Smart Contract Addresses (DApps)

  Entities that provide financial services using blockchain technology without centralized financial institutions or intermediaries, commonly referred to as DApps, are composed of smart contracts and typically have unique addresses for their smart contracts, similar to Crypto Asset wallets. For example, the liquidity pools of DEXs have their own unique addresses. These addresses are classified in this category.

  The key point in this segment is that these addresses do not necessarily have a specific legally responsible entity. While there are cases where an operating organization exists and publicly discloses its identity or where a DAO serves as the operating organization, as in the case of Ooki DAO discussed in Chapter 6, where the DAO was sued for securities law violations, this paper assumes a more stringent premise that these addresses do not have a named operating organization or that even if they do, a centralized approach to pursuing legal responsibility is not feasible due to the jurisdictional dispersion of the responsible entities.

  Therefore, to motivate these addresses to refrain from engaging in illicit activities, a three-step mechanism is necessary: (1) providing a means for users to assess the credibility of their counterparties at a low cost (i.e., the method proposed in this paper for assessing user credibility), (2) ensuring that the acceptance of illicit funds by DApps that do not implement such measures becomes public information, and (3) imposing penalties on DeFi users who utilize such platforms by lowering their own credibility scores. These mechanisms are expected to naturally lead to the avoidance of DApps that accept illicit funds by legitimate users.

- Self-Custodial Wallet Addresses

  Self-custodial wallet addresses are those where individuals or organizations holding the property rights to crypto assets manage the private keys and other access information associated with the wallets themselves. The managing entities can be either individuals or legal entities such as corporations. We confront the reality that while these addresses should have an entity, the actual manager is often unknown.

Therefore, even if a self-custodial wallet engages in criminal activities, it is not always possible to directly take legal action against the wallet holder by immediately identifying them as the perpetrator. Consequently, this paper takes the stance that even when criminal activities by self-custodial wallets are detected, legal enforcement against the holders is generally not possible. Recognizing the limitations of direct legal enforcement in such cases, the paper emphasizes the need for a collaborative effort between authorities and legitimate market participants to isolate illicit wallets and cut off their access to the broader financial system. What the authorities and other legitimate wallet holders and service providers can do is to thoroughly avoid transacting with wallets recognized as illicit and to completely cut off the means for these illicit wallets to convert the illegally obtained crypto assets into other forms of monetary value.

The paper also addresses the potential risks associated with the use of credentials to prove the identity of wallet holders. While such credentials can be valuable tools for establishing legitimacy, the framework stresses the importance of designing them in a way that protects user privacy and prevents the abuse of authority by centralized entities. By ensuring that only the holder has the power to disclose their personal information, the system maintains a balance between accountability and individual sovereignty.

It is debatable, but even if a wallet holds credentials that prove the identity of the wallet holder, it may not be desirable for the holder to be immediately identified by the authorities using the credential information and subjected to legal enforcement when the wallet commits a criminal act. If such measures are possible, it could give the authorities unlimited authority to register any wallet on the watchlist and effectively freeze any individual's Crypto Asset assets at any time. Therefore, the credentials themselves should be cryptographically designed to ensure that only the holder has the authority to disclose the associated personal information. This will be discussed in detail in Chapter 9.

8.2.2. Proofs Examples

By combining the three types of wallets based on the managing entity, as described last section, with the three aspects of legitimacy discussed in the previous section, specific proofs of legitimacy can be classified into nine categories.

In this section, we will actually explore examples of proof that each type of wallet can consider as proof of its own legitimacy. The degree to which holding these proofs should increase one's trustworthiness depends on the design of the trust score formula, and there is no definitive answer.

Note that the proofs discussed in this section are only samples to flesh out the discussion, and are not intended to be a list of things that all wallets should be forced to hold.

	Custodial Wallet Addresses (VASPs, etc.)	Smart Contract Addresses (DApps, etc.)	Self-Custodial Wallet Addresses (Investors, etc.)
Legitimacy of Wallet Holders	- Proof of a business license in the jurisdiction of operation - Proof of jurisdiction in which the business is conducted	- Not applicable as DApps typically do not have specific legal entity	- Not affiliated with antisocial forces, etc. - Meets the criteria for qualified investors (definition varies by jurisdiction) - Proof of jurisdiction of residence
Legitimacy of Wallet Conducts	- Conducts business operations appropriately	- Comply with securities laws, etc. - Has undergone code audits	- Has never accessed sanctioned VASPs and DApps - Has not been involved in other illicit activities on chain
Legitimacy of Crypto Asset Provenances	- Conducts appropriate screening checks when accepting crypto assets from external wallets	- Restricts access to legitimate users only	- Has only received crypto assets from legitimate wallets

Table 1

- Custodial Wallet Addresses

  - Proof of a business license in the jurisdiction of operation

    Business licenses should be issued by the authorities in a verifiable credential format.

  - Proof of jurisdiction in which the business is conducted

    Even if a valid license is obtained in the jurisdiction where the VASP is located, there may be cases where the jurisdiction has not ratified the

Travel Rule, for example. Therefore, the credibility of a VASP should be assessed based on both country risk and entity risk.

- Conducts business operations appropriately

  Even if a VASP has obtained an appropriate license in an appropriate jurisdiction in the past, there may be cases where the VASP faces temporary or permanent credibility concerns due to some scandal or other issues. In such cases, honest investors should be able to avoid using the VASP through this methodology.

  Since many of a VASP's business operations are conducted off-chain, a mechanism is needed to certify that there are no credibility concerns about the VASP, such as a third-party organization or an oracle chain that feeds such facts.

- Conducts appropriate screening checks when accepting crypto assets from external wallets

  There are two patterns of sources from which VASPs must not receive crypto assets or fiat currency for the exchange or conversion of crypto assets. One is individuals or organizations on the sanctions list, and the other is wallets on the crypto watchlist. These correspond to the first and second definitions of legitimacy defined in Section 8.1. VASPs are required to take appropriate measures to avoid receiving crypto assets or fiat currency from both of these sources. If the framework proposed in this paper works properly, it is expected that it will be possible to prevent receiving crypto assets from these sources. Moreover, it is assumed that if crypto assets are accepted from these sources, that fact will become evident in the on-chain data. This mechanism will be explained in a later chapter. Therefore, if this framework becomes widely adopted and mature to a certain extent, it is expected that it will be possible to prove whether such measures are being taken appropriately using on-chain data. Legitimate users will be able to use this data as a reference to identify properly operated VASPs, and legal institutions will also be able to take appropriate legal action.

  However, VASPs must prevent not only the deposit of illegally obtained crypto assets but also the funds used to purchase illegal crypto assets. This cannot be detected on-chain. Since these detections can only be detected by monitoring the circulation of illegal funds in existing finance, regulatory authorities in each jurisdiction will be responsible for monitoring

whether these are being properly implemented. However, as this is outside the scope of discussion in this paper, this paper assumes that these are being properly implemented based on the possession of the aforementioned appropriate VASP operating license.

- Smart Contract Addresses (DApps)

  - Legitimacy of Wallet Holders

    For DApps, this paper assumes that entities classified as DApps do not have a specific legally responsible entity, so there are no proofs of legitimacy of wallet holders. If there is a clearly existing operating organization, it should be classified as a VASP. When the DApps is operated by a DAO in a decentralized manner, the DAO could be considered a form of wallet holder, but this is a point of debate.

  - Comply with securities laws, etc.

    Any investor accessing financial services provided by a business entity located outside their jurisdiction must comply with the laws of the jurisdiction in which the service provider is registered, as well as the laws of the investor's jurisdiction. The former includes licensing requirements, financial product offering methods, and customer data handling, while the latter includes tax-related laws, foreign exchange regulations, consumer protection laws, and more. International financial regulations and treaties may also apply, involving the laws of multiple countries.

    Regarding DApps, the U.S. SEC has stated that they must comply with the same legal requirements as physical VASPs. In fact, in the United States, there have been a series of cases where developers of DApps and others have been charged with securities law violations. If U.S. resident investors can access a DApps, it must comply with U.S. securities laws. However, most DApps are accessible to anyone worldwide[25]. Applying the SEC's logic directly would mean that DEXs need to comply with the regulations of all jurisdictions worldwide.

    In the case of Tornado Cash, the developers stated that they could not comply with U.S. regulations and explicitly noted that U.S. residents should not access the platform. They also controlled their website to be

[25] In some cases, IP addresses are checked to restrict access to the homepage of the DApps from certain countries, but this is an access control that can be easily circumvented with a VPN, etc. Also, since access to smart contracts is possible without going through the WWW, this is not a reliable control.

inaccessible from the U.S. However, Tornado Cash itself is a blockchain application, and unlike websites, access cannot be restricted by IP. As a result, they were unable to prevent access by U.S. residents and were also pursued by the authorities on this point. This case demonstrates that DEXs need to strictly limit access to qualified users through KYC and cryptographic means. This methodology will also serve to protect DeFi developers.

- Has undergone code audits

- Restricts access to legitimate users only

  DApps need to demonstrate that they have implemented measures to ensure that only users who can prove their legitimacy, as proposed by this framework, can access their services. However, this alone is insufficient from the perspective of securities laws and other regulations. As mentioned in the 'Comply with securities laws, etc.' section, many existing DApps effectively provide services that would not be permitted from the standpoint of securities laws and other regulations.

  If these DApps are accessible from all jurisdictions, they would, strictly speaking, need to comply with regulations pertaining to securities laws in all jurisdictions, which is practically impossible. Therefore, DApps must select a few jurisdictions to comply with and, accordingly, control access to ensure that only users residing in jurisdictions where the DApps is compliant with securities laws can access the platform.

  In a broader sense, this is the appropriate user access control that is required. DApps should not only restrict access to users who can prove their legitimacy but also ensure that they are compliant with the securities laws of the jurisdictions they choose to operate in. This can be achieved by implementing robust access control mechanisms that verify the user's jurisdiction of residence and grant access only if the DApps is compliant with the securities laws of that jurisdiction.

- Self-Custodial Wallets

- Not affiliated with antisocial forces, etc.

- Meets the criteria for qualified investors (definition varies by jurisdiction)

Tokens that are recognized as securities must be controlled so that they can only be bought and owned by eligible investors in accordance with regulations applicable to the issuance and sale of the securities. From the perspective of investors, they must prove that they meet the conditions for holding the tokens when buying these tokens.

- Proof of jurisdiction of residence

- Has never accessed sanctioned VASPs and DApps

- Has not been involved in other illicit activities on chain

Illicit activities refer to Crypto Asset transactions deemed illegal under the laws and regulations of the wallet holder's jurisdiction. However, the definition of illicit activities varies by jurisdiction, making it difficult to determine the legality of past transactions for wallets that have not proven their jurisdiction of residence.

This paper takes a rigorous risk-based approach, suggesting that wallets unable to prove their jurisdiction of residence should be subject to the laws of all jurisdictions. Holding credentials proving one's jurisdiction will increase one's Trust Score.

The transaction approval protocol should disclose only the result, without exposing jurisdiction or Trust Score. However, wallets that cannot prove their jurisdiction should be considered high-risk and generally avoided to prevent unwitting involvement in illicit transactions.

Further details on the complexity of determining applicable laws and their impact on Trust Scores will be discussed in the Trust Score section.

- Has only received crypto assets from legitimate wallets

Considering the properties of crypto assets, such as the ease of creating multiple wallets, participants in decentralized financial transactions must not only directly verify the legality of their users but also confirm that the wallets with which their users have transacted in the past are not wallets managed by individuals or organizations on sanction lists or wallets that have engaged in illicit transactions. However, this is not easy and becomes a very costly confirmation process. Moreover, given that crypto assets can be routed through any number of wallets, there is no limit to the layers of history that need to be traced back for confirmation. This paper

attempts to resolve this issue.

- The other possible proofs

- Has received the necessary important explanations prior to purchasing Security Token A and has agreed to them.
- Is not classified as a PEP (Politically Exposed Person).
- Meets the Qualified Institutional Investor requirements of Country A.

8.3. Trust Scores

8.3.1. Concept

- Concept

  The proposed framework needs the concept of "Trust Scores" as a quantitative measure of a wallet's legitimacy based on its past interactions and holdings. Trust Scores serve as a key incentive mechanism to encourage compliant behavior and deter illicit activities in the DeFi ecosystem. Such a scoring system is expected to encourage Wallet Holders to comply with legitimate standards.

  The Trust Score mechanism is designed to incentivize wallets to maintain a high score by engaging in legitimate transactions and avoiding interactions with flagged or suspicious counterparties. Wallets with higher Trust Scores are expected to enjoy preferential treatment from service providers and other participants in the ecosystem, creating a virtuous cycle of compliance.

  Conversely, wallets that engage in or facilitate illicit activities will see their Trust Scores deteriorate, limiting their ability to interact with the legitimate economy. This dynamic creates a self-reinforcing system where legitimate actors are incentivized to transact only with other legitimate actors, effectively isolating and penalizing malicious entities.

  There is no definite answer to calculate the trust score. However, there has to be some kind of scoring system for this framework. Please note that the calculation method proposed here is one suggestion. It serves as a starting point for a concrete discussion on how to embed each of the legitimacy factors described in following chapters into the trust scores.

- Basic Idea of the Calculation

  The specific formula for calculating Trust Scores may vary depending on the

implementation, but we can establish the general principles.

The Trust Score calculation methodology should be designed to provide a fair and objective assessment of a wallet's legitimacy based on the proofs provided by the wallet and on-chain data.

As for the proofs, defining a wallet's trust score in a way that is consistent with the definition of legitimacy in this paper, the score is calculated based on three main factors: the legitimacy of the wallet holder, the legitimacy of the wallet's conducts, and the legitimacy of crypto asset provenances. These components are derived from the proofs provided by the wallet across the three dimensions of legitimacy, as discussed in the previous sections.

As for the on-chain data, the trust score should be, for instance, designed to decrease the more one transacts with illegal investors (more precisely, investors who cannot prove their legitimacy, i.e., non-accountable investors). However, if the trust score is given to a wallet, when the wallet receives crypto assets from a wallet with low trust score even once, the trust score of the wallet will be lowered, which could mean all crypto assets held in a wallet before the receipt are deemed fraudulent. In that case, the risk of reputational damage from a single transaction becomes very high, especially for VASPs and large e-commerce companies handling crypto asset transfers. Therefore, the reputational damage caused by receiving fraudulent crypto assets should be based on a graded scoring evaluation that takes into account the proportion of legitimate and illegitimate transactions up to that point.

In addition, we need to assign weights to each component of the Trust Score based on their relative importance and the level of assurance provided by the associated proofs. For example, the legitimacy of the wallet holder may be given a higher weight compared to the legitimacy of the wallet's past actions, as the former is more fundamental to establishing trust. For instance, the Trust Score calculation may also take into account the reputation and reliability of the entities issuing the proofs, such as credential providers and oracle services. This ensures that the Trust Scores are not unduly influenced by potentially unreliable or malicious actors.

Furthermore, the Trust Score mechanism should be designed to be resilient against attempts to game the system, such as creating multiple wallets to dilute the impact of illicit activities or engaging in token transactions to artificially inflate scores. This may involve implementing additional checks and balances, such as analyzing transaction patterns and applying time-based decay factors to the scores.

- Incentives for Maintaining a High Trust Score

  By designing VASPs to have an incentive to maintain a high trust score, participants in the entire DeFi economy will have an incentive to maintain a high trust score. The specific mechanism will be explained here.

  Firstly, when a VASP receives a transfer of crypto assets from an external wallet that is not a self-custodial wallet of an existing customer, or when it is not possible to determine with certainty whether the wallet is a self-custodial wallet of an existing customer, the Travel Rule stipulates that the recipient account manager should provide information about the external wallet holder to the VASP, which the VASP uses to decide whether to accept the crypto assets. However, this is a judgment based on verbal responses and is not 100% trusted. Therefore, VASPs should refuse to accept crypto assets that are not proven to have been obtained from legitimate sources, even if the wallet holder is not found to be an antisocial organization, based on their risk appetite.

  Consider a VASP A. If VASP A's custodial wallet frequently receives crypto assets from wallets with low trust scores, i.e., wallets that cannot prove their legitimacy, VASP A's wallet's trust score will decrease. The VASP A's trust score is supposed to be public, since, in fact, most VASP’s wallet addresses are labeled in blockchain explorers and are not anonymous. VASP A's users will know, through the decrease in VASP A's trust score, that VASP A's risk of fines or business suspension due to money laundering abetment, etc., is increasing. As a result, some users are expected to avoid using VASP A. This can be a significant business risk for VASP A, so VASP A is expected to optimize its risk preference in order to maintain a high trust score. As a result, VASP A is expected to transact only with wallets above a certain trust score or offer more favorable transaction terms to wallets with high trust scores in order to maintain their trust score high.

  Furthermore, Individual investors using self-custody wallets will also have an incentive to maintain a high trust score in order to use VASPs that have a rule that they will only transact with wallets that have a certain trust score or higher. VASPs are subject to sanctions such as fines or suspension or revocation of licenses under the laws of the jurisdiction in which they are located if they are found to have acted inappropriately. However, the crypto version of the travel rule advocated by FATF is not ratified by all countries. No one can stop the exchange of crypto assets for fiat currency by VASPs operating Crypto Asset exchange businesses in countries that have not ratified it. What we can do is that legitimate investors will unite to avoid using that VASP in order to impair their business. Ideally, if someone acquires crypto assets from them, they should be rejected for

transactions not only by VASPs that comply with the travel rule but also by all investors who hold credentials proposed in this paper. The focus is on how to weaken the business of illegal VASPs in this way.

This approach would be effective to discourage investors from using such non-compliant VASPs. It is difficult for individual investors to judge which VASPs they can use by checking VASP’s compliance status themselves. However, using this method, even individual investors can easily ensure that a VASP is operating properly by ensuring that the VASP is properly receiving and transferring crypto asset only to and from legitimate wallets. In other words, the VASP's acceptance of illicit funds will be determined in a decentralized manner by the collective, and based on that determination, the collective will unite to avoid using that VASP. While this may sound nuisance for VASPs, for VASPs operating with integrity, it is also a method to demonstrate their integrity with data. Also, wallets with higher trust scores may be able to get more favorable trading terms, which is happening in finance today. Conversely, Self-custody wallet holders may even have their ability to convert crypto assets into fiat currency through VASPs hindered if their trust score drops too low. Such an incentive mechanism plays an important role in the adoption of this method. Since legally mandating using this scoring system is not realistic due to the borderless nature of crypto assets, in order to encourage legitimate investors to use this method, it is important to provide strong financial incentives for using it.

This incentive mechanism can be similarly applied to DeFi. DeFi usually has fixed contract addresses, so the idea is to assign trust scores to these contract addresses. If this contract address accepts liquidity from irresponsible wallets, the score decreases. From the perspective of DeFi users, using DeFi with a low trust score will lower the user's own trust score, so an incentive is expected to work to avoid using such DeFi. This mechanism is expected to create an economy where legitimate investors exclusively transact with each other.

The trust scores of self-custody wallets should not made public. Therefore, it is necessary to prove in zero-knowledge that the score is above a certain number.

8.3.2. Standardization

- Why some standardization is necessary

  The evaluation method for calculating trust scores should be standardized. Otherwise, there is a possibility that a counterparty you have evaluated as legitimate may be evaluated as non-legitimate by many other investors and regarded as a careless investor who has transacted with non-legitimate

investors.

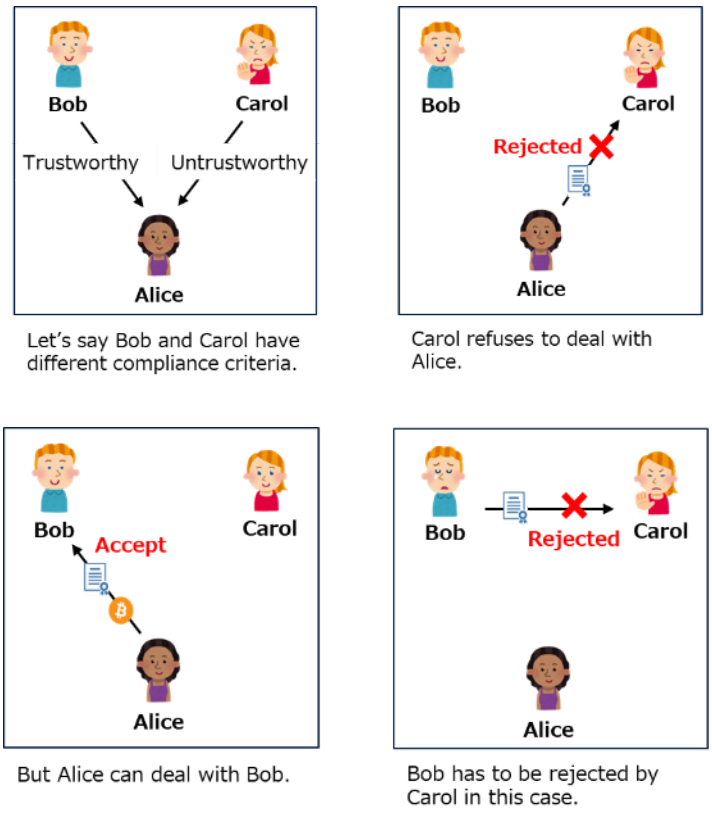


Figure 9

In the example above, Alice is trying to transact with Bob and Carol. Prior to the transaction, Alice needs to prove her legitimacy to them. At this time, suppose Bob and Carol have different legitimacy evaluation criteria. Bob considers Alice to be legitimate and receives crypto assets from Alice, while Carol considers Alice to be illegitimate and refuses to transact with Alice. At this time, even if Carol had considered Bob to be legitimate before Bob received funds from Alice, she cannot consider him legitimate after receiving the funds. This is because if Carol were to receive funds from Bob, it would ultimately mean receiving funds from Alice via Bob. The one facing a big problem here is Bob. Despite behaving legally as the manager of an accountable wallet and correctly verifying Alice's legitimacy in the transaction with Alice, Bob is considered by Carol to be a non-accountable, illegitimate investor and is in a situation where he cannot transact with her. The reason Bob has fallen into such a situation is that he evaluated Alice's legitimacy based on different criteria from Carol. If Bob wants to avoid falling into such a

situation, he needs to evaluate the legitimacy of his transaction partners using the same judgment criteria as the parties he wants to transact with in the future (in this example, Carol) as much as possible.

The concept of trust scores is similar to credit scores in the United States in that it is an indicator of an individual's degree of trustworthiness in financial transactions. There are multiple credit scores in the United States, and businesses that refer to them to grant credit select the appropriate credit score to refer to as needed when granting credit. In other words, such indicators need to be standardized but do not necessarily need to be unified into one. They may differ by jurisdiction. However, when transacting with servicers or investors in that jurisdiction who adopt the trust score widely used in that jurisdiction from other jurisdictions, the degree of legitimacy will be evaluated according to that trust score. Therefore, if one wants to transact globally, there is an expectation that an incentive will arise to constantly engage in trust score maintenance behavior with an awareness of the evaluation criteria of the trust score widely used in other jurisdictions, which is expected to serve as a reference for the evaluation method of the trust score that will likely be widely used in other jurisdictions and globally. Thus, it is expected that appropriate pressure will be applied for the evaluation methods to converge to some extent across the market as a whole against other evaluation methods.

- Exclusion of Arbitrary Evaluation Criteria

  It is important for the industry as a whole to establish a series of standardized legitimacy evaluation criteria. It is desirable to have evaluations that differ as little as possible from legal standards. Therefore, a neutral organization needs to consider the draft.

- Distinction from Preferences

  The jurisdiction to which the investor belongs and the self-compliance rules that the investor has may be taken into account in determining whether a transaction is acceptable, but such preferences should not be taken into account in the trust score. If that happens, the trust score will have different values depending on who measures it. Some may be willing to accept that, but this paper does not recommend it. This is because allowing it raises the risk of increasing centralization to some extent. It would also make it possible for a specific jurisdiction to design arbitrary formulas for calculating trust scores so that the trust scores of specific self-custody wallets or VASPs are calculated low. Therefore, just as the calculation formula for the degree of contribution of validators in currently operating public chains is fixed, it is desirable for the trust score calculation formula to be unified and fixed in a single protocol.

- Basic Formula

  As mentioned earlier, there is no fixed correct method for calculating trust scores in decentralized finance. Therefore, the trust score calculation formula shown in this section is an example of a calculation method when the trust score is pseudo-defined as the expected value of a wallet's reliability. This methodological framework merely provides an instance of the actual calculation of trust scores and should not be taken as the definitive calculation.

  Here, the trust score is basically defined as the probability of a wallet's legitimacy. As mentioned earlier, the legitimacy of a wallet in this paper is defined as three factors: "the legitimacy of the wallet holder," "the legitimacy of the wallet conducts," and "the legitimacy of the crypto assets provenance." Therefore, each factor of legitimacy can be also defined as the absence of illegality. And illegality is defined corresponding to the above three factors as "a wallet being managed by a sanctioned entity," "a wallet has engaged in illegal activity," and "a wallet has crypto asset from illicit source, which means it received crypto assets from a wallet that falls on either of the above two factors." A wallet is deemed illicit if it meets any of these conditions. In other words, the probability of a wallet's legitimacy can be defined as the complement of the union of these illegal factors.

  Therefore, if an event set that a holder of wallet W is illicit is w_1, an event set that wallet W has ever engaged in illicit activity is w_2 and an event set that a wallet W has ever received crypto assets from those wallets is w_3, since the events of a wallet being legitimate are the complementary events of the union of these events, wallet W's trust score $T(W)$ is expressed as follows.

$$T(W) = P\left(\overline{w_1 \cup w_2 \cup w_3}\right) \#(SEQ\ 数式\ \backslash\ *\ ARABIC\ 1)$$

  When any of $P(w_1), P(w_2)$ or $P(w_3)$ is close to 1, $T(W)$ can be approximated as follows.

$$T(W) \cong 1 - Max\left(P(w_1), P(w_2), P(w_3)\right) \#(SEQ\ 数式\ \backslash\ *\ ARABIC\ 2)$$

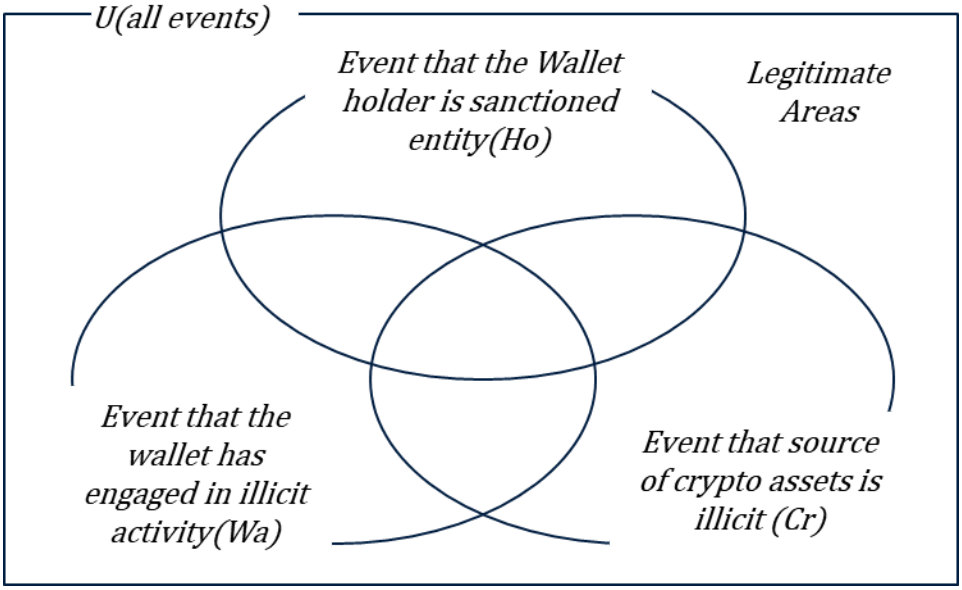


Figure 10

$$Trust\ Score = (Probability\ of\ not\ falling\ under\ any\ of\ the\ illegitimate\ events\ Ho, Wa\ or\ Cr)$$

$$= P(\overline{Ho \cup Wa \cup Cr})$$

$$= P(U - Ho \cup Wa \cup Cr)$$

$$= 1 - P(Ho \cup Wa \cup Cr)$$

$$\cong 1 - Max(P(Ho), P(Wa), P(Cr))$$

$$\cong Min(P(\overline{Ho}), P(\overline{Wa}), P(\overline{Cr}))$$

(If any of $P(Ho), P(Wa)\ or\ P(Cr)$ is close to 1)

$P(Ho)$: *probability of "the wallet holder is a sanctioned entity*

$P(Wa)$: *probability of wallet's past conduct is illegitimate*

$P(Cr)$: *probability that the crypto asset provenance is illegitimate*

$P(\overline{Ho})$: *probability that the wallet holder is legitimate*

$P(\overline{Wa})$: *probability that the wallet conduct is legitimate*

$P(\overline{Cr})$ *: probability that the crypto asset provenance is legitimate*

The specific calculation examples for $P(w_1)$, $P(w_2)$ and $P(w_3)$ are proposed in the following chapters.

8.3.3. Further Consideration

- Interoperability with Existing Systems

  To maximize the impact and adoption of the Trust Score mechanism, it is essential to ensure its compatibility and integration with existing systems and protocols in the DeFi ecosystem. This includes wallets, DEXs, lending platforms, and other DApps.

  The Trust Score mechanism should be designed as a modular and interoperable component that can be easily integrated into existing systems without requiring significant modifications to their underlying architecture. This may involve developing standardized APIs and data formats that allow seamless communication between the Trust Score system and other DeFi components.

  Moreover, the Trust Score mechanism should be compatible with existing compliance frameworks and regulations, such as the Travel Rule and AML/CFT requirements. This ensures that the system can be adopted by regulated entities, such as VASPs, without introducing additional compliance burdens.

- The Need for Continuous Improvement

  The Trust Score mechanism should be designed to evolve and adapt to the changing landscape of the DeFi ecosystem, including the emergence of new technologies, regulatory frameworks, and attack vectors. This requires ongoing research and development efforts to refine the scoring methodology, incorporate new data sources and analytical techniques, and address potential vulnerabilities.

- Privacy Considerations in Trust Score Disclosure

  While the proposed Trust Score system enables users to transact with counterparties who meet their desired level of legitimacy, it is essential to treat Trust Scores as sensitive personal information. When two parties, A and B, engage in a transaction, they should not directly disclose their Trust Scores to each other. Instead, the transaction should only proceed if A's Trust Score meets B's required threshold, and B's Trust Score meets A's required threshold. In case either condition is not met, the transaction should fail without revealing the

specific Trust Scores of the parties involved.

To achieve this privacy-preserving Trust Score comparison, zero-knowledge proof (ZKP) techniques can be employed. ZKP allows one party to prove to another that a given statement is true without conveying any additional information apart from the fact that the statement is indeed true. In the context of Trust Scores, ZKP can enable parties to prove that their scores meet the required thresholds without disclosing the actual scores. This mechanism must also be applied when using DeFi.

Figure 11

However, a potential challenge arises when considering the Trust Score calculation method described in Chapter 11, "Legitimacy of the Crypto Asset Provenances." In this method, an individual's (A's) Trust Score is influenced by the Trust Scores and transaction amounts of the parties from whom they receive crypto assets. Consequently, when A receives crypto assets from a counterparty B, A may be able to deduce B's Trust Score by comparing their own Trust Score before and after the transaction, along with the received amount.

To mitigate this privacy risk, further research is needed to develop advanced cryptographic techniques that prevent such reverse engineering of Trust Scores. Potential solutions may include:

- Obfuscation mechanisms

  Introducing noise or randomization in the Trust Score calculation process to make it more difficult to infer individual Trust Scores from changes in the recipient's score.

