

[Financial Services Agency Blockchain International Joint Research Project]

Research report on "The Evolution of Tokenization in the
Financial Sector and the Feasibility of the use of Blockchain
Technology for RegTech/SupTech"

November
2024

QUNIE

Acknowledgements and Disclaimers

Acknowledgements

- In preparing this report, we received useful advice and comments from Professor Naoyuki Iwashita of Kyoto University, Professor Kiyotaka Sasaki of Hitotsubashi University, and Research Professor Shinichiro Matsuo of Georgetown University in the U.S. We also received useful suggestions and advice from observers at the Digital Agency and from officials at the Financial Services Agency.
- However, all errors in the content of this report are attributed to the trustee, Qunie Corporation.

Disclaimer

- The contents of this report do not represent the official views of the JFSA.
- The contents in this report other than historical or current facts are forward-looking statements based on information available at the time of writing, and actual trends may vary due to a variety of uncertainties.

Research objectives and background

- Technological innovations such as blockchain have the potential to not only digitize financial services but also to implement financial systems with a certain degree of programmability through the tokenization of payment methods and financial products (e.g., stable coins, tokenized deposits, security tokens). It is imperative to identify and analyze key issues for the development of a robust financial system, while considering both the opportunities and risks associated with these advancements, including crypto-assets, which represent the initial application of blockchain technology.
- Numerous financial institutions, both in Japan and globally, including traditional entities such as banks, are investigating the potential applications of blockchain and tokenization technologies. The automation and autonomy inherent in these technologies have the capacity to enhance financial systems through improved efficiency in payment processes and the automation of compliance-related procedures. Conversely, it has been noted that these technologies may pose risks to stability of financial systems, customer protection, and anti-money laundering/combating the financing of terrorism (AML/CFT) efforts. These risks include potential alterations in the nature of financial transactions, such as an increase in peer-to-peer (P2P) and machine-to-machine (M2M) transactions, as well as transaction suspensions resulting from vulnerabilities in smart contracts.
- Furthermore, it has been suggested that regulatory bodies should maximize the utilization of technology, including blockchain-related innovations, to enhance regulatory oversight. For instance, the FSB report, although not specifically addressing blockchain, notes that technology "presents opportunities, risks and challenges for regulated financial institutions and regulators," and asserts that innovative technological tools employed by regulated financial institutions to support compliance with regulations and reporting obligations (hereinafter referred to as "RegTech") and innovative technological tools utilized by regulators to support regulatory operations (hereinafter referred to as "SupTech") "have the potential to provide important benefits to financial stability."
- Although the progress of tokenization is currently limited, in light of its future potential, it is important to analyze the implications of the advancement of tokenization on the financial system, as well as the possibility that regulated financial institutions and regulatory authorities may enhance their regulatory oversight responses through RegTech / SupTech utilizing blockchain technology.
- In this research, Chapter 1 summarizes the progress of tokenization, including specific examples and the response of supervisory authorities. Chapter 2 explores the possibility of using blockchain technology in RegTech / SupTech through the analysis of previous cases. Chapter 3 conducts a desk-based verification of "embedded supervision" and "supervisory nodes," which are considered to be one approach of RegTech / SupTech to systematically analyze their possibilities and challenges.

Table of contents

Chapter 1: The Evolution of Tokenization in the financial sector

1. The emergence and spread of blockchain-related technologies and decentralized financial systems
2. Comparison of Decentralized Finance and Traditional Finance
3. Review of the supervision of decentralized finance
4. Efforts to reduce risks in decentralized finance (RegTech)
5. Tokenization-related projects involving traditional financial institutions
6. Impact of Tokenization on the Financial Sector
7. The nature of tokenization in the financial sector
8. Summary

Chapter 2: Possibility of RegTech/SupTech based on Blockchain technology

1. RegTech / SupTech verification projects lead by regulators
2. RegTech in Decentralized Finance
3. Summary

Chapter 3: Desk-based verification of Regtech/Suptech utilizing the characteristics of blockchain

1. Elements of Supervision Scenario
2. RegTech and SupTech Supervision Scenarios
3. System functions required by Supervision scenario
4. System configuration of trading scenario
5. Verification items and results for system requirements
6. Summary

Abbreviations

The full names of the main abbreviations that appear in this document are listed below.

Abbreviations	Official name
AML/CFT	Anti Money Laundering and Combating the Financing of Terrorism
BIS	Bank for International Settlements
DeFi	Decentralized Finance
FATF	Financial Action Task Force
FSB	Financial Stability Board
KYC	Know Your Customer
CBDC	Central Bank Digital Currency
DAO	Decentralized Autonomous Organization
DLT	Distributed Ledger Technology

Glossary

In this document, the main technical terms that appear in Chapter 1 are defined as follows.

term	Definition
Tokenization	<p>FSB defines tokenization as "the process of creating digital representations of assets (tokens) and storing them on a distributed ledger," while the Bank for International Settlements (BIS) defines it as "the use of cryptocurrencies to trade financial or real assets." It defines it as "the process of digitally representing rights in a programmable platform."</p> <p>Tokenization can be applied to a wide range of items, including deposits, financial products, and real assets. Examples include security tokens, stable coins, and tokenized deposits.</p>
Blockchain-related technologies	<p>Although distributed ledger technology platforms are not necessarily used for tokenization, in this report we use the term "blockchain-related technologies" as a general term for technologies used for tokenization.</p>
Programmability	<p>Programmability generally refers to the ability to reduce manual work and achieve automation and efficiency by writing rules and conditions as programs and having them in computer algorithms. According to the report by Hojo and Hatogai (2022), for example, programmability in payment systems means the ability to control and automate the behavior of funds and securities as they are circulated by computer programs. While there have been efforts to programmize systems in the financial sector for some time, in this document the term programmability is used only in cases where blockchain-related technology is used.</p>
Smart Contracts	<p>A program that defines rules that are written to the blockchain and are automatically executed when functions are invoked through transactions.</p> <p>Ethereum and other platforms, smart contracts are written to the blockchain and executed by miners or validators during the transaction verification process. The execution log and post-execution evidence are recorded in the block, allowing anyone to confirm that authentic program code has been executed and to share the state. Smart contracts cannot normally be modified or deleted, and the results of execution cannot be undone, but if indirect references are used through support from development tools, there is room to make it possible to upgrade smart contracts by replacing the reference with a new contract address. Smart contracts can be executed by deploying them to the blockchain, but in DeFi Deployment work in Ethereum generally requires the private key of an externally owned account held by an administrator or authorized person (someone who holds the private key required to deploy smart contracts).</p>
Permissionless Chain	<p>A shared ledger in which an unspecified number of participating nodes verify and approve transactions on the network, and participation is possible without the administrator's permission.</p>
Permissioned Chain	<p>A shared ledger with limited participation, where only certain nodes authorized by the administrator can verify and approve transactions on the network.</p>

Source: Financial Stability Board (2023), "The Financial Stability Risks of Decentralized Finance."

Bank for International Settlements (2023), "Blueprint for the future monetary system: improving the old, enabling the new."

https://www.boj.or.jp/research/wps_rev/rev_2024/data/rev24j10.pdf

Glossary

term	Definition
Decentralized Finance (DeFi)	<p>So-called DeFi has been discussed in various documents and articles, but there is no clear definition. In this report, we follow the references and define it as "financial applications that build part of a decentralized financial system." After the launch of the Ethereum blockchain , DeFi was initially centered on issuing unique tokens for fundraising and DEXs (decentralized exchanges) that did not require the mediation of traditional exchanges for token exchanges, but as the DeFi ecosystem expands, various initiatives have emerged based on traditional finance, such as lending, derivatives, and insurance . There are also aggregators that provide services by consolidating multiple DeFi transactions into one .</p>
Decentralized Financial System	<p>The 2019 FSB report defines a decentralized financial system as "a system that may be brought about by decentralized financial technology." It further defines decentralized financial technology as "technology that has the potential to reduce or eliminate the need for one or more intermediaries or centralized processes in the provision of financial services." This report uses the above definition.</p> <p>* A decentralized financial system aims to build a decentralized system in contrast to the centralized systems seen in existing financial systems.</p>
DAO	<p>There is no clear definition of the decentralized autonomous organization (DAO) that operates DeFi , but in this report, based on reference materials and the example of MakerDAO , we define it as "an organization that is a member-owned community without centralized leadership and is run by rules encoded as a computer program (smart contracts)."</p> <p>※ Characteristics of DAOs in major DeFi projects</p> <ul style="list-style-type: none"> • An organization that does not have a managing company, representative, or board of directors, and is run autonomously by its participants • The organization's operating rules are coded into smart contracts. • A type of voting right (voting rights) is granted to token holders in the form of tokens called governance tokens, and voting is carried out on (some of) the organization's or community's decision-making based on the rules of the smart contract. • Since the participants are from multiple countries and are active globally, and the managing entity is not always clear, it is difficult to identify the country or region to which the organization belongs.

Chapter 1: The Evolution of Tokenization in the financial sector

Chapter 1: The Evolution of Tokenization in the Financial Sector

1. The emergence and evolution of blockchain-related technologies and decentralized financial systems

- The history of the emergence and evolution of blockchain-related technologies and decentralized financial systems is shown below.
1. The birth of blockchain technology
 - 2008 : A person (or group) known as Satoshi Nakamoto published a paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System." This paper first introduced the concept of a cryptocurrency called Bitcoin and its underlying technology, the blockchain .
 - 2009 : The first version of Bitcoin was released, marking the birth of blockchain technology.
 2. The evolution of Bitcoin and Blockchain technology
 - 2010 : The first Bitcoin transaction was made, reportedly purchasing two pizzas for 10,000 Bitcoin. This is considered one of the earliest economic transactions using Bitcoin .
 - 2011-2013 : Bitcoin gradually gained popularity and other cryptocurrencies (altcoins) emerged, such as Litecoin and Ripple .
 - 2015 : Ethereum was officially released. Ethereum is a platform that can execute smart contracts and is an example of blockchain technology being applied to things other than crypto assets .
 3. The rise of decentralized finance (DeFi)
 - 2016 : The DAO incident occurred , and the risk of attacks exploiting vulnerabilities in the program code of smart contracts began to be widely recognized. However, large amounts of funds were raised through initial coin offerings (ICOs), and many DeFi projects were launched.
 - 2018 : Early DeFi projects such as Compound and MakerDAO appeared . Stablecoins such as USDC and Dai were introduced, and decentralized finance transactions became more active. Around this time, Japan 's largest cryptocurrency theft incident occurred. Also, discussions about how to regulate ICOs intensified .
 - 2020 : The so-called " DeFi Summer " arrived, and decentralized exchanges (DEXs) developed rapidly. Uniswap , SushiSwap , and others became popular. Total value locked (TVL) in DeFi increased sharply.

Chapter 1: The Evolution of Tokenization in the Financial Sector

1. The emergence and evolution of blockchain-related technologies and decentralized financial systems

4. Recent Trends

- 2021 and beyond : The DeFi ecosystem has become even more complex due to the development of cross-chain technology (technology that realizes interoperability between different blockchains) . At the same time, the number of DeFi hacking incidents has been is also increasing, with large amounts of crypto assets being stolen every year.
- 2024 : The market capitalization of cryptocurrencies, which fell in 2022, has been recovering.

Figure 1-1-1 Trends in total market capitalization of crypto assets over the past five years (unit: trillion dollars)



Source: TradingView "Total Market Cap of Crypto Assets - Index Chart" <https://jp.tradingview.com/symbols/TOTAL/> as of May 20, 2024

Chapter 1: The Evolution of Tokenization in the Financial Sector

2. Comparison of Decentralized Finance and Traditional Finance

(1) Challenges regarding the regulation of decentralized finance identified in IOSCO's report

- IOSCO 's "Final Report with Policy Recommendations on Decentralized Finance" (published in December 2023) points out challenges regarding the regulation of decentralized finance. (See table below.)

Table 1-2-1 IOSCO Report on Regulatory Issues for Decentralized Finance

Regulatory challenges for decentralized finance	Specific details
The need for regulation to protect investors	<ul style="list-style-type: none"> In recent years, investors around the world have become increasingly exposed to decentralized finance, which has also led to increased investor losses amid regulatory noncompliance, financial crimes, fraud, market manipulation, money laundering and other illicit cryptocurrency market activities.
Applicability of existing regulatory frameworks based on similarities between decentralized and traditional financial markets	<ul style="list-style-type: none"> Given the similarities between the economic functions and activities of decentralized financial markets and traditional financial markets, many existing international policies, standards and jurisdictional regulatory frameworks are applicable to decentralized financial products, services, activities and arrangements.
Reducing regulatory arbitrage risk arising from differences in how rules are applied and enforced between decentralized and traditional financial markets	<ul style="list-style-type: none"> In the broader context of cooperation and coordination on decentralized finance among international organizations such as the FSB , FATF , and BIS , and standard-setting bodies such as IOSCO , CPMI-IOSCO (Committee on Payments and Market Infrastructures-IOSCO), and BCBS (Basel Committee on Banking Supervision) , IOSCO 's recommendations and guidance should promote a level playing field between crypto-asset markets and traditional financial markets and help reduce regulatory arbitrage risks arising from differences in how rules for decentralized finance and traditional financial markets are applied and enforced.
The need for consistent guiding principles	<ul style="list-style-type: none"> In crypto asset markets, it is common for individuals and entities, through a variety of arrangements, to offer financial products, provide financial services, and engage in financial activities substantially similar to those in traditional financial markets. Such activities are conducted, to varying degrees, using a number of technologies, including DLT . However, regardless of organizational form or technology used, these persons and entities should be treated in accordance with the Guiding Principle of " same activities, same risks, same regulatory outcomes . "

Chapter 1: The Evolution of Tokenization in the Financial Sector

2. Comparison of Decentralized Finance and Traditional Finance

(2) Characteristics of decentralized finance

The typical characteristics of decentralized finance are considered to be:

- It can be operated by a decentralized organization.
- It is possible to carry out transactions without the service provider knowing your identity.
- No bank account is required and it can be used globally as long as you have an internet connection
- The system usage fees are considered to be low
- It has new innovation such as lending services and decentralized exchanges (DEXs).
- It has high compatibility with crypto assets

IOSCO report states, "Regardless of the technology that may be used to offer or provide financial products and services or engage in financial activities, global market regulators should apply a ' same activity, same risk, same regulation and regulatory outcomes ' approach to financial markets," and as such, if decentralized finance is a type of financial system, it should be addressed in accordance with the objectives of financial regulation regardless of the form of the system. On the other hand, some of the above characteristics are considered to make it difficult to meet the objectives of regulations such as customer protection and AML/CFT .

An example is shown below.

- It can be operated by a non-centralized organization. If it is operated by a DAO , it is unclear who is responsible in the event of an accident.
- Being able to make transactions without the service provider knowing your identity is a hotbed of crime, such as tax evasion and money laundering.
- No need for a bank account, as long as you have an internet connection, can be a breeding ground for crimes such as tax evasion and money laundering.
- The system usage fees are considered to be low, as the cost of complying with financial regulations is insufficient.

Chapter 1: The Evolution of Tokenization in the Financial Sector

2. Comparison of Decentralized Finance and Traditional Finance

(3) Comparison of the characteristics of decentralized finance (early stage) and traditional finance

In traditional finance, transaction entities have completed KYC, and the main service providers are financial institutions that have been licensed under financial regulations and are under supervision by authorities, etc. There are multiple mechanisms for supervision of traditional finance, such as authorization by regulators, self-regulation, and response to supervision from authorities, etc. aimed at customer protection and financial market stability, and services are provided to customers based on these as the basis of trust.

In decentralized finance (especially in its early stages), the parties involved in transactions are unidentified, and the main service providers are DAOs, which also have unidentified parties. There are attempts to eliminate third parties in charge of management in many cases of decentralized finance, but if order is to be applied to this, it will be through peer monitoring and self-supervision, provided that cryptographic protocols are followed (see table below).

Table 1-2-2 Traditional Finance vs. Decentralized Finance

	Service Provider	Transaction entity	Basis of trust
Traditional Finance	Corporation	KYC- certified individuals and corporations	Self-regulation, industry regulation, and supervision by authorities
Decentralized Finance (Initially)	DAO	Individuals and corporations who have not completed KYC	Cryptographic protocol, mutual surveillance by participants

Further details on peer monitoring and self-supervision are provided below.

Even though it is difficult to make globalized decentralized finance comply with the laws of a specific jurisdiction region, participants are required to comply with them they belong to. Therefore, in decentralized finance, under the premise that transactions and blocks that do not follow the protocol will be eliminated, participants themselves must check whether the recipient of the remittance they are using for remittance is one that they would be punished for being involved with.

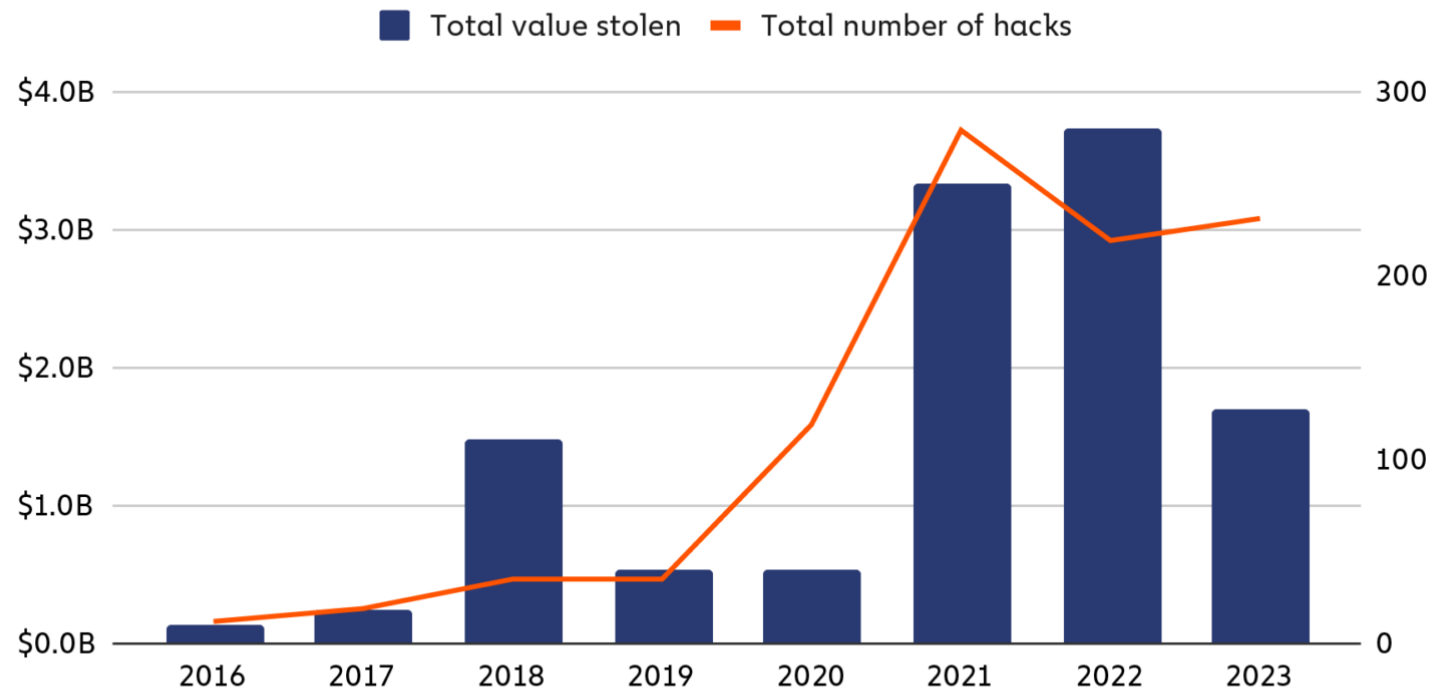
As such, traditional finance and decentralized finance have differences in service providers, trading entities, and supervision (basis of trust), as well as in the technologies applied and the players belonging to the ecosystem. However, as the IOSCO report states, "To promote a level competitive environment between cryptocurrency markets and traditional financial markets and reduce regulatory arbitrage risk, regulatory frameworks for DeFi (existing or new) should aim to achieve regulatory outcomes for investor protection and market integrity that are the same, or consistent, with those required in traditional financial markets," there is a growing discussion about the need to reconsider the way in which supervision of decentralized finance is based on the regulatory framework cultivated in traditional finance.