- Secure multi-party computation (SMPC)

Utilizing SMPC protocols to perform Trust Score calculations and comparisons in a distributed manner, ensuring that no single party has access to the complete information required to deduce another party's Trust Score.

- Trusted execution environments (TEEs)

  Leveraging TEEs, such as Intel SGX or ARM TrustZone, to perform Trust Score calculations within a secure, isolated environment, preventing unauthorized access to sensitive information.

- Differential privacy techniques

  Applying differential privacy methods to add controlled noise to the Trust Score updates, making it challenging to attribute changes in a recipient's Trust Score to specific transactions or counterparties.

Therefore, to address such issues, industry-standard rules are needed, such as using techniques to keep contract addresses as access destinations confidential. Without such unified standards and a certification mark for compliance with them, users will not be able to use these technologies with peace of mind. While many technologies called zero-knowledge proof techniques are useful for protecting privacy, it is necessary to define standards and criteria for what constitutes a technology that protects privacy, keeping in mind that personal information may be identified as a result depending on how it is used.

9. Legitimacy of the Wallet Holders

9.1. Concept

9.1.1. Risk-Based Approach in Traditional Finance

In traditional finance, as part of the onboarding process, financial institutions must verify that their customers and counterparties are not illegal individuals or organizations before conducting transactions for AML/CFT and related security lows. However, FATF and many regulatory authorities in each jurisdiction do not provide fixed KYC procedures to financial institutions. This is because the necessary KYC vary depending on customer attributes, the financial services they provide, and the transaction details (such as the amount), which makes it impossible to present a unified KYC process.

This flexible approach to modifying the KYC process, based on the risks of the transaction counterparty and the transaction details is called the risk-based approach. Instead of providing fixed KYC procedures, regulatory authorities impose penalties such as fines and license revocation on financial institutions if they fail to detect illicit activities. This motivates each financial institution to implement appropriate KYC and transaction monitoring without excessive or insufficient measures while maintaining a certain degree of operational discretion. Considering this, the role of financial institutions can be understood as standing between investors and investees, accurately measuring the risks of investors and investees, and providing appropriate investors with appropriate investees based on the results. In return for providing this function, they collect transaction fees and spreads.

This risk-based approach principle makes it difficult to separate the entity performing KYC from the entity providing financial services. The principle of the risk-based approach requires financial service providers to flexibly provide appropriate KYC within the scope of their responsibility. While some fixed processes in the KYC process, such as obtaining copies of identification documents, may be outsourced, the judgment of eligibility at the time of providing financial services and the responsibility for it must ultimately lie with the financial service provider.

9.1.2. A New Decentralized Financial Model Using Credentials

The new decentralized financial model using credentials that will be proposed in this paper aims to separate the risk assessor of investors and investees from the provider of financial services. Issuing credentials is essentially an act of granting a kind of credit. By using credentials, it is expected that only qualified users will be able to access decentralized financial services with certain usage conditions. This is expected to simplify the onboarding process for investors and enhance the self-management of personal information.

In the traditional financial system, financial institutions play a crucial role as intermediaries between investors and investees, facilitating transactions and hedging credit risk. In return for providing these functions, they collect transaction fees and spreads.

The issuance of credentials can be seen as an act of granting a kind of credit, in the form of credentials, by entities that already have credibility in the real world to other entities (wallets). In the new decentralized financial model using credentials, the issuance and cryptographic verification of credentials enable any financial service to cryptographically control access by any user. This allows investors to combine and utilize standardized, modular financial services on the blockchain from a single wallet.

By separating the risk assessment of investors and investees from the provision of financial services, this model is expected to simplify the onboarding process for investors and enhance the self-management of personal information and self-funding. On the other hand, financial service providers can focus their resources on developing service provision functions while ensuring compliance, leading to the creation of financial microservices and innovation.

For example, Project Guardian[26], implemented by the Monetary Authority of Singapore (MAS) and several financial institutions, was conducted based on this idea. In this project, investors undergo KYC and receive tokens (e.g., verifiable credentials or Soulbound tokens) that permit access to services, which they can then use to access specific DApps. However, it is important to note that in the Project Guardian proof-of-concept, the credential issuer and the DeFi platform are not completely isolated entities in the strict sense. This is because the credentials issued in this proof-of-concept are essentially access permits for DeFi. In other words, this credential issuer functions as a judge of the eligibility to provide certain financial transactions. From the perspective of the risk-based approach, since the financial service provider must bear the responsibility for the judgment and its consequences regarding the appropriateness of service provision, it cannot be a completely different entity.

To establish a truly open and decentralized financial economy, a compliance assessment framework that clearly separates credential issuers from DApps is needed. This will limit the role of issuers to verifying "objective facts" about credential holders rather than issuing credentials as a judgment of the appropriateness of financial transactions. Credentials should be issued as proofs of objective facts that yield the same results regardless of who the issuer is.

Moreover, a clear separation between credential issuers and financial service providers who utilize them is crucial to ensure that credential issuers are not held responsible for illicit financial activities. If that responsibility is significant, it will become more difficult to establish a business as a credential issuer. It is expected that credential holders will generate their own proofs of legitimacy using standardized credentials and access various DApps. Following sections will explain these implementation steps in more detail.

26

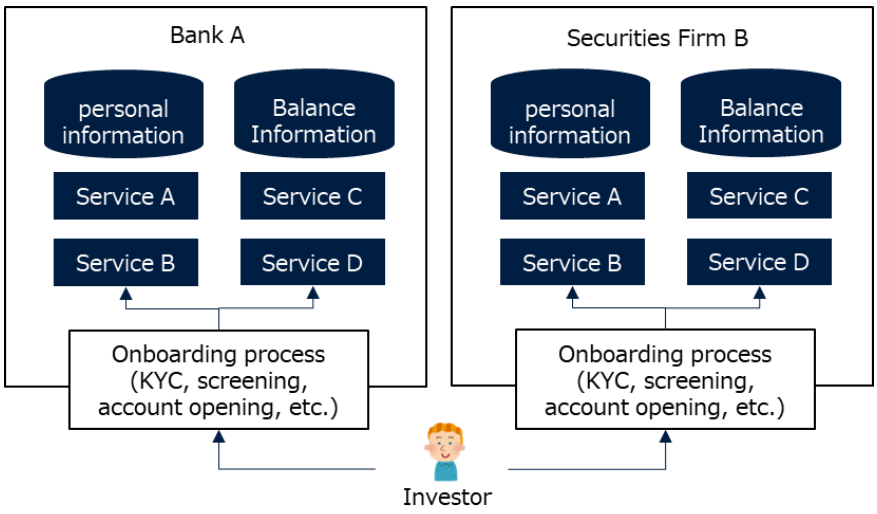


Figure 12

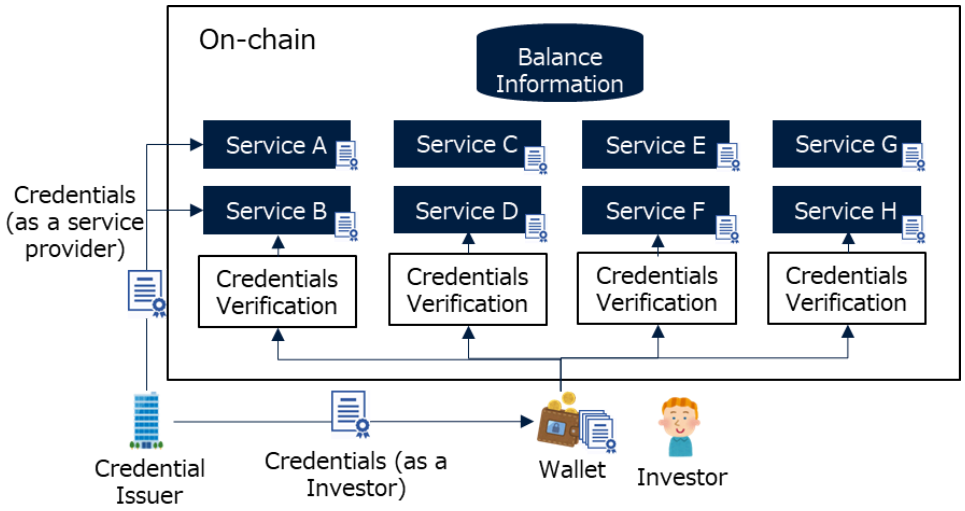


Figure 13

9.1.3. Risk-Based Approach in Decentralized Finance

The key point in implementing a risk-based approach is that credentials can only certify individual objective facts, and it is ultimately up to the verifier to decide whether to conduct transactions with the credential holder based on the claims[27] of the credentials. This is the fundamental concept of the risk-based approach.

27

Credentials themselves are digitally signed proofs of personal information such as the holder's name and address, and it is necessary to combine them to determine whether the person is suitable for the transaction. The issuer can only guarantee the information about objective facts about the holder. For example, any issuer cannot issue a credential that claim that the holder is a person with whom anyone can transact since it cannot be objective facts. In fact, even with the same investor attributes, the compliance judgment results may differ depending on the assessor. That is the risk-based approach.

However, the problem is that it is unrealistic to expect individual investors to genuinely judge the credibility of their transaction counterparties on a case-by-case basis. Therefore, some kind of compliance check tool or wallet application provided by a third party will need to have such functions built in as standard. However, this also raises the question of whether the responsibility lies with the investor or the compliance check tool vendor if the transaction counterparty is found to be compliant despite the tool indicating that the counterparty is compliant.

Moreover, credentials are essentially private information that some investors may be reluctant to hold, even if the design is highly sophisticated to minimize the risk of personal information leakage. On the other hand, some people may be very particular about the nationality of their transaction counterparties. In such cases, it is up to you to decide whether to transact without knowing the counterparty's nationality. This is the concept of the risk-based approach.

However, the more you relax your own compliance rules, the higher the risk of transacting with dishonest investors, and the more likely you are to be viewed as a high-risk investor by other investors, which will disadvantage you in future transactions. This is expected to work as an appropriate check to prevent investors from having unlimited risk appetites.

9.1.4. A New Framework for DeFi Compliance

In the Project Guardian proof-of-concept mentioned above, the credential issuer and the DeFi platform are not completely isolated entities in the strict sense. This is because the credentials issued in this proof-of-concept are essentially access permits for DeFi. In other words, this credential issuer functions as a judge of the eligibility to provide certain financial transactions. From the perspective of the risk-based approach, since the financial service provider must bear the responsibility for the judgment and its consequences regarding the appropriateness of service provision, it cannot be a completely different entity.

To establish a truly open and decentralized financial economy, a compliance assessment framework that clearly separates credential issuers from DApps is needed.

This will limit the role of issuers to verifying "objective facts" about credential holders rather than issuing credentials as a judgment of the appropriateness of financial transactions. Credentials should be issued as proofs of objective facts that yield the same results regardless of who the issuer is.

Moreover, a clear separation between credential issuers and financial service providers who utilize them is crucial to ensure that credential issuers are not held responsible for illicit financial activities. If that responsibility is significant, it will become more difficult to establish a business as a credential issuer. It is expected that credential holders will generate their own proofs of legitimacy using standardized credentials and access various DApps.

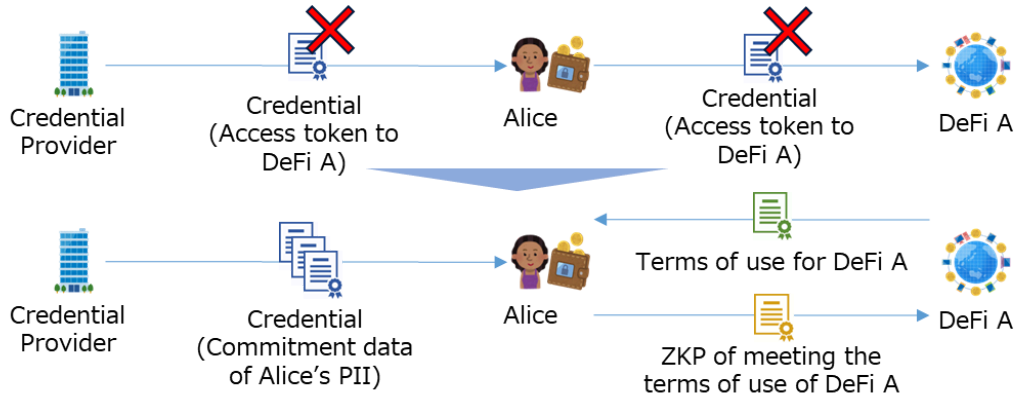


Figure 14

The position of this paper is that, at least, if a wallet cannot provide any proof about the holder, i.e. if one wishing to transact with the wallet cannot limit any attribution information about the wallet's owner, then one should not transact with the wallet, because the transaction may involve a transaction with an entity or individual on a sanctions list.

9.2. Procedure

9.2.1. Credentials Issuance Procedure Standardization

The issuance process needs to be standardized. In traditional finance, penalties and accompanying reputational risks motivated each financial institution to conduct KYC and transaction monitoring accurately. However, as described above, in case of the DeFi, when the credential issuer performing KYC and they are not financial service providers,

this motivation may not function well. If KYC procedures differ by jurisdiction or credential issuer, the results of KYC execution will not be universal. Credentials issued by organizations with "loose standards" and those with "strict standards" will differ in credibility. Furthermore, the rules to be complied with during financial transactions vary depending on the jurisdiction, services provided, financial products handled, and other factors, making it difficult to issue credentials that can be used to access all services. The requirements and procedures for credential issuers themselves also need to be discussed, such as who grants credentials to credential issuers.

To implement a risk-based approach in a business entity such as DeFi, credential issuers need to maintain neutrality in investment decisions and focus on providing objective facts about credential holders. Credential issuers should focus solely on issuing credentials that verify specific investor information, rather than functioning as an approval for token ownership or access to DeFi services. To emphasize this distinction, this paper refers to credentials related to investor information as "attribution credentials," emphasizing that credentials issued by credential issuers are primarily intended for identity verification rather than investment approval. As an example, this section considers the procedure for issuing an attribution credential that the holder is not on the sanction list.

9.2.2. Issuance Procedure Example 1

- Non-Sanctioned Proofs

  In traditional finance, each financial institution manages sanction lists in accordance with the regulations of the jurisdiction in which they are located and the rules established by the institution itself. Financial institutions collect sanction lists managed by the authorities in each jurisdiction and also maintain their own sanction lists, integrating them for screening purposes. As a result, the watchlists used for screening differ for each financial service provider.

  This lack of uniformity in sanction lists is highly inconvenient for decentralized finance, which assumes active P2P transactions. For example, suppose there is a VASP A with very loose screening rules. In that case, even if VASP B, which does not trust VASP A, rejects direct fund transfers from VASP A through the Travel Rule protocol process, there is no way to eliminate the possibility that the same funds will ultimately reach VASP B via P2P transactions. In this case, even if VASP B itself has very strict screening rules, VASP A with loose screening rules becomes a weak point, and the possibility of successful money laundering cannot be eliminated.

  To address this issue, this paper proposes that credential issuers do not directly

issue proofs of non-listing on sanction lists to users. Instead, credential issuers should issue credentials related to users' PII, which will have the same content regardless of who issues them. Subsequently, users generate credentials proving that they are not included in the relevant sanctions list by using both their own PII-related credentials and the sanctions list data employed as oracle data.

By separating the issuance of PII-related credentials from the generation of proofs of non-listing on sanction lists, the system promotes a more standardized and interoperable model of compliance verification. This approach ensures that the fundamental building blocks of compliance verification—the PII-related credentials—remain uniform and reliable, regardless of the specific sanction lists or screening procedures employed by different service providers. This process allows users to demonstrate their compliance with the specific requirements of their transaction counterparties or service providers, without relying on a single, centralized authority to assert their overall compliance status. This decentralized approach to compliance verification ensures that the weakest link in the system—such as a VASP with lax screening rules—does not compromise the overall integrity of the DeFi ecosystem.

- Prerequisites and Requirements

  - Origination of The Sanction List Data

    Firstly, please note that the sanctions list referred to here is a list of sanctioned organizations and individuals, as in the case of existing finance, and does not manage a list of wallet addresses. The FBI and other authorities publish a list of wallet addresses that are used to manage criminal proceeds, they rarely identify who manages the wallets. Such lists are also sometimes called sanction lists, but in this paper, to distinguish them from the former list, we will call the former list a sanctions list and the latter a crypto watchlist. The latter list will be used frequently in the next section, The Legality of Wallet Conduct.

    Secondly, this paper does not discuss the management or updating methods of the sanction lists themselves. Many of the individuals or entities on these lists are listed not due to crypto-related crimes but because of various real-world crimes and offenses. Ultimately, whether an entity is listed on these sanction lists heavily depends on the procedures of each jurisdiction, and providing a unified view on this matter would deviate from the main topic of this paper. In this section, we will discuss the challenges related to how the sanction lists issued by various authorities can be used as oracle data, such as the issues of verifying their

authenticity and completeness, and how to reference multiple existing sanction lists as a single oracle data source. However, we will not delve into how the sanction lists managed by each authority should be updated. By addressing the technical challenges associated with the reliable and efficient incorporation of sanction list data, the proposed system aims to leverage this information to promote compliance and deter illicit activities within the DeFi ecosystem. The use of oracle data to bridge the gap between off-chain sanction lists and on-chain compliance mechanisms is a critical component of the accountable wallet framework.

- The sanctions list referenced depends on the counterparty

  It is not possible to issue a fact that someone is not on a sanctions list as an objective fact that is universally applicable to everyone. This is because the scope and definition of sanction lists vary by jurisdiction and financial service provider. For example, even countries designated as blacklisted by FATF publish their own sanction lists. However, for whitelisted countries that have properly ratified FATF regulations, these sanction lists are clearly not ones they should reference.

  Therefore, it is evident that not all sanction lists on Earth should be referenced. Consequently, it is not possible to issue an attribution credential in the sense of not being on all sanction lists. The only fact that can be issued is that an individual is not on a specific sanctions list published by a particular authority, and it is ultimately up to your transaction counterparty or the entity seeking to provide you with services to decide which list should be used. Here, too, the principle that compliance is a relative matter determined by the transaction counterparty is crucial.

  In this case, if the sanctions list that the transaction counterparty requests to reference is properly digitally signed, using the non-membership proof technique for Merkle trees described later, it is possible to prove to others that one is not on that list based on digitally signed PII information. This will be discussed in more detail later.

- Decentralization of credential issuers

  PII can be issued by multiple credential issuers. For example, if it is a credential regarding a name, no matter who issues it, it will be exactly the same.

And if the names are the same, the results of the sanctions screening check based on the name will also be the same. Therefore, this proposal assumes that PII will be obtained in a decentralized manner from multiple credential issuers. This is also intended to prevent the credibility of the credential holder from being dependent on a single credential issuer. However, the results of sanctions screening checks may not necessarily be derived from credential issuers in the same way. Therefore, it is desirable to separate PII credentials and sanctions screening check result credentials.

- Sanctions lists are constantly updated

  Sanctions lists are constantly being updated, so credentials for the results of sanctions screening checks will always be outdated. However, PII does not change as much as sanction lists. Therefore, it is desirable to have PII-related credentials as fixed and to have a protocol in place to obtain sanctions check results based on them at any time and as many times as needed.

- Tipping-off rule

  Investors use credentials issued by credential issuers regarding their PII to further obtain credentials proving they are not sanctioned targets, but this needs to be done without disclosing actual personal information to anyone. Also, in order to comply with the tipping-off rule[28], it is realistic from an operational perspective to assume that the sanction list itself contains personal names that cannot be made public, so this paper treats the sanction list itself as data subject to personal information protection. Therefore, the sanction list referenced by the credentials as oracle data is expected to be published as data that cannot be decoded into the original data, such as hash values, generated based on the information of the sanctioned individuals. When using hash values, since the possible combinations of PII data are finite, this would be vulnerable to rainbow table attacks[29] if simple hash values were used, so hash values including salt[30] need to be used instead of simple hash values. Investors holding PII-related credentials use this list to generate their own credentials proving they are not on the list. This is expected to utilize the

28

29

30

non-existence proof of Merkle trees[31], which will be described later.

- Premise

  It is important to note that the actual process of sanctions screening in real-world scenarios is significantly more complex than the simplified version presented in this paper. The purpose of this simplification is to focus on the core concept of generating non-sanction proofs from personally identifiable information (PII), without delving into the intricacies of the screening process itself.

  For the purposes of this example, we will consider the case where the wallet holder is an individual, rather than a legal entity. Consequently, the sanction lists referenced in this process will only include individuals identified as antisocial forces, as opposed to organizations or corporations.

- Simplification of Sanction List Data

  In practice, the data published by various authorities, such as law enforcement agencies and financial regulators, may not have a uniform set of attributes. For instance, some sanction lists may include the residential addresses of the listed individuals, while others may not. However, to maintain the focus of our discussion, we will assume that the data published by different authorities contains a consistent set of attributes, without any significant variations.

- Sufficiency of Published Data for Unique Identification

  A crucial assumption in this process is that the data published by the authorities contains sufficient information to uniquely identify any given antisocial individual. While a person's name alone may not be enough to pinpoint a specific individual, as there could be multiple people with the same name, we presume that the sanction lists include additional attributes, such as date of birth, which collectively provide enough information to distinguish one person from another.

- Feasibility of Generating Proofs from Necessary Data

  Although the actual sanctions screening process employed by financial institutions may involve a vast array of data points and complex procedures, it is ultimately a process that can be executed by a Turing machine. This implies that, given the necessary data, it should be possible

---

31

to generate proofs that encapsulate the essence of the screening process, even if the real-world implementation is more intricate.

- Overview of procedure

The crypto asset holder (Alice) can prove that she is not on the sanctions list by following the steps below.

- Obtaining PII-related Credentials

Alice obtains credentials from a trusted credential issuer regarding her personally identifiable information (PII), such as her name, address, and date of birth.

The credential issuer generates a cryptographic commitment using Alice's PII and digitally signs the commitment data to ensure its integrity and authenticity.

The credential issuer securely transmits the PII-related credentials and the signed commitment data to Alice.

- Sanction List Preparation

The authorities responsible for maintaining the sanction list hash the PII of sanctioned individuals using a secure cryptographic hash function, such as SHA-256.

The hashed PII values are organized into a Merkle tree structure, with each leaf node representing a hashed PII value.

The authorities calculate the root hash of the Merkle tree and digitally sign it to ensure the integrity of the sanction list.

The signed root hash and the Merkle tree structure are made publicly available for reference.

Integrating multiple sanction lists into one.

- Non-Membership Proof Generation:

Alice calculates the hash value of her PII using the same cryptographic hash function used by the authorities.

Alice retrieves the publicly available Merkle tree structure and the signed root hash of the sanction list.

Alice identifies the two consecutive leaf nodes in the Merkle tree whose hash values encompass her calculated PII hash value.

Alice generates a non-membership proof by providing the following information:

The two consecutive leaf nodes (hashed PII values) encompassing her PII hash value.

The Merkle proofs (i.e., the necessary hashes) to reconstruct the Merkle path from the two leaf nodes to the root hash.

The digital signature of the root hash, as provided by the authorities.

Alice creates a zero-knowledge proof demonstrating that her PII hash value falls between the two consecutive leaf nodes without revealing the actual PII hash value. This can be achieved using range proof techniques, such as those based on Pedersen commitments.

- Proof Verification

Alice presents her non-membership proof, along with the signed commitment data received from the credential issuer, to the verifier (e.g., VASP A).

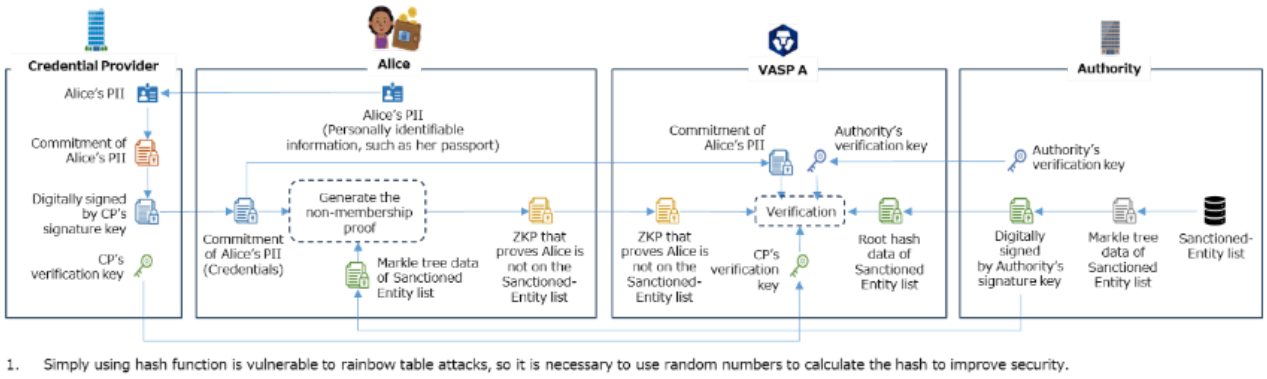
The verifier checks the digital signature of the commitment data to ensure its authenticity.

The verifier verifies the digital signature of the root hash to ensure the integrity of the sanction list.

Using the provided Merkle proofs, the verifier reconstructs the Merkle path from the two consecutive leaf nodes to the root hash and confirms that the calculated root hash matches the signed root hash.

The verifier validates Alice's zero-knowledge proof, ensuring that her PII hash value indeed falls between the two consecutive leaf nodes without learning the actual PII hash value.

If all the verification steps are successful, the verifier can conclude that Alice's PII is not present on the sanction list, without having access to her actual PII.



1. Simply using hash function is vulnerable to rainbow table attacks, so it is necessary to use random numbers to calculate the hash to improve security.

Figure 15

By following this detailed procedure, crypto asset holders can generate non-membership proofs using sanction lists prepared by authorities, while preserving the confidentiality of their PII. The use of cryptographic commitments, Merkle trees, digital signatures, and zero-knowledge proofs ensures the integrity, authenticity, and privacy of the process.

It is important to note that the specific implementation of the zero-knowledge proof technique may vary depending on the chosen range proof method, such as Pedersen commitments. Additionally, the procedure may need to be adapted to accommodate any variations in the sanction list structure or the cryptographic primitives used by different authorities.

Regular updates to the sanction list by the authorities should be accompanied by a refreshed Merkle tree structure and digitally signed root hash to ensure the proofs generated by crypto asset holders remain valid and up-to-date.

- Obtaining PII-related Credentials

This process involves the following detailed steps:

- Identity Verification

Alice, the crypto asset holder, initiates the process by approaching a trusted credential issuer, such as a regulated financial institution or a government-approved identity verification service.

Alice provides the necessary personally identifiable information (PII) to the credential issuer, such as her full name, address, date of birth, and any additional information required by the issuer's identity verification procedures.

The credential issuer validates Alice's identity using established know-your-customer (KYC) and anti-money laundering (AML) procedures,

which may include document verification, facial recognition, and cross-referencing with official databases.

- Credential Generation

  Upon successful identity verification, the credential issuer generates a digital credential containing Alice's PII.

  The credential is created using a standardized format, such as the Verifiable Credentials (VC) data model, which allows for cryptographic security and interoperability across different systems.

  The credential includes essential attributes such as Alice's name, address, date of birth, and a unique identifier associated with the credential.

  The credential issuer digitally signs the credential using their private key, ensuring its authenticity and integrity.

- Commitment Generation

  In addition to the digital credential, the credential issuer generates a cryptographic commitment using Alice's PII.

  The commitment is created by applying a secure cryptographic hash function, such as SHA-256, to Alice's PII, along with a random secret value known as a blinding factor.

  The resulting commitment is a cryptographic digest that uniquely represents Alice's PII without revealing the actual information.

  The credential issuer digitally signs the commitment data using their private key to ensure its authenticity and integrity.

- Transmission and Storage

  The credential issuer securely transmits the PII-related digital credential and the signed commitment data to Alice through an encrypted communication channel.

  Alice securely stores the received credential and commitment data in a digital wallet or a secure storage medium, ensuring their confidentiality and accessibility for future use.

  By obtaining PII-related credentials from a trusted issuer, Alice establishes

a verifiable and authenticated basis for generating non-membership proofs using sanction lists. The digital credential serves as a tamper-evident and cryptographically secure attestation of Alice's identity, while the signed commitment data enables Alice to prove the association between her PII and the credential without revealing the actual PII.

It is important to note that the security and reliability of the PII-related credentials depend on the trustworthiness of the credential issuer and the robustness of their identity verification and credential generation processes. Crypto asset holders should carefully select reputable and regulated credential issuers to ensure the integrity and acceptance of their PII-related credentials within the decentralized finance ecosystem.

- Sanction List Preparation

The preparation of a sanction list is a crucial process for ensuring that crypto asset holders can generate verifiable non-membership proofs. Authorities, such as government agencies or international organizations, are collecting, aggregating, and maintaining the sanction list, which defines individuals or entities subject to legal sanctions. These authorities publish this information, often on their official websites, to make it publicly available for relevant stakeholders. In this format, the data does not meet the necessary requirements for authenticity and completeness, making it unsuitable for generating non-membership proofs, therefore, further steps are required to ensure the authenticity and completeness of this data to issue non-sanctioned proofs. There are three primary methods that can be employed to secure the data and provide tamper-evident proofs:

- Digital signatures by authorities

In this method, the authorities themselves would hash the collected sanction list data and sign it digitally, ensuring the integrity of the data directly from the source.

However, this approach raises issues of public key certification and the need for standardized data formats. Requesting this from authorities worldwide may not be a realistic solution.

- Trusted organizations

Given the challenges associated with above method, an alternative approach involves a single trusted organization digitally signing it, and ensuring its authenticity and completeness. This method mirrors traditional financial systems where third parties curate and verify data for broader

use.

This process resembles the role of third-party service providers in traditional finance, where banks do not collect sanction lists themselves. However, this method also raises questions, such as why the organization can be trusted, how to ensure the organization does not tamper with the data, and what financial incentives the organization can have to provide such a service.

- Decentralized curation and verification

  To address the limitations of centralized approaches, a decentralized system for curating and verifying sanction list data can be developed. In this model, a network of independent nodes collaborates to collect, validate, and maintain the watchlist data. Each node is incentivized to act honestly through a staking mechanism, where nodes are required to stake tokens to participate in the network. Malicious behavior, such as submitting false or incomplete data, results in the slashing of the node's stake.

  This can be seen as a sanction-list-data version of oracle chains like Chainlink. The proposed protocol would retrieve the off-chain information of sanctioned person designated by regulatory authorities and bring it onto the blockchain. Similar to oracle chains, designing incentives for each node to act honestly is crucial.

  The decentralized network operates on a consensus mechanism, where nodes vote on the validity and completeness of the submitted watchlist data. Once a threshold of nodes approves the data, it is considered verified and added to the master watchlist. This master watchlist is then cryptographically signed by the network, ensuring its authenticity and immutability.

  To further enhance the security and reliability of the decentralized watchlist, the network can implement a multi-sig scheme, requiring multiple trusted nodes to sign off on any changes or updates to the watchlist. This helps prevent any single node from manipulating the data and ensures that the watchlist remains accurate and up-to-date.

Each of these methods ensures that the sanction list data remains verifiable, tamper-resistant, and usable for generating reliable non-membership proofs. The following steps outline the process after the sanction list is published, with the choice of who performs these steps (authorities, trusted organizations, or decentralized oracles) determining the specific method of implementation.

- Data Hashing

  Once the sanction list is available, the next step is to protect the privacy of individuals listed while still enabling efficient non-membership proof generation. The process involves hashing the personally identifiable information (PII) of sanctioned individuals using a secure cryptographic hash function, such as SHA-256.

  Regardless of whether the data is processed by the authorities, a trusted organization, or decentralized oracle nodes, this step ensures that the original PII cannot be reversed from the hash, safeguarding privacy while allowing users to confirm whether or not an individual is on the sanction list. To maintain compatibility across systems, a consistent hash function must be applied throughout the process.

- Merkle Tree Construction

  The hashed PII values are then organized into a Merkle tree, a cryptographic data structure that allows efficient and secure verification of data integrity. Each hash becomes a leaf node in the Merkle tree. The leaf nodes are then concatenated and hashed in pairs to generate parent nodes, and this process is repeated until a single root hash is produced.

  Depending on the entity managing this process—whether it be the original authority, a trusted third party, or decentralized nodes—the integrity of the Merkle tree structure must be verified. This ensures that the tree represents the full and accurate list of sanctioned individuals. A Merkle tree allows for compact, verifiable proofs to be generated, confirming the inclusion or exclusion of a particular individual’s hash from the list.

- Digital Signature

  To provide tamper-evident assurance, the root hash of the Merkle tree is digitally signed. If the authorities themselves are conducting the entire process, they would apply their private key to sign the root hash, ensuring that the data has not been altered since its initial publication. If a trusted third-party organization is handling the process, they would similarly sign the root hash, vouching for the completeness and accuracy of the data. In a decentralized system, a consensus mechanism involving multiple oracle nodes could be used to apply a collective signature to the root hash, ensuring that the list has been vetted and verified by a decentralized network of validators.

In all cases, the public key of the signing entity—whether it be the authorities, the trusted organization, or the decentralized network—must be made publicly available to enable the verification of the signature by anyone querying the sanction list. This ensures that users can trust the data to generate valid non-membership proofs.

- Publication and Distribution

  Once the root hash has been signed, the sanction list, along with its Merkle tree, root hash, and digital signature, must be published and made publicly available through secure and reliable channels. Depending on the chosen method, this could involve authorities distributing the list through their official channels, a trusted third-party organization curating and distributing the list, or a decentralized network ensuring the list is available for querying across the blockchain ecosystem.

  In decentralized systems, users can query the list using a small fee, and the distributed nature of the system ensures continuous availability and integrity. In the case of authorities or trusted organizations, distribution can occur through secure web portals or similar means to ensure easy and reliable access.

- Regular Updates

  Sanction lists require regular updates to reflect new additions, removals, or changes. Each update triggers the re-hashing of the data, reconstruction of the Merkle tree, and re-signing of the root hash. Again, the method of updating depends on whether the process is handled by the authorities, a trusted organization, or decentralized nodes. Each entity involved must follow the same rigorous cryptographic procedures to ensure that the list remains authentic and complete over time.

- Sanction List Integration

  In the previous section, we discussed the process of ensuring the authenticity and completeness of sanction list data, which can be performed by the authorities responsible for maintaining the sanction list, a trusted organization that collects and processes the data from multiple authorities, or a decentralized network of nodes that collaborates to curate and verify the data. However, an additional challenge arises when considering the integration of sanction lists from multiple jurisdictions.

- Importance of Sanction List Integration

  In traditional finance, each jurisdiction manages its own sanction lists, requiring financial institutions to reference multiple lists. Moreover, sanctioned organizations often use front companies rather than their actual names when attempting to open accounts, making it a time-consuming task for financial institutions to track and maintain this data. To address this issue, financial institutions typically rely on third-party service providers that integrate sanction lists from various jurisdictions and include information on front companies.

  The integration of sanction lists is equally important in decentralized finance. If sanction lists were not integrated, a prover who wants to demonstrate that they are not on any sanction list would need to generate a separate non-membership proof for each list. Given the large number of authorities and jurisdictions that maintain sanction lists, generating such a vast number of proofs would be impractical and burdensome.

  Furthermore, to enable seamless access to different DApps using the same set of credentials, sanction lists should be integrated to the greatest extent possible. If all the sanction lists required by a counterparty are included in the integrated list referenced by the prover, there would be no need to generate new credentials for each interaction.

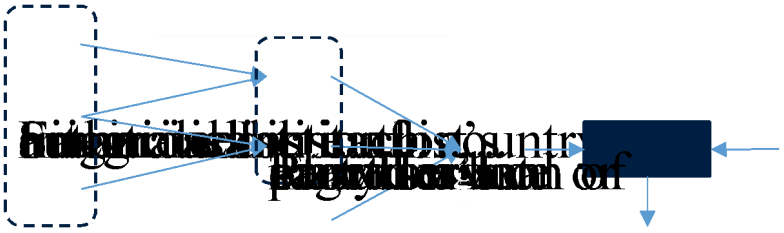


Figure 16

- Methods for Sanction List Integration

  To address the challenge of integrating sanction lists from multiple sources, two approaches can be considered:

- Integration by a Trusted Third Party

  In this approach, a trusted organization takes on the responsibility of collecting sanction lists from various jurisdictions, integrating them into a single, comprehensive list, and ensuring the accuracy and completeness of the data. This organization would perform the necessary due diligence to include information on front companies and other aliases used by sanctioned entities.

  Once the trusted organization has integrated the sanction lists, they can proceed with the steps outlined in the previous section, such as hashing the data, constructing a Merkle tree, and digitally signing the root hash. By combining the integration process with the methods for ensuring data authenticity and completeness, the trusted organization can provide a reliable and verifiable source of integrated sanction list data for use in generating non-membership proofs.

- Integration through an Oracle Chain

  An alternative approach to sanction list integration is the use of an oracle chain, such as Chainlink. In this method, a decentralized network of nodes is responsible for collecting, integrating, and updating sanction list data from multiple sources.

  The oracle nodes would be incentivized to act honestly and provide accurate information through a reward mechanism. They would collect sanction lists from various jurisdictions, integrate them into a single list, and perform the necessary steps to ensure data authenticity and completeness, such as hashing, constructing a Merkle tree, and digitally signing the root hash.

  The use of an oracle chain for sanction list integration offers the benefits of decentralization, transparency, and tamper-resistance. The incentive structure encourages nodes to maintain the integrity of the data, and the decentralized nature of the network reduces the reliance on a single trusted entity.

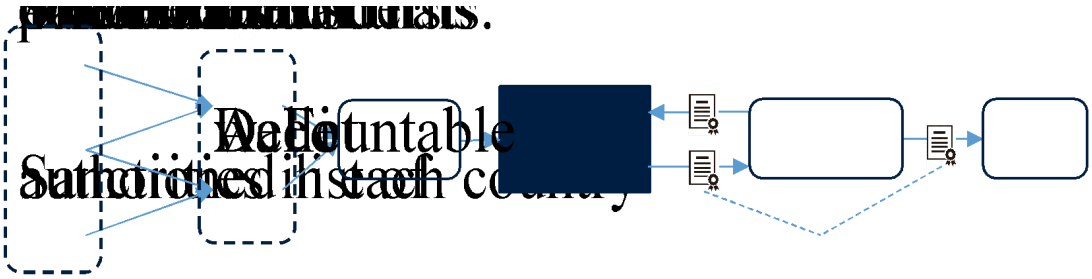


Figure 17

- Localized Sanctions List Integration

  From a practical perspective, it is not necessary to consolidate all sanction lists worldwide into a single, unified list. Instead, integrating sanction lists at the national level is often sufficient. For example, when transacting with a Japanese resident, verifying their absence from the sanction lists defined by Japanese authorities is crucial, while checking their presence on sanction lists of other countries is far less relevant. Even if the individual is involved in antisocial activities, they are unlikely to be listed on sanction lists outside of Japan.

  This principle can be applied more broadly: if you are a U.S. citizen residing in the United States and you trust the Japanese authorities when engaging in decentralized finance transactions with a Japanese counterpart, the non-existence proof that the Japanese party should submit to you, as an American, would only need to demonstrate their absence from the sanction lists defined by the Japanese authorities. However, this logic holds true only if you, as an American, have confidence in the Japanese authorities.

  In summary, when transacting with an individual from another country, if the counterparty can prove their nationality and country of residence, and you trust the authorities of that country, it is sufficient for the counterparty to provide proof of their absence from the sanction lists defined by the authorities of their country of residence.

  However, in practical implementations, information about an individual's country of residence is considered personal information. Therefore, this procedure must be conducted without disclosing the country of residence. In such cases, the verifier should be able to confirm that the transaction

counterparty (proof provider) resides in a trustworthy country and is not listed on the sanction lists defined by the authorities of that country, without knowing the specific country of residence. To facilitate this, verifiers should predefined a list of multiple trustworthy countries (a whitelist). If the verifier's whitelist is narrow, the proof provider should be warned, as it increases the likelihood of the verifier inferring their country of residence. The whitelist could include FATF-designated white countries or countries and jurisdictions that have ratified their recommendations.

Given these considerations, it becomes clear that integrating sanction lists at the national level is sufficient. Moreover, the procedures for conducting transactions within the same country (i.e., when the counterparty resides in the same country as oneself) may differ from those for international transactions (i.e., when the counterparty resides in a different country). Alternatively, since a crypto asset holder's country of residence can be easily inferred from on-chain data and does not individually identify them, it could be considered non-personal information and assumed to be public. However, this requires further discussion.

This localized approach to sanctions list integration offers several key benefits. First, it reduces the complexity and computational burden associated with verifying compliance against a single, global sanctions list. By focusing on the integration of lists at the local or regional level, compliance groups can streamline the verification process and minimize the need for proof providers to generate an excessive number of non-existence proofs.

Second, the localized integration of sanction lists respects the sovereignty and autonomy of different jurisdictions, allowing them to maintain control over their compliance requirements and enforcement mechanisms. This is particularly important in the context of decentralized finance, where participants may be subject to varying legal and regulatory obligations depending on their location and nationality.

Third, the formation of compliance groups based on localized sanctions list integration promotes the development of trust and collaboration among participants within shared jurisdictions. By adhering to common compliance standards and leveraging integrated sanction lists, members of a compliance group can more easily verify the legitimacy of their transaction counterparties, fostering a sense of shared responsibility and mutual accountability.

Generalizing this concept, accountable economies are likely to form

subset groups of wallets that determine the legitimacy of transaction counterparties using similar criteria, such as shared sanction lists. Transactions within the same group become straightforward. As will be discussed later, the third aspect of legitimacy—the provenance of crypto assets—focuses not only on the direct transaction counterparty but also on the legitimacy of their past transaction partners. If both parties can prove they belong to the same group, this issue can be easily resolved. Conversely, transactions with wallets belonging to other groups involve more complex procedures, similar to the differences between domestic and international transfers in traditional finance.

While the accountable wallet framework allows each wallet to freely determine the compliance criteria they require from transaction counterparties, it warns that setting excessively low standards and transacting with parties who barely meet those criteria may hinder future transactions with counterparties who maintain higher standards. In other words, although the determination of compliance criteria is free, in practice, users are likely to select one or more representative groups from among those that will inevitably form, and conduct transactions accordingly. Adhering to multiple compliance rules enables a wallet to be trusted by wallets from different groups.

When conducting transactions across groups, in addition to verifying the counterparty, it is necessary to assess the trustworthiness of the group's internal procedures for properly managing and updating sanction lists. This evaluation of procedural reliability is distinct from assessing individual trustworthiness and requires further discussion.

- Non-Membership Proof Generation

Non-membership proof generation is the process by which a crypto asset holder, Alice, demonstrates that her personally identifiable information (PII) is not present in the sanction list without revealing the actual PII. This process involves the following detailed steps:

- PII Hash Calculation

Alice retrieves her PII-related credential and the associated signed commitment data from her secure storage.

She verifies the integrity and authenticity of the credential and commitment data by checking the digital signature provided by the credential issuer.

Alice extracts her PII from the credential and applies the same cryptographic hash function used by the authorities in the sanction list preparation process, such as SHA-256, to calculate the hash value of her PII.

- Sanction List Retrieval

  Alice obtains the latest version of the publicly available sanction list, including the Merkle tree structure, the root hash, and the digital signature.

  She verifies the integrity and authenticity of the sanction list by checking the digital signature using the authorities' public key. This ensures that the sanction list has not been tampered with since it was signed by the authorities.

- Proof Generation

  Alice traverses the Merkle tree structure of the sanction list to locate the two consecutive leaf nodes (hashed PII values) that encompass her calculated PII hash value. She generates a set of Merkle proofs, which consist of the necessary hashes along the path from the two identified leaf nodes to the root hash of the Merkle tree. Alice creates a non-membership proof object that includes the following components:

  - The two consecutive leaf nodes (hashed PII values) encompassing her PII hash value.
  - The Merkle proofs, which allow the verifier to reconstruct the path from the leaf nodes to the root hash.
  - The digital signature of the root hash, as provided by the authorities.

  Let's assume Alice's PII hash value is "**003**b4726....5d39b0e5" as in the figure below. Alice compares her PII hash value with the hash values on the sanction list and identifies the two hash values that fall immediately before and after her hash value. In this case, the two hash values are “**002**a337.....27c4b45fe1” and "**004**7e90.....3fdf8258e8".

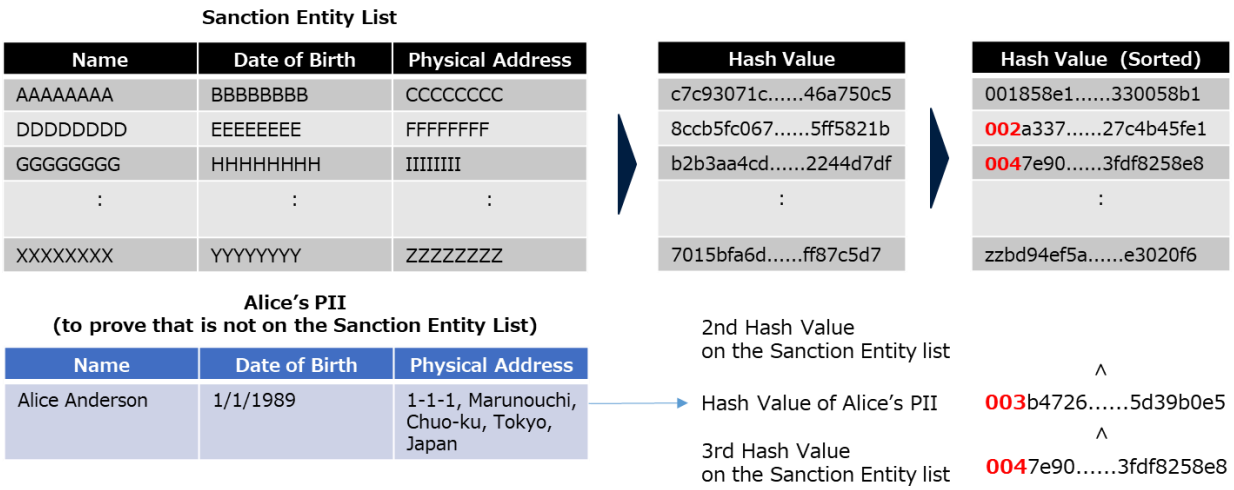


Figure 18

The verifier retrieves the same version of the sanction list used by Alice to ensure consistency. The verifier locates the two hash values in the sanction list that Alice provided in her non-membership proof. The verifier checks if Alice's PII hash value, which is not explicitly shared, falls between the two provided hash values. This confirms that Alice's hash value is not an exact match with any of the hash values on the sanction list. The verifier validates the digital signature on Alice's PII hash value using Alice's public key. This ensures that the PII hash value used in the proof genuinely belongs to Alice and has not been tampered with. If the PII hash value falls between the two provided hash values and the digital signature is valid, the verifier can conclude that Alice's PII is not present on the sanction list without learning the actual PII.

To enhance the privacy and security of the non-membership proof, Alice can employ zero-knowledge proof techniques, such as range proofs or set membership proofs, to demonstrate that her PII hash value falls between the two consecutive leaf nodes without revealing the actual hash value.

- Zero-Knowledge Proof Generation (Optional)

If Alice chooses to use zero-knowledge proof techniques, she generates an additional proof that demonstrates the relationship between her PII hash value and the two consecutive leaf nodes in the Merkle tree.

For example, Alice can use a range proof technique, such as Pedersen

commitments, to prove that her PII hash value lies within the range defined by the two leaf nodes without disclosing the actual hash value.

The zero-knowledge proof is generated using the cryptographic parameters and algorithms specific to the chosen proof technique, ensuring that it is secure, verifiable, and maintains the privacy of Alice's PII.

- Proof Packaging

  Alice combines the non-membership proof object, including the leaf nodes, Merkle proofs, and the digital signature of the root hash, along with the zero-knowledge proof (if generated) into a single proof package.

  She may include additional metadata, such as timestamps or proof version information, to facilitate the verification process and ensure the freshness of the proof.

- Proof Transmission

  Alice securely transmits the non-membership proof package to the verifier, such as a financial institution or a smart contract, as part of the transaction or verification process.

It is important to note that the specific implementation details of the non-membership proof generation process may vary depending on the chosen cryptographic primitives, zero-knowledge proof techniques, and the requirements of the decentralized finance ecosystem. The process should be standardized and well-documented to ensure interoperability and consistent verification across different platforms and jurisdictions.

- Proof Verification

  Proof verification is the process by which a counterparty, such as a VASP, a smart contract, a crypto holder who uses a self-custodial wallet, validates the non-membership proof provided by a crypto asset holder, Alice, to confirm that her personally identifiable information (PII) is not present in the sanction list. The verification process involves the following detailed steps:

- Proof Receipt and Parsing

  The verifier receives the non-membership proof package transmitted by Alice.

The verifier parses the proof package to extract the individual components, including the leaf nodes, Merkle proofs, digital signature of the root hash, and any additional metadata or zero-knowledge proofs.

- Sanction List Retrieval

  The verifier obtains the same version of the sanction list used by Alice during the proof generation process. This ensures that the verification is performed against the same Merkle tree structure and root hash.

  The verifier verifies the integrity and authenticity of the sanction list by checking the digital signature using the authorities' public key. This step confirms that the sanction list has not been tampered with since it was signed by the authorities.

- Merkle Proof Verification

  Using the leaf nodes and Merkle proofs provided in the non-membership proof, the verifier reconstructs the Merkle path from the leaf nodes to the root hash of the sanction list's Merkle tree.

  The verifier calculates the hash values along the path using the provided Merkle proofs and compares the resulting root hash with the signed root hash obtained from the sanction list.

  If the calculated root hash matches the signed root hash, the verifier can confirm that the leaf nodes and Merkle proofs are valid and consistent with the sanction list.

- Zero-Knowledge Proof Verification (if applicable)

  If Alice has included a zero-knowledge proof in the non-membership proof package, the verifier validates the proof using the appropriate verification algorithm corresponding to the specific zero-knowledge proof technique used.

  The verifier checks the validity of the zero-knowledge proof by verifying the cryptographic commitments, challenges, and responses provided in the proof, ensuring that they satisfy the mathematical properties required by the proof system.

- Proof Validation

If the Merkle proof verification and zero-knowledge proof verification (if applicable) are successful, the verifier can conclude that Alice's PII is not present in the sanction list.

The verifier checks the timestamp or other metadata included in the proof package to ensure that the proof is fresh and hasn't expired.

If all the verification steps are successful, the verifier can record the outcome of the verification process and proceed with the transaction or grant access to the requested service.

- Proof Retention and Auditing

  The verifier may store the non-membership proof and the associated verification results for audit purposes and to comply with regulatory requirements.

  The stored proofs can be used to demonstrate the verifier's compliance with sanction screening obligations and to facilitate audits or investigations by relevant authorities.

It is crucial for the verifier to use the same version of the sanction list and the same cryptographic primitives and algorithms as those used by Alice during the proof generation process. Any discrepancies or inconsistencies could lead to verification failures or false positives.

9.2.3. Issuance Procedure Example 2

- Proofs for Compliance with Counterparty's Transaction Rules

  In the context of the accountable wallet framework, crypto asset holders may need to prove their compliance with the transaction rules defined by their counterparties or the platforms they wish to use. For example, certain DeFi platforms may only be accessible to qualified investors due to the securities laws they adhere to. In such cases, users must demonstrate that they meet the specified criteria.

  To address this requirement, the proposed framework suggests that credential issuers should not directly issue credentials attesting to a user's eligibility for specific transactions or platforms. Instead, similar to the non-membership proof for sanction lists, crypto asset users should receive credentials from issuers that pertain to their personally identifiable information (PII) and other relevant attributes. Users can then combine these credentials to generate proofs

demonstrating their compliance with the transaction rules set by their counterparties.

One of the challenges in proving compliance is the uncertainty of transaction conditions at the time of credential issuance. For instance, if a counterparty requires Alice to prove her residence in a country registered on a specific whitelist, a simple solution would be for the credential issuer to provide Alice with a credential confirming that fact. However, whitelists may vary among different counterparties, and service providers may have different definitions. Moreover, actual transaction conditions can be more complex and depend on various service providers. Therefore, instead of having credential issuers directly attest to Alice's residence on a specific whitelist, Alice should use her location-related credentials to prove that she resides in a particular region or country that aligns with the whitelist defined by her counterparty. This approach allows Alice to demonstrate compliance without revealing her exact location, preserving her privacy.

Range proofs, particularly Bulletproofs, can be employed to generate such proofs. Bulletproofs enable the issuance of proofs based on any threshold determined after receiving the credentials (commitment data) and prove compliance with specified conditions through a privacy-preserving proof mechanism.

Bulletproofs are a special type of range proof within zero-knowledge proof technology that allows proving that a specific number falls within a certain range without revealing the number itself. This technology enables various proofs while maintaining privacy. For example, it can be used for:

> Age Verification: Proving that Alice is above a certain age without disclosing her date of birth.
>
> Financial Solvency: Proving that Alice's account balance exceeds a specific threshold without revealing the actual balance.
>
> Transaction Volume: Proving that Alice's transaction history surpasses a specified amount without disclosing transaction details.
>
> Location Verification: Proving that Alice's address falls within a designated area without revealing her exact location.

To achieve this, the credential issuer first creates a Pedersen commitment of Alice's PII. This commitment does not contain Alice's actual PII, but it provides a mathematical guarantee that the zero-knowledge proof (ZKP) she issues matches her real PII. The commitment should be digitally signed by the credential

issuer.

Alice then generates a ZKP (Bulletproof) using the commitment data, proving that her PII satisfies certain conditions without revealing the actual personal information. The ZKP must be mathematically consistent with the Pedersen commitment to ensure the accuracy of the proof.

- Overview of procedure

The detailed process for generating proofs of compliance with transaction rules using Bulletproofs can be outlined as follows:

- Credential Issuance

Alice obtains credentials from the credential issuer regarding her relevant PII and attributes, such as age, account balance, transaction history, and location.

The credential issuer creates Pedersen commitments for each attribute and digitally signs the commitments.

The credential issuer securely transmits the signed commitments to Alice.

- Counterparty's Transaction Rules

Alice's counterparty or the platform she wishes to use defines the transaction rules and conditions that users must meet.

The transaction rules specify the required thresholds or ranges for various attributes, such as minimum age, account balance, transaction volume, or allowed locations.

- Proof Generation

Alice identifies the relevant credentials and commitments needed to prove compliance with the counterparty's transaction rules.

For each required attribute, Alice generates a Bulletproof using the corresponding commitment data.

The Bulletproof proves that Alice's attribute value falls within the specified range or meets the required threshold without revealing the actual value.

Alice combines the generated Bulletproofs into a comprehensive proof package.

- Proof Verification

  Alice sends the proof package to the counterparty or platform for verification.

  The counterparty verifies the digital signatures on the commitments to ensure their authenticity.

  The counterparty validates each Bulletproof in the package to confirm that Alice's attributes meet the required conditions.

  If all the Bulletproofs are valid, the counterparty concludes that Alice complies with the transaction rules without learning her exact attribute values.

- Transaction Execution

  Upon successful verification of the proof package, the counterparty proceeds with the transaction or grants Alice access to the platform.

  Alice's privacy is maintained throughout the process, as she does not need to disclose her actual PII or attribute values.

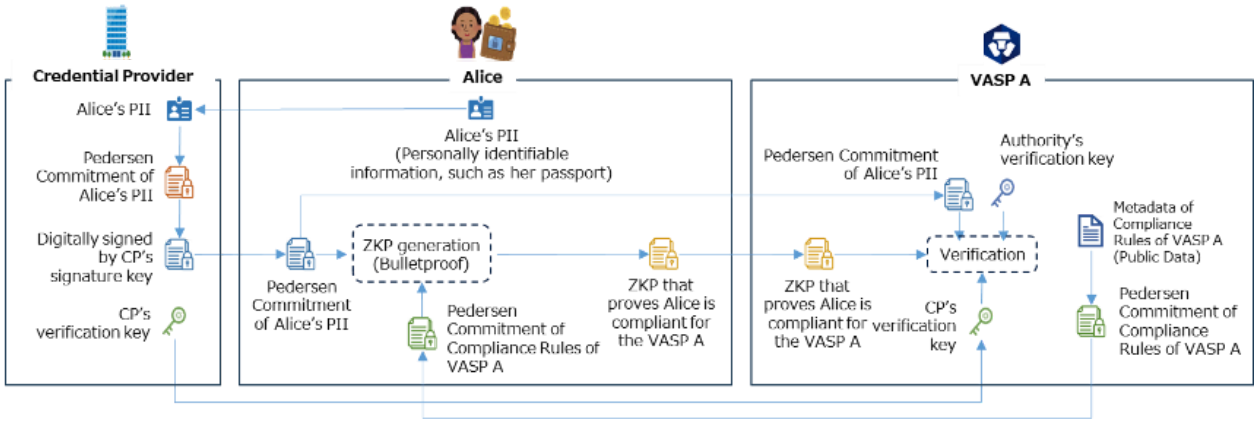


Figure 19

It is important to note that the security and robustness of this proof generation process rely on the proper implementation of the cryptographic primitives and the integrity of the credential issuance process. Furthermore, the proof generation and verification process should be standardized and widely adopted by platforms and counterparties to ensure interoperability and consistent user experience

across the decentralized finance ecosystem.

9.3. Technical Requirements

9.3.1. Technical Requirements for Credentials

While this paper primarily focuses on explaining the concept of accountable wallets and aims to discuss the topic without focusing on specific technologies, it is essential to consider the feasibility of the proposed solution in light of existing credential issuance and verification technologies. Therefore, we will briefly touch upon a few relevant technologies in a limited manner.

The term "credential" in this paper refers to a proof that certifies certain claims about the credential holder (in this context, attribute information about the crypto asset holder). The verifier (i.e., the transaction counterparty) must be able to verify, through some means, that the credential was indeed issued by the credential issuer (i.e., the KYC performer). This aligns with the properties of public key certificates, such as X.509. Additionally, the proofs of legitimacy and other aspects in this paper are strongly focused on self-sovereign self-attestation procedures, where individuals prove their own legitimacy using credentials they hold and manage themselves. This concept shares many principles with the digital identity concept of self-sovereign identity, such as Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs), which have been actively discussed by communities centered around the World Wide Web Consortium (W3C) since around 2014.

Although recommendation documents or candidate recommendation documents related to DIDs and VCs have already been published by W3C, IETF, and ISO/IEC, the experience with their use is insufficient. Moreover, the necessary technologies are not yet fully available across the entire ecosystem for their utilization, and it is not possible to determine which specific standards are most suitable for implementing the particular concept described in this paper. Therefore, while briefly mentioning potentially applicable specific technologies, this section will primarily focus on the technical requirements that are likely to be necessary for implementing the proposed method. It should be noted that these technical requirements heavily draw from the discussions surrounding existing DIDs and VCs.

Based on the discussions so far, the credentials mentioned in this document require the following technical requirements:

- Integrity

  The information held by the VC (i.e., the claims made by the VC) must be

protected by technologies such as digital signatures and safeguarded against data tampering. Verifiers should be able to detect if the VC has been tampered with.

- Authenticity

  The VC must record and enable the verification of the identity of the VC issuer (signer). It is worth noting that the VC guarantees that the issuer has indeed issued the VC and also asserts the claims made in the VC. However, it does not indicate whether the recorded information is true. How the verifier treats the information and the issuer (i.e., whether to accept it as truth) is a separate issue. Therefore, for the verifier to truly trust the claims made in the VC, they need to consider not only the authenticity of the VC but also the nature of the entity issuing the VC and the procedures followed for issuing the VC. In other words, the trustworthiness of the claims in the VC depends on the trustworthiness of the VC issuer. This means that when we measure the trustworthiness of a credential holder based on a VC, we also need to consider the trustworthiness of the VC issuer itself. We will discuss one method for this consideration in the Trust Score section.

- Confidentiality

  The credential holder must have full control over who can access all or part of the information held or claimed by the credential. Additionally, functionality is required to minimize the disclosure of credential information necessary for a proof by using selective disclosure techniques such as BBS signatures or zero-knowledge proof techniques.

- Issuance Time Recording

  Credentials must have their issuance time recorded and it should be unalterable after issuance.

  One reason why the issuance time is important is that credentials cannot be used to retroactively point out the legality or illegality of any transaction. For example, when verifying the legitimacy of a transaction that occurred at time T, the transaction parties' negligence in credential confirmation should not be judged based on credentials issued after time T. Conversely, if a VC existed at time T and the legitimacy of the VC holder could be verified using that VC, the person who transacted with the VC holder based on that VC should be guaranteed that the legitimacy of the transaction will not be questioned later. This is because without such a guarantee, those who properly verified the transaction counterparty and conducted the transaction would always face the risk of

unintentionally receiving guidance such as prosecution from regulatory authorities, making it impossible to transact with peace of mind. Since the essential purpose of this method is to prevent unintentional involvement in fraudulent transactions by verifying the legitimacy of the transaction counterparty prior to the transaction, the legitimacy of the verifier who properly followed such procedures must be guaranteed.

- Recording of Verification History

  The verifier of a VC must be able to keep a record of having verified a particular VC in some form. This is necessary because, as mentioned above, the verifier needs to have evidence that they properly verified the transaction counterparty and judged them to be legitimate in order to prevent unintentional involvement in fraudulent transactions. To achieve this, the verifier must be able to store a copy of the transaction counterparty's VC in their own managed storage for a certain period. Although this is a copy, the authenticity and integrity of the VC are ensured as it is digitally signed. As will be discussed later, the verifier will use this data to prove to the next transaction counterparty that they have been acting legitimately by verifying the legitimacy of the transaction counterparty prior to the transaction.

- Revocability by VC Holder

  The holder of the VC shall have the authority to delete the held VC at any time, solely by the holder's authority. This policy is based on the need for VC holders to be able to discard VCs that were sent to them against their will.

  In other words, this means that, in principle, VCs cannot be issued in a way that would disadvantage the holder by possessing them. For example, this includes VCs showing that the VC holder has committed a crime in the past. Since such VCs would be discarded by the holder even if issued, we will not consider issuing them. Of course, it is possible to design VCs in a way that prevents them from being discarded, but in that case, there is a concern that innocent VC managers may be sent dishonorable VCs. Additionally, even if the holder was not innocent, they could effectively discard the dishonorable VC by ceasing to use the wallet to which it was sent and using a different wallet instead, rendering the approach ineffective. Furthermore, this aligns with the "right to be forgotten" stipulated by the GDPR. From this perspective, credentials issued using technologies or standards that cannot be discarded even by the holder should not be recognized as credentials, and verifiers should not use them to verify the legitimacy of transaction counterparties.