3. Review of the supervision of decentralized finance

- According to Chainalysis report , the size of cryptocurrency thefts has been expanding in recent years, with \$ 3.7 billion stolen in 2022. In 2023 , the amount was down about 54.3% from the previous year to \$ 1.7 billion, but the number of hacking incidents increased from 219 in 2022 to 231 in 2023 .

Chart 1-3-1 Trends in cryptocurrency theft

Yearly total value stolen in crypto hacks and number of hacks, 2016 - 2023



© Chainalysis

- Regulators are becoming more aware of the risks posed by cryptocurrencies and DeFi .
- The FATF has specified that even arrangements called DeFi will be subject to the FATF standards if certain parties have control or sufficient influence over them (similar to centralized cryptocurrency exchanges, etc.). However , it has also pointed out challenges in identifying the regulator and ensuring enforceability.
- The EU 's Markets in Crypto Assets (MiCA) regulation does not cover fully decentralized services, and the definition of "cryptocurrency service provider" needs to be revised in order to extend regulation to decentralized finance intermediaries.
- Various regulatory approach to DeFi are being explored. For example, a research paper published by the Bank of France suggests that regulation through registration could strengthen the security of blockchain infrastructure, while oversight of DAOs through legal personality and control over intermediaries providing access to decentralized financial services could strengthen customer protection.
- In light of these demands, some decentralized financial systems are voluntarily seeking to implement supervisory capabilities.

Chapter 1: The Evolution of Tokenization in the Financial Sector

4. Efforts to reduce risks in decentralized finance (RegTech)

Here, we will introduce some examples of initiatives taken by businesses and solution providers to reduce risks such as

Fireblocks threat level check function before token transfer

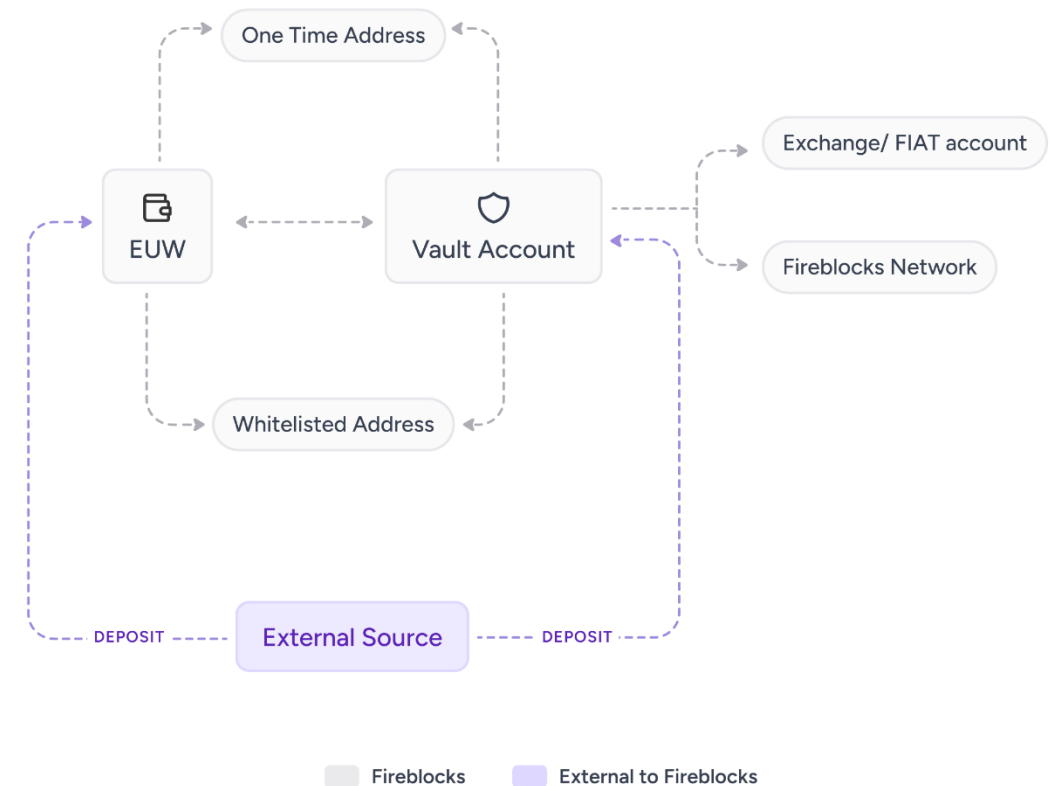
Fireblocks , a US company, provides a platform that comprehensively supports the storage, trading, issuance, and management of digital assets.

The company's platform offers real-time threat detection alerts aimed at preventing interactions with suspicious smart contracts, phishing sites, and dangerous dApps(decentralized applicatoins) and preview function to the estimated changes of token outstanding when there are interactions with smart contracts.

There is thought to be a need for a mechanism that identifies the token destination, origin, and system of origin before the payment is completed, and then advises the user on the threat level, since in a decentralized financial system it is often impossible to know who the other party is.

Figure 1-4-1 shows an example of the transaction flow we envision. When withdrawing funds from a user's Vault Account or embedded user wallet (EUW), the validity of the destination address is determined by referencing the whitelist addresses, and then the funds are sent to an external account (Exchange/FIAT account).

Figure 1-4-1 The transaction flow envisaged by the Company



Source: Fireblocks Fireblocks expands DeFi security capabilities to protect institutions from ever-evolving threats

<https://www.fireblocks.com/blog/fireblocks-expands-defi-security-capabilities-to-protect-institutions-from-ever-evolving-threats/>

<https://ncw-developers.fireblocks.com/docs/transaction-flows>

Chapter 1: The Evolution of Tokenization in the Financial Sector

4. Efforts to reduce risks in decentralized finance (RegTech)

Uniswap 's financial transaction

A a DEX , Uniswap provides a platform for trading cryptocurrencies using smart contracts.

After partnering with blockchain analysis company TRM Labs, Uniswap has announced that it is restricting access to wallet addresses related to embezzlement and sanctions (TRM Lab identifies wallet addresses related to sanctions, terrorist financing, hacking or stolen funds, ransomware, etc., and Uniswap blocks those addresses). Uniswap-trm.csv, which shows the targets of blocking, has been published on GITHUB, and 596 wallet addresses categorized as "fraud, hacked or stolen funds, sanctions" are listed (as of May 21, 2024).

The mechanism for restricting access to specific wallet addresses and restricting transfers can also be seen as similar to the mechanism for restricting transfers by freezing bank accounts.

Figure 1-4-2 UNISWAP source code (excerpt)

```
174     if (TOKEN_BLACKLIST.includes(address)) {
175         return (
176             <BlockedWrapper>
177                 <BlockedMessageWrapper>
178                     <AutoColumn gap="1rem" justify="center">
179                         <TYPE.light style={{ textAlign: 'center' }}>
180                             {BLOCKED_WARNINGS[address] ?? `This token is not supported.`}
181                         </TYPE.light>
182                         <Link external={true} href={'https://etherscan.io/address/' + address}>`More about ${shortenAddress(
183                             address
184                         )}`</Link>
185                     </AutoColumn>
186                 </BlockedMessageWrapper>
187             </BlockedWrapper>
188         )
189     }
```

Figure 1-4-2 shows an excerpt from publicly available source code from Uniswap that shows that addresses that meet certain conditions are excluded from processing. It is assumed that the above block processing is also performed in a similar manner.

Source: Uniswap Labs Address Screening Update <https://blog.uniswap.org/trm>

GITHUB uniswap-trm.csv <https://gist.github.com/banteg/1657d4778eb86c460e03bc58b99970c0>

GITHUB TokenPage.js <https://github.com/Uniswap/info/blob/a668245cfc786f57af67fb5e6d999d7b11b1f05/src/pages/TokenPage.js>

Chapter 1: The Evolution of Tokenization in the Financial Sector

4. Efforts to reduce risks in decentralized finance (RegTech)

Circle Financial Transaction

The U.S. Treasury Department has added Ethereum and USDC wallet addresses related to Tornado Cash to its so-called blacklist, following suspicions that the mixing service, which can obscure the details of cryptocurrency transactions, was used to launder proceeds from multiple cryptocurrency hacks, including those of the Lazarus Group , a suspected North Korean hacking syndicate .

In response to the sanctions from the U.S. Treasury Department, Circle froze the USDC held in the relevant USDC wallet addresses. According to data from the Ethereum blockchain explorer (Etherscan), at least 75,000 USDC was frozen.

Figure 1-4-3 is an excerpt from publicly available source code that shows the process of determining whether an address is on the blacklist, and the process of adding or deleting an address from the blacklist.

Source: <https://x.com/jerallaire/status/1557004767930499072>

<https://github.com/circlefin/stablecoin-evm/blob/master/contracts/v1/Blacklistable.sol>

Circle Pledges Action on User Privacy After Freezing \$75K Tornado Cash-Linked USDC <https://beincrypto.com/circle-pledges-action-after-freezing-75k-tornado-cash-linked-usdc/>

Figure 1-4-3 Circle 's source code (excerpt)

```
59     * @notice Checks if account is blacklisted.
60     * @param _account The address to check.
61     * @return True if the account is blacklisted, false if the account is not blacklisted.
62     */
63     function isBlacklisted(address _account) external view returns (bool) {
64         return _isBlacklisted(_account);
65     }
66
67     /**
68     * @notice Adds account to blacklist.
69     * @param _account The address to blacklist.
70     */
71     function blacklist(address _account) external onlyBlacklister {
72         _blacklist(_account);
73         emit Blacklisted(_account);
74     }
75
76     /**
77     * @notice Removes account from blacklist.
78     * @param _account The address to remove from the blacklist.
79     */
80     function unBlacklist(address _account) external onlyBlacklister {
81         _unBlacklist(_account);
82         emit UnBlacklisted(_account);
83     }
```

Chapter 1: The Evolution of Tokenization in the Financial Sector

4. Efforts to reduce risks in decentralized finance (RegTech)

Initiatives to balance AML/CFT and privacy using VC/DID

Coinbase , which operates cryptocurrency exchanges , and Circle , which issues and manages USDC have published the protocol called Verite based on standard specifications such as Verifiable Credentials and DIDs.

This protocol allows customers to issue credentials without disclosing any personal data. Potential use cases for the protocol include accredited investor status, social reputation, and NFT provenance tracking. These credentials can be stored in a wallet just like digital assets. Because the credentials are owned by the customers user, they can control how and when different organizations and protocols access them.

How Verite can help decentralized financial systems with RegTech

If money laundering incidents occurs in a decentralized financial system using Verite , whether the decentralized financial system operator or authorities can identify the criminals depends on several factors. If it occurs when KYC information is collected in advance and transaction transparency is ensured as described below, authorities may be able to identify the criminals by using appropriate procedures and technologies.

1) Feasibility to disclose personal information related to qualification certificates

Although the qualification certificate itself does not contain any personally identifiable information, it is designed and operated in such a way that the necessary information can be obtained by requesting disclosure from the certificate issuer through legitimate procedures.

2) Accuracy of KYC

To assure accuracy of KYC, it is essential to collect user's KYC information, verify the its authenticity by an appropriate entity register and record it off-chain. If so, it can be retrieved after going through the appropriate procedures.

3) Balancing privacy and anonymity

If the proof of credentials for DID does not go through KYC , it is possible to maintain anonymity, which may lead to the risk of criminals exploiting the anonymity. A mechanism must be established in advance that allows authorities to request information disclosure through appropriate legal procedures.

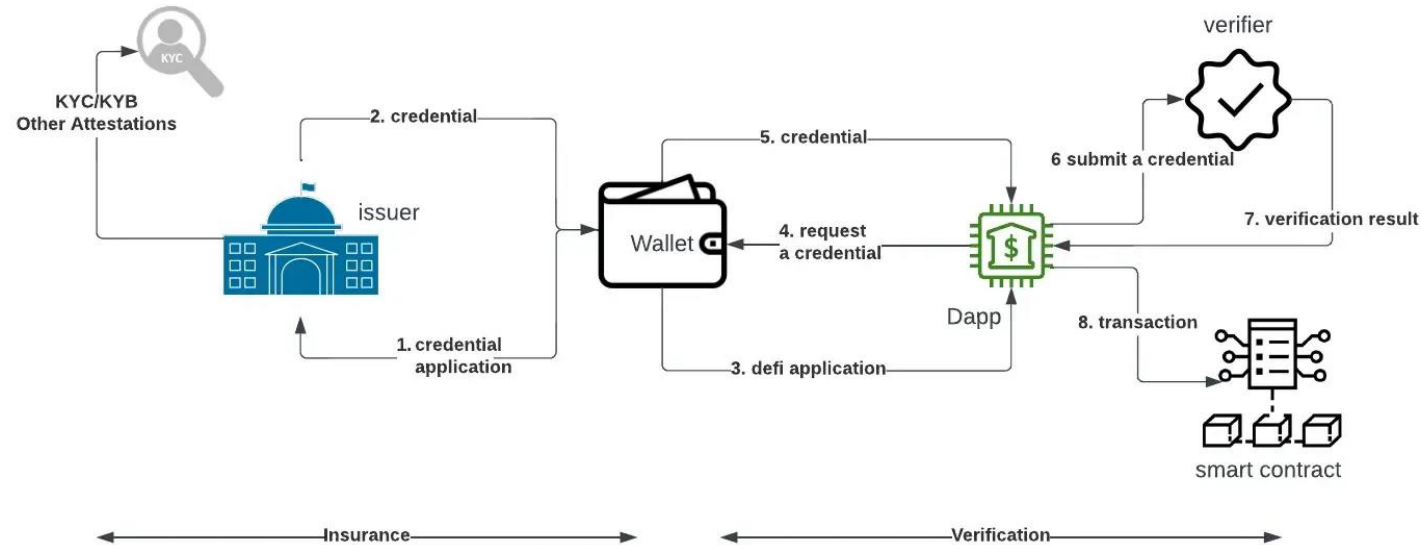
Chapter 1: The Evolution of Tokenization in the Financial Sector

4. Efforts to reduce risks in decentralized finance (RegTech)

Figure 1-4-4 shows the processing flow by Verite , where the wallet side, which represents the customer user, obtains verifiable credentials (VC) in the issuance flow, and the Dapp side verifies the VC in the verification flow before executing the transaction. An example process is as follows.

- The wallet holder submits a credential application to the certificate issuer.
- KYC (Know Your Customer) or KYB (Know Your Business) is conducted and the issuer issues a credential certificate.
- Once issued, the credential certificate is stored in the wallet.
- When the wallet holder uses a DeFi application, a credential certificate is requested by Verite (written as Dapp in the diagram).
- When the wallet holder presents the credential certificate, it is sent to the verifier.
- The verifier sends the verification result to Verite.
- Verite sends a transaction to the smart contract associated with the use of the DeFi application.

Figure 1-4-4 Verite Processing flow image



Project Guardian examines Regulated DeFi

We introduce the efforts of Project Guardian as an example of a verification project using the DeFi lending protocol AAVE by traditional finance companies to create programs (tokenization).

Project Guardian, a public-private partnership initiative on digital assets established by MAS in May 2022 , is to verify the feasibility of using digital technologies such as asset tokenization through pilot experiments while managing risks related to financial stability and fairness. Pilot experiments are being conducted in areas such as bonds, foreign exchange trading, and asset management, and financial institutions and policy authorities are encouraged to participate in order to deepen knowledge of the digital asset field and investigate use cases for various asset classes.

JP Morgan Chase, DBS Bank, and SBI Digital Asset Holdings are participating in this project , with the Financial Services Agency also participating as an observer.

Below, we will describe the pilot experiment regarding “issuance and exchange of deposit tokens, and buying and selling of tokenized government bonds.”

- The transaction infrastructure uses a modified version of the DeFi lending protocol AAVE.
- The content of the study will include whether cross-currency transactions of tokenized assets in wholesale can be traded, cleared and settled instantly between direct participants, the regulatory treatment of tokenized liabilities, and the impact of tokenized asset transactions on regulation and risk management, etc.

In addition, pilot experiments are also being conducted in "wealth management" and "trade finance."