- Revocability by Issuer and Prevention of Denial of Past Proofs

The credential issuer must be able to revoke previously issued credentials in case of errors or changes in the holder's circumstances. However, it should be noted that this revocation only means that the revoked credential can no longer be used for legitimacy judgments from the time of revocation onwards; it does not negate the fact that the credential was issued in the past. In other words, a transaction that was deemed legitimate based on a previously issued credential should not have its legitimacy denied due to the subsequent revocation of the credential. This is because transactions that were once deemed legitimate must be verifiable retroactively, no matter how much time has passed. Furthermore, this means that VC issuers are responsible for the accuracy of the information at the time of issuance. If an issuer could revoke a VC that erroneously led to a transaction being judged as legitimate when it was not, the issuer would bear no responsibility for the VCs they issue.

When invalidating a VC after issuance, it is necessary to address the "Phone Home" problem. If the verifier inquires the issuer about the validity of a certificate along with information that can identify the subject of the certificate, and the issuer can identify the inquirer, it may lead to a privacy violation as the issuer becomes aware of who received whose certificate. To mitigate this, techniques such as Bitstring Status List v1.0 (BSL) should be used.

- Non-Transferability

  Credentials are not assumed to be transferred to others after issuance. Therefore, credentials are premised on the fact that only the subject of the message holds them. In VCs, use cases are envisioned where the subject of the message and the actual holder may not be the same, but in this method, such use cases are not currently considered as there are no apparent beneficial applications. Therefore, credentials not held by the subject of the message are invalid.

- Availability

  Credentials must be accessible at all times. No one should be able to interfere with third-party access to credentials.

- Inheritance

  Credentials must be able to issue other credentials. In other words, credentials should also be usable as signing keys. As mentioned earlier, the credibility of credentials depends on the credentials held by the issuer, so this function is necessary. Moreover, in the legitimacy of crypto asset provenance introduced in this paper, to prove this legitimacy, it is necessary to demonstrate that the

currently held crypto assets were acquired legitimately. To generate this proof, it is necessary to receive similar VCs from the transaction counterparty at the time of receiving the crypto assets and use that proof to generate a VC proving one's own legitimacy. The newly generated VCs using VCs should also include information about the issuers of the referenced VCs, and the credibility of these issuers should be traceable. The inheritance relationship is not necessarily one-to-one, and the generation of one new credential from the data of two or more credentials is also conceivable. For example, issuing "The holder of this credential has more than $1M in financial assets across multiple banks" requires generation from credentials issued by multiple banks.

- Other Requirements

  - Permission for Multiple VC Issuers to Issue VCs with the Same Claim

    There is a question of whether the same claim should be allowed to be issued multiple times. There are arguments both for and against this. For example, according to "E. Glen Weyl, Puja Ohlhaver, Vitalik Buterin. Decentralized Society: Finding Web3's Soul, SSRN, 2022", Soulbound Tokens (SBTs), which have roughly the same functionality as the credentials in this paper, are assumed to serve as collateral for lending transactions. Therefore, they are generally not expected to be generated multiple times. Here, SBTs are envisioned to represent things like educational background. In other words, SBTs are a kind of granting of trust, and based on the proof of social trust such as educational background, the lender can trust the holder to a certain extent and lend funds accordingly. However, if these SBTs can be issued by the issuer to multiple wallets without limit, it effectively allows unlimited borrowing using those SBTs. Therefore, their paper suggests that, in principle, there should be only one issuance of an SBT for a single claim. For example, in the case of educational background, it should be guaranteed by the school, and the school should issue it only once. A drawback of this approach is that it becomes difficult for the same person to use multiple accountable wallets. It may also increase the verifier's reliance on the VC issuer for trust. As mentioned earlier, the credibility of a VC heavily depends on the credibility of its issuer. In this case, if the same fact is issued by multiple VC issuers, the credibility of that VC increases. This is also beneficial from the holder's perspective, as it prevents dependence on a single VC issuer and is highly desirable for ensuring self-sovereignty. Since this paper prioritizes the self-sovereign nature of self-attestation of one's own legitimacy, we allow multiple issuers to issue the same claim in order to

prioritize this aspect. Based on this premise, we also propose a calculation formula for the trust score discussed later.

- Credential Claims Should Be Independent Data

  The W3C's VC data model is primarily expressed in JSON-LD (a format for describing Linked Data[32] in JSON[33]), but this method recommends against using LD for VCs due to the importance of reproducibility of claims. When using LD, there is a risk that the data in a separate data registry referenced by the VC may change after the verification, making it impossible to reproduce the judgment made at the time of the transaction. It may seem that this issue can be resolved if the referenced data is digitally signed in the form of credentials, but this would introduce additional difficulties such as considering the credibility of the issuers of those credentials. Another approach could be to record the actual data instead of LD when storing a copy of the VC presented by the transaction counterparty in the past. However, this would still require a new signature procedure to ensure the correctness of the data, and since the VC issuer cannot be inquired about it due to privacy concerns, a signature by the current VC holder or the verifier would not fully guarantee authenticity. Therefore, the VCs handled in this paper should not be issued in a form that depends on other VCs or on-chain data in a way that lacks reproducibility.

- Not Focused on Specific Blockchains

  The proposed framework is designed to be blockchain-agnostic, operating at a system layer separate from the underlying blockchain infrastructure. This approach ensures broad applicability enabling the seamless integration of the Accountable Economy paradigm across diverse wallets and blockchains. By focusing on off-chain solutions and leveraging cryptographic proofs, the framework minimizes the need for direct modifications to existing blockchain architectures or token standards.

  Credential management is expected to be performed at a system layer separate from the blockchain used for financial transactions. By design, this system negates the need for direct enforcement in determining transaction permissions, as legitimate investors face the potential consequence of a reduced Trust Score when transacting with parties

---

32

33

whose legitimacy has not been verified.

Existing research often presupposes the existence of smart contracts or requires changes to token standards, but this paper does not propose solutions that necessitate modifications to existing public blockchains or token standard specifications.

Therefore, changes to the structure of the blockchain main layer are not proposed. The problem is solved in the off-chain layer.

We aim to design a protocol that can be used on any blockchain. Thus, it is not intended as a blockchain-native implementation. In other words, the blockchain used to execute Crypto Asset transactions and issue credentials can be different. Consequently, the results of compliance checks performed by this protocol do not have technical enforceability. Therefore, it is crucial to design disincentives for non-compliance with the results.

Standardizing the credential issuance specifications is crucial for the widespread adoption of credentials. Non-standardized credentials may not be verifiable, potentially preventing them from being trusted as intended. Moreover, standardization is essential for decentralizing credential issuance authority. If credential issuance specifications are not standardized, DeFi providers may find that only credentials issued by specific issuers are effectively valid in the market, potentially leading to a concentration of issuance authority and a threat to the rights of credential holders. Therefore, it is crucial that the technical specifications for issuance are unified. The credibility of credentials depends on the credibility of the issuer, so the credentials issued must be digitally signed along with the issuer's own credentials.

9.3.2. Technical Requirements for Credential Presentations

The requirements described in the previous subsection primarily pertain to the technical and issuance procedures for the credentials themselves, as outlined in the "Obtaining PII-related Credentials" step of the "Procedure" section. The next step is to define the requirements for the procedures that utilize these credentials. However, it is challenging to discuss these requirements in a general sense, as was done for the credentials themselves. For instance, this chapter introduces the proof of non-inclusion in a sanctions list as one of the proofs for demonstrating the legitimacy of wallet holders. The steps and techniques used for this proof are specific to this particular proof and the required oracle data. The previous chapter presented several proofs that are effective in demonstrating the legitimacy of wallet holders, but the issuance procedures for each proof must be specific to the purpose of the proof and the oracle data required for

issuance. Consequently, this subsection focuses on the general principles for designing procedures rather than the technical requirements for specific procedures.

■ Minimal Disclosure

Proving process must be minimized the disclosure of personal information when presenting their VCs. Minimal disclosure of personal information by the prover when presenting a proof. To achieve this, both technical and operational requirements must be met.

 Technical Requirement

When a prover self-attests their legitimacy, the following three principles of zero-knowledge proofs must be achieved:

- Completeness

If the prover's proposition is true, the verifier will always be able to confirm its truthfulness.

- Soundness

If the prover's proposition is false, the verifier can detect its falsehood.

- Zero-knowledge

If the prover's proposition is true, the verifier cannot obtain any knowledge other than the fact that the proposition is true, even if they attempt to dishonestly steal knowledge from the prover.

The first requirement above is a general principle of zero-knowledge proofs and is not a specific point of emphasis for this method, so it will not be discussed in detail. The requirement that this method particularly emphasizes, regarding the disclosure of personal information, is the following:

 Operational Requirement

When requesting a proof from the prover, the verifier should not demand a proof that unnecessarily identifies the prover. Additionally, when presenting a proof, the prover should be notified of sufficient warnings before the presentation to anticipate the risks associated with presenting that proof. These guidelines should be established.

- Risk of issuing ZKPs equivalent to proof of membership in a narrow set

  As mentioned earlier, when conducting transactions using credentials, the content of the credentials is not directly disclosed to the counterparty. Instead, techniques like ZKPs are used to disclose only the information of whether the prover meets the conditions required by the counterparty. However, it should be noted that even if the claims held by the credentials are highly encrypted and the proofs issued using them maintain zero-knowledge, zero-knowledge proofs regarding the attributes of crypto asset holders ultimately prove that the crypto asset holder belongs to a certain set. For example, if a verifier requests proof that the prover's country of residence is one of the whitelisted countries designated by the FATF, it can be considered a zero-knowledge proof if it can be proven without disclosing the prover's actual address. However, this ultimately discloses that the prover belongs to the set of whitelisted countries defined by the FATF. What if the transaction counterparty proves residence in a specific country? Furthermore, what if they request proof of residence in a particular U.S. state? In the United States, laws vary by state, and such verification may be necessary to fully comply with the law. However, this proof is still a zero-knowledge proof in a broad sense. Nonetheless, it is evident that the narrower the range, the higher the risk of identifying the prover. Therefore, it cannot be assumed that privacy is always protected as long as a zero-knowledge proof is used. Information that does not directly identify an individual but indicates that the individual belongs to a certain set will be defined as quasi-personal information for now. The parties to whom this quasi-personal information is disclosed are not limited to the verifier. For example, if a DApps publicly states that it can only be used by residents of a specific state and requires users to prove this fact when using it, the fact that a user resides in that particular state becomes apparent once the usage is revealed in on-chain data.

  While a single piece of quasi-personal information cannot identify an individual, the accumulation and combination of various pieces of quasi-personal information can lead to the identification of an individual. This phenomenon is known as re-identification. As mentioned earlier, issuing a zero-knowledge proof necessarily

leads to the disclosure of information that the issuer belongs to a specific set, regardless of how sophisticatedly the ZKP protocol is designed. Moreover, if quasi-personal information is repeatedly revealed in this manner, it becomes apparent that the individual belongs to the intersection of multiple quasi-personal information sets, allowing for the inference of belonging to a narrower set. In other words, the methodology presented in this paper encourages investors to hold various credentials to prove their legitimacy, but there is a dilemma that the more credentials an investor holds, the higher the risk of the investor being identified.

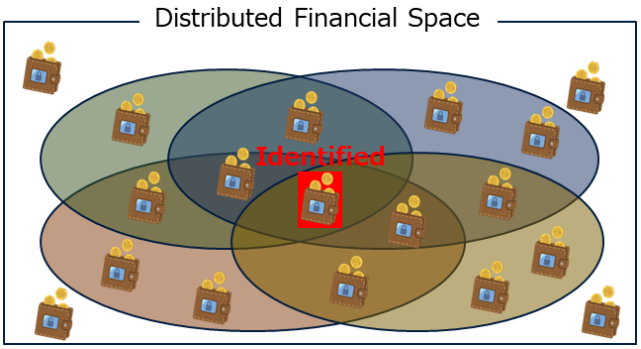


Figure 20

Realistically, it cannot be expected that all individuals can properly assess such risks on their own. Therefore, the industry needs to establish appropriate guidelines to ensure that verifiers do not unnecessarily demand proofs that could identify individuals during the process of issuing proofs for compliance checks using credentials. To mitigate these risks, the prover should not readily comply even if the verifier requests proof of belonging to a very narrow set. However, it is difficult to set clear criteria for this, and not all crypto asset users have high literacy regarding privacy risks. Therefore, it is necessary to implement appropriate interfaces and functionalities that display warning messages when the prover is requested to issue proofs, enabling users to understand and properly assess the risks. Verifiers should be guided not to request proofs that unnecessarily identify the prover when requesting proof issuance. Additionally, it is desirable to establish guidelines that require sufficient warnings to be provided to the prover before presenting a proof, allowing them to anticipate the risks associated with the proof presentation.

- Utilization of Unlinkability Techniques

  There is also a possibility of inferring relationships based on the same issuer of VCs. For example, if a single issuer issues a VC indicating that the holder is employed by Company A, it is easily inferred that everyone employed by the same company has a VC using the same public key. From that inference, it is easily inferred that the holder of that VC is employed by that company.

  This issue has already been discussed, and for example, OpenID's OpenID4VP allows for the issuance of certificates containing the same claims but different public keys (essentially copies of the certificate) to prevent users who have presented the same VC to multiple verifiers from being tracked. While the use of HD wallets[34] and other techniques can mitigate such privacy risks to a certain extent, they cannot be completely eliminated. To significantly reduce this risk, the only option is to perform mixing using techniques like CoinJoin. However, in that case, there is a possibility that money laundering perpetrators are included among the mixing counterparties, leading to the dilemma of not being able to achieve the original purpose of avoiding transactions with such individuals. Therefore, this paper recommends the use of privacy pools, as proposed in the paper "Blockchain Privacy and Regulatory Compliance: Towards a Practical Equilibrium, SSRN, 2023" by Vitalik Buterin, Jacob Illum, Matthias Nadler, Fabian Schar, and Ameen Soleimani, which suggests mixing with specific parties only. This idea allows for the legal use of mixing protocols. It enables legitimate users to mix their crypto assets separately from those associated with users on sanction lists or malicious users. Legitimate user addresses that reacquire crypto assets after mixing only with legitimate users and designated sources can receive membership proofs as evidence of that. However, their paper identified the challenge of how to distinguish between legitimate and illegitimate users. By using the self-attestation of legitimacy proposed in this paper, wallets that can prove their legitimacy using the same criteria can mix crypto assets with each other, achieving very high privacy.

■ Securing Mechanism

34

In addition to minimizing the disclosure of personal information, it is crucial to ensure the security and reliability of the credential presentation process. This involves providing robust mechanisms for both the prover to generate proofs and the verifier to validate them. The following key requirements should be met:

- User-friendly Proof Generation

  The process of generating proofs for credentials must be straightforward for the user, with minimal technical overhead. This involves leveraging advanced cryptographic primitives, such as zero-knowledge proofs (ZKP), to ensure that credential holders can efficiently and securely generate proofs without exposing unnecessary data. Tools and interfaces must be designed to abstract the underlying complexity, allowing non-technical users to perform the verification with ease.

- Cryptographic Soundness and Verifiability

  The verifier must have access to a reliable and cryptographically secure mechanism for validating the proofs presented by the prover. This typically involves the use of a standardized software stack that incorporates the necessary cryptographic primitives, algorithms, and protocols. The software used for proof validation should be open-source, extensively audited, and subject to rigorous verification to ensure its correctness, security, and absence of vulnerabilities. The verification process should be computationally efficient and able to handle a high volume of proof validations.

- Selective Disclosure Techniques

  To enhance privacy and minimize information leakage, the credential presentation framework should support selective disclosure techniques. The World Wide Web Consortium (W3C) has proposed two notable approaches: Verifiable Credentials Data Integrity (VC-DI) and Securing Verifiable Credentials using JOSE and COSE (VC-JOSE-COSE). VC-DI leverages the BBS Cryptosuite v2023, which utilizes BBS signatures, a zero-knowledge proof-based protocol that enables selective disclosure. Similarly, VC-JOSE-COSE introduces the Selective Disclosure JSON Web Token (SD-JWT), a JWT-based method that supports selective disclosure. These techniques allow provers to reveal only the minimal set of attributes necessary for a specific verification context, reducing the risk of unnecessary personal information exposure.

- Oracle Data Integrity

  In scenarios where the proof generation process relies on external data sources or oracles, it is imperative to ensure the authenticity, integrity, and completeness of the oracle data. Oracle services used for credential validation must be tamper-resistant, providing guarantees that the data has not been manipulated. This includes cryptographic attestation of the data source, ensuring that any third-party inputs into the verification process are reliable and auditable. Mechanisms should be in place to detect and prevent tampering, forgery, or manipulation of the oracle data.

- Optimized Proof Size and Efficiency

  The size of the proofs generated by the prover should be optimized to ensure practical usability and scalability. Excessively large proofs can lead to increased storage requirements, network overhead, and computational burden during the verification process. Techniques such as proof aggregation, compression, or the use of succinct non-interactive arguments of knowledge (SNARKs) can be employed to reduce the size of the proofs without compromising their security or integrity. The proof size should be reasonable and manageable, considering the limitations of the underlying blockchain or distributed ledger technology. While cryptographic operations are computationally intensive, ensuring that proofs remain within a reasonable size limit is essential for practical adoption.

- Interoperability

  The credential presentation framework should prioritize interoperability to facilitate widespread adoption and seamless integration with existing systems and protocols. This involves adhering to established standards, such as those proposed by the W3C, and ensuring compatibility with popular blockchain platforms, wallets, and decentralized applications (DApps). Interoperability enables credential portability, allowing provers to use their credentials across different domains and contexts without the need for re-issuance or redundant verification processes. It also promotes collaboration and synergy among various stakeholders in the decentralized finance ecosystem, fostering innovation and reducing fragmentation. Given that credential presentation processes often span multiple jurisdictions, the security mechanisms in place must align with various standards and be adaptable to local requirements. By adopting

widely accepted protocols such as VC-DI and VC-JOSE-COSE, and adhering to the principles of Self-Sovereign Identity (SSI), the system can ensure that verifiable credentials are recognized and accepted across borders, facilitating seamless global interaction.

9.4. Trust Score of Wallet Holders

9.4.1. Concept

The Trust Score of Wallet Holders refers to the probability that the wallet holder is a reliable manager, and this is defined as the complement of the probability that the wallet holder is a fraudulent person. To prove that a wallet holder is a legitimate person, attribution credentials will be used. In other words, the trust score of a wallet holder basically depends on the extent to which valid attribution credentials are held to prove one's legitimacy. That is, theoretically, holding more credentials increases trust score.

9.4.2. Basic Formula

- Basic Formula

  The possession of attribution credentials can also be said to be proof that the holder belongs to a certain set. For example, possessing a credential proving residence in the United States means proving that one belongs to the set consisting of U.S. residents. And when multiple attribution credentials are held, the set to which one belongs becomes the intersection and a more selective set. The fewer people belonging to the set, the lower the probability that the set includes antisocial forces or other people with whom transactions should not be conducted. For example, assuming a world population of 8 billion and 800,000 sanctioned individuals, the probability of a randomly selected person being a sanctioned individual is 0.01%. If 2 people are randomly selected, the probability of either being a sanctioned individual is approximately $1-(1-0.0001)^2 \approx 0.02\%$. For 10 people, it is approximately $1-(1-0.0001)^{10} \approx 0.18\%$, for 100 people, it is approximately 1%, and for 1,000 people, it is approximately 9.52%. In other words, if there is an arbitrary set consisting of a specific number of people, and the number of people belonging to that set is n, the probability of at least one sanctioned individual being in that set is $1-(1-0.0001)^n$. Generalizing this, let $n(A_1 \cap A_2 \cap \cdots \cap A_k)$ be the estimated number of people holding all attribution credentials $A_1 \; to \; A_k$, and let $P(A_{Criminals})$ be the probability of any Wallet Holder being a sanctioned individual. Then, $P(w_1)$

can be expressed as follows:

$$P\left(w_1\right) = (1 - P(A_{Criminals}))^{n(A_1 \cap A_2 \cap \cdots \cap A_k)}$$

If PII can uniquely identify a person by name, address, and date of birth, then by using the sanction determination function, it can be confirmed with 100% probability that the identified person is not antisocial. However, when the theoretical number of people can only be narrowed down to 10, not all 10 people must not be antisocial, and the probability of any one of the 10 people being antisocial is higher than when the target is one person. For example, when calculated based solely on nationality and date of birth, a rough calculation shows that if a Wallet Holder holds attribution credentials for country of residence and date of birth, it is narrowed down to approximately $8\ Bilion\ people \times \left(\frac{1}{190}\right) \times \left(\frac{1}{365 \times 80}\right) \approx 1,441$ people, and the probability of them being sanctioned is 13.42%, $P\left(w_1\right) = 86.58\%$, indicating that this information is insufficient.

Since this calculation formula assumes that the probability of a Wallet Holder not being a sanctioned individual increases with the comprehensiveness of attribution credentials, holding more attribution credentials leads to proving that one is not a sanctioned individual. In other words, the more attribution credentials held, the higher the trust score.

- Consider Dependent events

  When calculating this probability, the independence of each event must be considered. For example, a credential proving New York residence is part of a credential proving U.S. residence, so if the former is already held, additionally holding the latter does not lead to further narrowing of the group and thus does not have the effect of further increasing one's trust score.

- Not Consider Credentials that Lower the Trust Score

  Credentials are basically intended to have only positive factors. Also, credentials that lower credibility by possessing them are basically not considered. This is for the same reason as explained in “Revocability by VC Holder” under Requirements in Credentials.

  Criminals are unlikely to hold proof information that leads to conviction. For example, people are unlikely to actively try to obtain attribution credentials

proving residence in a jurisdiction recognized by FATF.

9.4.3. Credential Issuer’s Trust Score

- Concept

  The credibility of a credential issuer is not necessarily complete for everyone else. For example, credentials showing the results of KYC performed by an unreliable KYC Performer are not accepted by everyone. Believing the information in a credential and transacting with each other means believing the issuer of that credential.

  In other words, the reliability of a credential's claim depends on the trust score of the issuer. That is, the trust score should be adjusted so that credentials received from low-trust-score credential issuers depend on the degree of credibility.

- Proposed Fixed Formula

  If the issuer of attribution credential is not 100% reliable, the calculation formula for $P\left(w_1\right)$ is converted and defined as follows by the trust score a_i of credential issuer i, the issuer of credential A_i.

$$P(Ho) = (1 - P(A_{Criminals}))^{n\left(A_1 \cap A_2 \cap \cdots \cap A_k\right) + \sum_i^k \frac{1}{a_i}}$$

  If the owner possesses verification credentials of the same proof from multiple issuers, considering the above-mentioned complement events, under the assumption that the reliability of credentials is basically close to 100%, the highest reliability level among these issuers can be used for each a_i as a conservative approximate calculation.

- Responsibility

  If credential issuers bear no responsibility for the credentials they issue, there is little incentive to maintain the accuracy of the content of the credentials. Therefore, it is essential for credential issuers to bear a certain level of responsibility for the information guaranteed by the credentials they issue in order to maintain the reliability of the credentials. For example, if there is a deficiency in a credential issued by a credential issuer, resulting in some unforeseen situation and loss, there must be a mechanism in place for the credential issuer to be held legally liable or for the credential issuer's own trust score to be lowered.

However, in that case, since credential issuers bear risks, they also need to receive appropriate returns. To this end, a mechanism is needed where credential issuers receive issuance fees when issuing credentials, or a portion of transaction fees is returned to credential issuers when a financial transaction occurs using the issued credentials.

- Increasing Holder's Trust Score by Possessing Multiple Credentials Issued by Multiple Credentials Issuers

  The more credentials you have, the higher your credibility becomes. However, it should be noted that this has two meanings. As mentioned above, the trust score of a wallet holder is calculated by two factors: "the investor's credibility estimated from the information held by the credentials" and "the credibility of the credential issuer." For example, if a wallet holds not only a credential proving the date of birth but also a credential proving the current address, the former numerical value of the two factors constituting the trust score of the wallet holder is interpreted as increasing. This has been discussed in the previous sections.

  Next, let's consider how possessing two or more credentials that prove exactly the same content affects the trust score of the wallet holder. Possessing two or more credentials that prove exactly the same content is not a meaningless act. This is because credentials are not necessarily 100% credible, so under the assumption that the probabilities of each being false proof of information are independent events, the probability of all of them being found to be false proof of information is very low, as it can only occur if all of those credentials are falsely proving false information. This can be interpreted as an increase in the latter numerical value of the two factors constituting the trust score of the wallet holder.

9.4.4. VASP's Trust Score

- VASP credentials are not intended to identify the holder

  Usually, regulation-compliant VASPs are not operated anonymously, so there is no risk arising from the anonymity of the operating company. In this method, these VASPs are required to have attribution credentials representing their license status within their jurisdiction. However, depending on the jurisdiction, jurisdiction itself may not ratify with the AML/CFT guidelines set by FATF and others, so having this license alone does not necessarily mean that the VASP's trust score as wallet holder can be considered 100%. This is debatable as to how different calculations should be given.

- Trust Score Disclosure

Unlike non-custodial wallets, their credential and trust score should be made public on-chain. In that case, if a VASP's trust score is lowered, users will know that the VASP has a high risk of fines or business suspension due to abetting money laundering, etc., motivating users to avoid using that VASP. This may pose a business risk for VASPs, incentivizing them to optimize their risk preference (appropriately adjust their risk appetite).

9.4.5. DApps Trust Score

- DApps has no concept of holders

  This method attempts to solve unfair transactions conducted on blockchain not by legally resolving them, but by designing the system so that each address has an incentive not to engage in or become involved in fraudulent transactions. In this case, for legitimate users who intend to act legally to use DeFi without being involved in crimes such as money laundering, they have no choice but to use DeFi that does not involve any illegal users at all. However, at present, users are not given such options. Therefore, to achieve this, DeFi must be designed so that only those with certain credentials can participate in transactions, and law-abiding VAPSs and bona fide investors must use only this exclusive DeFi to avoid involvement in fraudulent transactions.

  The concept of VASP's trust score and the mechanism that incentivizes VASPs to maintain a high trust score can be similarly considered for DeFi. Strictly speaking, for DeFi, the trust score will be set for the smart contract address, and if that address accepts transactions or liquidity for the liquidity pool from non-accountable wallets or low-trust score wallets, the trust score will decrease. From the perspective of DeFi users, using DeFi with a low trust score will lower their own trust score, so an incentive is expected to work to avoid using such DeFi.

- DeFi's Compliance with Securities Laws and Other Regulations

  The U.S. SEC has stated that DeFi must comply with regulations such as anti-money laundering measures and securities laws in the same way as physically existing VASPs, and is not exempt from application. In fact, in the U.S., DeFi developers have been successively prosecuted for securities law violations. When considering this issue, if DeFi is considered to be accessible by residents of any jurisdiction and must therefore comply with the securities laws or similar laws of all jurisdictions, it is obviously impossible. Therefore, DeFi should declare in the form of credentials which jurisdiction's securities laws it intends to comply with. Then, it should be controlled so that only investors who can prove through

credentials that they reside in the jurisdiction declared to be in compliance can access it. Today, most DeFi interfaces are managed on the regular WWW, so many DeFi restrict users based on their country of residence estimated from the accessor's IP address, but this is a usage restriction that can be easily bypassed using a VPN and is not considered effective. Therefore, strictly speaking, usage should be restricted on-chain using credentials, and DeFi that does not do so should be considered as having no intention of complying with the securities laws of each country, and their trust score should be lowered. In other words, when calculating the trust score of a DeFi contract address, in addition to the decrease in trust score due to accepting funds from non-custodial wallets or low-trust score wallets, which is done for regular self-custody wallets, the implementation or non-implementation of appropriate user restrictions using credentials should also affect its trust score.

There are debates among various regulatory authorities about which jurisdiction's regulations DeFi should comply with, but if these issues are to be strictly addressed, the above approach would be taken. This would also lead to protecting the creators of DeFi code themselves, preventing the arrest of Tornado Cash's creators as seen in the previous chapter.

- Obtaining Some Kind of Formal Certification from External Parties

  When complying with securities laws, it is desirable to obtain certification from an external certification body as to which country's securities laws are being complied with. It is also conceivable to obtain credentials certifying that there are no vulnerabilities in the source code. Possessing credentials showing these certifications should be designed to improve the trust score of DeFi.

  To promote this method, standardization of credential specifications as participation qualifications for DeFi, standardization of contract code specifications for verifying such credentials in transactions on DeFi, and procedures for external certification bodies to certify DeFi built in accordance with such standard specifications need to be established through standard guidelines.

9.5. Further Considerations

9.5.1. Incentive Design

- Incentive is Key

  Having a trusted institution perform KYC on wallet holders and issuing credentials or other indications of KYC verification to the wallet is common

proposal for achieving compliant decentralized finance. However, many of these proposals either lack or completely fail to consider the incentive design for issuing and holding credentials. Even the most perfect transaction verification system is meaningless if it is not used. It is crucial to provide economic incentives for legitimate users to make efforts to avoid transacting with criminals, rather than merely appealing to their moral sense. Credential issuers must have economic incentives to issue credentials to others. If issuers cannot sustain their issuance business, the economic model that relies on them will never be sustainable.

- Incentives for Credential Issuers

  An important point that has not been much discussed in previous research but is crucial for the widespread adoption of safe transactions through credentials is the discussion of incentives. This is divided into the incentive to issue credentials and the incentive to hold credentials. This section discusses the need for incentives on the issuer side.

  Fundamentally, for the credibility of credentials themselves to be high, it is important that issuers take responsibility for their content. While there is room for discussion on what responsibilities to bear, for example, if an unintended transaction occurs due to incorrect credential information and a loss is incurred, the issuer may be considered responsible. However, if there is no return for issuing credentials, it is hardly conceivable to take on risk. Credentials issued without any risk borne by the issuer will not gain trust. The government sector may be an exceptional entity that does not necessarily seek direct financial return for issuing credentials, but the scenario of governments around the world distributing credentials of the same standard to all of humanity in unison is too unrealistic, so here, the private sector is assumed to be the issuer of credentials. Therefore, how the issuance of credentials becomes a business is one important perspective. As will be discussed later, the credibility of any credential depends on the credibility of the credential issuer, which is a very important role expected to motivate all participants in the Accountable Economy to act with integrity through the Trust Score mechanism. The system's credibility cannot be maintained without economic incentives for credential issuers, who give credibility to the system. This is the same reason Bitcoin was able to become an autonomous system.

  A simple method of securing financial incentives is a model where the person who will hold the credential pays the credential issuer an issuance fee at the time of credential issuance, but since it is not common in existing finance for customers to pay account opening fees to financial institutions during the onboarding process, this method is unlikely to lead to widespread adoption of

credentials. Therefore, it is desirable for the issuance of credentials itself to be free. In that case, a model that aligns with existing finance would be for the credential issuer to receive a portion of the transactions that utilize the credentials. In this case, credential holders and DeFi platformers would need to pay fees to the credential issuer for all transactions that utilize the credentials, but not only Crypto Asset issuers but also stablecoin issuers, security token issuers, DeFi vendors, etc. can safely circulate tokens by utilizing the credit information of credential issuers, so it would be sufficiently justified to pay a portion of the transaction fees[35] to the credential issuer in return for providing this function. This can be said to have replaced the function of hedging credit risk between investors and investees, which has been played by existing financial institutions, with credentials. Indeed, credential issuers are expected to play the role of intermediating the "credit information" of various participants in this economy by issuing various credentials to them. Since KYC generally needs to be updated regularly, credentials are expected to be treated similarly, so it also makes sense to collect ongoing credential reference fees. To reliably receive compensation for referencing credentials in transactions that utilize credentials, credentials need to be designed with a high degree of sophistication. A mechanism is needed where a certain amount of gas fee[36] is always incurred when referencing and all of it is pooled into a wallet managed by the credential issuer, not the validator.