Source: MAS First Industry Pilot for Digital Asset and Decentralized Finance Goes Live

<https://www.mas.gov.sg/news/media-releases/2022/first-industry-pilot-for-digital-asset-and-decentralised-finance-goes-live>

MAS Proposes Framework for Digital Asset Networks <https://www.mas.gov.sg/news/media-releases/2023/mas-proposes-framework-for-digital-asset-networks>

4. Trends in supervisory response to decentralized finance

Figure 1-4-5 Example of verification configuration using Project Guardian

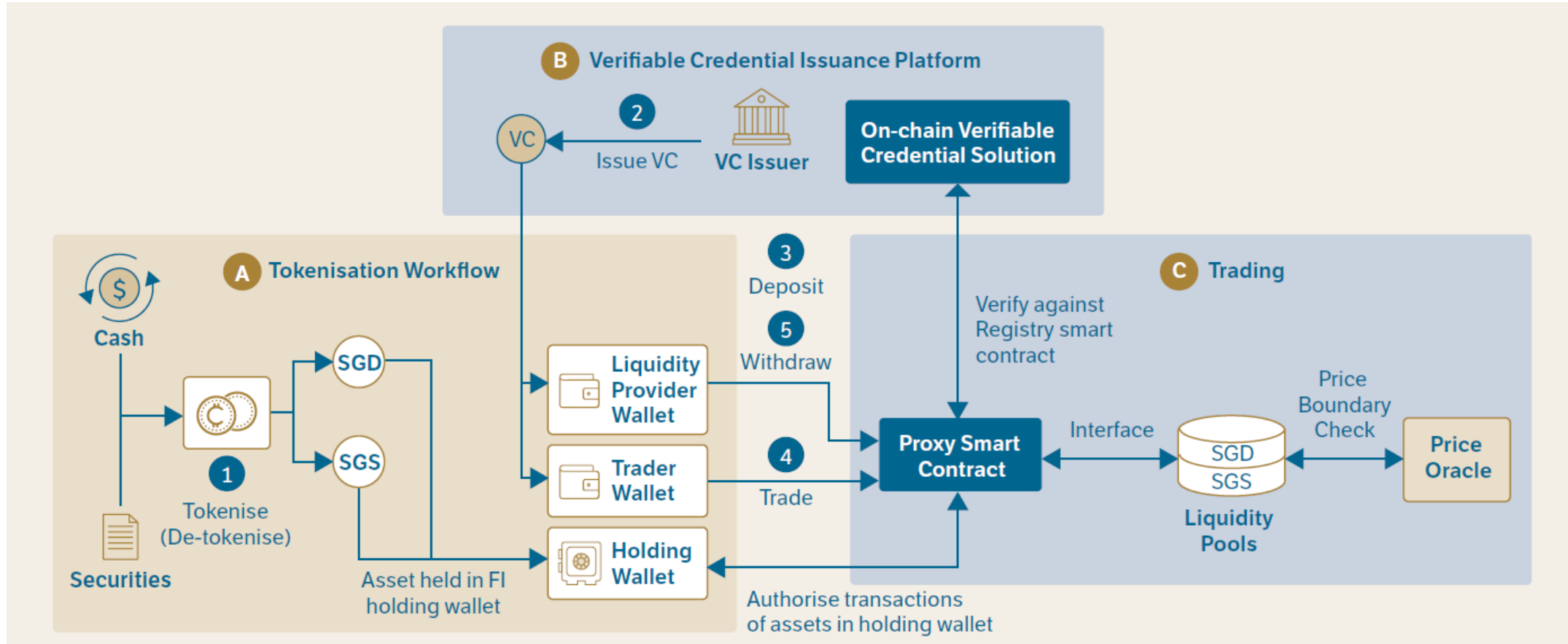


Figure 1-4-5 shows the system configuration when DBS Bank and SBI Digital Asset Holdings cooperated to verify the feasibility of executing foreign exchange and government bond transactions against a liquidity pool consisting of tokenized Singapore Government Securities (SGS) bonds, Japanese Government Bonds (JGB), Japanese Yen (JPY), and Singapore Dollar (SGD) as part of Project Guardian efforts. Various systems are being tested, one of which is Aave.

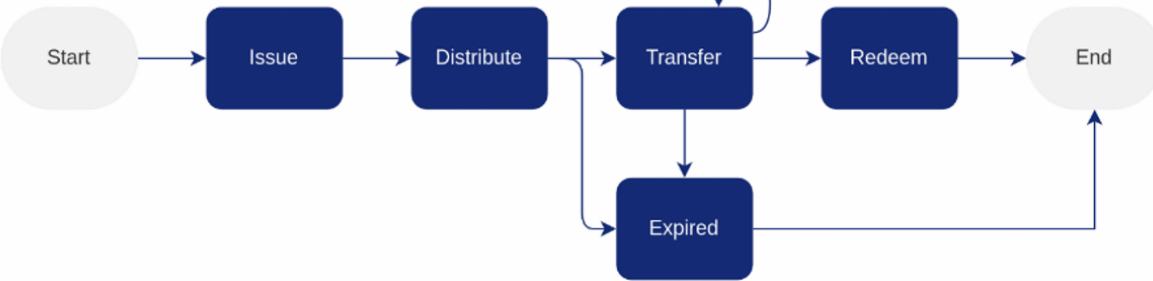
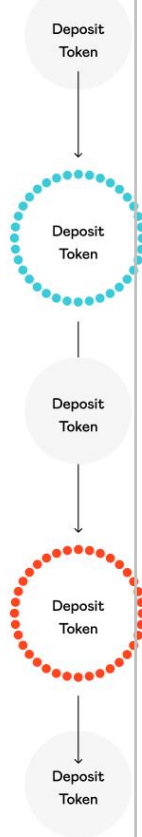
Source: <https://www.mas.gov.sg/-/media/mas-media-library/development/fintech/project-guardian/project-guardian-open-interoperable-network.pdf>

5. Tokenization-related projects involving traditional financial institutions

- This paper summarizes published literature on domestic and international projects that examine tokenization by traditional financial institutions such as banks.
- The seven projects surveyed in this chapter are as follows:
 - Purpose Bound Money (Monetary Authority of Singapore)
 - Project Guardian (Monetary Authority of Singapore)
 - Drex Project (Brazilian Central Bank, hereafter referred to as BCB)
 - Project Mariana (Bank for International Settlements , BIS)
 - JPM Coin (Onyx / JP Morgan)
 - Project Ion (DTCC)
- Published literature was selected from the projects surveyed and organized according to the following criteria:
 - Project Objective
 - Research content and findings related to financial stability, customer protection, etc.
 - Benefits and risks

Chapter 1: The Evolution of Tokenization in the Financial Sector

5. Tokenization-related projects involving traditional financial institutions

Project name	Type of Blockchain	Name of document	author	Publication date	Project Overview	Descriptions related to this research
<p>Purpose Bound Money (Project Orchid)</p>	<p>This paper is not limited to any particular blockchain. (The token standard for the Ethereum chain is ERC721 . ERC1155 can be implemented.)</p>	<p>Purpose Bound Money (PBM) Technical Whitepaper</p>	<p>MAS</p>	<p>2023 June</p>	<p>[Summary] This document describes digital money that limits the purposes of use as " Purpose Bound Money " (PBM) , and provides a technical overview of Programmable Money is conceptually similar . MAS is leading a project called Project Orchid , which is formulating guidance for PBM and working on PoC. The subject of this study is the Phase1 report of Project Orchid. The diagram below illustrates the life cycle of a PBM token.</p>  <pre> graph LR Start([Start]) --> Issue[Issue] Issue --> Distribute[Distribute] Distribute --> Transfer[Transfer] Transfer --> Redeem[Redeem] Redeem --> End([End]) Transfer --> Expired[Expired] Expired --> End Transfer --> Issue </pre> <p>[Project Participants] The International Monetary Fund, Banca d'Italia , Bank of Korea, and fintech companies, etc.</p> <p>[Research Contents] Digital money explores the possibility of programming unique characteristics into the individual bearer asset and limiting the purpose of use. On the other hand, implementing programming logic directly on a digital money also has the aspect of restricting free exchangeability. It would constrain the use of digital money as a viable medium of exchange if the conditions for its use are varied and dynamic. It would be possible for a digital money issuer to provide multiple versions of digital money, each with different logic programmed into it, as an alternative. However, such a method may not be practical as these digital monies would not be fungible with one another and would fragment the liquidity in the market. In this paper, we study various models to enable digital money to be freely exchanged and maintain the compatibility of digital money.</p>	<p>The diagram below illustrates deposit tokens moving between jurisdictions and being subject to jurisdiction-specific rules.</p>  <p>Jurisdiction 1 Application of specific financial rules</p> <p>Jurisdiction 2 Application of specific financial rules</p>

Chapter 1: The Evolution of Tokenization in the Financial Sector

5. Tokenization-related projects involving traditional financial institutions

Project name	Project Overview
Purpose Bound Money (Project Orchid)	<p>[Purpose] The project aims to address the challenge of digitalization efforts in the financial sector by identifying the need for interoperable payment ecosystems with avoiding the risk of proliferation and fragmentation of markets and studying programmability, fungibility of money and Models of Programmability.</p> <p>[Benefit] The followings are examples of how PBM could be used.</p> <ul style="list-style-type: none"> • As a "prepaid package," it can be used when a company needs to collect an upfront fee for assurance before producing a good or providing a service. It can address the risk of non-payment by payment terms to fulfill the company obligations before the consumer "withdraws" the pre-committed amount. • As a "cross-border payment" , by embedding existing regulatory requirements such as AML/CFT into PBM as conditions , compliance checks can be automated, significantly reduce costs and increase efficiency in cross-border payments. In the context of the G20 roadmap to strengthen cross-border payments, this could contribute to regulatory and policy interoperability. • As a "donation," it facilitates greater transparency and accountability. For example, PBMs could be used to ensure that only the intendent beneficiary can spend the money and only when certain conditions are met. • As "trade finance," it helps businesses to manage the risks and complexities of international trade transactions. To facilitate trade involving multiple parties across borders with different currencies, trade finance providers offer a range of services such as letters of credit, bank guarantees and documentary collections. These services help to ensure payments are made safely and efficiently, while also protecting against the risks of non-payment and fraud. • As a "commercial lease", PBM could replace security deposits where parties to the lease agreements are guaranteed for full recovery of security deposits. In cases of disputes, the PBM could be paused till the dispute is resolved. <p>[Risk]</p> <ul style="list-style-type: none"> • Currently, most retail users are not familiar with the use of digital asset wallets and this unfamiliarity could increase the risk of exploits by malicious actors. To mitigate this, account abstraction, also known as smart contract wallets, can be used to improve the user experience and security of digital asset transactions. This technology allows for features such as account recovery, transaction limits, and freezing of lost accounts, without requiring users to understand the underlying technology. • Purpose-bound tokens, which represent a payment obligation rather than a store of value, are subject to the risk of payment failure because payments are made on a deferred basis instead of an atomic and real-time basis. • Security programming framework should be applied across the digital money layer as well as the PBM Wrapper smart contract. This becomes particularly important when a PBM Creator aspires to integrate complex logic into components, such as delayed transfers or supply chain payment management. To proactively mitigate potential system security risks, such as the introduction of malicious code, it is highly recommended to conduct an independent audit. Furthermore, for distributed ledger-based networks, a trusted third-party organisation could be engaged to function as an 'oracle', offering dependable external data inputs into the network.

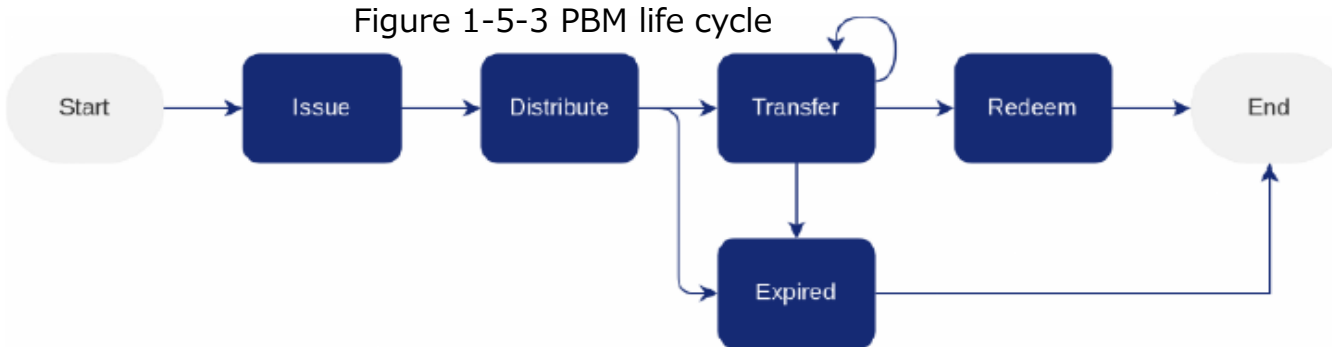
Chapter 1: The Evolution of Tokenization in the Financial Sector

5. Tokenization-related projects involving traditional financial institutions

Project name	Project Overview
Purpose Bound Money (Project Orchid)	<p>[Technical overview of PBM]</p> <ul style="list-style-type: none"> System Structure <p>PBM aims to function across different types of ledgers and assets. It is envisioned that PBM can be implemented on both distributed and non-distributed ledgers. The PBM protocol is based on a layer model involving four digital assets (access layer, service layer, asset layer, and platform layer), with programming logic in the service layer and digital money in the asset layer. When digital money is bound as a PBM, it straddles the service and asset layers.(see Figure 1-5-1).</p> <div style="display: flex; justify-content: space-around;"> <div data-bbox="377 511 1556 1129"> <p>Figure 1-5-1 Overview of PBM system architecture</p> </div> <div data-bbox="1745 511 2382 1035"> <p>Figure 1-5-2 Components of PBM</p> </div> </div> <ul style="list-style-type: none"> Components <p>A PBM consists of two main components, as shown in Figure 1-5-2: a wrapper that defines the intended use; and an underlying store of value that serves as collateral. The PBM wrapper can be programmed to ensure that the PBM can only be used for its intended purposes, such as validity for a specific time period, at specific retailers, or in a given denominations. When the conditions specified in the PBM wrapper are met, the underlying digital money will be released and transferred to the recipient. The underlying digital money bound by the PBM serves as collateral for the PBM. The digital money must meet the functions of money, namely as a good store of value, a unit of account, and a medium of exchange.</p>

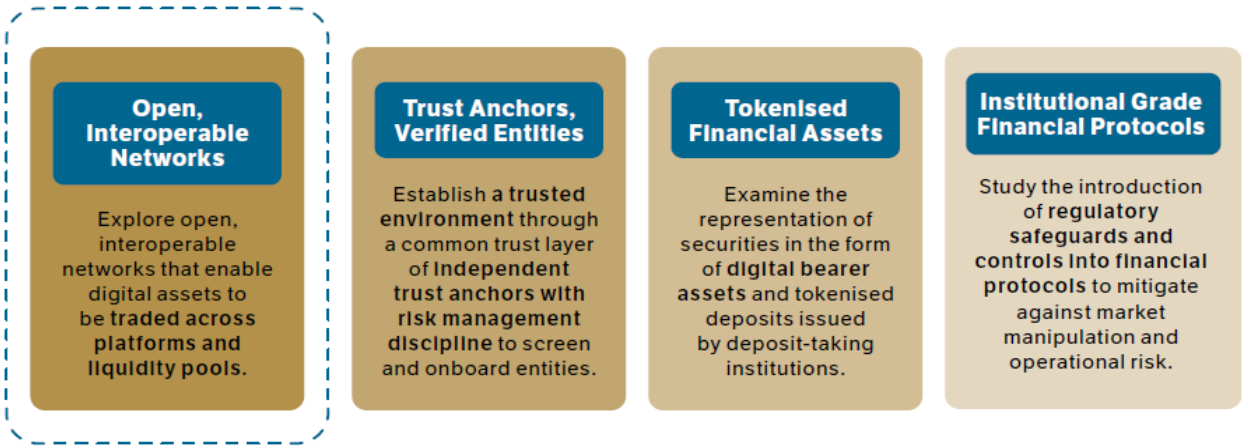
Chapter 1: The Evolution of Tokenization in the Financial Sector

5. Tokenization-related projects involving traditional financial institutions

Project name	Project Overview
Purpose Bound Money (Project Orchid)	<ul style="list-style-type: none"> Roles and Interactions In a PBM ecosystem, it is possible for an entity to hold multiple roles, or for a single role to be performed by different entities. PBM Creator: Responsible PBM Holder: Holds one or more PBM Tokens. This entity can redeem non-expired PBM Redeemer : Receives the underlying digital money when PBM tokens are transferred. Life Cycle The life cycle can be shown in the stages of Issue, Distribute, Transfer, Redeem, and Expired (see Figure 1-5-3). In the stage of Issue, the PBM smart contract is created and the PBM token is minted. In the stage of Distribute, after the PBM token is minted, they are distributed by the PBM creator to the PBM holder for usage. In the stage of Transfer, the PBM token is transferred from one entity to another in a wrapped state according to its programmed rules. The redeem stage occurs after all the conditions specified in a PBM have been fulfilled. At this point, the PBM token is unwrapped, and ownership of the underlying digital money token is transferred to the receiving entity. The expired stage refers to situations where one of the conditions specified in the PBM have unmistakably been violated or expired (e.g., expiry date), rendering the PBM token to be permanently unusable for the PBM Holder. <p style="text-align: center;">Figure 1-5-3 PBM life cycle</p>  <pre> graph LR Start([Start]) --> Issue[Issue] Issue --> Distribute[Distribute] Distribute --> Transfer[Transfer] Transfer --> Redeem[Redeem] Redeem --> End([End]) Transfer --> Expired[Expired] Expired --> End Transfer --> Transfer </pre> <ul style="list-style-type: none"> Sequence flow In this paper, we explore one design where the PBM is divided into the following three components: (1) access control via whitelisting and blacklisting; (2) PBM Wrapper expiry date; and (3) PBM token type expiry date. Design Considerations This paper considers issues such as interoperability, digital money, privacy, policy considerations, digital readiness, and secure programming.

Chapter 1: The Evolution Advancement of Tokenization in the Financial Sector

5. Tokenization-related projects involving traditional financial institutions

Project name	Type of Blockchain	Name of document	author	Publication date	Project Overview	Descriptions related to this research
Project Guardian	Permissioned Blockchain	Enabling Open and Interoperable Networks	BIS Committee on Payments and Market Infrastructures	June 2023	<p>[Summary] This report highlights one of the fundamental principles of Project Guardian – the establishment of open and interoperable networks. A common framework is introduced for understanding design options that enable the trading of digital assets across networks and liquidity pools. This framework considers the core principles of financial market infrastructure and takes reference from projects that have sought to push the boundary on these topics. This paper was developed in collaboration with experts from the BIS Committee on Payments and Market Infrastructures, with the cooperation of participating financial institutions.</p> <p>[Project participants] DBS Bank , HSBC , SBI Digital Asset Holdings , United Overseas Bank , Marketnode , Standard Chartered , ONYX by JPMorgan</p> <p>[Research Contents] This report introduces a framework for designing open and interoperable digital asset networks based on tokenised real-economy assets and financial assets. This report introduces a framework for designing open, interoperable digital asset networks based on tokenized real economic and financial assets.</p> <p style="text-align: center;">Figure 1-5-4 Scope of Project Guardian (enclosed by dotted line)</p>  <p style="text-align: center;">Figure 1: Guardian Themes</p>	<p>Based on the fintech cooperation framework concluded between the two authorities in March 2017 , the FSA and MAS announced that the FSA will participate as an observer in Project Guardian , a public-private partnership initiative on digital assets established by MAS in May 2022 (June 26 , 2024) .</p>

Source: <https://www.mas.gov.sg/publications/monographs-or-information-paper/2023/project-guardian-open-interoperable-networks>

Figure 1-5-4 is an excerpt from this document and simplified by our company.

Chapter 1: The Evolution Advancement of Tokenization in the Financial Sector

5. Tokenization-related projects involving traditional financial institutions

Project name	Project Overview
Project Guardian	<p>[Purpose] Project Guardian aims to advance best practices and technical standards among in the industry to prevent fragmentation of markets as digital assets and decentralized protocols proliferate. The project also seeks to explore the role of regulated financial institutions as trust anchors to screen, verify and issue credentials, enabling participants to only trade with verified parties.</p> <p>[Benefit]</p> <ul style="list-style-type: none">• HTLC (Hashed Time Lock Contract) is introduced as one of the technologies that enables direct asset exchange between different blockchains without a trusted third party or central authority . HTLC uses a set of hash locks and time locks implemented through smart contracts on different networks. It may be used in atomic swaps and payment channel networks.• Whitelisting requires service providers to screen and onboard participants individually to gain access to its function automatically. Consequently, service providers will need to ensure they have adequate risk and compliance processes and controls in place.• The combination of steps in the trade and settlement process brings about operational efficiencies in the trade execution and reduces settlement risks.• A potentially novel and notable feature of digital asset networks is shorter settlement cycles, including potentially instant settlement. This has implications for both credit and liquidity risks. Faster (or instant) settlement could reduce (or eliminate) replacement cost risk (a form of credit risk) and therefore reduce (or eliminate) the amount of margin required. However, this would likely involve pre-positioning cash and digital assets pretrade, which would increase liquidity costs.• Digital asset networks may perform other functions than those of FMIs for financial transactions, such as issuance of tokens, listing, registration, trading/market making, asset servicing and credit provision. These other functions may give rise to credit and liquidity risks to digital asset networks and their participants, and the relevant international standards (other than the PFMI) that may apply to those functions would need to be considered. <p>[Risk]</p> <ul style="list-style-type: none">• Validators, under this model, are known entities who are also permissioned by the governing body of the platform, and serve to ensure the integrity of the transactions that are recorded. For their effort, the validators are paid in fiat currencies. In some models, the validators may be regulated financial institutions, and subject to technology risk management controls.• Due to their decentralized nature, digital asset networks are likely to operate in multi-jurisdictional environments, subject to risks arising from potential conflicts.• The inability of an FMI to continue as a going concern could have systemic risk implications for its participants and the broader financial markets. As the operational arrangements (e.g., DLT) supporting a digital asset network are novel and notable, thorough consideration of how the operational arrangements affects observance of the Operational Risk Principle is necessary.• The issuance of tokens on a public permissionless network increases the complexity and potential surface area of attacks. As such, there is a risk of software or smart contract vulnerabilities such as attacks or cybersecurity breaches.• The use of open-source public protocols that are not maintained by regulated financial institutions would mean that it is possible for the underlying software to be forked.• There may be liquidity and maturity mismatch between the tokens that are traded and the assets that are used to back them. For example, a tokenised asset may offer the opportunity for its holders to redeem its underlying value at any time, but if the tokenised asset is backed by reserve assets that have a maturity profile that does not match, this might increase the redemption run-risk.• The distribution power of public and permissionless platforms, which offer ease of access but potentially introducing risks to financial stability and integrity are emerging. The Guardian proposes a framework to address these risks.• If responsibility for the digital asset arrangement is distributed across multiple entities, including potentially anonymous legal entities, this may be more challenging to demonstrate.

Chapter 1: The Evolution Advancement of Tokenization in the Financial Sector

5. Tokenization-related projects involving traditional financial institutions

Project name	Type of Block chain	Name of documents	author	Publicati on date	Project Overview	Descriptions related to this research
Project Guardian (Wealth Management)	Permi ssion ed Block chain	The Future of Wealth Management Ultra-efficient portfolio of traditional and alternative investments using tokenization	JPMorgan Chase Apollo	2023	<p>[Overview] As part of the Guardian initiative, MAS is conducting joint research and proof-of-concept experiments with overseas financial authorities and overseas companies. This paper reports on the results of a proof-of-concept experiment conducted under Project Guardian , a joint initiative of the MAS , which explored asset tokenization and cross-chain interoperability on permissioned blockchain networks, in collaboration with J.P. Morgan and Apollo.</p> <p>[Project participants] MAS, BIS, DBS Bank, HSBC, Marketnode, JPMorgan Chase & Co, Apollo, SBI Digital Asset Holdings, Standard Chartered, United Overseas Bank,etc</p> <p>[Research Contents] This paper describes limitations in discretionary portfolio management in the wealth management industry. The project proposes how tokenization can harmonize the treatment of public and private assets in portfolio management, creating significant value for asset managers, wealth managers and investors, and provide a proof of concept for delivering a scalable, next-generation system for seamless portfolio management. The proof of concept analyzes the benefits and considerations.</p> <p>[Purpose] A project promoted by MAS aims to improve the efficiency and liquidity of the wholesale fundraising market and to build a new financial market infrastructure using tokenization and DLT.</p>	-

Chapter 1: The Evolution Advancement of Tokenization in the Financial Sector

5. Tokenization-related projects involving traditional financial institutions

Project name	Project Overview
<p>Project Guardian (Wealth Management)</p>	<p>With the infrastructure in place, we the project executed a series of tests to demonstrate what the next generation of portfolio management could look like: Notably the project showed that the PM was able to update the target asset allocation for a given model (i.e., replace one asset for another), and the system automatically rebalanced all investor portfolios that tracked that model by initiating, placing and settling orders to redeem from and subscribe into the relevant funds, even though those funds were held on three different chains. Additionally, the project showed that when an investor deployed more capital for investment, the system could automatically place and settle orders in the right allocations according to the model, irrespective of what asset types were included in the model, or on which chain those assets were recorded. Essentially, by tokenizing funds and representing discretionary portfolios as smart contracts, we showed how tens of thousands of portfolios could be programmatically linked to representative models and automatically rebalanced en-masse when changes to those models occurred—even when these models included alternative investments. The multi-chain, multi-portfolio, multi-manager POC ecosystem and the Crescendo portfolio management solution are illustrated in the images below.</p> <p>Figure 1-5-5 End-to-end portfolio management and interoperability proof of concept</p> <p>The diagram illustrates the end-to-end portfolio management and interoperability proof of concept. It shows a flow from Investors to Portfolio Manager, then to Digital Assets, and finally to Fund Managers across three different blockchain environments: Provenance, Onyx, and Avalanche. The Portfolio Manager handles model creation, client relationship management, and portfolio rebalancing. Fund Managers issue and redeem funds based on orders from the Portfolio Manager. The diagram also shows how 'Buy / Sell Orders' are communicated cross-chain via an interoperability solution.</p> <p>Tokenize JP Morgan, Apollo & WisdomTree Funds on Onyx Digital Assets Blockchain</p> <p>Tokenize Apollo funds on Provenance Blockchain</p> <p>Tokenize WisdomTree Funds on Avalanche Blockchain</p> <p>Issue and redeem funds as per orders received from PM</p> <p>Model creation & management Client relationship management Portfolio rebalancing</p> <p>'Buy / Sell Orders' communicated cross-chain via interoperability solution</p>

Chapter 1: The Evolution Advancement of Tokenization in the Financial Sector

5. Tokenization-related projects involving traditional financial institutions

Project name	Project Overview
Project Guardian (Wealth Management)	<p>[Benefit]</p> <ul style="list-style-type: none">• Greater efficiency: Leveraging smart contracts to represent and record the ownership of assets could collapse the PM and operations roles into a single automated process, enabling portfolios to be deployed and rebalanced programmatically at scale. The presence of cash and fund ownership records on a shared ledger, combined with smart contract-enabled trade execution, could limit the need for costly reconciliations and occurrence of trade errors. At scale, the time and cost savings could allow wealth managers to reinvest in research and client-facing services like educating clients on how alts could fit into their portfolios. Efficiency benefits could accrue to others in the ecosystem as well, including asset managers, fund administrators, and other service providers. From an investor perspective, eliminating these friction points could enable PMs to be fully invested more consistently, meaning their portfolios would experience less cash drag (Unmanaged funds that investors hold as a buffer to cover the gap between the rights accrual of sold receivables and newly purchased receivables, etc.) . Assuming the average PM holds ~3% cash and a balanced portfolio could generate ~8% over cash in the long-term, the net result to a client is a ~24bps reduction in costs.• Potentially improved liquidity: Given the ease of sharing information across multiple parties on the same ledger system, and the ability to easily transfer ownership of tokenized assets, representing assets such as alts on a blockchain could potentially facilitate better liquidity markets for these assets. Today, selling an alts holding on a secondary market is typically a manual process negotiated on a bilateral basis. This can become problematic for individual investors, as oftentimes their holdings are not large enough to attract buyers given the time and paperwork required to complete a transaction. Simplifying these operational processes using smart contracts, coupled with alternative liquidity methods, such as the automated netting of subscriptions and redemptions, could add additional liquidity levers.• Enhanced investment outcomes through alternative investments: Streamlined processes and enhanced liquidity, as described above, could allow alternatives to be included in model portfolios and improve expected returns for investors and/or reduce volatility. It may also be possible to automatically rebalance portfolios based on changes to model portfolios, which could minimize deviations from target asset allocations, resulting in portfolios that align better with their optimal state.• Combining the efficiency of robo-advisory with the alpha of active management: Automated portfolio construction and management could provide a streamlined experience similar to robo-advisory offerings, but with a dedicated PM and higher potential returns through three sources of alpha: 1) the inclusion of alts; 2) manager due diligence on active strategies (e.g. identifying a top large cap growth fund); and 3) setting topdown asset class allocations based on CIO macro insights.• Flexibility and broader access: Leveraging interoperability solutions to connect distinct blockchain networks could provide access to tokenized investments across disparate chains, allowing PMs to build holistic solutions with the inclusion of these investment opportunities, which otherwise might not be accessible. <p>[Risk]</p> <ul style="list-style-type: none">• Investment Universe: The universe of tokenized investments must hit critical mass i.e., with respect to how many assets under management a wealth manager could deploy, the breadth of tokenized offerings available by asset class and a coalescing around operating models. While there continues to be many announcements in this space, the reality is that today you cannot build a robust portfolio of tokenized investments. The total inventory of tokenized real-world investments is approximately \$1.3 billion¹⁶ and is almost entirely composed of tokenized U.S. treasuries and private loans. It will take time for a respectable marketplace of tokenized investments to emerge, but there is demand from both fund managers and investors to further tokenize investments.• Liquidity: In this POC , we used subscriptions and redemptions placed directly with the fund managers as the mechanism by which investors entered or exited investment vehicles. To make this real, we would need to extend this work to consider purchases and sales on secondary markets so we could consider the full range of options to enter and exit positions. Similarly, we believe there is merit in exploring how alternative investment funds with capital calls could be included in this context. As mentioned earlier, alternative investment funds require additional liquidity considerations, given they are generally less liquid than traditional investments. While tokenization has the potential to enhance liquidity by creating a more efficient secondary transaction process, this technology does not, in and of itself, create liquidity.

Chapter 1 The Evolution of Programmability (Tokenization) in the Financial Sector

5. Tokenization verification project involving traditional financial institutions

Project name	Project Overview
Project Guardian (Wealth Management)	<p>[Research results]</p> <p>The POC mainly examined the following items:</p> <ul style="list-style-type: none">• How to improve the efficiency and scalability of order execution and settlement across multiple asset classes and ownership registries.• A method of incorporating alternative investments, which are more difficult to manage and have limited liquidity than traditional public assets, into a discretionary portfolio.• How to overcome the fragmentation and interoperability challenges posed by multiple owner registries developed with different technology protocols.• A method to simplify the use of multi-user, multi-asset shared ledgers by abstracting the technical complexities inherent in blockchain technology. <p>According to the results of POC , offering discretionary portfolios including alternative investments to wealthy individuals could have the following potential benefits for key stakeholders:</p> <ul style="list-style-type: none">• Wealth Managers: A wealth management firm with a portfolio of 100,000 clients reduces their monthly rebalancing process from 3,000+ steps to just a few clicks.• Investors: Programmatic rebalancing and near-instant settlement reduces costs by nearly 20% by eliminating cash drag .• Asset managers, wealth managers and distributors: unlock \$ 400 billion in new revenue opportunities annually through the broad distribution of alternative investments to high net worth individuals.• Service providers (fund administrators, transfer agents, etc.): Leveraging automation and digitization improve efficiency, reduce costs, increase transparency and mitigate risk.

Chapter 1: The Advancement of Tokenization in the Financial Sector

5. Tokenization-related projects involving traditional financial institutions

Project name	Type of Blockchain	Title of the article	author	Publication date	Project Overview	Descriptions related to this research
DREX Project	Polygon, etc.	Lift Papers Laboratories Review Finance Innovations e Technologies LIFT Paper Financial Technology Innovation Laboratory Journal No.5	Brazil Central Bank	April 2023	<p>[Overview] DREX is a central bank digital currency (CBDC) project that the Brazilian Central Bank (BCB) has been developing since 2020 , and will be backed by the Brazilian real (BRL) , the country's legal tender .</p> <p>LIFT, established in 2018 by BCB in partnership with Fenasbac as a research institute to foster innovation and commercialize ideas in an open and collaborative way , has previously made 256 proposals, and 91 projects were selected, of which 76 prototypes have been finalized. This paper presents the results of research conducted on eight LIFT Lab projects that present the latest proposals for innovation in national financial systems.</p> <p>[Project participants] In addition to BCB and Fenasbac , the document includes more than 10 other topics, each with participation from banks, fintech companies, technology providers, and others, etc.</p> <p>[Research Contents] The paper covers features such as microcredit, interoperability between Real Digital and other networks, and digital BRL (named Pix) such as NFC, offline QR codes, and credits. In addition, the paper features LIFT Challenge projects, a special edition of LIFT Labs focused on Real Digital use cases. Nine prototypes are featured, focusing on financial, non-financial, and cryptocurrency buying and selling, as well as projects focused on decentralized finance, Internet of Things, international remittances, and offline payments.</p>	<p>With the primary motivation of "transitioning to a cashless economy", it goes beyond the role of CBDC as a payment system and seeks to show how innovation can be used to impact everyday life and how central banks have a key role to play in fostering innovation in collaboration with the private sector.</p> <p>Real Digital 's infrastructure and LIFT 's use case to offer learnings for central banks around the world about the potential of programmable CBDCs , including allowing authorities to analyse the propagation of economic shocks from information contained in payment network data.</p>

Source: <https://revista.liftlab.com.br/>

Chapter 1: The Advancement of Tokenization in the Financial Sector

5. Tokenization-related projects involving traditional financial institutions

Project name	Project Overview
DREX Project	<p>[Purpose]</p> <p>BCB aims to improve financial market efficiency and promote financial inclusion through the introduction of DREX, whose retail version will be offered by regulated financial intermediaries. Financial intermediaries will convert demand deposits and e-money balances into DREX, allowing their clients to use various intelligent financial services. Retail DREX will enable citizens to access various financial transactions using digital assets and smart contracts, which will be settled on wholesale DREX issued by BCB within the DREX platform. DREX will reduce the costs of traditional and innovative financial transactions, ultimately supporting the democratization of finance.</p> <p>Role of the BCB: Expanded influence on monetary and fiscal policy.</p> <ul style="list-style-type: none"> - Improved data observable by authorities allows government policy implementation to be more informed. - Part of monetary and fiscal policy implementation can be automated and made conditional on information contained in the database in an automated way (as opposed to the previous main tool being interest rate payments).The role of the BCB : Expanding influence on monetary and fiscal policy. <p>[Benefit]</p> <ul style="list-style-type: none"> • It reduces verification costs, as smart contracts automatically check for compliance with credit line rules and ensure proper use of funds. • CBDCs could create cheaper and easier-to-use foreign exchange services for citizens. • The tokenization process seeks to minimize the amount of data that companies need to hold to conduct transactions, which can provide a wide range of benefits, including lower transaction costs, increased transparency, liquidity, efficiency, access to alternative capital sources, and decentralization. • By making various ledgers, both public and government, interoperable at a liquid and low cost, people can enjoy benefits such as reduced costs of services, increased competitiveness among players, and greater customer uptake among low-income groups. • Facilitating blockchain interoperability is critical because it stimulates competition, reduces costs, enables economies of scale, and increases user convenience. • Facilitating interoperability increases the visibility of assets in a country's economy and allows crypto-active investors from around the world to contribute capital to the national financial system, increasing user convenience and increasing the supply of capital to assets in a country's economy. It also increases user convenience for cryptocurrencies. • In terms of foreign exchange, exchanges between assets in the pool are done without the need for centralized order books, significantly reducing the reliance on suppliers from external markets, as well as democratizing and simplifying the process of providing liquidity for assets traded on the blockchain. The liquidity of these exchanges can also be seen by decentralized agents (arbitrage), eliminating the need to rely solely on centralized institutions and reducing the risk of exchange rate exposure for institutions providing such services.

Chapter 1: The Advancement of Tokenization in the Financial Sector

5. Tokenization-related projects involving traditional financial institutions

Project name	Project Overview
DREX Project	<p>[Risk]</p> <ol style="list-style-type: none"> 1. The risk of double spending Offline and online transactions require entirely different frameworks, , which complicates implementation and creates the risk of double-spending. 2. Risks Related to Privacy and Bank Secrecy Act The transaction history on the public network is accessible to anyone and is tied to the public keys of the wallets participating in each transaction. If the identity of the wallet owner is exposed, it could potentially lead to a chain reaction that exposes the identities of other participants who interacted with that wallet. This risk violates Bank Secrecy Act and directly impacts the reliability of the system. The limitations of public blockchains make it difficult to address risks related to the Bank Secrecy Act. 3. Investor risk of price mismatch The risk of a "mismatch" between the amount claimed and the amount received for a volatile currency. This is related to the operation of AMMs and is caused by the price difference between when a token is added and when it is withdrawn from the liquidity pool. 4. Risk of loss of intermediation for commercial banks This raises concerns that CBDC could disintermediate commercial banks. Supplementary explanation: If CBDC transforms the structure of financial transactions, it may redefine the traditional role of commercial banks. Until now, commercial banks have acted as intermediaries when customers make payments, but if CBDC becomes widespread, that intermediary role may become unnecessary, raising concerns that commercial banks' raison d'être may decrease. There is also a view that the role of commercial banks will decrease as direct CtoC (C2C) transactions increase, which could lead to major changes in the business models and functions of commercial banks. 5. Transition Risk Transition risk arises when real-time gross settlements are migrated to the CBDC infrastructure. Supplementary explanation: If interoperability between the existing payment system and the new CBDC infrastructure is not ensured during the period in which the existing payment system and the new CBDC infrastructure are operated simultaneously, settlements may be delayed or fail. If data formats and protocols differ between the systems, errors may occur in the transmission and processing of information. 6. Risk of Impermanent Loss Because AMM fees are a function of price differentials, liquidity providers are subject to the risk of impermanent loss. 7. Risk of uncertainty in token value Uncertainty about the value of tokens could result in financial losses to holders. Even stablecoins have exchange rate risk.