35

36

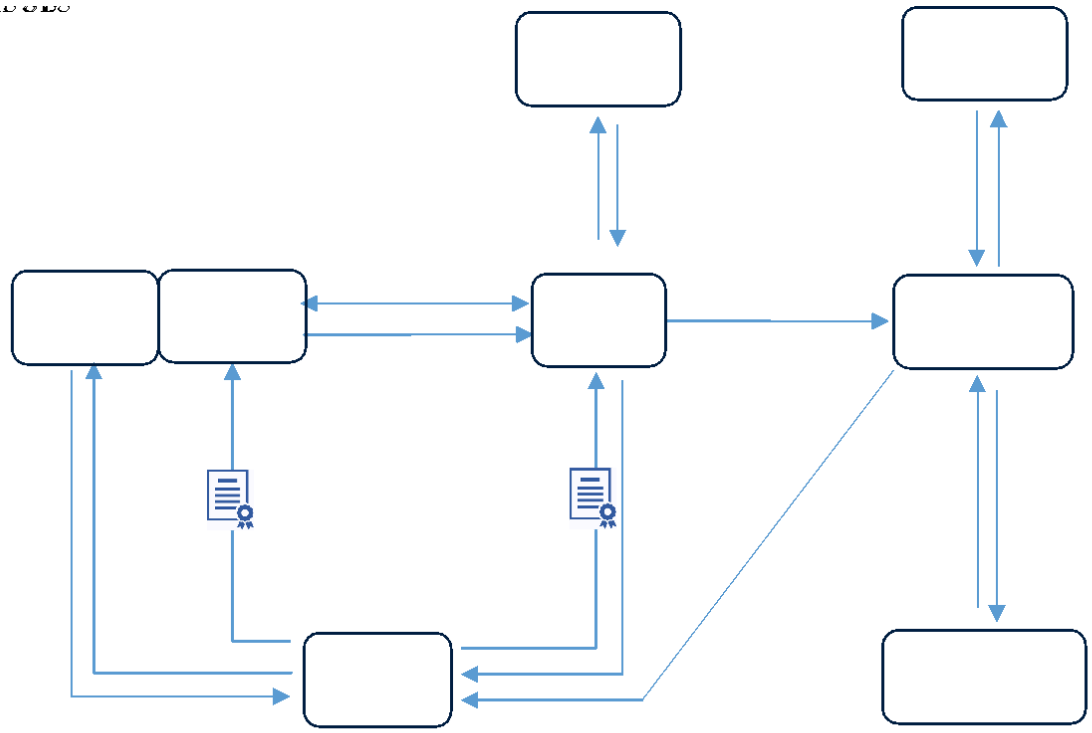


Figure 21

This kind of mechanism can be justified as a reasonable business expense because it enhances compliance in all kinds of decentralized finance, including DeFi. Also, if the issuance of attribution credentials becomes a profitable business, the barriers to entry for issuance will be lowered, leading to diversification of issuers and improved sustainability of the framework. However, each issuer inherently has varying levels of trust, which affects the credibility of the credentials they issue, so further in-depth discussion is needed on how this will work to create a natural motivation for issuers to adhere to honest practices.

- Fee Collection Scheme for Reference

- Incentives for Credential Holders

  For the methodology to become widespread, there also need to be incentives on the credential holder side. The goal of the methodology proposed in this paper is to make the value of crypto assets managed in wallets that hold credentials relatively higher than that of crypto assets managed in wallets that do not. In addition to the increase in the relative market value of currently held crypto assets, by credentializing various credit information one possesses, it is expected

that one will be able to conduct financial transactions on more favorable terms. This is expected to become an incentive for holding credentials.

The concept of Trust Scores described in Chapter 4 motivates VASPs to maintain high Trust Scores. As a result, VASPs are expected to be motivated not to welcome transactions with wallets that do not have sufficient credentials. When accepting Crypto Asset deposits from such wallets, traditional costly on-chain data checks will be required. This takes time and money, and customers will have to wait for their Crypto Asset deposits to be reflected. This is also expected to become an incentive for holding credentials.

9.5.2. Compliance Layers

- Multiple Compliance Layers

  As shown below, compliance rules exist at various layers. Just as with laws in the world, in addition to the rules imposed by the jurisdiction, there are rules as VASPs' self-regulation. When both compliance rules need to be followed, the transaction is executed only if it complies with both compliance rules. Also, although it is unlikely, if the rules conflict, it should be stipulated which rule takes precedence. In this example, of course, the rules imposed by the jurisdiction take precedence. For transactions with counterparties, whether between a VASP and a self-custodial wallet or between self-custodial wallets, the stricter law should apply to both parties. All transactions must be controlled so that only those that satisfy all of the following are actually executed.

- Jurisdiction Layer

  First, it is considered to vary by jurisdiction. Even in traditional finance, antisocial organizations, etc. are designated by each jurisdiction. Since cross-jurisdictional transactions are expected to occur frequently in Crypto Asset transactions, the sanction lists to be referenced should include not only the sanction lists of the jurisdiction in which one is located but also the sanction lists of the jurisdictions with which one may potentially transact. For example, there are many U.S.-originated DApps. These DApps should exclude investors on the U.S.-designated sanction list. In this case, even users outside the U.S. who wish to use the DeFi platform should not have a transaction history with the U.S.-designated sanction list. Therefore, the sanction lists that any wallet should reference include not only the sanction list designated by the jurisdiction in which it is located but also the sanction lists designated by other jurisdictions with which it may potentially transact. However, it is unlikely to comply with the sanction lists of all jurisdictions. This is because if even one jurisdiction arbitrarily registers

wallets on the sanction list, well-intentioned investors may be unintentionally designated. Therefore, it is conceivable to limit the sanction lists to be referenced to those designated by the jurisdictions that FATF designates as whitelisted countries for the Travel Rule.

- VASP Layer

  Based on the risk-based approach principle, VASPs are expected to manage their own sanction lists separately from the sanction lists designated by the authorities in each jurisdiction. Therefore, users of a VASP need to also refer to the sanction list published by that VASP.

- Token Layer

  Some tokens, such as security tokens, are subject to securities laws in each jurisdiction, so trading is conducted with additional trading restrictions imposed. The most typical example is insider trading. If you want to hold a token, you need to prove that you are not an insider of that security token.

- Individual Layer

  In addition, each investor should be able to have preferences such as avoiding transactions with investors from specific jurisdictions. However, if the compliance rule sets that individuals require to their counterparties are very specific, there is a high risk that the PII will be identified. In order to minimize such risks, a mechanism is needed to warn individuals when the compliance rule sets required by a counterparty are very specific.

9.5.3. Anonymity Revocation

- Two Anonymity Revocation Methods

  When legal institutions, etc. perform anonymity revocation on a wallet under investigation, there are two methods. One is to have the issuer of the DID or VC disclose the information such as personal identification documents received from the holder at the time of issuing the DID or VC to the legal institution, which is the simplest method if the wallet holds a DID or VC. However, in this case, the legal institution can know the owner of the wallet under investigation, but cannot directly seize or invalidate the crypto assets held by the wallet. In this case, after confirming the guilt of the wallet, the wallet must be registered on a blacklist as described in the next chapter, and other wallets and servicers must be controlled so as not to transact with the wallet. However, this operation does not necessarily require anonymity revocation, and it is fully feasible while keeping the wallet holder anonymous. In addition, if it becomes known that DID and VC issuers can

easily disclose personal information of wallet holders who are only at the stage of suspicion, there is a risk that investors will hesitate to obtain DIDs and VCs, which could pose a serious problem for the spread of the methodology.

- Prior Research

  The second method is a cryptographic approach. One possibility is to add a mechanism that allows legal institutions to decrypt or recover personal information stored in encrypted IPFS, etc., or wallet signing authority, under certain conditions (i.e., when a warrant or judgment is issued). However, a single entity must not have the authority to disclose any investor's personal information or seize wallet assets. Prior research "Balancing Privacy and Accountability in Blockchain Identity Management (iacr.org)" proposes a protocol using anonymous AES key sharing, where Anonymity Revokers (ARs) have the authority to decrypt privatized KYC information. It states that ARs must always be one or more independent individuals, and personal information can be revoked or wallet assets can be seized if a certain number or more of members agree (sign). This could be used, for example, to execute anonymity revocation when both the judiciary and the administration agree (sign). In such a system model, it is important to design it so that more than half of the people do not have an incentive to disclose information with malicious intent. Even if revocation authority is distributed among independent legal institutions, as long as they belong to a single jurisdiction, it is difficult to say that revocation authority is completely distributed, and it is always difficult to give investors the assurance that personal information will never be disclosed unless they engage in wrongdoing. Unless it is designed very well, it may end up being centralized after all, losing the meaning of using a blockchain.

- The Risks of Wallet Anonymity Revocation

  While the concept of anonymity revocation may seem appealing as a means to combat criminal activity, the Accountable Wallet framework takes a cautious stance on this matter. The primary concern is that granting authorities the power to freely identify the true owner of any wallet, without the occurrence of a crime, would effectively give them the ability to register any wallet on a watchlist and freeze any individual's crypto assets at any time.

  To mitigate this risk, the anonymity revocation procedure would need to be meticulously constructed, both cryptographically and procedurally, to ensure that it is executed only when a crime has actually occurred. One potential approach is to completely separate the judiciary and administration, requiring a court decision or other judicial judgment for anonymity revocation, which the oracle chain would then incorporate and organize to prevent revocation solely based on

administrative judgment.

However, even with such safeguards in place, it remains challenging to provide users with the assurance that their personal information will never be disclosed unless they engage in wrongdoing. The complexity of verifying that the government of a particular country does not effectively control both signature authorities, even if advanced cryptographic techniques like Multi-Party Computation (MPC) are employed, renders this task nearly impossible.

Furthermore, the mere existence of an anonymity revocation mechanism, regardless of its intended purpose, may erode user confidence in the privacy and security of their assets. The fear of potential misuse or abuse of this power could deter individuals from adopting the Accountable Wallet framework, undermining its effectiveness in promoting compliance and legitimacy within the decentralized finance ecosystem.

Instead of relying on anonymity revocation, the Accountable Wallet framework focuses on empowering users to make informed decisions about their transaction partners and incentivizing compliant behavior through the use of trust scores and attestations. By providing users with the tools to verify the legitimacy of their counterparties and encouraging them to transact within the Accountable Economy, the framework aims to create a self-regulating system that deters illicit activities without compromising user privacy.

It is important to acknowledge that no technological solution can completely eliminate the risk of criminal activity in decentralized systems. However, by prioritizing user privacy and autonomy, while still providing mechanisms for voluntary compliance and self-regulation, the Accountable Wallet framework seeks to strike a balance between the need for security and the fundamental principles of decentralization.

In conclusion, while the idea of wallet anonymity revocation may seem tempting as a quick fix for combating criminal activity, the risks associated with its implementation far outweigh the potential benefits. The Accountable Wallet framework, by focusing on user empowerment, self-regulation, and incentivized compliance, presents a more sustainable and privacy-preserving approach to fostering a secure and legitimate decentralized finance ecosystem.

However, there does need to be sanctions against the manager of a wallet that has engaged in illegal activities. In other words, the PII needs to be recognized by the authorities in an encrypted state, and the fact that the manager of that PII is in a sanctioned state needs to be shared among regulated VASPs. In other words, if an attribution credential is obtained using a certain PII and a wallet

holding that attribution credential engages in a criminal act, even if an attribution credential is issued again using the same PII from a different credential issuer, the issuance of the attribution credential should be refused due to the past criminal act or should already be designated on the sanction list. This should be designated based on the criminal acts of the wallet and will be discussed in detail in the next chapter.

10. Legitimacy of a Wallet Conduct

10.1. Concept

10.1.1. Definition

- Differences from the previous chapter

  In many cases, the addresses of the perpetrators of exploits, price manipulation, and other unfair transactions can be identified on-chain. The fundamental issue is that even if the addresses involved in illegal activities can be identified, in most cases, the assets cannot be invalidated or confiscated due to the anonymity of Wallet Holders and the self-sovereignty of crypto assets in blockchain systems, as discussed in the background section.

  The anonymity of decentralized finance often leads to criminal acts and proceeds being held by wallets with unknown managers. From a legal standpoint, these are criminal acts with unidentified suspects. In this case, legitimate investors must avoid transacting with wallets that have committed crimes, even if the suspects are unidentified. In other words, while the previous chapter discussed with whom one should not transact, this chapter discusses which wallets one should not transact with. The sanctions targets differ between the previous chapter and this chapter. In the previous chapter, specific organizations and individuals were the targets of sanctions, while in this chapter, wallets are the targets.

- Definition of the Legitimacy of a Wallet Conduct

  Ideally, credentials could be issued to prove a wallet's legitimacy, but proving that any wallet has not committed a crime in the past is a so-called devil's proof of proving a negative, which is difficult to directly achieve. Therefore, it is challenging to issue credentials with such meaning. Conversely, considering the idea of attaching some kind of mark to wallets involved in illegal transactions, this approach is also ineffective because both credentials and wallets can be

discarded.

Therefore, what this method proves is technically a proof of not being designated as an illegal wallet. It involves demonstrating that one's own wallet has not been listed on the crypto-watch list, which will be defined later. In other words, the order is that crypto-watch lists are defined in some way, and one self-certifies that they do not fall under or are not involved with them. For example, if an exploit occurs and the authorities tasked with cracking down on it observe and identify the addresses presumed to be controlled by the perpetrator of the exploit by authorities or decentralized oracles, which will be defined later, the trustworthiness of those addresses becomes zero if they are definitively determined to have been involved in the incident. Similarly, if a hacking attack on a Crypto Asset exchange occurs and the destination addresses of the hack are clearly identified, the trustworthiness of those addresses becomes zero, and other accountable wallets must avoid transacting with or receiving Crypto Asset from those addresses. The next section will provide an overview of how to generate evidence to prove that a wallet has not been involved in illegal activities.

- Which crypto-watch list to refer to prove the legitimacy

  In the context of proving the legitimacy of a wallet's conduct, the ultimate determination of legality hinges on the wallet's ability to demonstrate its absence from relevant crypto watchlists. These watchlists, maintained by various jurisdictions and regulatory bodies, serve as the definitive sources for identifying wallets associated with illicit activities, such as money laundering, terrorist financing, or other prohibited transactions. Consequently, the selection of which watchlists to reference when generating proofs of legitimacy becomes a critical factor in establishing a wallet's compliance with legal and regulatory standards.

  The process of proving a wallet's legitimacy involves generating cryptographic proofs of non-membership, which conclusively demonstrate that the wallet does not appear on any of the specified watchlists. However, given the multitude of watchlists maintained by different jurisdictions worldwide, it is neither practical nor necessary to prove non-membership across all existing watchlists. Instead, the focus should be on referencing the watchlists that are most relevant to the wallet's specific context, taking into account factors such as the wallet's transactional history, the jurisdictions of its counterparties, and the prevailing regulatory landscape.

  The choice of which watchlists to reference when generating proofs of legitimacy has a direct impact on the outcome of the wallet's compliance assessment. A wallet that successfully demonstrates its absence from a carefully selected set of watchlists, curated based on its unique circumstances, can assert its legitimacy

with a high degree of confidence. Conversely, a wallet that fails to consider the appropriate watchlists or relies on an incomplete or outdated set of watchlists may find its legitimacy called into question, even if it is not actively engaged in illicit activities.

This raises the crucial question: Which jurisdiction's watchlists should be referenced when attempting to prove a wallet's legitimacy? The answer to this question is not straightforward, as it depends on a range of factors specific to each wallet and its transactional history. However, by examining the different approaches to sanctions and the nature of cross-jurisdictional crypto transactions, it is possible to develop a framework for determining the most relevant watchlists in a given context.

The process of sanctioning wallet addresses generally follows two distinct methods, each of which has different implications for proving the legitimacy of a wallet. These methods determine the jurisdictional sources of crypto watchlists that must be referenced.

- Method 1: Wallet Addresses Associated with Illicitly Obtained Crypto Assets

This category encompasses wallet addresses that have been identified as recipients of crypto assets obtained through illicit means, such as:

- Wallets that received crypto assets stolen from a cryptocurrency exchange
- Addresses published by the FBI as being controlled by North Korea and holding stolen crypto assets
- Wallets that acquired crypto assets through exploits such as flash loan attacks or sandwich attacks on DeFi platforms

In cases falling under Method 1, there is typically a clear victim who has been wrongfully deprived of their crypto assets. A fundamental principle in many jurisdictions is that such theft or exploit-related crimes must be reported by the victim to the relevant authorities. Consequently, for a wallet involved in an exploit to be added to a crypto watchlist by the authorities, the exploit victim must first file a report with the authorities in their jurisdiction. For instance, if a U.S.-based cryptocurrency exchange falls victim to a hacking attack and loses crypto assets, they will report the incident to U.S. authorities.

However, a complication arises from the fact that the perpetrator of the exploit may not necessarily reside in the same jurisdiction as the victim. Moreover, if the stolen crypto assets are held in a self-custodial wallet, the

concept of geographical location becomes irrelevant due to the nature of blockchain technology. In other words, regardless of where the hacking incident occurs, the perpetrator and the illicitly obtained assets could be located anywhere in the world, while the crime is typically only reported to the authorities in the victim's jurisdiction. This poses a significant challenge in apprehending the culprits and prevents them from easily converting the stolen assets into other forms of monetary value.

To effectively combat such incidents, it is imperative that all well-intentioned cryptocurrency users, regardless of their jurisdiction, cooperate in rejecting transactions with the perpetrators, even if the crime is only recognized and reported by the authorities in the victim's jurisdiction. In the context of an accountable wallet proving its own legitimacy, this means demonstrating that none of the wallets from which it has received crypto assets have been reported by their respective jurisdiction's authorities as being involved in the illicit acquisition of those assets.

Consequently, the oracle data required for generating such proofs is the crypto watchlist maintained by the authorities in the jurisdiction where the sender of the crypto assets resides. It is not necessary to reference watchlists from every jurisdiction worldwide or even the watchlist of the recipient's jurisdiction.

This concept aligns with the notion of "Localized Sanctions List Integration" discussed in Chapter 9, which suggests that when proving the legitimacy of a wallet holder, it is sufficient to demonstrate one's absence from the sanction lists published within one's jurisdiction of residence, rather than proving non-inclusion on every sanction list globally. Applying this principle to the legitimacy of wallet conduct, the relevant crypto watchlists are not those published by the wallet holder's jurisdiction, but rather those issued by the jurisdictions where the senders of the previously received crypto assets reside. The rationale behind this is that the reporting of exploits and crimes typically originates from the victim's location. If an individual or entity that sent you crypto assets reports to their local authorities that the transaction was the result of an exploit, the transaction will be recognized as illicit. Your own jurisdiction of residence is irrelevant in proving your non-involvement in criminal activities; what matters is that none of the wallets that sent you crypto assets have filed reports of exploits or theft with their respective authorities. For example, if you have received crypto assets from wallets whose holders reside in countries A and B, as evidenced by credentials, you would need to prove

that your wallet is not listed on the crypto watchlists designated by the authorities in those specific countries. The legitimacy of crypto assets received from wallets involved in exploits and subsequently transferred to other wallets will be addressed in the next chapter on Crypto Asset Provenance, through the design of a mechanism that lowers the trust scores of the receiving wallets.

- Method 2: Wallet Addresses Associated with Illicit Activities or Functions

  In this category, wallet addresses are sanctioned not necessarily for holding illicitly obtained funds, but for their involvement in illegal activities, such as money laundering or illegal transactions. Examples include:

- Smart contract addresses of protocols like Tornado Cash (which may not be illegal in all jurisdictions)
- Wallet addresses used as payment destinations on dark web marketplaces trading illegal goods
- Wallets suspected by authorities to be controlled by terrorist organizations, even if the crypto assets they hold were not obtained through illicit means

  In contrast to Method 1, there may not be a clear victim in cases falling under Method 2. Consequently, proving legitimacy based on oracle data derived from victim reports is not feasible. Taking the example of Tornado Cash, the protocol has been sanctioned by the United States due to its frequent use by criminals to obfuscate the trail of funds after crypto asset thefts, making it difficult for law enforcement to trace the proceeds of crime. However, the operators of Tornado Cash are not directly involved in the thefts themselves.

  Furthermore, not all users of Tornado Cash employ the protocol for money laundering purposes; many individuals use it simply to protect their transaction privacy, which is not inherently illegal. Nevertheless, by using Tornado Cash, even users with no intention of laundering money inadvertently mix their crypto assets with those of malicious actors, potentially aiding in the obfuscation of criminal proceeds. From this perspective, it is understandable that some entities may prefer not to transact with anyone who has interacted with Tornado Cash, regardless of their intentions.

  Generalizing this line of reasoning, the critical factor in Method 2 sanctions is whether your previous transaction counterparties are themselves subject to sanctions, as determined by the preferences of your current or

future transaction partners. For example, U.S. residents are prohibited from using Tornado Cash due to its sanctioned status by the U.S. Treasury Department. In practice, this means that they cannot transact with counterparties who have a history of direct or indirect interaction with Tornado Cash. As a result, when engaging in a transaction, U.S. residents would require their counterparty to prove the absence of any direct or indirect use of Tornado Cash, and only proceed with the transaction if such proof is provided and verified. In this case, the jurisdiction of the transaction counterparty becomes relevant for proof generation. Similar to Method 1, there is no need to reference crypto watchlists from every jurisdiction worldwide or to consider your own jurisdiction. This approach aligns with the fact that Tornado Cash is not universally sanctioned by all countries. The present discourse does not argue for or against the sanctioning of Tornado Cash itself; this is a matter for individual crypto asset users to decide based on their own judgment. The crucial point is to provide a methodology for implementing such policies for those who wish to adhere to them.

10.1.2. Interjurisdictional Harmonization and Consensus

- Jurisdictional Relevance in Cross-Border Crypto Transactions

  In conclusion, when proving the legitimacy of a wallet's conduct, it is essential to determine which jurisdiction's crypto watchlists are relevant. For wallets that have received assets from other wallets, the primary focus should be on ensuring that the jurisdictions governing the sources of the assets have not flagged the transactions as illicit. Similarly, when engaging in future transactions, the relevant reference points are the jurisdictions governing the transaction counterparties.

  This means that it is unnecessary to reference every global watchlist when proving the legitimacy of a wallet's conduct. Instead, the non-membership proof should focus on the specific legal frameworks that apply to the transaction sources or counterparties involved. Therefore, the wallet holder's own jurisdiction is often irrelevant to the proof of conduct. What matters is whether the authorities governing the wallets that sent assets to the holder have flagged those transactions as suspicious or illegal.

  For example, if Wallet A receives crypto assets from Wallet B, which is located in a jurisdiction that maintains a crypto watchlist, Wallet A's legitimacy is determined by whether Wallet A appears on the watchlist maintained by Wallet B's jurisdiction. If no such reports have been filed, Wallet A can generate a valid non-membership proof demonstrating the legality of its conduct.

The same principle applies to future transactions. New counterparties engaging with Wallet A may require proof that Wallet A has not previously interacted with wallets listed on watchlists maintained by their own jurisdictions. In this manner, the legitimacy of a wallet's conduct is determined by the legal frameworks of external jurisdictions, rather than the wallet holder's own jurisdiction.

- Influence of Major Jurisdictions on Global Crypto Activity

  It is also important to consider the influence of large jurisdictions, such as the United States, on global crypto markets. While sanctions imposed by one jurisdiction may not be legally binding in other regions, the economic significance of certain jurisdictions often results in a form of de facto compliance by users in other regions. For instance, if a substantial proportion of global cryptocurrency users are located in the United States, sanctions imposed by U.S. authorities on specific addresses can affect the global reputation and trust associated with those addresses. Even users in non-U.S. jurisdictions may choose to avoid interactions with sanctioned addresses to ensure their continued access to U.S.-based markets and services, or to avoid reputational damage.

  On the other hand, sanctions that do not gain widespread acceptance may have limited effect. If users in other jurisdictions determine that a particular sanction is unwarranted and continue to interact with the sanctioned address, the influence of the sanction may be diminished. This dynamic creates a form of market-driven consensus, where the power of sanctions is not merely a function of the legal authority imposing them, but also of the broader market's acceptance of their legitimacy.

10.1.3. Challenges

The key consideration here is who designates the addresses as the transfer destinations and through what procedures, how other nodes validate that information with each other, and how the addresses are officially designated as criminal proceeds transfer destinations to become public information. If there is an entity that everyone can trust with certainty, and that entity designates an address as a criminal proceeds transfer destination, it may be acceptable to publicly set the trustworthiness of that address to zero. However, in reality, an entity that everyone can trust with certainty, including regulatory authorities, does not exist due to the borderless nature of decentralized finance.

Moreover, there is a dilemma between the speed of sanctions designation and the validity of the sanctions designation process. It is challenging for such entities to designate any address as a criminal proceeds transfer destination at the moment an

incident occurs. There are issues with designating without going through legal procedures. However, if legal procedures are made an absolute requirement, the criminal proceeds transfer destination addresses may be able to convert the proceeds into other forms of monetary value before being designated.

Therefore, as discussed in the previous chapters, when such incidents occur, any address must be immediately designated as a "suspect" through democratic procedures. When an address is designated as a suspect address in this manner, its trustworthiness immediately decreases, but it is merely an estimate and not definitive information. There is no correct answer to this estimate, but this section proposes a specific formula and attempts to define the trustworthiness of suspect addresses.

10.1.4. Premise

Note that this method itself is not a method for detecting illegal transactions on-chain or determining the illegality of any transaction. Various discussions are being held on these matters, such as judicial discussions[37] and discussions as on-chain data analysis methods[38], but ultimately, the determination of illegality can strictly only be made by the judiciary and administration of each jurisdiction. Therefore, it is not productive to extensively discuss the regulatory trends of each jurisdiction in this paper.

This paper assumes that the list of illegal wallets is a given. In fact, the struggle of regulatory authorities in each country in cracking down on crypto assets is the difficulty of identifying the actual perpetrators of fraudulent transactions, and since the wallets that executed the fraudulent transactions are often easily viewable on-chain, it is not an unrealistic assumption to assume that the authorities will publish a list of wallet addresses involved in fraudulent transactions. In fact, in the United States, the FBI and other jurisdictional authorities have already published online the wallets involved in illegal transactions. Rather, what this chapter problematizes are guidelines on what data format those authorities in each jurisdiction should disclose that information in, how to aggregate it into a single dataset, and how legitimate investors can prove their legitimacy to others by not being listed in that data.

Therefore, given these realistic preconditions, the only action that regulators, regulation-compliant VASPs, and investors who intend to act legally can take is to completely avoid transacting with these addresses. The key to achieving this lies in cutting off all means for criminals to convert their illegal crypto assets into other forms of value.

37

38

10.2.Procedure

10.2.1. Procedure Structure

As mentioned earlier, the legitimacy of a wallet is defined as the probability that the wallet has not been involved in any illegal activities. This section outlines the methods for generating evidence that guarantees non-involvement in such activities. The structure for issuing this proof is divided into two parts.

- Creation of a crypto watch list

  Creation of a list of wallet addresses involved in illegal activities as oracle data, hereafter referred to as the "crypto watchlist." There are two main methods for providing this list, and both mechanisms are necessary.

- Centralized Designation

  This method involves the designation of wallet addresses by authorities in each jurisdiction. Ultimately, the final determination of legality must depend on legal procedures. However, in this case, there is a risk of wallet addresses being unreasonably designated as sanctioned by authorities, leading to a depreciation of asset value. Therefore, a crucial point emphasized by our method is that the decision regarding which lists to reference among the various crypto watchlists designated by authorities worldwide should be made by the parties involved in the transaction. It is important to note that our method does not discuss the procedures by which authorities designate wallets as sanctioned. The focus of our discussion is on how to incorporate these designations into the blockchain. Currently, many authorities simply publish these addresses on their websites, which poses challenges in terms of format inconsistency and the inability to verify the authenticity and completeness of the data. Consequently, it is not possible to generate a verifiable proof of non-inclusion in these lists. Whenever off-chain data is used as trusted data, the oracle problem arises. A mechanism is needed to accurately and promptly update and share the crypto watchlist, which will be discussed further.

- Decentralized Designation

  This method involves the decentralized designation of wallet addresses by nodes. While the crypto watchlists provided by authorities offer responsible disclosure regarding the potential involvement of listed wallets in criminal

activities, the responsibility associated with such disclosure often leads to a rigorous process for inclusion, resulting in significant delays. Consequently, criminals may be motivated to transfer their crypto assets to other wallets using anonymization techniques before being listed, making it difficult for authorities to include them on the list. To address this issue and detect criminal activities before the authorities do, a reporting system that incorporates decentralized oracles is proposed. This approach is referred to as decentralized designation.

- Issuance of non-membership proofs using the above data

  This proof demonstrates that one's own wallet is not listed on the crypto watchlist and is not associated with the listed wallets. Generating such proofs is not particularly challenging when using non-membership proof techniques. The main issue lies in how to prepare the oracle data in the first step to generate these proofs.

To ensure the reliability and effectiveness of the crypto watchlist, it is essential to establish clear guidelines and standards for the inclusion of wallet addresses. This may involve collaboration between regulatory authorities, law enforcement agencies, and decentralized networks to develop a robust and transparent process for identifying and verifying wallet addresses involved in illegal activities.

Furthermore, the development of interoperable data formats and secure data-sharing protocols is crucial to facilitate the seamless integration of crypto watchlists from multiple sources. This will enable the creation of a comprehensive and up-to-date database of wallet addresses associated with illegal activities, enhancing the accuracy and effectiveness of non-membership proofs.

In addition to technical considerations, it is important to address the legal and ethical implications of creating and maintaining a crypto watchlist. This includes establishing clear guidelines for the protection of user privacy, ensuring due process in the designation of wallet addresses, and providing mechanisms for appeal and redress in cases of erroneous or unjustified inclusion.

10.2.2. Centralized Designation

The centralized designation of wallet addresses involved in illegal activities or managing proceeds from such activities is the responsibility of authorities in each jurisdiction. The primary objective is for investors to use this data to self-prove, in a format easily verifiable by others, that they are not listed on these watchlists. However, if the data does not meet requirements such as authenticity and completeness, third parties cannot perform verification.

- Key Problems with Centralized Designation

  - Trust and Authenticity

    A critical concern in centralized designation is the integrity of the blacklist itself. Trusting a single or a set of authorities to manage these lists introduces the risk of both data manipulation and incomplete coverage. It is essential that the data provided by regulatory authorities meet the highest standards of authenticity and completeness, ensuring that it can be trusted by all network participants. Without such assurance, users cannot generate valid "proof of absence" from a watchlist, undermining the purpose of designating a wallet as accountable.

  - Jurisdictional Fragmentation

    Each country or jurisdiction may maintain its own regulatory framework and list of blacklisted addresses. This divergence complicates the creation of a unified global solution. Wallets that are designated as illegal or suspicious in one country may not be flagged in another, creating loopholes that illicit actors can exploit by routing transactions through different jurisdictions. The absence of global consensus on how to handle such data presents significant regulatory challenges, making enforcement difficult across borders.

  - Updating and Maintenance

    Maintaining an up-to-date and accurate list of wallets involved in illegal activities is labor-intensive and often reactive rather than proactive. Crypto assets can be swiftly moved across wallets or obfuscated through tumbling services and cross-chain transactions, making it difficult for authorities to keep pace. This problem is exacerbated by the decentralized and pseudonymous nature of blockchain networks.

- Proposed Solutions for Centralized Designation

  To address these challenges and ensure crypto watchlist data meets the necessary requirements. This is similar story as sanction list data’s authenticity and integrity. Several methods are considered:

  - Method 1 - Authorities Digitally Sign the Data

    Jurisdictional authorities typically publish crypto watchlists on their

websites. In this format, the data does not meet the necessary requirements for authenticity and completeness, making it unsuitable for generating non-membership proofs. One potential solution is for authorities in each jurisdiction to calculate the root hash of all designated wallet addresses and digitally sign it, enabling wallet owners to use this data for proof generation. However, this approach raises issues of public key certification and the need for standardized data formats. Requesting this from authorities worldwide may not be a realistic solution.