Chapter 1: The Advancement of Tokenization in the Financial Sector

5. Tokenization-related projects involving traditional financial institutions (continued)

Project name	Project Overview
DREX Project	<p>8. Blockchain Operational Risks Digital asset holders are exposed to the following risks: Cyber attacks Custody risk (loss of assets, access restrictions, theft, theft of private keys) Blockchain Availability Outage</p> <p>9. Risk of Loss of Control over Monetary Policy The use of a public network would complicate the process of governing the interoperability of CBDC with other tokens, thereby risking a loss of control over monetary policy.</p> <p>10. Risks associated with the use of bridges Due to the underdeveloped nature of the bridge, there are the following risks: (i) The impact of code flaws on smart contracts and the potential loss of funds (ii) Technical risks due to software failures and attacks (iii) Risk of censorship by bridge operators (iv) Custodial risk of funds theft by bridge operators</p> <p>11. Risks associated with Oracle Issues Oracle issues could lead to smart contract security failures and the inability to run a project. Risk details: (i) Information security risks (inaccurate or false information) (ii) Risk of delays in updating data (iii) reputational risk to Oracle management organizations</p>

Chapter 1: The Advancement of Tokenization in the Financial Sector

5. Tokenization-related projects involving traditional financial institutions

Project name	Project Overview
DREX Project	<p>[Risk mitigation measures]</p> <ol style="list-style-type: none"> 1. Mitigation measures for the risk of double spending Improve integration and interoperability between offline and online frameworks. Implement rigorous verification processes and security protocols to prevent double spending. 2. Mitigating Risks Related to Privacy and Bank Secrecy Act Employ privacy-preserving techniques (e.g., zero-knowledge proofs, anonymization protocols). Use permissioned blockchain to strengthen access control. KYC/AML procedures will be thoroughly implemented, and measures to prevent data leaks will be implemented. 3. Measures to mitigate Investor risk of price mismatch Introduce strategies to hedge against price fluctuation risks. Choose currencies and assets with low volatility. Monitor prices in real time and trade at the right time. 4. Measures to mitigate the risk of loss of intermediation for commercial banks For commercial banks to take on new roles in distributing and managing CBDC . Enhance value-added services for commercial banks and maintain their relevance in the ecosystem. 5. Migration measures for Transition Risk Promote standardization to ensure interoperability between existing payment systems and CBDC infrastructure. We will conduct thorough testing and monitoring during the transition period to detect and resolve any issues early. 6. Measures to reduce Risk of Impermanent Loss Provide risk education and information to liquidity providers. Employ algorithms and AMM models that minimize impermanent losses . Provide insurance products and hedging instruments to cover risks. 7. Measures to mitigate the risk of uncertainty in token value This will make the reliability of tokens' backing assets and issuers more transparent. Utilize financial products to hedge currency risk. Choose a reliable stablecoin.

Chapter 1: The Advancement of Tokenization in the Financial Sector

5. Tokenization-related projects involving traditional financial institutions

Project name	Project Overview
DREX Project	<p>8. Measures to mitigate Blockchain Operational Risks Implement strong security measures (firewalls, encryption, intrusion detection systems, etc.). Use a reliable custody service for safekeeping of your assets. Strengthen private key protection measures, such as multi-signatures and hardware wallets. Increase redundancy and availability of the blockchain network.</p> <p>9. Measures to mitigate Risk of Loss of Control over Monetary Policy Regulators and central banks will be involved in the interoperability standardization process and ensure proper governance. Put in place technical and institutional mechanisms to maintain the effectiveness of monetary policy.</p> <p>10. Measures to reduce Risks associated with the use of bridges The Bridge's smart contract code will undergo a security audit by a third party. Choose reliable bridges and mature protocols. A decentralized bridge is used to reduce the risks associated with centralization.</p> <p>11. Risk Mitigation Measures associated with Oracle Issues Use multiple oracle sources to ensure data accuracy and reliability. Improve the update frequency of oracle data to enhance real-time performance. Increase transparency and governance of the Oracle management organization.</p>

Chapter 1: The Advancement of Tokenization in the Financial Sector

5. Tokenization-related projects involving traditional financial institutions

Project name	Type of Blockchain	Title of the article	author	Publication date	Project Overview	Descriptions related to this research
Project Mariana	Ethereum	Cross-border exchange of Wholesale CBDCs using Automated Market Makers Final report	BIS Innovation Hub	September 2023	<p>[Overview] Project Mariana looks to the future and envisions a world in which central banks have issued central bank digital currencies (CBDCs) and explores how foreign exchange(FX) trading and settlement might look. Mariana borrows ideas and concepts from decentralised finance (DeFi) and studies whether so-called automated market-makers (AMMs) can simplify FX trading and settlement with a view to enhancing market efficiency and reducing settlement risk.</p> <p>[Project participants] BIS Innovation Hub (BISIH), Bank of France, Monetary Authority of Singapore, Swiss National Bank</p> <p>[Purpose] Enhancing cross-border payment processes with CBDC</p> <p>[Benefit] The AMM delivers the contours of a possible future tokenised FX market that has a number of potential benefits. These include supporting simple and automated execution of FX transactions, providing options to broaden the range of currencies, eliminating settlement risk and enabling transparency.</p> <p>[Risk] The 24 hours a day 7 days a week availability of wCBDC may increase operational complexities for central banks, eg to ensure consistent remuneration across different forms of central bank money (out of scope for this PoC). Moreover, while the PoC demonstrates that central banks can manage their wCBDCs without necessarily owning or controlling the underlying platform, the wCBDC smart contracts may introduce new vulnerabilities. Specifically, it may introduce new types of security risks, which require a thorough review.</p>	<p>The AMM in this project will set the price and automatically execute FX transactions. Using an algorithm that allows instant settlement, Singapore Dollar and Swiss Franc wCBDC Pool the following:</p> <p>Source: FINADIUM " BIS tests cross-border wholesale CBDC settlement https://finadium.com/bis-tests-cross-border-wholesale-cbdc-settlement-with-central-banks/</p>

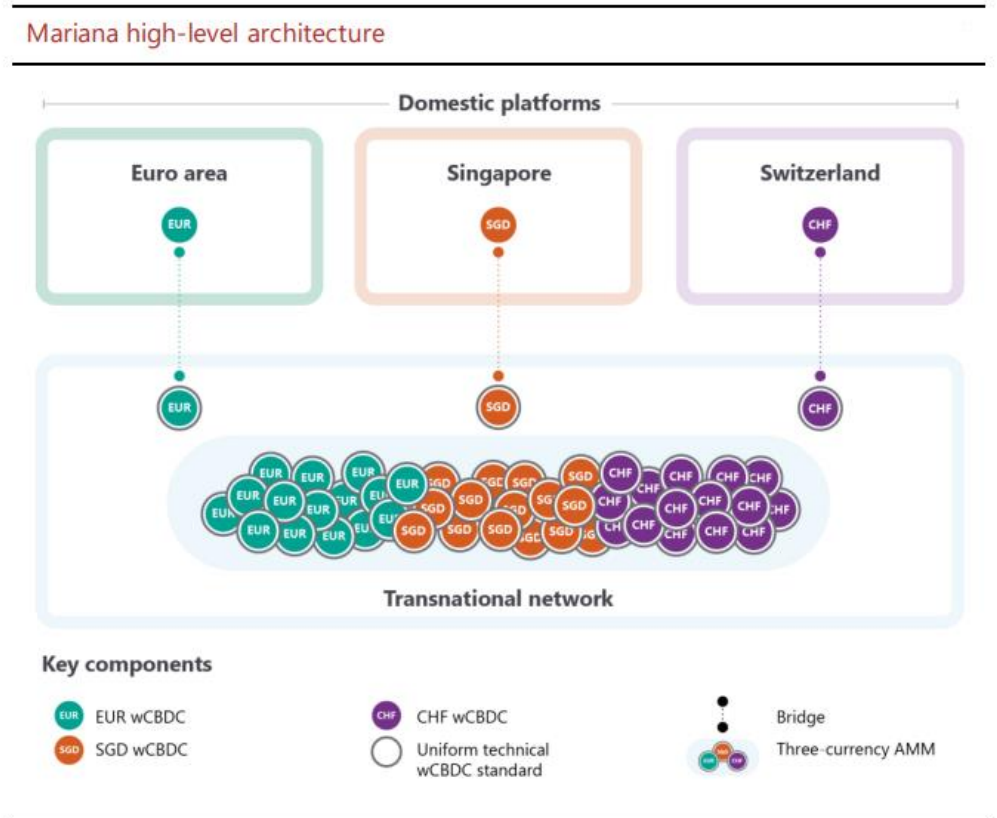
Source: <https://www.bis.org/publ/othp75.pdf>

Chapter 1: The Advancement of Tokenization in the Financial Sector

5. Tokenization-related projects involving traditional financial institutions

Project name	Project Overview
Project Mariana	<p>[Research Contents]</p> <ul style="list-style-type: none"> The primary objective of Project Mariana was to build a PoC of a 24 hours a day, seven days a week wCBDC ecosystem with an interbank FX market based on an AMM. Project Mariana is a proof of concept (PoC) for a global interbank market for spot FX featuring both an AMM and wholesale CBDCs (wCBDCs). This project examines if this new approach can simplify existing interbank FX processes. It also explores whether this approach can contribute to enhancing crossborder payments through improved transparency and reduced settlement risk. To this end, it tests three main components, in particular (i) a common technical standard for interoperability between wCBDCs; (ii) so-called bridges for wCBDC transfers between different networks; and (iii) an AMM for the FX trading and settlement. Mariana extends previous work looking at the feasibility of cross-border and FX transactions using wCBDC arrangements and distributed ledger technology (DLT) platforms (Bech et al (2023), BISIH et al (2022b) and BISIH (2023)). The experiment looks at the trading and settlement of spot FX transactions between commercial banks involving hypothetical euro (EUR), Singapore dollar (SGD) and Swiss franc (CHF) wCBDCs (see Figure 1-5-6). In particular, the project sought to explore how the amount of liquidity available to the pool, as well as how the parameterisation of the pre-defined algorithm, affect market liquidity (ie the ease with which wCBDCs can be traded for one another). These two objectives are mapped into corresponding use cases at the centre of the experiment (discussed below). Use case 1 focuses on FX transactions using wCBDCs in an AMM. Use case 2 considers the liquidity provision by commercial banks to facilitate FX transactions.

Figure 1-5-6 PoC Architecture



Chapter 1: The Advancement of Tokenization in the Financial Sector

5. Tokenization-related projects involving traditional financial institutions

Project name	Project Overview
Project Mariana	<p>[Research results]</p> <ul style="list-style-type: none"> • First, wCBDCs are implemented as smart contracts, enabling central banks to manage their wCBDC without the need to directly operate or control the underlying platform. Their design followed best practices from the public blockchain space, building on a widely used standard (ie ERC-20), as well as enabling upgradeability. • Second, bridges may serve as a mechanism to enable broader interoperability in an emerging tokenised ecosystem. As implemented in the PoC, they may enable the seamless and safe transfer of wCBDC between domestic platforms and the transnational network without manual intervention. The bridge design features controls and safeguards and ensures resilience through on-chain (ie bridge smart contracts) and off-chain (ie communication between bridge smart contracts) infrastructure managed by central banks. • Third, the AMM, as tested and calibrated in Project Mariana, fulfilled requirements based on selected FX Global Code (FXGC) principles. It delivers the contours of a possible future tokenised FX market that has a number of potential benefits. These include supporting simple and automated execution of FX transactions, providing options to broaden the range of currencies, eliminating settlement risk and enabling transparency. However, the use of AMMs requires the pre-funding of liquidity and their adoption would therefore entail a significant departure from the ex post funding (deferred net settlement) in use in today's FX markets. • The Project Mariana PoC was a first step towards understanding the potential benefits and challenges of AMMs for wholesale FX transactions using wCBDCs. Further work is needed on a range of aspects. • While tokenisation and DeFi may have potential benefits, a thorough investigation of security questions is needed. • More broadly, future work could extend Project Mariana into three areas. First, moving beyond technical feasibility, the commercial viability of AMMs for wholesale FX transactions vis-à-vis existing arrangements requires clarification. Collaboration between relevant stakeholders in FX markets would be required to enable such exploration. Second, tokenisation may raise questions about monetary policy implementation, from very specific ones (eg remuneration of wCBDCs) to very broad ones (eg monetary policy instruments building on DeFi ideas and concepts). Third, further work is needed to understand the role of central banks and wCBDCs in a broader tokenised ecosystem potentially including stablecoins, tokenised deposits and financial instruments, such as tokenised bonds and securities.

Chapter 1: The Advancement of Tokenization in the Financial Sector

5. Tokenization-related projects involving traditional financial institutions

Project name	Type of Blockchain	Title of the article	author	Publication date	Project Overview	Descriptions related to this research
JPM Coin	Permissioned Blockchain / Quorum	DEPOSIT TOKENS A foundation for stable digital money	Oliver Wyman, Onyx by JP Morgan Chase,	2022	<p>[Overview and Objectives] JPM Coin is a deposit token backed 1:1 by the US dollar and was launched in 2020 to support real-time gross settlements between JPMorgan 's institutional clients. This paper focuses on JPM Coin as a use case for deposit tokens, their benefits, and how they are distinguished from stablecoins and CBDCs . In doing so, this paper intend to provide a focused discussion of deposit tokens as a distinct type of digital money, contribute to the ongoing policy discussions about different forms of digital money, and inform stakeholders as industry and regulators look ahead to understand the role commercial banks will play in the future digital money landscape.</p> <p>[Project participants] JPMorgan Chase</p> <p>[Research Contents] The current state of digital money around the world, examples of deposit token use, and policy considerations</p> <p>[Research results] Deposit tokens are rooted in the existing deposit-taking activities of banks and are not the same product as non-bank stablecoins or CBDCs, and the frameworks for innovation and regulation should recognize the distinctions. For deposit tokens to create productive linkages between traditional banking systems and blockchain, they must exist as an extension of those traditional systems, both in design and in regulation.</p>	<p>Takis Georgakopoulos, JP Morgan's global head of payments , said on October 26 , 2023 that JPM Coin processes more than \$ 1 billion in transactions per day .</p> <p>*JPM 's entire settlement operations process nearly \$ 10 trillion per day , which is roughly one- thousandth of the amount .</p>

Source: <https://www.jpmorgan.com/onyx/documents/deposit-tokens.pdf>

<https://www.coindesk.com/business/2023/10/26/jpmorgan-handles-1b-transactions-daily-in-digital-token-jpm-coin-bloomberg/>

Chapter 1: The Advancement of Tokenization in the Financial Sector

5. Tokenization-related projects involving traditional financial institutions

Project name	Project Overview			
<p>JPM Coin</p> <p>Blockchain-based deposits refer to deposit claims against a licensed depository institution for stated amounts recorded on blockchain. They are economic equivalents of existing deposits recorded in a novel form used to pay, settle trades between digital assets, and generally act as a store of value and means of exchange on blockchain ledgers. Applying blockchain technology in this manner allows payments made with commercial bank money to benefit from programmability, instant and atomic transaction settlement, and improved transparency as to the status of transaction. These features help to address common pain points in liquidity management and cross-border payments.</p>	Table 1-5-7 Comparison of Blockchain-Based Deposits, Stablecoins coins, CBDCs			
		Blockchain-Based Deposits	Stablecoins	CBDCs
	Common issuer	Commercial banks	Non-bank private entities	Central banks
	Examples	<ul style="list-style-type: none"> •SGD deposit tokens by JPMorgan •Blockchain deposit accounts on JPM Coin System 	<ul style="list-style-type: none"> •USDC by Circle and Coinbase •USDT by Tether •BUSD by Paxos and Binance 	<ul style="list-style-type: none"> •Digital Yuan (extended pilot) •Swedish E- krona (pilot) •Digital Euro (investigation)
	Adoption	<ul style="list-style-type: none"> •JPM Coin System is live with material transaction volumes •Deposit token projects are generally in the pilot phases 	<ul style="list-style-type: none"> •Over US\$140 billion market capitalization (as of November 2022) since 2014 when the 1st major stablecoin was issued 	<ul style="list-style-type: none"> •Over 90 % of central banks are reportedly investigating CBDCs - live projects are still in early pilot phases
	Backing assets	<ul style="list-style-type: none"> •Claim on the issuer, like regular deposits 	<ul style="list-style-type: none"> •1:1 assets held by issuer to meet redemptions, typically held as HQLA 	<ul style="list-style-type: none"> •Central bank balance sheet
	Regulatory oversight	<ul style="list-style-type: none"> •Subject to the similar supervision and oversight as other regulated bank deposits 	<ul style="list-style-type: none"> •No regulatory framework in most markets, although regulatory frameworks are emerging 	<ul style="list-style-type: none"> •Secured and governed directly by national entities
	Risk management practices	<ul style="list-style-type: none"> •Subject to mandatory minimum liquidity, capital and risk management requirements by regulators •Subject to banks' internal risk management practices 	<ul style="list-style-type: none"> •No unified risk management framework •Subject to issuers' internal risk management practices 	
Emergency protections	<ul style="list-style-type: none"> •Strength of existing bank balance sheet •Access to contingency funding sources at central bank •Resolution and recovery planning to overcome financial distress 	<ul style="list-style-type: none"> •Liquidation of reserve assets •Resolution under traditional bankruptcy laws 		

Chapter 1: The Advancement of Tokenization in the Financial Sector

5. Tokenization-related projects involving traditional financial institutions

Project name	Project Overview
JPM Coin	<p>[Benefit]</p> <ul style="list-style-type: none"> • A deposit token integrated into the banking system provides new benefits when it becomes programmable by automating manual solutions, enabling complex logic for transactions without manual intervention, and reducing the risk of human errors or delays. Such automation drives efficiency not just in payment execution, but also in liquidity and collateral management, as well as reconciliation processes, among other areas. • The benefits of deposit tokens can be optimized by design choices that enhance their fungibility with other bank-issued deposit tokens and non-tokenized forms of money. • It simplifies clients' liquidity needs and delivers next-generation corporate treasury services. JPM Coin is a permissioned system that acts as a payment rail and deposit ledger, allowing participating JP Morgan clients to transfer US dollars on deposit with JP Morgan within the system, facilitating the movement of liquidity and ensuring timely settlement. It supports DVP (delivery-to-payment) , PVP (payment-to-payment) , machine- to- machine payments and more across borders. • Cross-border payments in particular is a space where we anticipate some of the most pronounced benefits of merging information and value on shared ledgers. It has been estimated that a multi-currency CBDC could cut costs by 80 %. Deposit tokens could unlock similar benefits by reducing fees, settlement times, and counterparty risks. • Tokenized asset marketplaces are settled atomically or simultaneously and near instantly, it can remove the risk that parts of a transaction are not settled because a counterparty fails or cannot deliver an asset. • Financial stability: It believes that it has the potential to improve the stability of the overall financial system by providing a more efficient and secure payment system than traditional payment systems. It is based on distributed ledger technology (DLT), which helps improve the transparency and traceability of transactions. • Customer Protection: It has strong security measures in place to protect customers from unauthorized access and theft. It is designed to protect customer privacy and give customers transparency and control. <p>[Risk]</p> <ul style="list-style-type: none"> • By leveraging the existing practices and regulations applied to traditional commercial bank deposits, deposit tokens can be positioned to address certain risks posed by stablecoins approaching systemically significant scale, preventing strain on stablecoin issuers and instability in the space. • Like traditional deposits, deposit tokens are a claim against an issuing depository institution. They should therefore be subject to the liquidity requirements and risk management standards imposed on deposit-taking banks today that seek to ensure the safety and soundness of deposits recorded using non-blockchain methods. • Reducing direct human involvement also introduces risks, such as potential for unnoticed errors due to software bugs, as well as limitations. Smart contracts should be reviewed and audited, and anticipated problems should be corrected. Banking institutions today regularly develop and employ sophisticated software in the course of providing banking services and their practices are subject to technology risk management standards overseen by risk management committees. Such expertise and risk management practices include robust development of programmability solutions, as with any other bank developed or bank employed software. • Real-time transparency of on-chain activity such as redemptions could exacerbate the perception of redemption risk by showing the activity of users making large redemptions, potentially inducing concerns that other users will not be able to redeem similar amounts and inciting run risk. • Bridging and wrapping stablecoins has typically been carried out by smart contracts written by third parties, which introduces additional operational and technical risk.

Chapter 1: The Evolution of Tokenization in the Financial Sector

5. Tokenization-related projects involving traditional financial institutions

Project name	Type of Blockchain	Title of the article	author	Publication date	Project Overview	Descriptions related to this research
DTCC Project Ion Platform	Permissioned Blockchain / Corda	BUILDING THE SETTLEMENT SYSTEM OF THE FUTURE	Murray Pozmanter Head of Clearing Agency Services and Global Business Operations	2021 September	<p>[Overview and Objectives] In this document, the Depository Trust Clearing Corporation (DTCC) lay out its vision for the most robust and efficient settlement system of the future, including its support for the efficiency offered by central counterparty clearing. We also provide an update on DTCC's DLT offering. Project Ion will introduce clearing and settlement capabilities using distributed ledger technology (DLT).</p> <p>[Project participants] DTCC subsidiaries National Securities Clearing Corporation (NSCC) and The Depository Trust Company (DTC)</p> <p>[Research Contents] Pursuing efficiency in clearing and settlement using DLT</p> <p>[Research results] Project Ion demonstrated that payments in a T+1 or T+0 environment could be a valid use case for DLT. DTCC tested a Project Ion proof of concept as a DLT use case in mid- 2020 and expanded the functionality into a fully-fledged prototype in 2021. The prototype provided pilot uses with multiple interfaces including adoption of a DLT Node, an API interface, and user interfaces. The proposed design was inspired by key concepts from its strategic roadmap work, the Settlement Optimization and Accelerated Settlement initiatives, and was specifically modeled around T+0 settlement cycle- though capable of supporting any settlement cycle.</p> <p>Multiple DTCC clients participated in the prototype and provided feedback to help shape DTCC's view of possible enhancements to DTCC core clearance and settlement processes and workflows .</p>	<p>Project Ion is a stock settlement platform provided as an alternative service to the existing settlement service of DTCC (Depository Trust & Clearing Corporation) , and claims to have processed 160,000 transactions per day on peak days. Corda DLT is used as the blockchain-related technology . As of the end of March 2024, the pilot is still in operation as an MVP (minimum viable product) .</p> <p>Source: DTCC Consulting " DTCC's Project Ion platform "</p>

Source: <https://www.dtcc.com/dtcc-connection/articles/2021/september/16/building-the-settlement-system-of-the-future>

Chapter 1: The Evolution of Tokenization in the Financial Sector

5. Tokenization-related projects involving traditional financial institutions

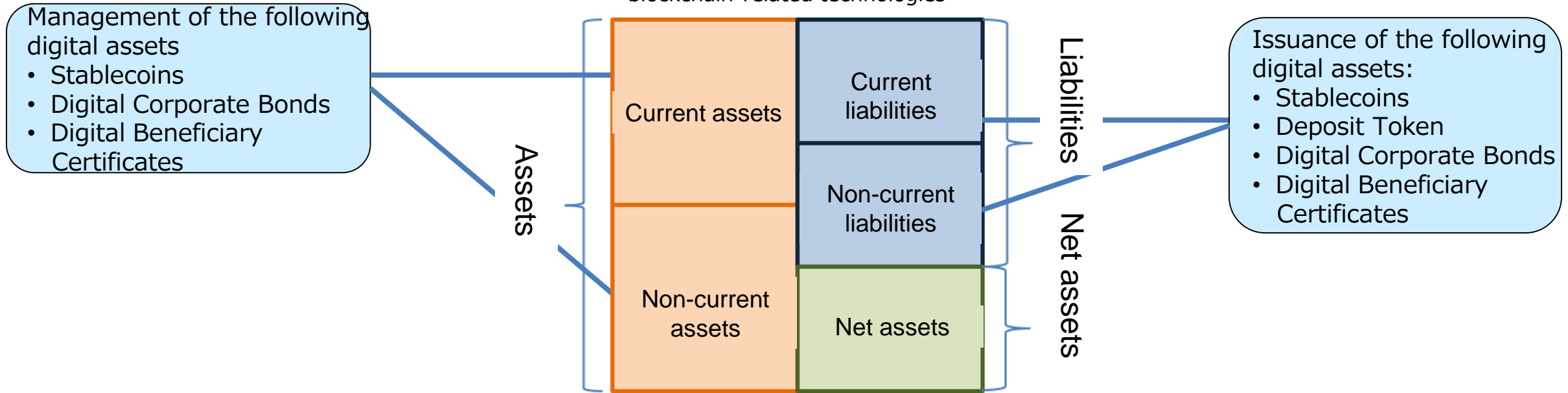
Project name	Project Overview
DTCC Project Ion Platform	<p>[Benefit]</p> <p>Shortened settlement times reduce market risk and margin requirements, which will allow firms to use those resources in other ways.</p> <ul style="list-style-type: none">•Margin Reduction: For broker/dealers, a move to T+1 would lead to a significant reduction in margin and collateral requirements. Today an average of over \$13.4 billion is held in margin every day to manage counterparty default risk in the system. Shortening the settlement cycle would help strike an improved balance between risk-based margining and procyclical impacts. Last year, DTCC's risk analysis and risk model simulations showed that the Volatility component of NSCC's margin could potentially be reduced by approximately 41% by moving to T+1, assuming current processing and without any other changes in client behavior. Over the last year, the Volatility component has accounted for approximately 60% of NSCC's total margin. Notably, in times of market volatility, this amount is significantly greater.⁴•Risk Reduction: While a shorter settlement cycle would deliver reduced margin requirements to the industry and lower costs for investors, the systemic and process improvements needed to achieve T+1 would also enhance market resilience. The move to T+1 would have many benefits, such as reducing systemic risk, operational risk, liquidity needs, buy-side counterparty exposure, and broker-to-broker counterparty risk. Faster settlement times reduce market risk and margin requirements, freeing up firms to use their resources in other ways.

Chapter 1: The Evolution of Tokenization in the Financial Sector

6. Impact of Tokenization on the Financial Sector

- Below is a diagram that maps the assets and liabilities in the balance sheet of a traditional financial institution and use cases using blockchain-related technologies.
- In the future, traditional financial institutions may have more opportunities to actively handle these digital assets and liabilities, which could lead to an even greater impact on their balance sheets .

Figure 1-6-1 Balance sheet and blockchain-related technologies



Digital Assets	Overview
Stablecoins	Major stablecoins (USDC , USDT , BinanceUSD , DAI , etc.) was expected to remain above \$ 120 billion in 2023 .
Deposit Token	There are moves toward practical use, such as JPM Coin by the US bank JPMorgan Chase .
Digital Corporate Bonds	In Japan, 13 bonds were issued in 2023, totaling 15 billion yen.
Digital Beneficiary Certificates	In Japan, 29 bonds were issued in 2023 , totaling approximately 100 billion yen.

Chapter 1: The Evolution of Tokenization in the Financial Sector

7. The nature of tokenization in the financial sector

- In Japan, almost all tokens handled by traditional financial institutions are issued on permissioned chains. Meanwhile, overseas, there are examples of tokens using permissionless chains such as Ethereum (such as BlackRock's BUIDL Fund). In addition, many of the tokens handled by cryptocurrency exchanges are mainly issued on permissionless chains.
- There are many differences in the nature of transactions between tokens handled by traditional financial institutions and cryptocurrencies handled by cryptocurrency exchanges.

Table 1-7-1 Differences in the nature of token transactions handled by regulated financial institutions

Aspects	Permissionless chains	Permissionless chain handled by traditional financial institutions	Permissioned chains handled by traditional financial institutions
Main Tokens	Crypto assets, stable coins	Security tokens, stable coins	Security tokens, stable coins
KYC	<p>An address (generated from a public key) alone cannot prove identity.</p> <p>Cryptocurrency exchanges continuously manage KYC-certified customer attributes by linking them to addresses.</p>	<p>An address (generated from a public key) alone cannot prove identity.</p> <p>Traditional financial institutions continuously manage KYC-certified customer attributes by linking them to addresses.</p>	<p>Since only authorized users participate, the customer information obtained through KYC serves as a trusted guarantee of identity, similar to a public key certificate.</p>
Token Transfer Restrictions	<p>Investors can transfer tokens to personal wallets they control and transfer tokens from personal wallets to wallets whose KYC are not completed.</p> <p>Restrictions can be applied on an address-by-address basis based on blacklists.</p>	<p>As a general rule, it is necessary to design the system so that tokens cannot be moved to personally managed wallets controlled by investors.</p> <p>Management of the tokens will be entrusted to traditional financial institutions.</p>	
Revocation authority for public key certificates	<p>Since there is no mechanism for public key certificates (which guarantee that a public key really belongs to a person), there is no revocation authority either.</p> <p>However, there are ways to revoke public keys and replace them with new key pairs by introducing a mechanism for public key certification through smart contracts, as exemplified by social recovery wallets.</p>		<p>Traditional financial institutions have the revocation power.</p>

Source: <https://decrypt.co/222694/blackrock-ethereum-fund-build>

Chapter 1: The Evolution of Tokenization in the Financial Sector

8. Summary

In Chapter 1, Part 1, entitled "The Emergence and Spread of Blockchain-Related Technology and Decentralized Financial Systems," begins with the birth of cryptocurrencies and describes the current situation in which many transactions are being conducted in decentralized financial systems as an applied application of blockchain-related technology.

In Chapter 1, Part 2, "Comparison of the Characteristics of Decentralized Finance with Traditional Finance," We explained the differences between decentralized finance and traditional finance, such as the fact that in traditional finance, transaction parties have completed KYC and the main service providers are licensed financial institutions under industry regulations and are under supervision by financial authorities, whereas in decentralized finance (especially in the early stages), transaction parties are unclear and the main service providers are DAOs .

In Chapter 1, Section 3, "Reviewing the Supervision of Decentralized Finance," introduces the movement to consider industry regulations in response to the increase in hacking and other incidents in decentralized finance.

In Chapter 1, Section 4, we introduced examples of initiatives aimed at protecting users, etc., under the heading of "Case Studies of Decentralized Finance."

In Chapter 1, Section 5, titled "Verification project on tokenization involving traditional financial institutions," we introduced research conducted by traditional financial institutions and financial regulatory authorities on tokenization and decentralized finance, including financial stability and user protection.

In Chapter 1, Section 6, "The Impact of Tokenization on the Financial Sector," introduces market trends for digital assets that may be recorded on financial institutions' balance sheets , and suggests that if the trend toward expanding tokenization continues, the impact on traditional financial institutions may also increase.

In Chapter 1, Section 7, "The Nature of Tokenization in the Financial Sector," we pointed out that there were trends that differ from the situation surrounding cryptocurrency exchanges.

This chapter has introduced the trend of tokenization in the financial sector and attempts to comply with financial regulations in decentralized finance-related systems. In order for regulated financial institutions to manage tokenization and decentralized finance-related systems and for regulatory authorities to supervise them, it will be necessary to understand the mechanisms and seek more appropriate management and supervision procedures.

Therefore, in Chapter 2 , we will investigate cases of SupTech by financial regulatory authorities and RegTech by regulated financial institutions in relation to blockchain-related technologies.

Chapter 2 Possibility of RegTech/SupTech based on Blockchain technology

Chapter 2 Possibility of RegTech/SupTech based on Blockchain technology

1. RegTech / SupTech verification projects involving financial authorities

In this document, the main technical terms that appear in Chapter 2 are defined as follows.

term	Definition
Embedded Supervision	<p>This refers to a technology that automatically monitors transactions and accounting data by incorporating supervisory functions into distributed ledgers. It is expected that this will reduce the need for companies to actively collect, verify, and provide data.</p> <p>This definition is based on " Embedded supervision: how to build regulation into decentralised finance" published by the BIS in September 2019.</p> <p>In this document, embedded supervision is considered to be the case where regulated financial institutions embed compliance functions into the decentralized financial systems and related systems they manage, or where regulators embed supervisory functions into systems related to decentralized financial systems that they wish to supervise.</p>
Supervisory Node	<p>A supervisory node is what node constantly monitors the transactions of financial institutions. In this document, we assume that the regulatory authorities themselves will be in charge of the nodes.</p>
SupTech	<p>This refers to technologies used by regulatory authorities and other organizations to support regulatory operations.</p> <p>In contrast to traditional supervision and audit work, which mainly involves paper-based documents and manual data analysis, SupTech aims to enable regulatory authorities and other parties to make these operations more efficient, automated, and sophisticated by utilizing IT technologies such as AI, big data, cloud computing, and blockchain.</p>
RegTech	<p>This refers to technologies used by regulated financial institutions to support compliance with regulatory, reporting and other legal requirements.</p> <p>While traditional compliance work such as regulations and reporting obligations has mainly involved paper-based documentation and manual data analysis, RegTech aims to enable regulated financial institutions to streamline, automate and enhance these operations by utilizing IT technologies such as AI, big data, cloud computing, and blockchain.</p>

We will introduce supervisory nodes as SupTech from among the verification projects of authorities , etc. We will investigate previous cases and literature on embedded supervision as SupTech or RegTech.

Next, in Section 2-2, in light of IOSCO 's guiding principle of " same activities, same risks, same regulations and regulatory outcomes ," we will compare the functions of decentralized finance using blockchain technology with those of traditional finance that meet regulatory requirements and are equivalent to RegTech , and consider the significance of RegTech in the decentralized finance.

Chapter 2 Possibility of RegTech/SupTech based on Blockchain technology

1. RegTech / SupTech verification projects involving financial authorities

In Chapter 1, we introduced the trend of tokenization in the financial sector and attempts to comply with financial regulations in decentralized finance-related systems. In order for regulated financial institutions to manage tokenization and decentralized finance-related systems and for regulatory authorities to supervise them, it will be necessary to understand the mechanisms and seek more appropriate management and supervision procedures.

Therefore, in Section 2-1, we will investigate previous cases and literature on supervisory nodes as SupTech and embedded supervision as SupTech or RegTech from among the verification projects conducted by authorities and other organizations .

- The projects surveyed in this chapter are as follows:
 - A New Use Case: A Supervisory Node (Boston Federal Reserve Bank)
 - Embedded supervision: how to build regulation into decentralised finance (BIS working paper)
 - The Use of Supervisory and Regulatory Technology by Authorities and Regulated Institutions (FSB)
 - “ Decentralised ” or “disintermediated” finance: what regulatory response? (French ACPR)

Chapter 2 Possibility of RegTech/SupTech based on Blockchain technology

1. RegTech / SupTech verification projects involving financial authorities

Project name	Type of Blockchain	Title of the article	author	Publication date	Project Overview	Descriptions related to this research
Boston Fed PoC Project	Ethereum, Hyperledger Fabric	Beyond Theory: Getting Practical With Blockchain	Federal Reserve Bank of Boston	February 2019	<p>[Overview] This paper reports on two blockchain proof-of-concept (PoC) projects conducted by the Federal Reserve Bank of Boston from 2016 to 2017.</p> <p>[Project participants] A team of engineers from within the Boston Fed</p> <p>[Research Contents] With the aim of learning the technology rather than actually implementing it, we considered and implemented a specific use case, namely, "reconciliation between each depository institution and the Fed's general ledger." We have summarized the key points obtained from this experiment when implementing a blockchain platform.</p> <p>[Research results] (Benefits and Suggestions) 1. The project's desired outcomes were largely achieved by a team within the Fed using existing technologies and frameworks. (Challenges) 1. The open source community was volunteer-based. Technical support was immature, and documentation and QA were insufficient. In addition, technology was evolving rapidly, and we were often forced to make large-scale code revisions. 2. Ethereum did not support private transactions and was not suitable for the use case. Hyperledger Fabric can set up private channels, but it results in a very complicated network diagram. (Next approach) A "supervisor node" was considered as a new use case for Hyperledger Fabric . Although no concrete demonstration was conducted, a configuration in which a supervisor node is placed at the center of each private channel of Hyperledger Fabric is being considered.</p>	The Boston Fed's website also includes an introductory text along with the document, which reads, "Going beyond the fundamentals of distributed ledger technology, the Boston Fed will develop two use cases for learning purposes to understand how a blockchain platform can help it perform specific functions within its business. There is no intention to move these into a production environment. This report describes the use cases, the technologies employed, and the insights gained."

Source: <https://www.bostonfed.org/publications/fintech/beyond-theory-getting-practical-with-blockchain.aspx>

Chapter 2 Possibility of RegTech/SupTech based on Blockchain technology

1. RegTech / SupTech verification projects involving financial authorities

Project name	overview
Boston Fed PoC Project	<p>Supervisory node is a general term that can include many roles beyond the Fed 's role as a regulator, such as auditor, enforcer of rules for the payment network, data reporting agency, etc. Therefore, some of the experiments are more general and not necessarily tied to a specific role as a regulator. The project recognizes the following challenges in what can be achieved by combining blockchain technology and smart contract logic with artificial intelligence and machine learning:</p> <ul style="list-style-type: none">• What business functions can a supervisory node perform (auditor, regulatory overseer, enforcer of the rules of the payment network)?• What architectural problems do supervisor nodes cause?• Can access to data be restricted to only what is needed to perform stated functions?• Could monitoring nodes be compromised or pose operational risks to the network?• If multiple blockchain platforms are utilized for a particular business process (e.g. delivery vs. payment, or DVP) , what are the implications for the overseer node architecture and performance?• If sister supervisory agencies sharing supervisory responsibilities could develop a single supervisory node structure, what new architectural/technical issues would that raise?• What can be done to detect and manage bad actors in private payment networks? (This goes beyond the role of the Federal Reserve and may be more appropriately applied to parties charged with enforcing rules, such as private payment network operators) .• How can fraud be detected? If it can be detected in a shared network by nodes supported by AI logic, what are the possible responses?