- Method 2 - Trusted Organization Digitally Signs the Data

  Given the challenges associated with Method 1, an alternative approach involves a single trusted organization collecting crypto watchlist data published by authorities, digitally signing it, and ensuring its authenticity and completeness. This process resembles the role of third-party service providers in traditional finance, where banks do not collect sanction lists themselves. However, this method also raises questions, such as why the organization can be trusted, how to ensure the organization does not tamper with the data, and what financial incentives the organization can have to provide such a service.

- Method 3 - Decentralized Curation and Verification

  To address the limitations of centralized approaches, a decentralized system for curating and verifying crypto watchlist data can be developed. In this model, a network of independent nodes collaborates to collect, validate, and maintain the watchlist data. Each node is incentivized to act honestly through a staking mechanism, where nodes are required to stake tokens to participate in the network. Malicious behavior, such as submitting false or incomplete data, results in the slashing of the node's stake.

  This can be seen as a crypto watchlist version of oracle chains like Chainlink. The proposed protocol would retrieve the off-chain information of sanctioned wallet addresses designated by regulatory authorities and bring it onto the blockchain. Similar to oracle chains, designing incentives for each node to act honestly is crucial.

  The decentralized network operates on a consensus mechanism, where nodes vote on the validity and completeness of the submitted watchlist data. Once a threshold of nodes approves the data, it is considered verified and added to the master watchlist. This master watchlist is then cryptographically signed by the network, ensuring its authenticity and

immutability.

To further enhance the security and reliability of the decentralized watchlist, the network can implement a multi-sig scheme, requiring multiple trusted nodes to sign off on any changes or updates to the watchlist. This helps prevent any single node from manipulating the data and ensures that the watchlist remains accurate and up-to-date.

10.2.3. Decentralized Designation

- Approach

  The centralized determination of fraudulent transactions, while effective in principle, encounters significant limitations in practice. The primary issue is the delay in identifying and sanctioning wallets involved in illegal activities. By the time a centralized authority has flagged a wallet as illicit, the perpetrators may have moved funds across multiple wallets, making it exceedingly difficult to trace the criminal proceeds. Moreover, the wallet that receives the proceeds of crime might not necessarily be complicit in the illegal activity itself, and thus designating such wallets can be legally and ethically problematic. This leads to a common dilemma: by the time the actual wallet involved in the criminal act is blacklisted, it may be emptied, and the funds may have passed through otherwise innocent wallets.

  To overcome these limitations, a decentralized approach to wallet designation becomes necessary. The goal is to detect and sanction wallets involved in illicit activities more swiftly and systematically by leveraging decentralized systems that work in tandem with centralized authorities. This decentralized designation method does not replace the centralized process but serves as a complementary layer, enabling rapid identification of suspicious activities and preliminary sanctioning by decentralized nodes.

- Immediate Detection and Reporting

  One of the advantages of decentralized systems, such as blockchain, is the public and immutable nature of transaction data. In many cases, the addresses involved in hacks, market manipulation, and unfair trading can be identified immediately. This transparency allows for the potential of real-time detection of malicious activities.

  The proposed system relies on a decentralized network of compliance oracles. These oracles would monitor blockchain activities and report suspicious or fraudulent addresses in a trustless, decentralized manner. Oracles could be

nodes operating under specific incentive structures to ensure accuracy and timeliness in reporting. This system could function similarly to oracle chains like Chainlink, where nodes are rewarded for providing accurate data and penalized for false reports. Hence, this proposed system is referred to as the compliance oracle network.

- Core Features of the Compliance Oracle System

  - Incentivized Reporting

    In the compliance oracle system, nodes are incentivized to detect and report illicit activity promptly. When an oracle node identifies suspicious transactions—such as a large-scale exploit or market manipulation by a wallet—the node can submit a report, staking tokens or collateral as a form of credibility. If the report is accurate and the address is confirmed to be involved in illegal activities, the node is rewarded based on its reporting speed and the amount of staked collateral. However, if the report is inaccurate or malicious, the staked collateral can be partially or fully confiscated, providing a strong disincentive for false reporting.

  - Validation of Reports

    To avoid a situation where a single node can unilaterally mark an address as suspicious, the compliance oracle system requires that reports be validated by other nodes in the network. This peer validation mechanism ensures that multiple independent entities confirm the malicious activity before the wallet is designated as suspicious. These validating nodes will also stake tokens and receive rewards for accurate validation, further promoting a decentralized, transparent, and trustworthy process.

  - Suspect Lists and Early Action

    Once a wallet is flagged as suspicious, it is added to a suspect list that other participants in the blockchain ecosystem can query. This list serves as an early warning system for legitimate actors. Any wallet or decentralized application (DeFi protocol) interacting with a flagged address can suspend or halt transactions to avoid becoming involved with illicit funds. While this preemptive suspension might not carry the legal weight of an official sanction, it provides an important precautionary measure, significantly reducing the likelihood that illicit funds are laundered through legitimate wallets or protocols.

    The key advantage of this decentralized suspect list is that it allows for rapid containment of suspicious activities. Even before an official

investigation or designation by a centralized authority is complete, the community can already take protective actions based on decentralized intelligence.

- Transition from Suspect to Sanctioned

  The decentralized suspect list serves as a preliminary filter for potentially fraudulent wallets. However, an official designation by a government or regulatory body is still required to formally classify a wallet as involved in illegal activities. Once a centralized authority investigates and confirms that a wallet has indeed been involved in illicit activity, the wallet's status is upgraded from "suspect" to "blacklisted". This information is disseminated back into the compliance oracle network, ensuring that all nodes and wallets are aware of the official status change.

  The system provides a seamless integration between decentralized intelligence and centralized enforcement, ensuring a speedy response to fraud without sacrificing the legitimacy and legal backing required for full sanctioning.

- Incentive Structures for Nodes

  To ensure active participation and accuracy, the compliance oracle system must be built on a solid foundation of incentive mechanisms:

  - Reporting Incentives

    Nodes that are the first to detect and report fraudulent behavior are rewarded based on how early they submit their report and how much stake they commit to their claim. The faster and more accurate the detection, the higher the rewards.

  - Staking and Penalties

    Nodes must stake a certain amount of tokens when submitting or validating reports. If a report turns out to be false, the node's stake is confiscated, creating a self-regulating mechanism to discourage malicious reporting.

  - Validation Rewards

    Nodes that validate reports are similarly rewarded based on the accuracy of their validation, encouraging a robust and decentralized validation process.

- Privacy Concerns and the Tipping-off Rule

One key challenge of decentralized designation is maintaining privacy while still ensuring that illicit activities are detected and sanctioned. Even in a decentralized system, it is important that the personal identities of wallet holders are protected until legal action is necessary. In compliance with personal data protection laws, no node in the compliance oracle network would be able to directly access the real-world identity of a wallet holder. Instead, reports are based purely on on-chain behavior, with nodes focusing on the transaction patterns and blockchain activities of wallets, rather than the identities behind them.

When a wallet is escalated from suspect to sanctioned, the identity of the wallet holder may need to be revealed for legal prosecution. In this case, the compliance oracle system could be designed to work with attribution credentials issued by trusted credential providers. If a wallet holding such credentials is blacklisted, the credential issuer could, through a cryptographically secure process, reveal the real identity of the wallet holder under legally defined circumstances. This ensures that wallets holding legitimate credentials can be prosecuted when involved in illegal activity, without compromising privacy prematurely.

- Sanctioning Across Multiple Wallets

  To prevent bad actors from circumventing sanctions by creating new wallets, the system must be designed to impose penalties across multiple wallets managed by the same person. If a user commits a criminal act with one wallet, that user should not be able to simply create a new wallet and obtain fresh credentials to avoid detection. This can be addressed by using unique identification numbers derived from the same PII (personally identifiable information) used in the attribution credentials. By hashing the PII into unique identifiers, the system ensures that multiple wallets tied to the same individual are appropriately flagged if one of their wallets engages in illegal activity.

  This approach prevents sanctioned users from “resetting” their identity by creating new wallets, while still maintaining a high degree of privacy for legitimate users. The system effectively deters individuals from committing fraud with one wallet and escaping detection by using a new wallet, as any wallet linked to their PII will be automatically subject to the same penalties.

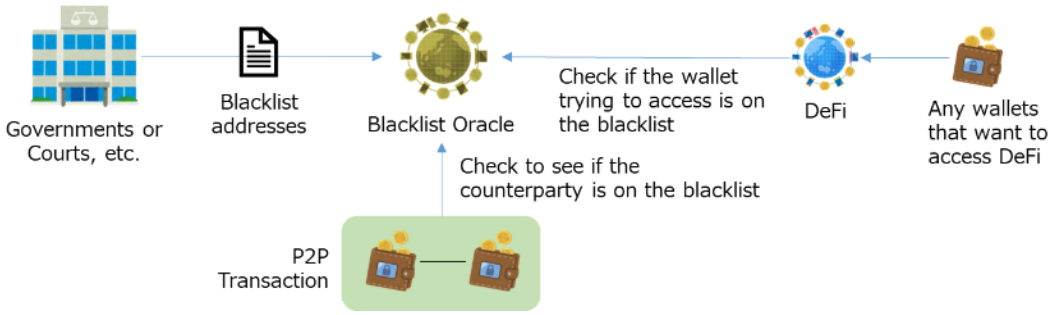


Figure 22

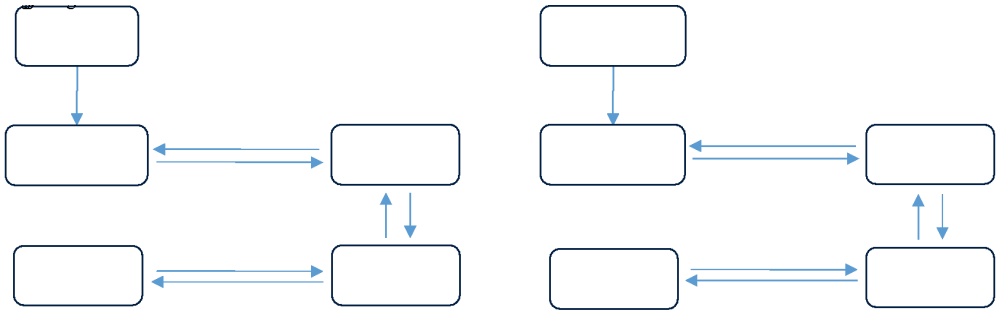


Figure 23

- Determining the Applicable Jurisdiction

  Also, legality of transactions will ultimately be judged by the administration and judiciary, which depends on the jurisdiction. For example, the U.S. authorities have effectively banned the use of Tornado Cash by U.S. residents. Therefore, VASPs operating in the U.S. must refuse to receive crypto assets from wallets that have used Tornado Cash. On the other hand, in jurisdictions without such laws, receiving crypto assets from wallets that have used Tornado Cash is legal. Therefore, whether users who have used Tornado Cash should be considered users who have engaged in illegal activities depends on the user's jurisdiction of residence.

  Therefore, credentials need to provide information to determine which jurisdiction any given transaction belongs to, and a mechanism is needed for credentials to play that role.

  Transactions with unknown applicable jurisdictions are theoretically subject to regulations of all jurisdictions. In other words, wallets that cannot prove their jurisdiction of residence must not use Tornado Cash.

(Illustrate this with an equation)

10.2.4. Non-membership Proofs Issuance

- Crypto Watchlist as oracle data for generating non-membership proofs

  The legitimacy of a wallet's conduct is primarily determined by the jurisdictional authorities governing the wallets from which the assets were received and those with which future transactions will be conducted. The wallet holder must prove that they are not listed on the crypto watchlists maintained by these jurisdictions, rather than attempting to demonstrate non-membership on all global watchlists. This approach ensures both computational feasibility and legal relevance. By referencing the relevant jurisdictions, wallet holders can provide reliable evidence of their legal status, while authorities can effectively manage compliance within their own boundaries.

  From the perspective of proving the legitimacy of a wallet's conduct, a wallet must demonstrate two key aspects:

  > First, that it is not listed on the crypto watchlists designated by the authorities in the jurisdictions where the senders of the crypto assets currently held by the wallet reside.
  >
  > Second, that it is not listed on the crypto watchlists specified by the wallet's intended transaction counterparty (which typically align with the watchlists of the counterparty's jurisdiction). This approach ensures that the scope of the required proofs remains focused and practical, while still allowing users to transact in accordance with their individual preferences and jurisdictional requirements.

  By localizing the proof to the jurisdictions that matter in each specific transaction, wallet holders can provide credible evidence of their legal status, while authorities can effectively manage compliance within their own boundaries.

- Non-membership Proofs

  Wallet Holders need to prove that their wallet address is not on the Crypto Asset watchlist defined by the jurisdiction. Since wallet address is already public, privacy-focused methods are not necessary. Wallet holder can simply use the non-membership proof technique.

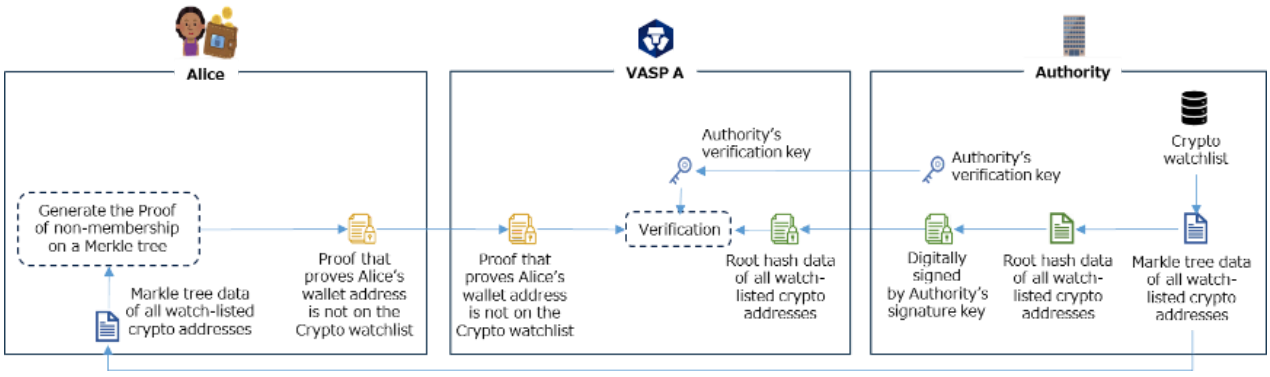


Figure 24

(A bit more technical explanation here)

- Integrating Watchlists from Multiple Jurisdictions

  Regardless of the method chosen for ensuring the authenticity and completeness of crypto watchlist data, another challenge arises when considering the integration of watchlists from multiple jurisdictions. Each jurisdiction may have its own format, standards, and update frequencies for their watchlists, making it difficult to create a unified, global watchlist.

  To address this issue, the chosen method should include a standardization process for the watchlist data. This can involve developing a common data schema, establishing uniform update intervals, and creating a protocol for merging watchlists from different jurisdictions. The goal is to create a single, comprehensive watchlist that covers all relevant jurisdictions while maintaining the integrity and timeliness of the data.

  One approach to integrating multiple watchlists is to use a hierarchical structure, where regional or national watchlists are consolidated into larger, international watchlists. This allows for the efficient management of watchlist data at various levels of granularity, enabling users to choose the appropriate level of coverage for their needs.

10.3. Trust Score of Wallet Conducts

10.3.1. Concept

The reliability of a Wallet Conduct refers to the reliability assessment based on the

transactions the wallet has conducted so far. Here, reliability is defined as the degree of probability that the wallet has not been involved in any criminal activities observed in the decentralized finance space.

For example, if an exploit occurs and the authorities tasked with cracking down on it observe and identify the addresses presumed to be controlled by the perpetrator of the exploit, the reliability of those addresses becomes zero if they are definitively determined to have been involved in the incident. Similarly, if a Crypto Asset exchange is hacked and the destination addresses of the hack are clearly identified, the reliability of those addresses becomes zero, and other accountable wallets must not transact with or receive Crypto Asset from those addresses.

The key issue here is who designates the addresses as transfer destinations and through what procedures, how other nodes validate that information with each other, and how the addresses are officially designated as criminal proceeds transfer destinations to become public information. If there is an entity that everyone can trust with certainty, and that entity designates an address as a criminal proceeds transfer destination, it may be acceptable to publicly set the reliability of that address to zero. However, in reality, an entity that everyone can trust with certainty, including regulatory authorities, does not exist due to the borderless nature of decentralized finance.

Moreover, there is a dilemma between the speed of sanctions designation and the validity of the sanctions designation process. It is difficult for such entities to designate any address as a criminal proceeds transfer destination at the moment an incident occurs. There are issues with designating without going through legal procedures. However, if legal procedures are made an absolute requirement, the criminal proceeds transfer destination addresses may be able to convert the proceeds into other forms of monetary value before being designated.

Therefore, as discussed in the previous chapters, when such incidents occur, any address must be immediately designated as a "suspect" through democratic procedures. When an address is designated as a suspect address in this manner, its reliability immediately decreases, but it is merely an estimate and not definitive information. There is no correct answer to this estimate, but this section proposes a specific formula and attempts to define the reliability of suspect addresses.

The incidents considered to affect the reliability of a Wallet Conduct are not limited to those clearly classified as criminal acts in any jurisdiction, such as exploits. In some jurisdictions, the use of specific DApps is legally prohibited. For example, in the United States, all citizens residing in the country are prohibited from using Tornado Cash. In this case, it is necessary to clarify whether sending Crypto Asset to Tornado Cash is an illegal act or receiving Crypto Asset from Tornado Cash is an illegal act. The conclusion is that the act of sending Crypto Asset to Tornado Cash is an action that affects the

reliability of a Wallet Conduct as defined in this section, while the act of receiving Crypto Asset from Tornado Cash is related to the reliability of the Crypto Asset held, which will be discussed in the next section. Therefore, this section considers how the reliability of a wallet is affected based on the destination and amount of Crypto Asset sent to illegally designated addresses.

10.3.2. Factors

As repeatedly mentioned, there is no single correct method for calculating the trust score of a Wallet Conduct, and the calculation method presented here is merely a proposal as a basis for discussion. The trust score of a Wallet Conduct should essentially be defined as the probability or degree to which the wallet has been involved in any illegal activities. When calculating the Trust Score of a Wallet Conduct, several key factors must be considered:

- Factor 1: Crypto watchlists defined by the jurisdictions of the senders who have sent crypto assets to your wallet

  As discussed in the Definition section, it is crucial to consider whether the senders of crypto assets to your wallet have reported to the authorities in their respective jurisdictions that the transactions were non-consensual or executed through illegal means such as hacking, and if those authorities have recognized the incidents as criminal cases.

  This applies not only to self-custodial wallets but also to VASPs. For example, if an exploit occurs at VASP A located in Jurisdiction A, and Authority A, which oversees Jurisdiction A, identifies the addresses to which the exploited crypto assets were sent and sanctions them, the receiving addresses should lose the ability to prove their legitimacy.

  However, when strictly calculating the trust score, there are a few additional considerations:

  - If the sender did not have proof of jurisdiction

    The senders of crypto assets to you may not necessarily possess credentials proving their jurisdiction of residence. In such cases, the receiving wallet cannot generate non-membership proofs for crypto watchlists by narrowing down the jurisdictions using the aforementioned logic. One approach to this issue is to deem wallets that cannot prove their jurisdiction of residence as inherently ineligible for recognition as accountable wallets. This means that crypto assets received from such wallets would inevitably be considered as lacking provable legitimacy,

resulting in a decrease in the trust score.

- If not the entire amount is illegal

  Even if the wallet you want to calculate the trust score for has received crypto assets from a sender's wallet that filed a damage report and had the damages recognized by the authorities, if the amount represents a very small portion of the total crypto assets held by the wallet, it would be unreasonable for the trust score to immediately drop to zero. This is because if even a small amount of such damages could result in a wallet being sanctioned, authorities could arbitrarily impair the value of crypto assets held by inconvenient wallets. If a wallet is unfairly sanctioned by an authority, the authority must specify the transactions that led to the sanction. If the recipient has no recollection of or firmly believes in the legality of those transactions, by abandoning the crypto assets obtained through those transactions using methods such as donations, as explained in the next chapter, they should have a means to deny involvement. In such cases, the value of the wallet's other pre-existing assets must not be impaired. Therefore, even if a wallet you want to calculate the trust score for has received crypto assets from a sender's wallet that filed a damage report and had the damages recognized by the authorities, the degree of decrease in the trust score should be adjusted according to the percentage of the total crypto assets held by the wallet that the damages represent.

- If designated as a suspect by an oracle

  If a wallet is designated as a suspect in an exploit by oracle nodes through the Decentralized Designation mechanism described earlier, the certainty of the designation is expected to be estimated based on factors such as the amount staked by the nodes at the time of designation. A calculation method based on this should be established by the industry. One approach could be to consider the trust score of the designator itself.

- Factor 2: Crypto watchlists defined by the jurisdiction to which you belong

  Illegal acts are acts that violate the law, and without determining the applicable law, that is, the jurisdiction to which the parties to the transaction belong, their illegality cannot be judged, making it difficult to consider the Trust Score of Wallet Conducts.

  If the jurisdiction of residence is revealed through the credentials held by the

wallet, the applicable law for that wallet becomes relatively clear. However, the determination of applicable law is not solely based on the location of the service user; the applicable law of the location of the service provider is also relevant. On the other hand, for wallets whose jurisdiction of residence is not proven through credentials, the applicable law is unclear, making it difficult to judge the legality of past transactions.

For example, in the United States, there is debate over whether Ethereum (ETH) is a security. If recognized as a security, securities laws would apply to ETH transactions, just like traditional securities transactions, and not only businesses dealing with ETH sales but also, strictly speaking, DeFi would be subject to securities laws. In contrast, some jurisdictions may consider ETH a commodity. In this case, if a DeFi platform handles ETH and is accessible to anyone, it would strictly be subject to the securities laws of all countries.

On the other hand, for illegal acts such as money laundering, which are generally considered illegal in all jurisdictions regardless of location, it may seem that the applicable law does not matter. However, even in this case, there is a problem. If a wallet is deemed to be involved in money laundering, there is ambiguity regarding which jurisdiction's authorities should list that wallet on their crypto watchlist, creating a potential loophole for transactions that all authorities consider outside their purview. This is because, in traditional finance, authorities generally have no obligation or duty to monitor or judge the illegality of acts committed by foreign residents in foreign countries. In borderless decentralized finance, authorities cannot know the residence of on-chain transactors, meaning that, strictly speaking, those transactors could potentially reside in any given country. To rigorously enforce the law, authorities would need to monitor all on-chain transactions worldwide, which is unrealistic. Conversely, if authorities only target transactions involving residents or entities of their own jurisdictions, illegal on-chain transactions could go unchecked by all authorities. In other words, when taking a stricter risk-based approach with the lowest risk appetite and most conservative stance, transactions by wallets or DeFi that cannot prove their jurisdiction of residence should be subject to the laws of all jurisdictions.

As mentioned, the compliance rules applicable to you are determined by your counterparty. In this case, the sanctions lists or crypto watchlists you must prove your absence from vary depending on the counterparty, potentially altering whether you are considered a criminal or criminal wallet. If you cannot demonstrate to your counterparty which jurisdiction you belong to, for those who absolutely want to avoid transactions that violate securities laws or engage with criminals, you would theoretically need to prove compliance with the compliance rules of all jurisdictions worldwide. For example, regarding non-existence proofs,

you would need to prove your absence from all global sanctions lists and crypto watchlists. In other words, when the compliance rules applicable to you are treated as a variable, the compliance rules that result in the lowest trust score calculation are applied to you, and that becomes your trust score.

(Insert equation here)

Conversely, possessing credentials that can prove your jurisdiction of residence increases your trust score. This aligns with the basic stance of this paper, which aims to provide investors with the most reliable means to prevent unconscious involvement in illegal transactions, suggesting that wallets unable to prove their jurisdiction of residence should be generally considered high-risk, low-trust-score wallets that should be avoided for transactions.

However, even if a wallet holder's location is revealed through credentials, if there are jurisdictions with absolutely no regulations regarding crypto assets and the manager resides there, it may be impossible to regulate that wallet. In such cases, proving residence does not necessarily increase the trust score.

To address these issues, accountable users who intend to act legally should have common criteria for considering country risk, such as the standards set by FATF for "white countries" and "black countries," when transacting with other accountable wallet users.

- Factor 3: The jurisdictions of your future transaction counterparties

  While this factor must be considered for the reasons stated in the Definition section, it is somewhat incompatible with the standardization of trust score calculation methods. A basic concept in this paper is that individuals should be free to choose which compliance rules they want to adhere to and impose on their counterparties. However, if your trust score calculation method varies depending on the rules adopted by your counterparty, it deviates from the standardization of trust score calculation. Therefore, this factor may be better organized as a factor for determining transaction eligibility rather than a factor for calculating trust scores. This will be a subject for future discussion.

- Factors Not to Consider

  - Sending Crypto Assets to Illegal Wallets or Smart Contracts

In this chapter on the Legitimacy of Wallet Conducts, wallets that exploit crypto assets through fraudulent means and manage such illicitly obtained assets are considered fraudulent wallets. However, there are arguments that acts of sending crypto assets to wallets deemed fraudulent by authorities or sending crypto assets to DApps considered fraudulent by authorities (e.g., Tornado Cash in the United States) should also be penalized as fraudulent acts. This paper takes the stance that such acts should not be penalized.

If sending crypto assets to fraudulent wallets were subject to penalties, investors who wish to send crypto assets to such wallets would do so via instantly prepared wallets. If penalties were imposed on the original wallet for sending crypto assets to fraudulent wallets through instant wallets, it would mean punishing the original wallet based on the actions of a separate wallet (the instant wallet) that may not necessarily be related to the original wallet, lacking rationality.

Moreover, if sending crypto assets to fraudulent wallets leads to a loss of credibility for the sending wallet, there would be an incentive to move other crypto assets to a different wallet before sending to the fraudulent wallet. In this case, penalizing the empty sending wallet would have no effect.

To prevent such behavior, one could consider using credentials to determine if a transfer is to oneself or others, or deem the act of sending crypto assets to non-accountable wallets (i.e., wallets without credentials) as fraudulent. However, forcibly trying to prevent this problem could incentivize the sale of wallets themselves (similar to account selling in traditional finance), which is not a desirable enforcement approach.

The above reasoning does not contradict the main purpose of this framework, which is to avoid inadvertently receiving illegal crypto assets. If your current transaction counterparty has obtained crypto assets through fraudulent means, you should not receive crypto assets from them. However, if it is ensured that the counterparty's crypto assets were not fraudulently obtained, the act of them sending crypto assets to fraudulent wallets in the past does not mean you received fraudulent crypto assets. In other words, the wallets your counterparty sent crypto assets to in the past do not affect the determination of legitimacy.

This principle also applies to DApps and smart contract addresses. Some jurisdictions legally prohibit the use of certain DApps. For example, in the United States, all residents are prohibited from using Tornado Cash. In this case, it is necessary to clarify whether sending crypto assets to Tornado

Cash or receiving crypto assets from Tornado Cash constitutes the illegal act of "using" Tornado Cash. This paper takes the stance that sending crypto assets to Tornado Cash is not illegal, while receiving them is. Making the act of sending illegal would be ineffective for the same reasons as sending through instant wallets, as mentioned above. Furthermore, if a wallet unintentionally receives crypto assets from Tornado Cash, the trust score will initially decrease upon receipt, but the next chapter will describe the procedure for recovering the trust score by abandoning the received crypto assets.

- Subsequent Events after the Transaction

  There is a debate about whether the credibility of Wallet B should be impaired when Wallet A transfers Crypto Asset to Wallet B and Wallet A is later found to have engaged in some wrongdoing and is registered on the watchlist. In conclusion, this paper takes the position that the credibility of Wallet B should not be impaired by subsequent events or facts that come to light later. The handling of some subsequent events is explained below.

  When Crypto Asset is received, the sender's wallet is determined not to be a fraudulent wallet, and after receiving the Crypto Asset from that wallet, the sender's wallet engages in some wrongdoing (subsequent event)

  It is unreasonable for your chained credential to be impaired due to wrongdoing committed by the wallet that sent Crypto Asset to you after sending it to you. It is considered that you have already legitimately provided some goods or services in exchange for this payment, and it would be contrary to the nature of the currency if the payment were to be impaired later.

  When Crypto Asset is received, the sender's wallet is determined not to be a fraudulent wallet, and after receiving Crypto Asset from that wallet, it is discovered that the sender's wallet had engaged in some wrongdoing "in the past" (subsequently revealed fact)

  In this case as well, it cannot necessarily be said that the recipient is at fault. If the chained credential is properly verified at the time of the transaction and the data received does not allow detection of any wrongdoing in the Crypto Asset or the sending wallet, it cannot be said that the recipient's wallet holder was negligent, so having the received Crypto Asset invalidated or other such outcomes as a result would risk creating investors who unwittingly suffer losses due to the introduction of

this method, which could have a significant negative impact on the adoption of the method.

For example, if the counterparty wallet is a malicious investor that is undetectable by credential verification alone and has executed some unfair trade, even if the recipient can prove through attribution credentials that they are a different person from the sender, the recipient knowingly purchased the illegally obtained Crypto Asset from the sender for their own benefit. In this case, the Crypto Asset recipient should be punished even if they can prove through attribution credentials that they are a different person from the sender. However, for this to happen, it must be verifiable that at the time of the transaction, the recipient had the means to confirm that the sender had illegally obtained the Crypto Asset. In other words, the recipient cannot be held accountable if the sender was not on the crypto watchlist or other lists at the time of the Crypto Asset receipt. Considering this, the most important thing is to immediately register the wallet that committed the crime on the crypto watchlist. However, it inevitably takes time to definitively determine a crime as a crime. Therefore, a mechanism for designating suspects, as described in the previous chapter, is necessary. It is also necessary to avoid transacting with wallets on which suspicion has been cast, and wallets that receive Crypto Asset from such wallets will be punished.

10.3.3. Other Considerations

- Privacy of the sender's location

  Regarding the privacy of the sender's location when they do provide proof of jurisdiction, three approaches can be considered:

  Firstly, the sender may not necessarily need to prove their jurisdiction narrowly. Demonstrating residence in one of the multiple jurisdictions designated as "white countries" by FATF could suffice. However, in this case, recipients of crypto assets from such senders would need to prove their absence from the crypto watchlists defined by the authorities of all those jurisdictions in their next transactions. This increases the cost of proof generation for the recipient, and whether this is acceptable for the sake of protecting the sender's privacy is debatable. This approach aligns with the notion that multiple jurisdictions should unite to form a single accountable economy.

  Secondly, the sender could send their jurisdiction information to the recipient as encrypted data, allowing the recipient to generate non-existence proofs using the

encrypted data without learning the actual jurisdiction. While theoretically possible, this approach may raise concerns about increased proof generation costs.

Thirdly, given that a wallet holder's jurisdiction can often be inferred from on-chain data, the sender's jurisdiction could be treated as public information from the outset. In the envisioned world of accountable wallets, for DApps to strictly comply with regulations and provide their services, they may need to choose a single jurisdiction, adhere to its securities laws, and restrict users to residents of that jurisdiction. This implies that if a wallet's usage history of such DApps becomes public through on-chain data, the wallet's jurisdiction of residence also becomes public knowledge. Recognizing this as an unavoidable issue, jurisdiction information could be treated as public.