Chapter 2 Possibility of RegTech/SupTech based on Blockchain technology

1. RegTech / SupTech verification projects involving financial authorities

Project name	Type of Blockchain	Title of the article	author	Publication date	overview	Descriptions related to this research
BIS Research Activity Report	Decentralized finance/distributed ledger in general	Embedded supervision: How to build regulation into decentralised finance	Raphael Auer	September 2019 (revised May 2022)	<p>[overview]</p> <p>This paper proposes a new concept of "embedded supervision," which is a framework for monitoring compliance in decentralized markets by automatically reading the market ledger. Unlike traditional legal regulations, decentralized markets ensure data reliability based on economic agreements. Therefore, regulators need to have advanced technical know-how and strong will to realize embedded supervision.</p> <p>[Expected effects of embedded supervision]</p> <ol style="list-style-type: none"> 1. Increased efficiency through automation Embedded supervision is based on distributed ledger technology, which can automate fundamental aspects of market transactions, such as matching supply and demand and price discovery. This technology has the potential to automate exchanges, over-the-counter markets, and in the future securities and derivatives trading. For example, asset-backed tokens banks have could be automatically verified to comply with Basel III capital standards by calculating ownership and risk weights of balances in the distributed ledger. Similarly, token ecosystems could automatically monitor the asset backing of stablecoins. 2. Reduce administrative costs Supervising automated financial transactions can reduce compliance management costs, which are significant burden for both regulators and financial institutions. 3. Reducing settlement risk Automating transactions is also expected to help minimize operational risks associated with settlement failures. 4. Increased accessibility to data A distributed ledger automatically records all basic transaction data, and with embedded supervision this data can be easily accessed. <p>Embedded supervision represents an innovative approach to ensuring compliance in decentralized markets, and is a promising way to advance the technology as it offers numerous benefits, including automation, cost savings, risk reduction, and improved data accessibility.</p>	<p>In this document, "embedded oversight" refers to technology that automatically monitors transactions and accounting data by incorporating oversight functions into a distributed ledger.</p> <p>"Embedded supervision" can take advantage of the benefits of distributed ledgers and has the potential to make regulatory oversight more efficient and sophisticated (see left). Furthermore, one important point made in this paper is that in order for decentralized financial systems to become widespread and expand, the concept of "economic finality" (the state in which a transaction is deemed to have been finalized and ownership transferred) needs to be fundamentally redefined. In traditional financial systems, a centralized authority guarantees the confirmation of transactions and the transfer of ownership. However, in a decentralized financial system, such a central authority does not exist, so the concept of economic finality must be redefined. This paper argues that clarifying the concept of economic finality in a decentralized financial system can lead to safer and more efficient financial transactions.</p>

Source: <https://www.bis.org/publ/work811.htm>

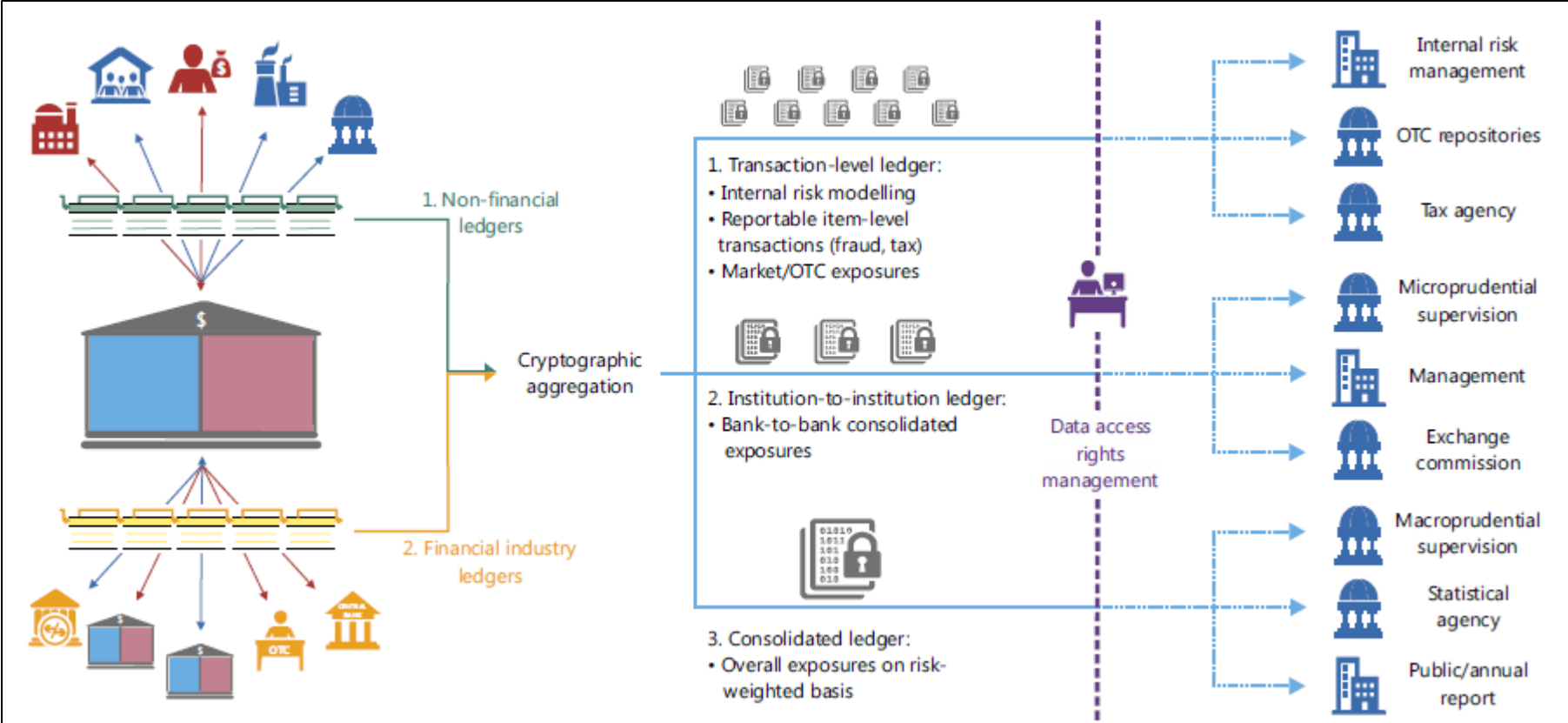
Chapter 2 Possibility of RegTech/SupTech based on Blockchain technology

1. RegTech / SupTech verification projects involving financial authorities

Project name	overview
BIS Research Activity Report	<p>[Principle of embedded supervision] The following guidelines show the use of embedded supervision:</p> <ul style="list-style-type: none">• Embedded supervision can only work as part of an overall regulatory framework that is supported by effective legal and supporting institutions.• Embedded supervision can also be applied to decentralized markets to achieve economic finality.• Embedded supervision needs to be designed within the economic market consensus, taking into account how the market will react to automatic supervision.• Embedded supervision should promote low-cost compliance and ensure a level playing field between large and small businesses. <p>[Operational Considerations] In order for regulators and financial institutions to have an incentive to actually implement embedded supervision, it is necessary to take into account the following points regarding the operational aspects of embedded supervision:</p> <ol style="list-style-type: none">1. Fairness: The aim should be to level the playing field between large and small financial institutions by reducing compliance costs.2. Reducing marginal costs: Regulators and financial institutions should aim to reduce the marginal costs of doing business by making it easier to access reliable public information, such as statistics and registration information.3. Limitations of the distributed ledger itself: The distributed ledger, which is the technological foundation of embedded supervision, also has security vulnerabilities. The use of a distributed ledger merely simplifies the processes of standard transactions and contracts, and in cases where a complex situation arises, it is necessary to rely on traditional legal procedures. <p>Embedded supervision reduces the cost burden on financial institutions and provides high-quality data to supervisors. However, the reliability of the ledger data requires legal guarantees. From a technical standpoint, it is necessary to consider a mechanism that uses encryption technology to ensure that supervisors can access only the data they need.</p> <p>[Novelty compared to conventional research] While conventional regulations are based on existing legal systems, this paper proposes a new monitoring framework that utilizes the characteristics of decentralized markets. What is novel is that it specifically explores the possibility of automated monitoring based on economic consensus.</p> <p>[Limit] The proposed framework relies heavily on legal foundations and operational support bodies to ensure the economic credibility of the distributed ledger, and further research is needed into the impact of oversight on market participants.</p> <p>[Potential Applications] The paper suggests that simplifying regulatory compliance in DeFi markets could improve market access for smaller financial institutions and new entrants, while the immediate availability of ledger data could lead to more efficient financial oversight.</p>

Chapter 2 Possibility of RegTech/SupTech based on Blockchain technology

1. RegTech / SupTech verification projects involving financial authorities

Project name	overview
<p>BIS Research Activity Report</p>	<p>Embedded supervision can verify regulatory compliance by reading distributed ledgers in both the wholesale (Figure 2-1-1 , yellow blockchain) and retail banking markets (same, green blockchain). Supervisors can access all transaction-level data. Alternatively, through the use of smart contracts, Merkle trees, homomorphic encryption, and other cryptographic tools, supervisors may have verifiable access only to selected portions of such microdata, or to relevant linked positions such as institution-to-institution or sectoral exposures. Firms would only need to define the relevant access rights and would no longer need to collect, compile, or provide the data.</p> <p style="text-align: center;">Figure 2-1-1 Compliance process with embedded oversight</p>  <p>The diagram illustrates the compliance process with embedded oversight. It shows three types of ledgers: 1. Non-financial ledgers (yellow), 2. Financial industry ledgers (green), and 3. Consolidated ledger (blue). These ledgers feed into a central 'Cryptographic aggregation' block. This block is divided into three sections: 1. Transaction-level ledger (containing internal risk modelling, reportable item-level transactions, and market/OTC exposures), 2. Institution-to-institution ledger (containing bank-to-bank consolidated exposures), and 3. Consolidated ledger (containing overall exposures on a risk-weighted basis). A vertical dashed line separates the aggregation from 'Data access rights management', which then feeds into various entities: Internal risk management, OTC repositories, Tax agency, Microprudential supervision, Management, Exchange commission, Macroprudential supervision, Statistical agency, and Public/annual report.</p>

Chapter 2 Possibility of RegTech/SupTech based on Blockchain technology

1. RegTech / SupTech verification projects involving financial authorities

Project name	overview
BIS Research Activity Report	<p>This can be verified automatically by calculating the relevant distributed ownership ledger credit balances and associated risk weights. Such calculations can be applied to stock positions, such as end-of-period compliance, but can also be used for real-time sensitivity analysis of balance sheet exposure to market fluctuations, such as automatically calculating value-at-risk through simulation of ledger-based structured products and contractual obligations. Similarly, the backing of all assets for "on-chain" collateralized stablecoins can be verified automatically.</p>

Chapter 2 Possibility of RegTech/SupTech based on Blockchain technology

1. RegTech / SupTech verification projects involving financial authorities

Project name	Type of technology	Title of the article	author	Publication date	Project Overview	Descriptions related to this research
Survey of national authorities and regulated institutions regarding the use of	SupTech and RegTech	The Use of Supervisory and Regulatory Technology by Authorities and Regulated Institutions	Financial Stability Board	October 2020	<p>[Overview]</p> <ul style="list-style-type: none"> • SupTech and RegTech is explained from the perspective of the supply side and the demand side. The demand side is due to increased complexity of regulations, enhanced efficiency and effectiveness, and increased expenditures, while the supply side is due to increased availability, structured and unstructured expanded data utilization, improved AI technology, improved data architecture, etc. • There are benefits of SupTech and RegTech such as improved monitoring, surveillance and analytical capabilities, improved data collection and visualization, real-time risk indicator generation, and forward-looking judgment-based supervision and policy formulation. For regulated institutions , they enhance risk management capabilities for compliance and reduce reporting costs. • The risks SupTech and RegTech includes are data quality, cyber risks, costs, and reputational risks. There is also the possibility of the systems of certain regulated institutions being misused. There may also be competition with the private sector for talent such as data scientists and engineers. • There are many challenges in collecting, storing, managing and analyzing data, including data heterogeneity, diversity and duplication. Unstructured data is useful but difficult to analyze. Increasing data volume can increase storage costs. Excel is used as a data analysis visualization tool, but some institutions use Python or R. SupTech tools based on natural language processing (NLP). • In the use of SupTech and RegTech, cooperation between regulators and regulated entities, as well as collaboration with technology vendors, is becoming more active in order to reduce costs and improve data. Regulated entities have increasingly applied new technologies, with AI and machine learning technologies being used for fraud detection, reporting, risk management, AML/CFT , etc. Excessive reliance on RegTech by regulated entities can cause problems, such as the existence of bias due to reliance on past data and cyber risks, and dialogue between regulators, RegTech providers, and regulated entities is necessary. 	The FSB inquired of the current status of SupTech and RegTech to regulatory authorities and regulated institutions in each country, and received responses. Many institutions have implemented the use of SupTech by authorities and RegTech by regulated institutions , and the content is evolving rapidly. Due to the development of efficiency, effectiveness, and technologies such as AI , it is expected that they will be used even more in the future, but there are many concerns, such as a shortage of technical personnel. Cooperation is needed between public institutions, the private sector, and technology providers.

Source: <https://www.fsb.org/uploads/P091020.pdf>

Chapter 2 Possibility of RegTech/SupTech based on Blockchain technology

1. RegTech / SupTech verification projects involving financial authorities

Project name	overview
Survey of national authorities and regulated institutions regarding the use of	<p>[Project participants]</p> <ul style="list-style-type: none">• Argentina, Australia, Brazil, Canada, China, ECB , France, Germany, Hong Kong, India, Indonesia, Italy, Japan, South Korea, Mexico, Netherlands, Russia, Saudi Arabia, Singapore, South Africa, Spain, Switzerland, Turkey, UK and USA• 28 case studies from national institutions <p>[Research results]</p> <ul style="list-style-type: none">• According to the IIF research, challenges in applying RegTech stress testing indicate that strong governance and oversight are needed to minimise the impact on financial stability.• Human-based oversight processes will also be important• The rules are converted into a machine-readable format, enabling regulatory reporting by regulated entities and pull-based monitoring by authorities via APIs and other mechanisms.• AI has the potential to provide timely insights into financial activities and analyze data more efficiently than traditional human analysis, but without proper oversight, it may pose new risks from transparency, accountability, and data bias. The ethics of using AI in regulation should be carefully understood and aligned with the public interest, and concerns about data reliability, bias, and ownership may arise. Governance that maintains transparency and fairness is important to manage these risks.• Cloud-based services can help improve cooperation among regulators by enabling more efficient and effective information sharing between them. They can also lead to over-reliance on third-party providers.• Regulators can learn and exchange information about SupTech tools through resources such as innovation labs - a recent example is the BIS Innovation Hub. There is a strong willingness to collaborate across regulators and cooperation between supervisors is envisaged.• Looking ahead , authorities need a clear SupTech strategy that is tailored to their unique objectives and user-centric. Authorities need to attract and retain the talent they need with the requisite digital skillsets. Hiring experts with a strategic understanding of the tool development or acquisition objectives is important, and to keep pace with technological developments, authorities should consider engaging and exploring innovative collaborations with a range of external parties, including other financial authorities, academia, technology vendors, and international organizations. Additionally, appropriate staff training programs are critical to advance and accelerate knowledge.• Standard setters and authorities should evaluate common data standards and taxonomies in relevant regulatory areas, including potential international collaboration, to increase scalability and interoperability of reporting solutions.• As the volume and richness of collected data grows rapidly, authorities will need to embrace new technologies, use advanced analytical tools, and have appropriate data governance frameworks in place, including accountability for the tools and transparency of how their use informs decision-making, as well as accountability within authorities.• As SupTech and RegTech are still relatively new fields, pilots and proofs of concept will not necessarily be successful from the get-go . However, authorities and regulated institutions can encourage and foster a spirit of collaboration and innovation, and authorities can encourage open dialogue and discussion that will lay the foundations for the future regulatory landscape.

Chapter 2 Possibility of RegTech/SupTech based on Blockchain technology

1. RegTech / SupTech verification projects involving financial authorities

Project name

overview

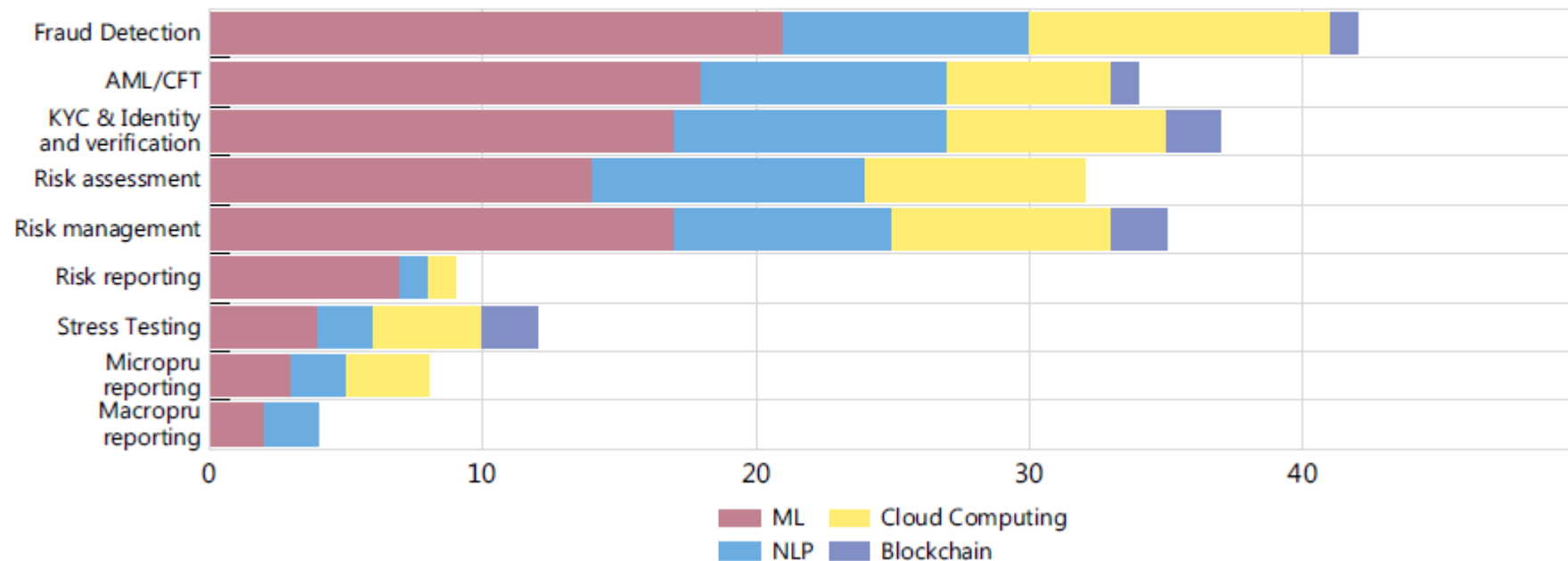
- Below are some of the findings from a survey of members of this project regarding the technologies used in RegTech tools.
- The key technologies driving RegTech tools are ML, NLP, and cloud computing, with blockchain technology showing a relatively low proportion.
- Areas in which blockchain technology is being applied include KYC, identity verification, identity authentication, and risk management.