- Suspicious Transactions

  Suspicious transactions refer to transactions that are not necessarily crimes themselves or cannot be definitively confirmed as crimes at the time of observation, but have a high probability of being conducted to conceal criminal acts or evidence of crimes that has not yet been fully gathered.

  The compliance oracle mechanism is expected to promptly detect wallets involved in illegal activities and share that information. However, it may not function if the time required to detect illegal transactions is shorter than the block time. If the time to detect an illegal transaction is longer than the block time, the wallet involved in the illegal activity can move the proceeds to another wallet before being designated. While it would be ideal to similarly designate the transfer destination wallet, as mentioned earlier, the transfer destination wallet is not necessarily involved in the criminal activity. Therefore, from the recipient's perspective, it is desirable to have a means to avoid transactions that appear to be money laundering attempts, even if the sender's wallet has not been designated as illegal.

  For example, tumbling refers to the act of moving Crypto Asset in a complex manner through multiple wallets. This act itself is not a crime. However, wallets engaging in such activities are considered to be intentionally making it difficult to trace the flow of funds. Therefore, such acts should be designated as suspicious transactions. Wallets with high compliance standards are expected to be configured to avoid transactions with wallets that have recently engaged in such transactions. This should be designed so that market principles work in this way, rather than relying on users' goodwill.

- Incorporating Tax Compliance into Accountable Wallets

Ensuring comprehensive taxation of investment activities conducted through wallets with unknown managers is an immense challenge. Consequently, investors seeking to evade taxes may be incentivized to engage in investment behaviors using anonymous self-custodial wallets. A straightforward solution to prevent this is to require wallets to include information that enables the identification of their managers. However, simplistic approaches risk severe breaches of personal information.

From the perspective of excluding so-called illegal wallets from the legitimate economy, as proposed in this methodology, the judgment of whether to exclude a wallet does not necessitate personal information. The only crucial factor is whether the wallet is properly paying taxes, not the individual's identity. The proof and issuance process must be designed to selectively disclose only this specific information.

Furthermore, the taxes to be considered are not limited to capital gains taxes alone. For instance, gift taxes may arise in the context of crypto asset transfers between wallets. The critical issue here is identifying the managers of the two wallets involved. If the wallets are managed by different individuals, the transfer may be subject to gift tax. Conversely, if both wallets are managed by the same individual, the transfer is not subject to gift tax.

The approach to this issue aligns with the broader principle: the essential aspect is proving that the transfer is not subject to gift tax, rather than disclosing who manages the wallets. By employing DIDs or VCs that prove wallet management, combined with zero-knowledge proof techniques, it is possible to demonstrate that the wallets are managed by the same individual without revealing the manager's identity. The issuance of such proofs using zero-knowledge techniques is necessary.

This selective disclosure of tax compliance status, without compromising personal information, is a critical component of the accountable wallet framework. By enabling wallets to prove their legitimacy in terms of tax obligations, while preserving the privacy of their managers, the system incentivizes compliance and facilitates the exclusion of non-compliant wallets from the legitimate economy.

11. Legitimacy of the Crypto Asset Provenances

11.1. Concept

11.1.1. Legitimacy of the Crypto Asset Provenances

- Avoid Transactions with Sanctioned Addresses

  First, in terms of the motivations of criminals, when their wallets are registered on sanction lists or crypto watchlists, legitimate investors and VASPs are expected to avoid directly transacting with these wallets, so the owners of these listed wallets will attempt to transfer the crypto assets to other wallets.

  This means that all investors who intend to act legally must confirm before each transaction that the counterparty has not received any crypto assets from the wallets registered on the sanction list.

- Legitimacy of Crypto Asset Acquisition Routes

  To reduce the risk of being involved in crime, as proposed in Chapters 9 and 10, it is necessary to avoid transacting with wallets managed by illegal Wallet Holders or wallets that have engaged in illegal activities. As a countermeasure, we explained the use of credential technology as a method to prove various information about the owner.

  However, these measures alone are not sufficient. It is necessary to verify whether the counterparty is applying these rules in the past transactions. In other words, if the counterparty has transacted with wallets managed by illegal Wallet Holders or wallets that have engaged in illegal activities in the past, there is a possibility of unintentionally being involved in illegal crypto asset laundering through that wallet.

- Need to verify the legitimacy of indirect counterparties

  When conducting a crypto asset transaction, in order not to be involved in fraud, it is necessary to confirm that the crypto assets held by the counterparty have not been obtained through illegal means. This is the same for the counterparty, and you need to prove to the counterparty that the crypto assets you currently hold have been obtained through legal means.

  To fully prove this, proving that all the direct transaction partners have been legitimate is not enough. It is also necessary to prove that the counterparty's transaction partners, i.e., the indirect transaction partners, are also legitimate.

  If the wallet unintentionally receives crypto assets sent from a wallet registered on the sanction list, the method for dealing with it will be explained later.

- Accountability for the past transactions

  In a world where the accountable wallet system is properly established, it is unlikely that criminals will commit crimes using wallets with attribution credentials.

Therefore, crimes will mainly be committed by wallets that do not have attribution credentials.

As mentioned earlier, investors who intend to act legally are expected to transact only with investors who have attribution credentials. However, the example in this section shows that even if your direct transaction partner has an attribution credential, it is meaningless if the transaction partner has received crypto assets from a wallet that does not have an attribution credential. To solve this problem, the introduction of a mechanism where a wallet becomes non-accountable at the moment it transacts with a non-accountable wallet is necessary.

- Case Study

(Insert Image)

In the above example, Wallet B became non-accountable because it transacted with the non-accountable Wallet A, resulting in inadvertently obtaining crypto assets from Wallet A, which had actually obtained them illegally. In this case, even if Wallet A was not designated on the sanction list at the time of transaction with Wallet B, Wallet B should bear responsibility, as discussed in the previous section. However, Wallet C should not bear responsibility even if Wallet B, the transaction partner at the time, did not have a track record of transacting with wallets on the sanction list before the transaction. Otherwise, money laundering could be achieved by preparing two accountable wallets, so the conclusion is that Wallet C should not conduct transactions with Wallet B, even if the transaction partner had no track record of transacting with wallets on the sanction list at the time of the transaction, if it has a track record of transacting with non-accountable wallets.

11.1.2. Unintentional receipt of illicit crypto asset

The question arises as to whether ALL crypto assets managed by a self-custodial wallet should be considered illicit funds if that wallet has received illicitly obtained crypto assets. In other words, this is the case where legally obtained crypto assets and illicitly obtained crypto assets coexist in a single address.

The conclusion is that they should not be considered as such. It would lack legitimacy if all of a well-intentioned investor's assets were to be rejected by VASPs because they received a small amount of crypto assets from a wallet on a sanction list as payment for legitimate business transactions. This also serves as a countermeasure to the case

introduced in the background section, where money launderers randomly distributed USDC to unrelated wallets to obstruct the investigation. The mere receipt of illicit crypto assets by an external wallet does not immediately render the wallet itself illicit.

However, the basic concept of this paper is that honest investors must be diligent to prevent malicious investors from stopping money laundering and other illicit transactions. Therefore, if an honest investor managing a wallet receives illicit crypto assets as defined in the previous two paragraphs and knows that they were illicitly obtained but fails to take appropriate measures such as reporting to the authorities or returning them, that wallet will also be considered to have been involved in illicit activities, and some or all of the crypto assets managed by that wallet will be deemed illicit.

Since crypto assets are fundamentally fungible, there needs to be a mechanism in place for each address to cryptographically and tamper-proof record how much of the currently held crypto assets were legally obtained and how much lack proof of legal acquisition. Furthermore, this paper assumes that non-VASP investors do not have access to sanction lists. This is closely related to the discussion of how to handle cases where illicit crypto assets are sent against one's will and will be discussed in the section about the procedure.

11.1.3.Chained Credentials

- Concept of the Chained Credentials

  This is because if the transaction partner is a dishonest investor, they may try to transact with you after passing through multiple wallets to obscure the fact that they obtained the crypto assets through some illegal means. This detour can be done without limit, so you would need to check an unlimited number of indirect wallets when transacting, which is obviously not realistic.

  Chained credentials proposed in this section are a technology to solve above problem. In this section, we introduce "credentials that prove that the crypto assets currently managed in the wallet have been obtained through legal means.

  Chained credentials are a technology that issues credential presentations proving that for a certain recent period, only transactions with wallets that have not engaged in fraud, including indirect transactions (i.e., the transaction partner's transaction partners), have been conducted.

  If these credentials can prove that all the crypto assets currently held by the wallet have been acquired through legitimate means, by verifying each other's possession of such credentials, transactions can be conducted with peace of

mind. If a wallet holding this credential means that the wallet has only transacted with wallets holding similar credentials, then the credential holder can inductively prove that all transaction routes through which the currently held crypto assets were acquired were legal. In other words, if you have this credential, your transaction partner does not need to scrutinize all your past transactions using on-chain data to confirm that the crypto assets you hold have been legally obtained.

Hereafter, these credentials for explaining the acquisition routes of held crypto assets to external parties will be referred to as chained credentials to distinguish them from other credentials.

- For efficient screening checks on deposit

  When any self-custody wallet tries to deposit crypto assets to a VASP, the VASP needs to confirm from a compliance perspective that the crypto assets held by the wallet have been obtained legally. This involves not only the verification work based on the travel rule but also investigating the circulation routes of multiple layers of the sender's wallet, which is a very costly investigation for the VASP. Also, failure to detect fraudulent transactions in this process and being pointed out by the authorities or others is also a business risk for them.

  Conversely, receiving crypto asset deposits from wallets that can reliably prove their legitimacy using credentials is good for VASPs both in terms of cost and business risk. Therefore, it would be commercially affirmed to financially favor these deposits and charge deposit fees for deposits that are not. Additionally, crypto assets for which legality cannot be proven may take time to be reflected in the customer's account balance as it takes time to investigate their legality. These factors are expected to act as penalties for those who do not possess chained credentials, which in turn is expected to serve as an incentive to possess credentials.

11.1.4. Partially Accountable Wallets

- Coexistence of Accountable and Non-Accountable Crypto Assets in a one wallet

  How much of the crypto assets currently held by any wallet were received from accountable wallets and how much were received from non-accountable wallets remains as tamper-proof data through credentials and on-chain data. Therefore, it is desirable to control the wallet so that it has the right to send only the amount for which legitimacy can be proven by credentials as legitimate crypto assets to the outside with credentials attached. However, this is a control as an accountable wallet, and as a crypto asset wallet, it is not possible to restrict the

external sending of crypto assets for which legitimacy cannot be proven. In that case, if an accountable wallet sends more than the amount that can be legally sent externally, the excess amount cannot be accompanied by correct credentials and is assumed to be a non-accountable fund transfer. Under such an arrangement, even if non-accountable crypto assets are unintentionally sent from outside, the sending of existing accountable crypto assets is not hindered before proper handling of those crypto assets.

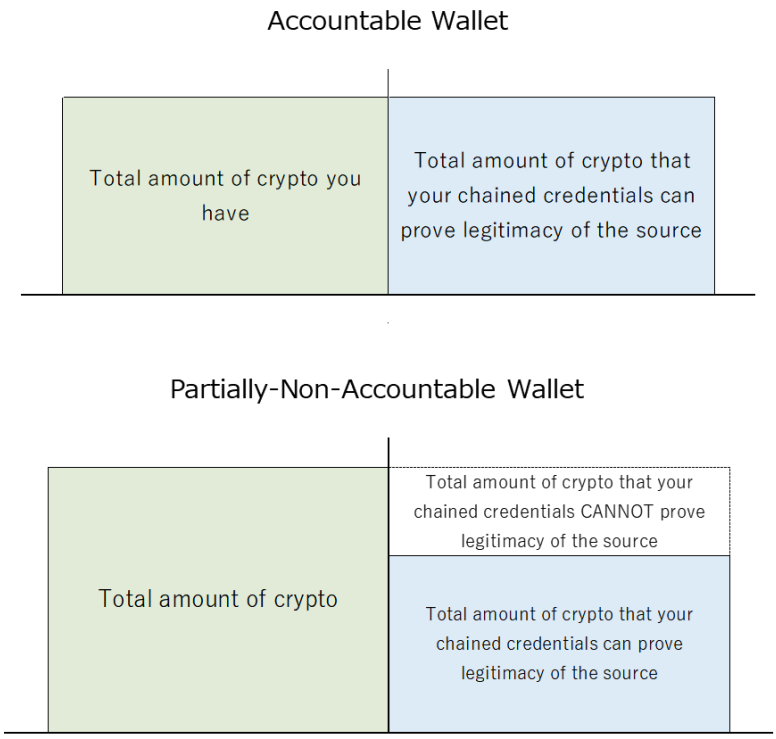


Figure 25

11.2. Requirements

11.2.1. Two Types of Chained Credentials

As mentioned earlier, chained credentials serve as a tamper-proof explanation of the acquisition routes for the crypto assets held by the wallet.

Based on this, any chained credential has chained credentials that were referenced when generating that chained credential, but tracing back the referenced chained credentials will eventually lead to the original chained credential. In other words, chained credentials can be broadly classified into two types: original chained credentials and inherited chained credentials.

- Original Chained Credentials

  The question of who should first issue and hold the original chained credentials is also a problem of the adoption of the method itself. This is because, realistically, at the start of the method, all wallets already hold crypto assets, and there are no chained credentials for those crypto assets. Therefore, at first, there will inevitably be a procedure to issue chained credentials for wallets that already hold crypto assets.

  Consideration is needed regarding which entity will issue such credentials and the procedures involved. A credential issuer-like organization specially guarantees the legitimacy of the crypto assets held by the self-custody wallet. VASPs issue chained credentials as Trust Anchors. (To be discussed)

- Inherited Chained Credentials

  For inherited credentials, clear standardization is needed for how the information from the inherited credentials is incorporated and the computational processing involved in generating the new credentials. A simple example of a Crypto Asset transfer flow and the corresponding inheritance relationship of credentials is shown below.

  In the above example, before sending to Ted, Alice has 1 BTC in her wallet that she received from Bob, an accountable investor. Before Alice sends the 1 BTC to Ted, she sends the chained credential (strictly speaking, the credential presentation generated from that credential) to Ted. The chained credential sent to Ted includes information that Alice legitimately acquired that 1 BTC, but the accuracy of this information is verified by Ted. The verification of the correctness of this credential is done using on-chain data and Bob's public key, which issued the chained credential to Alice. Therefore, chained credentials need to be sent before the transaction. The recipient of the chained credential has the obligation to verify it, which requires confirming that the chained credential matches the chained credential it references and the on-chain data.

11.2.2.Exceptional Events

As mentioned above, if a wallet receives crypto assets from a wallet designated on the sanction list, it is basically either designated on the sanction list itself or treated by other legitimate investors as if it were designated on the sanction list. However, there are a few exceptions to this. In these exceptional cases, even if crypto assets are received from the sanction list, the wallet should not be designated on the sanction list and be reducing its own trust scores.

In simple terms, the criterion for judging whether an exception is recognized is whether the crypto asset recipient was at fault. If not, the recipient should not be designated on the sanction list. In that case, since some of the goods or services are deemed to have already been provided at the time of receiving the crypto assets, the received crypto assets should not be obligated to be returned or disposed of.

- Exception 1 - Subsequent Events

  The first exception for recipients is that if the recipient unintentionally receives crypto assets from a wallet that gets registered on the sanction list due to actions taken by the sender's wallet after sending the crypto assets, the recipient should not be registered on the sanction list for receiving the crypto assets.

- Exception 2 - Subsequently Revealed Facts

  If the sender had engaged in some wrongdoing before the transaction but the sender's wallet was not registered on the sanction list at the time of the transaction, it is a difficult question whether the recipient should be registered on the sanction list or treated as if they were registered for receiving crypto assets from that wallet.

  For example, in the case of a commercial transaction, if the seller of goods confirms that the buyer is not listed on the sanction list before conducting the transaction, even if the crypto assets used for payment were actually obtained illegally, the recipient had no way of knowing that fact. In this case, it would be unreasonable for the sales proceeds received in crypto assets to become non-convertible to legal tender or other assets. This would mean that even a diligent legitimate investor who confirms in advance that the transaction partner is not on the sanction list could end up on the sanction list.

  However, there are also issues with always deeming the recipient innocent in such cases. If the recipient is considered innocent in these cases, the wallet that illegally obtained the crypto assets has a strong incentive to immediately transfer the illegally obtained crypto assets to another wallet before being designated on the sanction list. This is because if such exceptions exist, assuming that the sanction list designation takes longer than the block generation time, the wallet that illegally obtained the crypto assets can simply evacuate the assets to an empty wallet immediately after completing the illegal act. In this case, the empty wallet can only be seen as having received crypto assets from a wallet that was not designated on the sanction list at the time of receipt, so it cannot be designated on the sanction list. Of course, this is clearly an evacuation destination for illegal funds and could be designated on the sanction list. However, that would be a judgment based on human intuition that it is "obvious,"

which is qualitative and problematic.

Moreover, what if the evacuation destination is not an empty wallet but a wallet that has been transacted through DeFi? Even if the DeFi is configured to restrict access from wallets designated on the sanction list based on this proposal, if it is accessed immediately after the illegal act is committed, it can be accessed at the time because it is not yet designated on the sanction list, and legitimate investors using that DeFi will end up transacting with that wallet. In this case, there is a possibility that among the legitimate investors, there are numerous wallets prepared by the manager of that wallet, and if those wallets are unconditionally acquitted, money laundering will effectively be established.

In other words, regardless of the route, if such exceptions are unconditionally applied, the evacuation destination of the funds can escape sanction list designation, and the sending wallet is already empty, resulting in a situation where the illegally obtained crypto assets are managed by a wallet that is not designated on the sanction list.

Therefore, in this case, it is concluded that the fund recipient cannot be unconditionally acquitted.

So how should the culpability of the recipient be determined? It should be judged based on whether the recipient is related to the sender. Attribution credentials can be used to prove that they are not related parties.

- Exception 3 - Statute of Limitations

  The illegality of transactions prior to a certain period is not questioned?

  (This also helps prevent infinite credential accumulation.)

  (To be discussed)

11.2.3. Technical Requirements of the Credentials

This requirement is in addition to the technical requirements for credentials stated in Section 9.

- (Multiple Credentials) Inheritance

  The newly generated credentials need to incorporate information from the previously referenced credentials. If any wallet unintentionally receives crypto assets from a wallet that did not have the correct chained credentials in past transactions, the credentials are designed so that a new correct chained credential cannot be generated, preventing the use of those crypto assets to

transact with legitimate investors. Chained credentials are fixed to the individual and designed to be non-transferable. This chapter describes the requirements and design of these credentials.

From this aspect of chaining, it is designed to become a chain of trust through the chaining of credentials. It resembles a blockchain in terms of chaining, but the difference is that in a blockchain, each block is verified by third-party verifiers, while in chained credentials, the recipient of the credential becomes the verifier. The verifier who fails to conduct proper verification and becomes involved in fraudulent transactions will have their trust impaired by that transaction, and their wallet will be more likely to be judged as fraudulent by other wallets, resulting in various financial disadvantages. This is designed to encourage verifiers to conduct appropriate verification.

- Protecting Transaction Privacy

  Chained credentials themselves must also be privacy-preserving. Therefore, regarding information about past transactions and acquisition routes of currently held cryptocurrencies, no more information should be disclosed than is publicly available in on-chain data.

11.2.4.Compatibility

- Compatibility with the Privacy Pools

  While privacy may facilitate crime, it is also an important technology. Today, Bitcoin can be said to have virtually no anonymity. In light of this, blockchain technologies that enable the sending and receiving of crypto assets while obfuscating information such as the transacting parties and the transaction amounts on-chain, using zero-knowledge proof techniques like ZK-SNARK, have become prevalent in recent years.

  The crucial point here is to be able to prove one's innocence to others or authorities while obfuscating the transacting parties and transaction amounts.

  In the paper "Blockchain Privacy and Regulatory Compliance: Towards a Practical Equilibrium, SSRN, 2023" by Vitalik Buterin, Jacob Illum, Matthias Nadler, Fabian Schar and Ameen Soleimani, the idea of privacy pools is proposed. This idea is that this method reconciles compliance and privacy of Crypto Asset transactions to legally use mixing protocols. With this, legitimate users can mix their crypto assets separately from those associated with wallets of users on sanction lists or malicious users. This allows legitimate users to avoid mixing crypto assets with illegitimate users. And legitimate user addresses that

re-acquire crypto assets after mixing them only with legitimate users and designated sources can receive membership proofs as evidence of that.

One of the unresolved challenges highlighted in this paper is how to form groups of legitimate users (association sets). These need to be set in a fair manner, but with conventional methods, basically only a centralized organization can designate them. However, the accountable wallets proposed in this paper are considered usable for forming association sets.

In the example above, accountable wallets are used to form Association Set 1 among those who can prove their legitimacy, and crypto assets are mixed within that set. This allows wallets belonging to this set to mix crypto assets and protect the privacy of transactions without assisting money laundering by illegal entities. It serves as a method to form groups (association sets) formed by legitimate investors in a more democratic way that is not centralized, which was identified as a challenge in the paper proposing privacy pools. The membership proof obtained after mixing corresponds to the chained credential in this paper. In actual design, it needs to be rigorously designed so that only those who have mixed with legitimate entities can obtain chained credentials that prove it. Basically, since the mixing protocol itself is also nothing more than a single address as a smart contract address, the mixing protocol cannot issue more chained credentials than it has received, so as long as the chained credentials are properly designed, it should not be a problem.

As of the time of writing, this framework does not conform to blockchains like Zcash and Monero, where the blockchain itself natively conducts anonymous transactions. This is because chained credentials, as mentioned earlier, need to refer to actual transaction data recorded in on-chain data in the process of issuance and verification, and that processing cannot be executed in Zcash or Monero. If one really wants to use accountable wallets in these blockchain transactions, it is necessary to fork the chain and control it so that only those who can prove their legitimacy as accountable wallets can hold the coin in question. While theoretically possible, these coins are designed with anonymity as the highest priority, and although accountable wallets are designed with privacy in mind, they have the potential to disclose more personal information than wallets that do not have any credentials at all, so the ideas are incompatible, and it is unlikely that such usage will become widespread.

The current powerful protocol for proving legitimacy is the travel rule protocol, but this protocol only covers exchanges between VASPs and has major concerns about personal information. If this methodology is established, it will become a protocol with higher anonymity than the travel rule, allowing one to prove one's

innocence without disclosing unnecessary personal information to the other party.

- Compatibility with Hierarchical Deterministic Wallets

  Full compatibility with Bitcoin, which is considered to be the most widely used crypto asset today, is an essential requirement for the adoption of this method. Bitcoin has a feature called hierarchical deterministic wallets. In Bitcoin, for users using self-custody wallets, the receiving addresses for Bitcoin are disposable. When an address is used to receive Bitcoin, a new address is generated and used. These disposable addresses are managed by a single master secret key. This is also called an extended private key. In contrast, there is an extended public key, which can be used to know the balances of all different addresses. Generally, for privacy protection, this key is a public key but is not made public.

  In other words, when the transaction partner is using a hierarchical deterministic wallet, there may be cases where the direct transaction partner's wallet does not have credentials. Therefore, this method needs to be designed to accommodate this, so that if the wallet is of the hierarchical deterministic wallet type and the parent wallet has the correct credentials, receiving crypto assets from that wallet is not a problem even if the child wallet itself does not possess credentials.

11.3. Procedure

11.3.1. Issuance Procedure Example 1

- Proof of Never Having Received Crypto Assets from Wallets Registered as Sanctioned Entities or on Crypto Asset Watchlist

  Wallet Holders need to prove that all senders of crypto assets to them are not authorized entities and that their wallets are not on the Crypto Asset watchlist. Specifically, they need to prove that the senders had Proof 1 and Proof 3 at the time of the transaction.

  This page focuses on the latter, proving that crypto assets have never been received from wallets registered on the Crypto Asset watchlist. Alice must prove that the addresses of all senders of transactions reaching her are not on the watchlist. Similar to Proof 3, for each transaction, a non-membership proof needs to be generated for all sender wallets to verify that they are not registered on the watchlist. On-chain data accurately records all transactions related to Alice. However, due to its size, it is unrealistic to directly use this vast amount of data to generate non-membership proofs. Solutions include converting this data into a more manageable format such as Merkle tree data. In that case, a further

challenge is to prove that the Merkle tree contains all transactions sent to Alice. To efficiently create a Merkle tree without the risk of tampering, a proof generation protocol specialized for each blockchain is required.

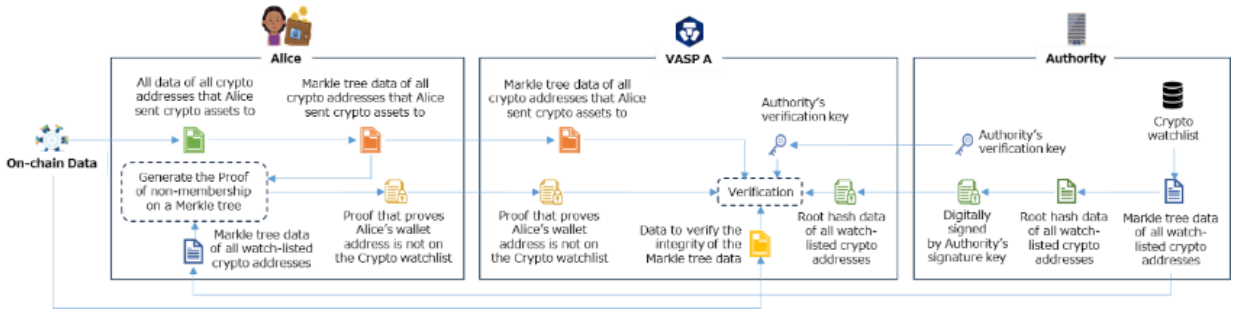


Figure 26

11.3.2. Issuance Procedure Example 1

- Proof of Never Having Indirectly Received Crypto Assets from Wallets Registered as Authorized Entities or on Crypto Asset Watchlist

  Wallet Holders need to prove that all wallets through which the crypto assets passed before reaching them were not managed by authorized entities and were not on the Crypto Asset watchlist.

  Specifically, Wallet Holders need to prove that the senders had Proof 4 and 5 at the time of the transaction. This allows for inductive proof of the legitimacy of the origin.

  Issuing Proof 5 requires nesting of Proofs 4 and 5 received in previous transactions, but technical challenges and options to solve them exist.

- Option 1: Nesting Zero-Knowledge Proofs Using Zero-Knowledge Proof Technology

  Issuing Proofs 4 and 5 requires nesting of ZKPs, which is not technically trivial.

  If all commitment data is available, it is theoretically feasible. Verification requires many commitments and verification keys, but it may become operationally unrealistic.

- Option 2: A Trusted Third Party Takes Charge of Issuing Proof 5

  A potential solution involves a trusted third party, such as a credential provider (CP), that can obtain data from Proofs 4 and 5 and issue a new nested Proof 5.

  This process relies on the trustworthiness of the CP, but the overall

trustworthiness of the proof structure does not diminish since the trustworthiness of the proofs already depends on the CP.

It is important to design the protocol so that the CP does not unnecessarily obtain data or arbitrarily refuse to issue a specific proof, infringing on the wallet's ability to pay. A system that keeps the content of the proof and the identity of the requester anonymous would help mitigate these risks and ensure that requests are not arbitrarily denied.

- Option 3: Using Blockchain to Issue Proofs as Soulbound Tokens

  The unique characteristic of Proof 5, similar to the features of Soulbound Tokens (SBTs), theoretically suggests that the blockchain could assume the role of the CP through smart contracts.

  However, this approach raises concerns about its feasibility due to the significant increase in transaction gas costs. Further research and discussion are needed to find a viable solution in this aspect.

11.3.3. Unintentional Receipt from Illicit Wallets

- Issues

  Currently, we have not been able to establish the correct way to handle cases where crypto assets from fraudulent wallets or crypto assets that we do not recognize are sent to our wallets. If unrecognized crypto assets arrive at one's own self-custody wallet, there is a possibility that they were sent by criminals, so knowingly using them could be considered a transfer of criminal proceeds. However, most crypto assets and standard addresses cannot refuse receipt, and if they are held or used as is, there is a risk of being considered to have profited from fraudulent transactions. However, those who frequently conduct crypto asset transactions using self-custody wallets may also unintentionally use funds they do not recognize. Furthermore, since crypto assets are basically fungible, when crypto assets are sent from outside, there is a risk that they cannot be separated from the crypto assets that one originally held.

  However, it is unreasonable to impose penalties on recipients who unintentionally receive illegal crypto assets. However, it is also difficult to distinguish the recipient's intent based solely on on-chain data. When any user's wallet receives crypto assets from an address designated on the sanction list, there are three possible interpretation patterns regarding the presence or absence of the recipient's fault. Depending on the interpretation pattern, the position of this paper on how to determine its illegality is stated.

- Pattern 1: In Case of Good Faith and No Fault

  In this pattern, the recipient is considered to have received crypto assets from a wallet registered on the sanction list without any corresponding transaction and without any consent at all. A concrete example is the case of the diffusion of USDC by money launderers using Tornado Cash, which was described in the previous chapters. This is a good example that a wallet that received fraudulent crypto assets should not necessarily be regarded as a wallet involved in fraudulent transactions. The act of scattering fraudulent tokens to countless wallets regardless of the recipient's intentions, known as dusting, is also a good example. This is due to the nature of crypto assets being basically impossible to refuse receipt.

  However, in this case, the recipient of these crypto assets should not hesitate to burn the crypto assets or transfer them to an address designated by the authorities. Therefore, the only way for the recipient to prove their own good faith and lack of fault is to dispose of the crypto assets received unintentionally from addresses designated on the sanction list in some way and prove that they have been disposed of. In this method, it is assumed that the crypto assets will be transferred to an address designated by the authorities as a method of disposal, and a credential proving this will be issued to the wallet by the authorities. This will be discussed in more detail later.

- Pattern 2: In Case of Good Faith with Fault

  In this pattern, it is assumed that the recipient has received crypto assets from a money launderer due to the recipient's fault, although they have no involvement with the money launderer. The fault here refers to transacting with a fraudulent wallet without taking appropriate measures despite having the means to verify the legitimacy of the transaction partner. For example, when receiving crypto assets as a means of payment when providing some goods or services, it is conceivable that the crypto assets are received from the payer's wallet without confirming that it is registered on the watchlist. Due to this fault, the recipient of the crypto assets, who is the provider of goods or services, unintentionally becomes complicit in money laundering. Also, according to the definition of accountable wallets so far, along with this transaction, the wallet of the provider of goods or services, as a wallet that has received crypto assets from a watchlist-designated wallet, becomes unable to prove the legitimacy of the crypto assets it holds to others. Therefore, in this case as well, the only way for the recipient's wallet to maintain its legitimacy is to dispose of the crypto assets received from addresses designated on the sanction list in some way and prove that they have been disposed of. However, in this case, since the manager of the

wallet has already provided some goods or services, disposing of the crypto assets received as payment for them will result in a loss.

There may be objections to this argument. This is because in normal commercial transactions, the provider of goods or services is not obligated to confirm the legitimacy of the payer's funds up to the source of the funds. However, when it comes to crypto assets, due to their high transferability and self-sovereignty, if all recipients of crypto assets are considered innocent as long as they are acting in good faith, it would become impossible to stop money laundering. For example, suppose there is a wallet that has acquired crypto assets illegally, and someone has entered into a contract to purchase crypto assets from this wallet with money. In that case, it is impossible to determine from on-chain data alone whether the sending of crypto assets is based on a legitimate commercial transaction (i.e., in good faith) or whether the recipient is intentionally trying to acquire illegally obtained crypto assets while knowing that they are fraudulent crypto assets (i.e., in bad faith). The position of this paper is that, since it takes the stance that one is responsible for proving one's own legitimacy, if one wants to maintain one's legitimacy, one should have confirmed the legitimacy of the counterparty's payment at the time of the transaction prior to the commercial transaction or acquisition of crypto assets.

It should be noted that in various commercial transactions, payment is often made after the fact, so problems may arise. Additional discussion more in line with reality is needed regarding exceptions for small transactions and mechanisms for credit guarantee transactions such as credit cards to deal with this problem.

- Pattern 3: In Case of Bad Faith

  In this pattern, it is assumed that the recipient of the crypto assets intentionally receives crypto assets from a wallet registered on the watchlist. For example, those who have acquired crypto assets illegally may engage in an act called tumbling, where they pass the assets through multiple wallets in a complex manner to obscure the route in order to obstruct the authorities' investigation. In this case, since all the wallets prepared for this purpose are owned by the person who acquired the crypto assets illegally, the first case to be considered is where the wallet holding the illegally acquired crypto assets and the one receiving the crypto assets from it are the same person. In other words, proving that one is not the same person is the primary means of proving that one has no relationship with the sender wallet that committed the crime, which has been discussed up to the previous section. However, even if there is no relationship, there are cases where crypto assets are intentionally purchased from criminals with malicious

intent. For example, there may be cases where one is intentionally involved in transactions to purchase illegally obtained crypto assets at a discount through the dark web. In this case, even if it can be proven through attribution credentials or other means that the sender and recipient of the crypto assets are different individuals, the recipient knowingly purchased the crypto assets that were illegally obtained for their own benefit through the dark web or other means. In this case, the recipient of the crypto assets should be punished even if they can prove through attribution credentials that they are a different person from the sender. However, for this to happen, it must be verifiable that at the time of the transaction, the recipient had the means to confirm that the sender had illegally obtained the crypto assets. In short, if the sender was not registered on the crypto watchlist or other lists at the time of receiving the crypto assets, the recipient's guilt cannot be questioned. Considering this, the most important thing is to immediately register the wallet that committed the crime on the crypto watchlist. However, it inevitably takes time to definitively confirm a crime as a crime. Therefore, a mechanism for designating suspects, as described in the previous chapter, is necessary. It is also necessary not to transact with wallets on which suspicion has been cast, and wallets that receive crypto assets from such wallets will be punished.

- Criteria for Illegality

  From a legal perspective, in many jurisdictions, the cases in Pattern 2 would often be considered legally innocent. However, considering that this method is a way to prove one's legitimacy in a complete form, based on credentials, on-chain data, and sanction list information, without any room for discretion and mechanically, Pattern 2 is a transaction that cannot fully prove legitimacy. In other words, considering the limitations of the data accessible to us for determining the legitimacy of transactions, when a recipient receives illegal funds, it is impossible to determine from on-chain data whether the act was in good faith or bad faith.

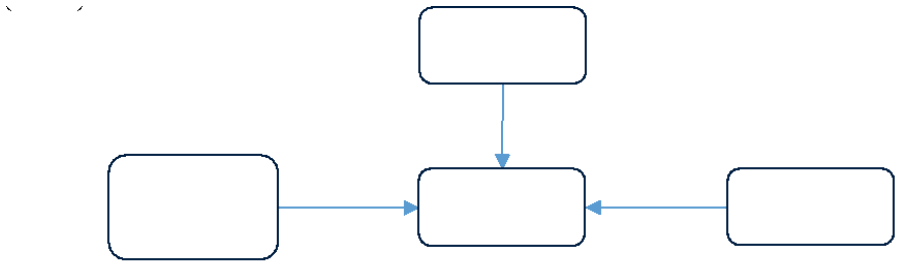
  The position of this paper is that even if Wallet Holders act in good faith, if their actions are negligent, the Crypto Asset received by the wallet from other fraudulent wallets is not permitted to be converted into fiat currency or other assets through VASPs or other means. In other words, the distinction between good faith and bad faith is irrelevant to the determination of penalties. Without penalties for negligent acts, it is impossible to encourage well-intentioned investors to become careful investors, even if they act in good faith. If a well-intentioned investor carelessly transacts with a money launderer, it becomes a weak point, and the efforts of VASPs to prevent the inflow of illegal crypto assets become meaningless. Legal penalties for transactions with fraudulent wallets may vary by jurisdiction, but this paper clearly positions that they should

be determined based on the presence or absence of negligence.

Therefore, in order to prove their innocence, recipients must actively demonstrate that they have absolutely no relationship with this illegal transaction. The methods for this are to relinquish ownership of the illegal crypto assets acquired through carelessness and to take care not to acquire such illegal crypto assets in the first place. If one fails to make this effort and acquires illegal crypto assets, it will be considered involvement in fraudulent activities in this method, and one will not be able to fully prove one's legitimacy. Automatic Processing by Wallet Apps

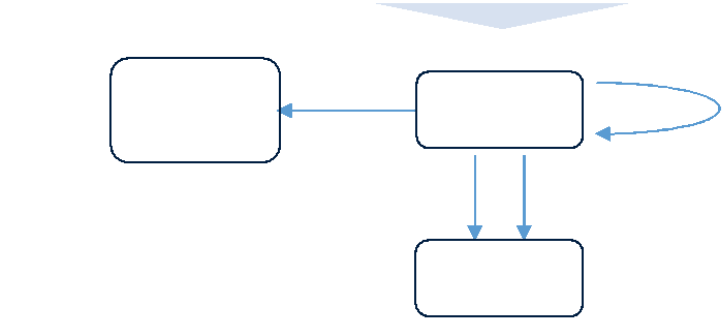
Wallet applications should automatically detect illegal crypto assets sent to the wallet and execute actions such as automatically transferring them to the authorities' tipping address based on user settings. If such actions are not taken, there is a risk that the wallet will become unavailable for use at unintended timings.

It should be noted that the wallet's trust score, which will be discussed later, depends on the percentage of assets received with chained credentials. Therefore, it is important to take appropriate actions for illegal assets (i.e., a substantial amount without chained credentials) that are unintentionally sent and improve this score. Failure to take such measures risks temporary restrictions on transactions with VASPs and other accountable wallets.



BTC UTXOs	Chained Credentials UTXOs	Issuer of Chained Credential
0.8 BTC	Chained Credential for 0.8 BTC	from Accountable wallet B
0.5 BTC	Chained Credential for 0.5 BTC	from Accountable wallet D
0.6 BTC	No Chained Credentials for 0.6 BTC	from Non-Accountable wallet C

1.9 BTC in total in a wallet A



BTC UTXOs	Chained Credentials UTXOs	
0.8 BTC	Chained Credential for 0.8 BTC	Has been sent to Wallet E
0.2 BTC	Chained Credential for 0.2 BTC	Has been sent to Wallet E
0.3 BTC	Chained Credential for 0.3 BTC	from Wallet A (itself)
0.6 BTC	No Chained Credentials for 0.6 BTC	Returned to Non-Accountable wallet C

0.3 BTC in total in a wallet A

Figure 27

- Options for Relinquishing Ownership of Fraudulent Crypto Assets

  - Burning Crypto Assets

    Burning fraudulent crypto assets or crypto assets suspected of being fraudulent is not a recommended method in this paper, because if it is later found that the crypto assets should have been received after all, it will be irreversible.

  - Sending Crypto Assets Back

    Sending crypto assets back may be regarded as sending crypto assets to criminals, but as mentioned earlier, sending crypto assets to criminals is not permitted by law or social norms, so it is a method that requires some legal consideration. However, it is possible to arrange that it is not an act that affects credit in any way in this method.

As for gas fees, they can be deducted from the crypto assets in question and sent to ensure that no actual harm is done.

- Donation/Tipping

  It is assumed that the assets will be transferred to an address prepared by the authorities or charitable organizations. This allows for relinquishing ownership while also utilizing the crypto assets for another socially meaningful purpose.

  Since it must also be proven to others in the form of credentials or other means that appropriate measures were taken, the authorities that receive the transfer of fraudulent crypto assets will issue a credential to the wallet as proof of abandoning them. This will be discussed in more detail later.

- Isolation of Crypto Assets

  In VASPs, even when crypto assets are sent from outside to a customer's receiving address, they are not immediately reflected in the customer's account (wallet). The reflection in the customer's account is suspended until a sufficient number of blocks (said to be 6 blocks for Bitcoin) have been accumulated and the compliance review by the VASP is completed.

  Introducing a similar process in self-custody wallets is also an option. That is, introducing a settlement process on the receiving side as a clear acceptance and approval process. This would partially exempt legal responsibility for crypto assets that are unintentionally sent and prevent unintended decreases in trust scores in accountable wallets.

  Methods such as using separate sending and receiving addresses or using HD wallets can be considered for this implementation. It also requires a lot of legal arrangements and is not an easy idea to adopt, but it is one methodology.

- Proof of Appropriate Handling of Opaque Crypto Assets

  If wallet holders unintentionally receive crypto assets from wallets that cannot prove 1-5, they must take appropriate measures such as transferring them to a reporting address.

- Handling of Opaque Crypto Transactions

  If Alice unintentionally receives crypto assets from a self-custody wallet or

protocol flagged on the Crypto Asset watchlist, she must transfer these assets to the authorities. This action is necessary to prove that she has no relationship with the sender and to maintain her compliance status.

Even if the sender's wallet is not registered on the watchlist, crypto assets received from wallets lacking proof of legitimacy should be treated as opaque. This is because these crypto assets may be involved in money laundering activities to maintain the highest standard of legitimacy.

By transferring opaque crypto assets to the authorities, Alice should receive Proof 6, proving that she took appropriate action to dispose of the opaque crypto assets. Alice can use this to avoid issuing non-membership proofs for transactions where she unintentionally received opaque crypto assets.

	On-chain data			Off-chain data	
#	Sender	Receiver	Amount	Crypto watchlist	Legitimacy Proofs
Incoming Transaction 1	Wallet A	Alice	0.1 BTC	No	Yes
Incoming Transaction 2	Wallet B	Alice	0.03 BTC	No	Yes
Incoming Transaction 3	Wallet C	Alice	0.005 BTC	**Yes**	**No**
Incoming Transaction 4	Wallet D	Alice	0.002 BTC	No	**No**

- Alice cannot generate Proof 4 because of the Incoming Transaction 3.
- Alice cannot generate Proof 5 either because the Incoming Transaction 4.

Figure 28

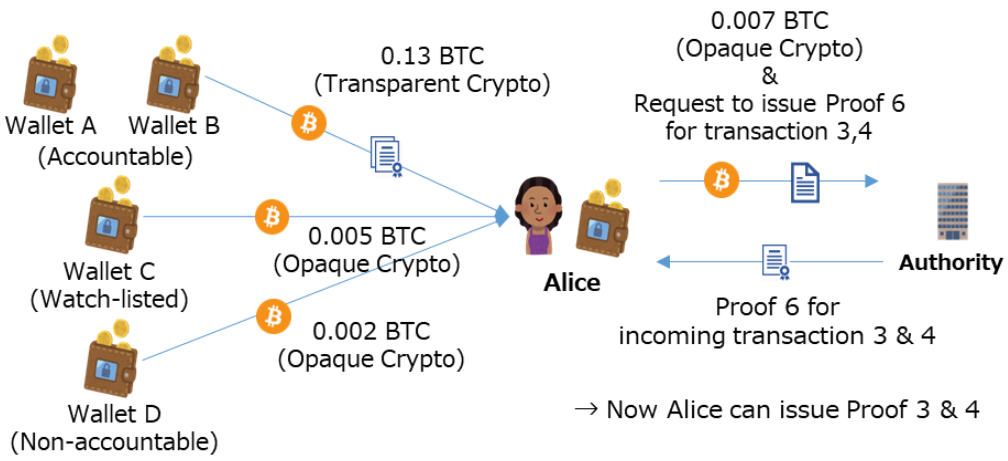


Figure 29

11.3.4. Relationship of Each Proof

An important aspect of our proposal is the mechanism for inheriting proofs across the entire transaction chain. This mechanism allows the legitimacy proven by one prover to prove the legitimacy of the entire transaction chain of that prover. Below is an example of the legitimacy proof chaining mechanism.

- Verification of legitimacy across the entire transaction chain

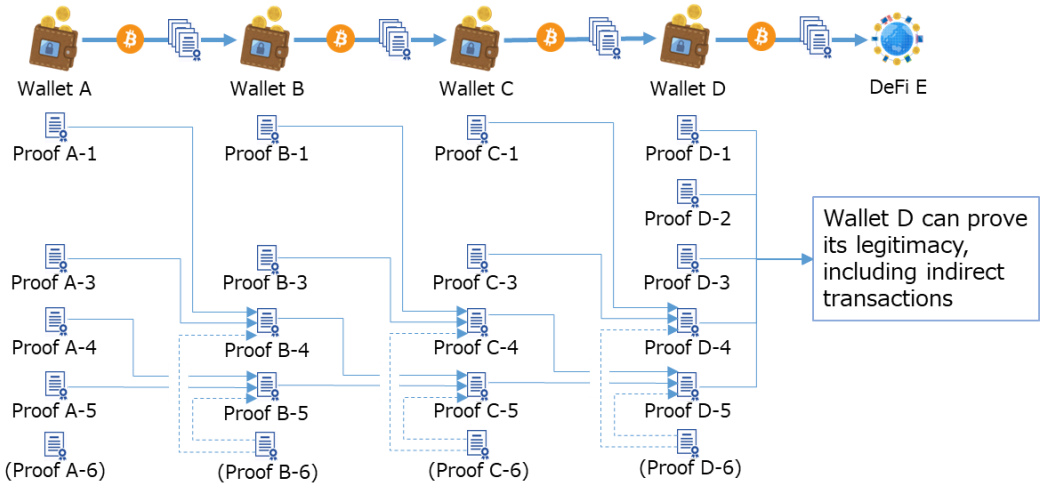


Figure 30

1. Goal: Wallet D proves the legitimacy of all involved wallets (Wallets A - D) to use DeFi E.
2. Step 1: Wallet D establishes the legitimacy of its owner by presenting Proofs D-1, D-2, and D-3.

3. Step 2: Wallet D provides Proof D-4 by receiving Proofs C-1 and C-3 from Wallet C.
4. Step 3: Wallet D provides Proof D-5 by receiving Proofs C-4 and C-5 from Wallet C.
5. Repeat the above steps in order to ensure that Wallets A and B have all the necessary proofs (Proofs X-1, X-3, X-4, and X-5).

11.4. Trust Score of the Crypto Asset Provenances

11.4.1. Concept

Here, a trust score is assigned to a wallet based on the acquisition routes of the crypto assets it currently holds. As explained in the previous chapters, the legitimacy of the senders of the crypto assets currently held by the target wallet is considered, but the legitimacy of the recipients of the crypto assets sent by the target wallet in the past is not considered. This is mainly because the investment behavior of the recipient wallets is outside the scope of responsibility of the investing wallet.

For example, if an accountable wallet directly receives crypto assets only from its own account at a VASP that has obtained a formal license in a jurisdiction that has ratified the travel rule, the wallet is considered to have acquired the crypto assets completely legally, and the reliability of the crypto assets held is 100%.

Also, as mentioned above, receiving crypto assets from wallets with high reliability, i.e., wallets with high trust scores, as proposed so far, should also be designed to positively affect the trust score. Conversely, receiving from non-accountable wallets should be designed to reduce the trust score. In actual implementation, it is considered that the trust score of the credential issuer itself will be further multiplied as a coefficient.

Money launderers may try to intentionally raise their trust scores by unnecessarily sending clean crypto assets from VASPs to their self-custody wallets, but this would be difficult for criminals. This is because if the sent crypto assets are found to include laundered funds, there is a risk of more crypto assets being confiscated by the authorities.

11.4.2. Proposed Formula

The reliability of currently held crypto assets is calculated as the weighted

average of the trust scores of the sources determined by the chained credentials. In the example below, when calculating the reliability of crypto assets currently held by a wallet that receives crypto assets from three wallets with different trust scores, the probability of legitimacy of Wallet D, P(w_3), is calculated as (0.2×100%+0.15×90%+0.1×0%)/(0.2+0.15+0.1) ≒ 74.4%.

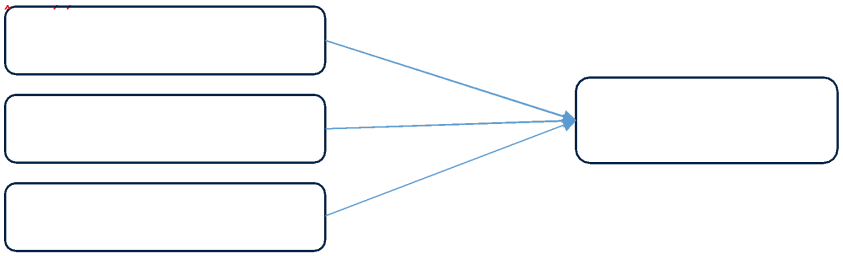


Figure 31

This calculation is expressed in a general formula as follows:

$$P(\overline{Cr}) = \frac{\sum_{k}^{n} C_k TS_k}{\sum_{k}^{n} C_k}$$

C_k =*Amount received kth.*

TS_k =*Trust score of the kth remitter*

- Problem of Weighted Average Between Different Crypto Assets

  If the crypto assets held by the wallet subject to the calculation of the reliability of held crypto assets are of a single type, the above weighted average calculation for deriving the trust score is easy. However, if the wallet holds different types of crypto assets, calculating the weighted average between different crypto assets requires obtaining the market value of the crypto assets. In this case, the process becomes complicated in terms of how to obtain the market value of crypto assets from a reliable source, how to verify it, and which market value to use (at the time of acquisition or at the time of verification). Moreover, if the market value at the time of verification is used, the trust score will constantly fluctuate with future crypto asset prices, which may raise questions about practicality. Since reflecting crypto asset prices in a very timely manner to calculate trust scores is not considered an essential factor of operating the trust score system, a simplified

consideration system should be examined for this point, prioritizing the clarity of the system.

11.5. Further Considerations

11.5.1. Handling of Small Transactions

In the travel rule, in some jurisdictions, there is often a threshold value set for the application of screening checks to be excluded depending on the deposit amount for crypto assets deposited from outside. Regarding this, it is necessary to consider whether a similar exemption is necessary for chained credentials, i.e., whether it is acceptable to receive crypto assets from a party without chained credentials if the received amount is below a certain threshold. The position of this paper is to proceed with the following discussion on the premise that there is no exemption provision. This is because if an exemption is provided, it would be possible to prepare multiple wallets without credentials on the spot and receive crypto assets in a distributed manner from each wallet without exceeding the threshold.

If it is a VASP, if there are multiple deposits below the threshold amount from multiple wallets to a single customer account in the same period, it can be judged as suspicious and the VASP has the authority to stop it against the intentions of the sender and the customer. Therefore, the exemption for small transactions can be affirmed in the travel rule, but in transactions between self-custody wallets, if this exemption is provided, when the manager of the wallet to which the person trying to avoid the application sends is the same person, there is no third party to stop it like a VASP in the travel rule, so the application of this method can be avoided as much as desired. As a countermeasure against this act, even in cases where not only the wallets that directly sent funds to the VASP are examined, but also wallets that sent a total amount above a certain threshold via one wallet are subject to censorship, a flaw arises where the net can be slipped through by using multiple wallets across multiple layers. Therefore, this paper does not provide an exemption for screening checks for small remittances.

11.5.2. Bootstrap Problem

- The bootstrap problem refers to the "chicken and egg" problem of self-hosting environments, with a typical example being how to compile the first compiler when creating a compiler in the programming language that is the target of compilation. It's like "not having clothes to go buy clothes" or "not having glasses to look for glasses."

Credentials face a similar problem. In other words, if your credibility is defined by what kind of credentialed people you have transacted with so far, if no one has credentials, the credibility of credentials cannot be defined.

In this paper, we state that transacting with someone who doesn't have credentials will unconditionally damage your own credentials, but this would only result in imposing a huge constraint on yourself, and no one would use it.

Upon careful consideration, we are beginning to think that it might be okay to go through one or two wallets without credentials. We will solve this problem using the search tree model.

- Dealing with Existing Wallets

  What if the wallet had crypto assets through illegal routes from the beginning? In this case, when issuing credentials, it is necessary to confirm not only the identity of the individual but also the crypto assets held. If the acquisition route is unknown, the basic policy is to refuse issuance. Also, there seem to be various specific issues to consider regarding one wallet being certified at multiple exchanges. Conversely, having multiple VASPs certify a single wallet may be one way to increase the credibility of the wallet. Everything is a chain of trust. In that sense, VASPs may not be different. This means that credentials received from VASPs that accept illegal funds do not lead to credibility.

11.5.3. For the Compliant DeFi

This method, for instance, could be used for fundraising. Fundraising from a large number of small investors is very difficult since KYC cost could easily be higher than the rising, but this method may make it possible. This may eliminate the need for fundraisers who cannot maintain a robust KYC system to raise funds from large financial institutions at high fees.

Compliance is key, especially in the security token economy. In permissionless blockchains, it is difficult to limit investors who can hold tokens. Because of that, many projects are already using permissioned blockchains to meet compliance. However, these are synonymous with recording token holders using timestamp technology[39], and are merely a technology that complicates conventional securities management, and there are doubts about the meaning of using blockchains. This type of platformers often promotes their platform that illiquid products can be sold in smaller lots, but in existing finance, the biggest barrier that illiquid products cannot be sold in small lots is the cost, and it is a completely meaningless solution that goes against this. In order to

39

immediately escape from this unhealthy situation, it is necessary to establish a technology to circulate security tokens on permissionless blockchains while complying with regulations.

Transactions should only be conducted openly on permissionless blockchains, but without the additional information provided by such as an accountable wallet, no one can properly take a risk-based approach to avoid being involved in criminal activity. While the credentials themselves do not disclose personal information on-chain, it would be desirable to have a mechanism where only the issuer of the security token can see the personal information when the security token is held. In this method, we assume that the credentials themselves do not even hold encrypted personal information, so the holder needs to claim it themselves. This requires a mechanism for the holder to safely convey that personal information to the issuer when voting rights need to be exercised or dividends received. Also, in the case of being limited to qualified institutional investors, the information of the holder is often required before purchase, so this needs to be addressed.

12. Conclusion

This paper comprehensively analyzed the factors that distinguish legitimate wallets from illegal wallets. By implementing a unified wallet credibility evaluation method, the trust score encourages investors to prove their legitimacy to avoid transacting with wallets that cannot prove their legitimacy, forming an economy where only verifiably legitimate wallets interact with each other.

Those who cannot prove their legitimacy are forced to transact within a separate economy composed of similarly unverified wallets. As a result, the liquidity available to illegal wallets in the decentralized market is expected to be significantly less than that of legitimate wallets, greatly decreasing the value of their assets. This outcome is expected to function as a deterrent against criminal activity and to effectively serve as a punitive measure within decentralized finance.

Future research challenges include selecting and integrating the various factoral technologies necessary to realize the proposed framework. This includes addressing the technical implementation challenges and investigating the economic principles that emerge during the introduction of the framework. We need to evaluate the potential of this method to limit the liquidity of assets in wallets involved in fraudulent transactions, thereby lowering the value of such illegal assets. Quantifying this effectiveness is essential to provide concrete evidence to regulators and VASPs to support the adoption and recommendation of this method. Furthermore, it is also important to explore how individual investors can economically benefit, for example through preferential

transaction terms, by improving their trust scores through credential ownership. This multifaceted approach underscores the need to comprehensively evaluate the economic and technological aspects of the framework.

- Enhanced Enforceability

  VASPs and self-custody wallet holders faced the challenge of preventing the receipt of illegal crypto assets and proving the legitimacy of crypto assets to transaction partners due to the lack of effective mechanisms.

  Our approach introduces rigorous technical solutions that enable mutual verification of the legitimacy of transaction partners. This method allows VASPs to effectively verify the legitimacy of self-custody wallets, excluding illegal wallets.

- Enhanced Privacy

  Existing methods of verifying the legitimacy of transaction partners, such as the travel rule protocol, require personal information from users.

  Our framework is designed to allow DApps and VASPs to determine whether users are legitimate investors without excessively collecting personal information.

  However, further discussion is needed on whether privacy can be protected even if multiple zero-knowledge proofs are issued.

- Improved Efficiency

  Verifying the legitimacy of transaction partners requires advanced chain analysis techniques or manual collection of transaction details from users, both of which are costly.

  If senders actively prove their legitimacy, these costly investigations can be significantly reduced.

  To promote this framework and foster a more efficient and compliant digital transaction environment, further discussion is needed on how to provide them with incentives to actively prove their legitimacy.

13. Appendix A – References

1. Md. Abdul Hannan, Md. Atik Shahriar, Md Sadek Ferdous, Mohammad Jabed Morshed Chowdhury, Mohammad Shahriar Rahman. A systematic literature review of block-chain-based e-KYC systems. Computing, 105:2089–2118, 2023.

2. Vitalik Buterin, Jacob Illum, Matthias Nadler, Fabian Schar and Ameen Soleimani. Blockchain Privacy and Regulatory Compliance: Towards a Practical Equilibrium, SSRN, 2023.

3. Nigang Sun, Yuanyi Zhang and Yining Liu. A Privacy-Preserving KYC-Compliant Identity Scheme for Accounts on All Public Blockchains. Sustainability, 14-14584, 2022.

4. Vincent Schlatt, Johannes Sedlmeir, Simon Feulner, Nils Urbach. Designing a Frame-work for Digital KYC Processes Built on Blockchain-Based Self-Sovereign Identity. In-formation & Management, 59 (2022) 103553, 2022.

5. Diksha Malhotra, Poonam Saini, Awadhesh Kumar. Singh How Blockchain Can Au-tomate KYC: Systematic Review, Wireless Personal Communications, 122:1987–2021, 2021.

6. Schlatt V, Sedlmeir J, Feulner S, Urbach N. Designing a framework for digital KYC processes built on blockchain-based self-sovereign identity. Information & Management, 103553, 2021.

7. Rajyashree UA, Doulani S, Pareek S. Blockchain-enabled e-KYC system. International Journal of Computer Vision, 137–143, 2019.

8. Khaqqi KN, Sikorski JJ, Hadinoto K, Kraft M, Incorporating seller/buyer reputation-based system in blockchain-enabled emission trading application. Appl Energy, 209:8–19, 2018.

9. Pfitzmann A, Hansen M A terminology for discussing privacy by data minimization: anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management. TU Dresden, 2010.

10. Beardsley EL. Privacy: autonomy and selective disclosure. Privacy & personality, pp 56–70, 2017.

11. TRM Labs. Inside North Korea's Crypto Heists: $200M in Crypto Stolen in 2023; Over $2B in the Last Five Years, August, 2023. https://www.trmlabs.com/post/inside-north-koreas-crypto-heists. Accessed, August, 21, 2023.

12. U.S. Department of the Treasury. Illicit Finance Risk Assessment of Decentralized Fi-nance. https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf, April 2023. Accessed, April, 10, 2023.

13. Ivan Damgård, Chaya Ganesh, Hamidreza Khoshakhlagh, Claudio Orlandi, and Luisa Siniscalchi. Balancing Privacy and Accountability in Blockchain Identity

Management. CT-RSA, pp 552–576, 2021.

14. D.A. Zetzsche, R.P. Buckley, D.W. Arner, M.C. van Ek. Remaining regulatory chal-lenges in digital finance and cryptoassets after MiCA. Study Report requested by the ECON Committee. PE 740.083, 2023.
15. Monetary Authority of Singapore, Project Guardian, June, 2023. https://www.mas.gov.sg/-/media/mas-media-library/development/fintech/project-guardian/project-guardian-open-interoperable-network.pdf. Accessed, August 2, 2023.
16. Michi Kakebayashi, Joseph Beverley. Soulbound Tokens (SBTs) Study Report, Block-chain Governance Initiative Network, BGIN SR 008, 2023.
17. E. Glen Weyl, Puja Ohlhaver, Vitalik Buterin. Decentralized Society: Finding Web3's Soul, SSRN, 2022.
18. Financial Action Task Force. Targeted Update on Implementation of the FATF Stand-ards on Virtual Assets and Virtual Asset Service Providers, June 2023. https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/June2023-Targeted-Update-VA-VASP.pdf.coredownload.inline.pdf. Accessed, July 3, 2023.
19. Bhaskaran K, Ilfrich P, Liffman D, Vecchiola C, Jayachandran P, Kumar A, Lim F, Nandakumar K, Qin Z, Ramakrishna V, et al. Double-blind consent-driven data sharing on blockchain. IEEE International Conference on Cloud Engineering (IC2E), IEEE, pp 385–391, 2018.
20. QUNIE CORPORATION. [Research on understanding the actual situation using on-chain/off-chain data in decentralized financial systems] Bunsangatakinyu System ni okeru On-chain/Off-chain data wo katsuyo shita jittai haaku ni kansuru kenkyu (in Japanese), Japan Financial Services Agency Blockchain International Joint Research Project, June, 2023. https://www.fsa.go.jp/policy/bgin/ResearchPaper_qunie2_ja.pdf. Accessed, July, 3, 2023.
21. Jonathan Heiss, Robert Muth, Frank Pallas, and Stefan Tai. Non-disclosing Credential On-chaining for Blockchain-Based Decentralized Applications. ICSOC 2022, LNCS 13740, pp. 351–368, 2022.
22. Sundareswaran N, Sasirekha S, Paul IJL, Balakrishnan S, Swaminathan G. Optimised KYC blockchain system. International conference on innovative trends in information technology (ICITIIT), IEEE, pp 1–6, 2020.
23. Benedikt B¨unz et al., Bulletproofs: Short Proofs for Confidential Transactions and More, IEEE Security & Privacy, 2018.

24. Shostack A, Threat modeling: designing for security. Wiley, Hoboken, 2014.

Works [1], [4], and [5] offer comprehensive insights into the effectiveness of KYC in purifying economic systems.

Study [2] proposes a mixing method to balance transaction privacy and the engagement of ethical investors. This paper contributes to this discussion by proposing a method for evaluating wallet trustworthiness as a tool for constructing practical association sets.

Study [3] introduces a method for verifying attributes within investors, aligning with the focus of this paper on attribute compatibility in P2P transactions.

The discussion extends to the economic aspects of credentials, with [6] highlighting the risks associated with centralized issuance and [8] demonstrating how credentials can enhance the convenience of financial services.

[7] proposes the integration of KYC data and reputation scores, while this paper advances a comprehensive evaluation method considering Wallet Holders, transaction behavior, and Crypto Asset Provenances.

The importance of privacy in credential issuance is critically evaluated in [9] and [10], while noting the residual risk of privacy breaches despite advanced anonymization techniques.

Studies [11] and [12] provide detailed explanations of the specific mechanisms adopted by hackers for money laundering using crypto assets, emphasizing the need for robust KYC technologies.

14. Appendix B – Acknowledgement

(Informative)

(Note) The views expressed in this report are based on the personal views of the authors and not the views of the organizations to which they belong.

A.1 Editors and Co-editors

A.2 Contributors (Alphabetical)

A.3 Reviewers (Alphabetical)

Blockchain Governance Initiative Network (BGIN) aims at providing an open and neutral sphere for all stakeholders to deepen common understanding and to collaborate to address issues they face in order to attain sustainable development of the blockchain community. As an open network, we are now actively and widely seeking interested

parties to join this initiative, so as to accommodate diverse opinions from a wider range of blockchain stakeholders. This paper was discussed in Block #9, Block #10 and during our bi-weekly IKP Working Group (co-chair: Nat Sakimura; co-chair: Mitchell Travers).

For those who are interested, please contact us via bgin-admin@mail.bgin-global.org.