Survey of national authorities and regulated institutions regarding the use of

Deployment of RegTech tools

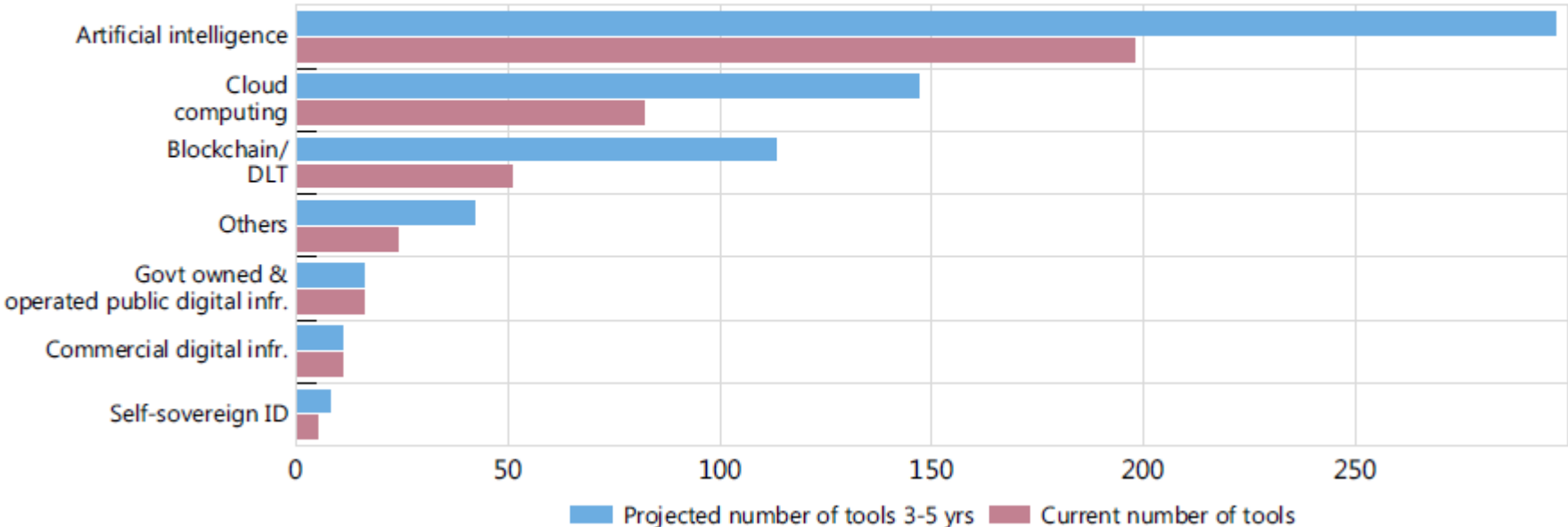
No. of authorities who have the tool used in each area

Graph 18



Chapter 2 Possibility of RegTech/SupTech based on Blockchain technology

1. RegTech / SupTech verification projects involving financial authorities

Project name	overview																								
Survey of national authorities and regulated institutions regarding the use of	<ul style="list-style-type: none">Looking ahead, we asked project members about the number of SupTech tools they currently have in place, and the breakdown of tools they expect to adopt over the next 3 to 5 years. AI , cloud computing, and blockchain /DLT applications were judged to be the tools most likely to be adopted in the future. <hr/> <h3 data-bbox="461 444 1564 482">Technologies use in SupTech tools – current and future</h3> <p data-bbox="461 501 1182 534">Current and projected number of SupTech tools</p> <p data-bbox="2066 501 2211 534">Graph 16</p>  <p>The chart displays the current and projected number of SupTech tools for seven categories. The x-axis represents the number of tools, ranging from 0 to 250. The y-axis lists the technologies. Blue bars represent the projected number of tools for the next 3-5 years, and red bars represent the current number of tools. The categories are: Artificial intelligence, Cloud computing, Blockchain/ DLT, Others, Govt owned & operated public digital infr., Commercial digital infr., and Self-sovereign ID.</p> <table border="1"><thead><tr><th>Technology</th><th>Current number of tools</th><th>Projected number of tools 3-5 yrs</th></tr></thead><tbody><tr><td>Artificial intelligence</td><td>~200</td><td>~280</td></tr><tr><td>Cloud computing</td><td>~80</td><td>~150</td></tr><tr><td>Blockchain/ DLT</td><td>~50</td><td>~110</td></tr><tr><td>Others</td><td>~25</td><td>~45</td></tr><tr><td>Govt owned & operated public digital infr.</td><td>~15</td><td>~20</td></tr><tr><td>Commercial digital infr.</td><td>~10</td><td>~15</td></tr><tr><td>Self-sovereign ID</td><td>~5</td><td>~10</td></tr></tbody></table>	Technology	Current number of tools	Projected number of tools 3-5 yrs	Artificial intelligence	~200	~280	Cloud computing	~80	~150	Blockchain/ DLT	~50	~110	Others	~25	~45	Govt owned & operated public digital infr.	~15	~20	Commercial digital infr.	~10	~15	Self-sovereign ID	~5	~10
Technology	Current number of tools	Projected number of tools 3-5 yrs																							
Artificial intelligence	~200	~280																							
Cloud computing	~80	~150																							
Blockchain/ DLT	~50	~110																							
Others	~25	~45																							
Govt owned & operated public digital infr.	~15	~20																							
Commercial digital infr.	~10	~15																							
Self-sovereign ID	~5	~10																							

Chapter 2 Possibility of RegTech/SupTech based on Blockchain technology

1. RegTech / SupTech verification projects involving financial authorities

Project name	Type of Blockchain	Title of the article	author	Publication date	Project Overview	Descriptions related to this research
Public consultation on DeFi	DeFi Ethereum	" Decentralized " or "disintermediated" finance (DeFi): what regulatory response?	Olivier Fliche , Julien Uri, Mathieu Vileyn FinTech- Innovation Hub Conrôle Authority prudentiel et de résolution (ACPR, Prudential Authority)	September	<p>[Overview]</p> <ul style="list-style-type: none"> The ACPR published a discussion paper classifying the risks of decentralized finance (DeFi) and proposing corresponding regulatory proposals, and solicited extensive comments. A wide range of topics were discussed, including the phenomenon of centralization in DeFi , the risks of layer 2 solutions, and the need for smart contract authentication. And various perspectives were presented, focusing on strengthening public chains and regulatory standards for smart contracts. <p>[Research results]</p> <ul style="list-style-type: none"> While the use of public chains was supported, there was disagreement over the method and extent of smart contract authentication. Diverse views were expressed regarding the risks of Layer 2 solutions and decentralized oracles. The proposal to apply MiCA rules to stablecoins has met with mixed reactions. In response to the inherent risk of centralization in DeFi , proposals were made on "minimizing governance" and auditing by public institutions. In addition, the need for access restrictions to protect customers was widely acknowledged. <p>[Novelty compared to conventional research]</p> <p>When considering the regulation of DeFi , concrete practical proposals were made, such as discussing the vulnerabilities of public chains and setting standards for smart contract authentication.</p>	<p>The results of this public consultation will be used as input by ACPR for the European discussion on MiCA regulations. The aim is to explore the possibility of further use by presenting governance and operational guidelines for client protection in DeFi. As there are many industry participants, there are very few voices of opposition to its use, and there is a trend towards further development and use. Further consideration is being called for regarding smart contract authentication.</p> <p>Participants made a variety of technical proposals, and while some of the problems were potentially solvable, some very fundamental problems were identified, and further research and consideration will be required.</p>

Source: <https://acpr.banque-france.fr/en/decentralised-or-disintermediated-finance-defi-what-regulatory-response>

Chapter 2 Possibility of RegTech/SupTech based on Blockchain technology

1. RegTech / SupTech verification projects involving financial authorities

Project name	overview
Public consultation on DeFi	<p>[Research Contents]</p> <ul style="list-style-type: none">• DeFi risk analysis: The risk of decentralized governance is that the majority of governance tokens will be monopolized, which may give the appearance of "false decentralization." Although transparency of governance mechanisms is important, it is impossible to completely eliminate centralized elements. Therefore, the principle of "minimizing governance" can be considered as one of the proposals. One idea is also proposed to make this one of the standards for smart contract authentication.• This research distinguishes between DeFi's three-tiered structure – blockchain infrastructure, applications and user devices – and describes its highly centralized governance, exploring regulatory options tailored to its characteristics.• This research noted that DeFi governance is dominated by monopolies and oligopolies due to its nature of increasing returns, and that the role of infrastructure and cloud providers hosting blockchain nodes is crucial.• Regarding the risk of flash loan attacks on protocol governance, this could potentially be minimized through protection mechanisms in the protocol and a transparent process of proposal submission and voting.• Infrastructure risks to various "Layer 2" solutions due to technological heterogeneity include the security of blockchain connection bridges.• Regarding the risk of computer attacks against blockchains and protocols, there are risks such as "sandwich attacks," but problems have also been pointed out not only with Layer 1 blockchains, but also with mempools used in Layer 2 solutions.• The report also points out AML/CFT risks due to the pseudonymity used in most blockchains, which makes it difficult to balance this with the requirement to protect participants' privacy. However, technological innovation has led to the development of digital ID solutions that may be able to resolve this issue.• The principle of authenticating smart contracts was supported, but the method for doing so was still under consideration .• It points out the need or a regulatory framework for intermediaries and user interfaces. <p>[Restrictions]</p> <p>Given the immaturity of DeFi technology, the effectiveness and technical appropriateness of the proposed regulations require continued consideration.</p> <p>[Potential Applicability]</p> <p>Complementing the European MiCA regulatory framework, the proposed DeFi regulations could contribute to improving financial stability and protecting users.</p>

Chapter 2 Possibility of RegTech/SupTech based on Blockchain technology Potential

2. RegTech in Decentralized Finance

Fireblocks, Uniswap, Circle, Verite) discussed in Chapter 1 , the following table shows the equivalent RegTech functions, which are innovative technologies that can be used by trading entities in decentralized financial systems to support compliance with regulations and reporting obligations . In addition, in light of IOSCO 's guiding principle of "same activity, same risks, same regulations and regulatory outcomes," we will compare the equivalent RegTech functions of decentralized finance using blockchain technology with those of traditional finance that meets regulatory requirements , and consider the significance of RegTech in decentralized finance. * The RegTech- related functions introduced here are the implementation status of functions that allow regulated institutions to respond efficiently when requested to do so as a supervisory response, and it should be noted that verification of whether these functions are effective in meeting the regulatory requirements of each country is required separately . Whether or not efficient supervision can be achieved is verified from the perspective of SupTech, and will be described in Chapter 3 .

Decentralized Financial System	Regulation function	RegTech- related features	RegTech- related functions	Providers of supervisory data	Relevant laws and regulations, including regulations and reporting obligations
Fireblocks	Transaction Monitoring	<p>Enable real-time transaction screening, risk scoring and compliance actions for all transactions. You can freeze both sending to and receiving from risky wallets.</p> <p>Transactions are evaluated according to predefined rules and monitored in real time (freezing is done manually). Although it is not possible to complete all of the verification decisions for suspicious transactions and the necessary information reporting to authorities by rule judgment alone, it is expected that efficiency will improve due to the traceability characteristic of blockchain technology.</p>	<p>Traditional financial institutions use centralized systems to monitor transactions . Transaction monitoring is primarily done using automated tools (rules-based systems and machine learning algorithms). Transactions may be monitored in real time or using historical transaction data over a period of time, as well as customer profile and risk assessment data .</p> <p>This includes human-involved surveys such as interviews with customers and requests for documents (in person or over the phone), which are difficult to automate.</p>	Manager of a decentralized financial system using Fireblocks	AML/CFT /CPF
	Account Screening	<p>Automating address screening to identify potentially risky wallets before they interact with the platform, using on-chain data such as transaction history and wallet activity for screening.</p> <p>The traceability characteristic of blockchain technology is expected to lead to improved efficiency.</p>	<p>Traditional financial institutions use systems to screen accounts, primarily using automated tools (rules-based systems and machine learning algorithms) with the final decision left to a compliance officer.</p> <p>This includes human-involved surveys such as interviews with customers and requests for documents (in person or over the phone), which are difficult to automate.</p>		

Source: Fireblocks " Compliance Integrations " <https://www.fireblocks.com/platforms/compliance/>

Chapter 2 Possibility of RegTech/SupTech based on Blockchain technology Potential

2. RegTech in Decentralized Finance (continued)

Decentralized Financial System	Regulation function	RegTech- related features	RegTech- related functions	Providers of supervisory data	Relevant laws and regulations, including regulations and reporting obligations
Fireblocks	Travel rules	<p>Automatically generate Travel Rule reports for transfers from VASPs and validate requests from other providers across jurisdictions.</p> <ul style="list-style-type: none"> • End-to-End Travel Rules for VASP • Approving and denying data transfer requests • Automate transactions that meet your criteria • Automatic identification and verification of business partners • Securely exchange and store customer information • Travel rule reporting <p>Additional travel rule information: The FATF has requested that national regulatory authorities introduce the "Travel Rule." In Japan, the Travel Rule requires cryptocurrency exchanges and electronic payment instrument traders to notify sender and recipient information when transferring cryptocurrency or electronic payment instruments, in order to make it possible to trace the transaction route of cryptocurrency or electronic payment instruments. (Article 10-3 and Article 10-5 of the Act on Prevention of Transfer of Criminal Proceeds)</p> <p>VASPs are required to collect and disclose certain customer data when trading digital assets above certain thresholds, but jurisdictions around the world currently have different disclosure and threshold requirements and enforcement approaches. Firms need solutions that can help them manage and comply with Travel Rule requirements across jurisdictions to ensure compliance for themselves and their counterparties.</p>	<p>The FATF has stated the following in its Recommendation 16 : Wire Transfers (Overseas Remittances):</p> <p>"Countries must ensure that financial institutions include accurate required originator and recipient information in wire transfers and related messages , and that such information is attached to the wire transfer or related messages throughout the transfer chain."</p> <p>In addition, the FSA's report (Issues with the Travel Rule in the 12- Month Review of the New FATF Standards for Cryptocurrencies and Cryptocurrency Exchange Businesses – Comparing Cryptocurrency Transfers to Bank Remittances) states the following (excerpt):</p> <p>This requirement is generally met by financial institutions including the necessary information accurately when sending payment instructions to SWIFT or the settlement system. (Omitted) Even if you know the recipient's bank account number, there is no way to transfer money if you do not know "where" the account is located. This common understanding is well established, and when you want to receive money, you will tell the other party the bank name (and in some cases the bank's country of location, branch name or branch number) and the account holder name along with the account number. Sometimes the recipient financial institution or business corporation is specified by SWIFT code, but even in that case, you can identify which bank or business corporation it is by simply looking at the list of codes published by the central administrator. In contrast, there is no such list for cryptocurrency wallet addresses. Not only do addresses differ depending on the type of cryptocurrency and whether it is sent or received, but they may also change each time.</p>	Manager of a decentralized financial system using Fireblocks	AML/CFT/CPF

Chapter 2 Possibility of RegTech/SupTech based on Blockchain technology Potential

2. RegTech in Decentralized Finance (continued)

Decentralized Financial System	Regulation function	RegTech- related features	RegTech- related functions	Providers of supervisory data	Relevant laws and regulations, including regulations and reporting obligations
Fireblocks	Travel rules	Regarding the above, Fireblocks can be said to have a system that can provide comprehensive support based on the VASP list that it has certified (VASP's country of location, financial supervisory authority, registration, license, etc.).	-	-	-
	KYC	<p>Aave Arc 's Fireblocks Permissioned DeFi , a DeFi liquidity marketplace , allows participants to participate in Fireblocks by passing the participant approval process and KYC . This will allow users to deposit, borrow, and liquidate within Aave Arc.</p> <p>In this regard, Fireblocks is a centralized system that relies on a list of verified participants. Since the current aim is to achieve equality with traditional financial functions, it is thought that the RegTech functions of decentralized finance do not offer any particular advantages. However, if the use of blockchain-related technology in the future enables financial institutions to safely share KYC data with each other, it is expected that the issue of duplicate costs in KYC operations , which is a sharing challenge in the financial sector, will be reduced.</p> <p>Furthermore, by using cryptographic techniques such as zero-knowledge proofs, it is possible to protect the personal information of customers while providing the necessary information for KYC, allowing customers to complete the KYC process without sacrificing their privacy.</p>	<p>RegTech- related features of KYC processes in traditional finance include:</p> <ul style="list-style-type: none"> •To verify the identity of a customer, the system scans and automatically reads the information on the ID and address proof presented by the customer and analyzes their authenticity •Analyze (existing) customers' attributes such as occupation customers' transaction history and financial status to automatically assess the risk of money laundering and terrorist financing <p>Automatically verify that your customers are not on sanctions lists (when opening an account and updating the sanctions list)</p> <p>Additional information on KYC:</p> <p>There are three types of KYC methods: face- to-face, by mail, and online. In Japan, the online method uses the following classifications under the Criminal Proceeds Act: "E) Taking a selfie and submitting a photo ID," "F) Taking a selfie and the IC information from the photo ID," "G) Taking a photo of the photo ID, the IC information, and a bank inquiry or small amount transfer to a bank account," and "W) Electronic signature for the public personal authentication service of the My Number card."</p>	Manager of a decentralized financial system using Fireblocks	AML/CFT/CPF

Source: Fireblocks " Compliance Integrations " <https://www.fireblocks.com/platforms/compliance/>

2. RegTech in Decentralized Finance (continued)

Decentralized Financial System	Regulation function	RegTech- related features	RegTech- related functions	Providers of supervisory data	Relevant laws and regulations, including regulations and reporting obligations
Uniswap	Transaction review and account screening	It is thought to provide similar functionality to Fireblocks.	See the column of Fireblocks.	Uniswap 's DAO (It is difficult to identify the responsible party.)	AML/CFT/CPF
	KYC	It provides the ability to link with external KYC solutions such as Fireblocks and Verite. *Please note that this document does not confirm which jurisdiction's KYC requirements external KYC solutions, including Fireblocks, meet.	See the column of Fireblocks and Verite.		

2. RegTech in Decentralized Finance (continued)

Decentralized Financial System	RegTech- related features	RegTech- related functions	Providers of supervisory data	Relevant laws and regulations, including regulations and reporting obligations
Circle	<p>Balance Verification: USDC reserves are disclosed weekly along with associated mints / burns. A Big Four accounting firm provides third-party assurance each month that the value of USDC reserves is greater than the amount of USDC in circulation. Reports are prepared in accordance with attestation standards set by the American Institute of Certified Public Accountants</p> <p>Since the balance verification process for USDC reserves (net of mint and burn) is public information on-chain, Circle 's supervisory verification process for the disclosed information is characterized by transparency (objectivity) and immediacy.</p> <p>Regarding checking the balance at the wallet address level, there are tools available that allow viewing of on-chain data, which also have characteristics such as transparency (objectivity) and immediacy.</p>	<p>Balance confirmation: Here, we will introduce the Balance Gateway service provided by the Accounting Audit Verification Center LLC as an example of a RegTech solution for bank balance confirmation procedures.</p> <ul style="list-style-type: none"> • Supports multiple confirmation letters (creditor/payor balances, bank transaction balances, securities transaction balances, attorney confirmations, etc.) • You can check it online (the following steps are all online procedures) <ol style="list-style-type: none"> 1. Preparation of a request for response by the audited company or accounting auditor 2. Approval of the request for response by the audited company 3. Request for response from accounting auditor 4. Respondents enter their answers 5. Confirmation of the answers from the accounting auditor <p>Balance Gateway is a service provided by accounting firm Tohmatsu and is not available to other accounting firms or compatible with all financial institutions.</p>	Circle	<p>It is not mandatory (there is no legal basis) to provide written confirmation (such as balance confirmation letters, remaining balances, etc.) in customer protection/accounting audits .</p>

Source: Circle " Transparency & Stability " <https://www.circle.com/en/transparency>

Accounting Audit Confirmation Center LLC " What is Balance Gateway ?" <https://auditconfirmation.co.jp/bg.html>

Chapter 2 Possibility of RegTech/SupTech based on Blockchain technology Potential

2. RegTech in Decentralized Finance (continued)

Decentralized Financial System	RegTech- related features	RegTech- related functions	Providers of supervisory data	Relevant laws and regulations, including regulations and reporting obligations
Circle (Verite)	<p>Verite is a decentralized authentication and identity protocol proposed by Circle that aims to enable</p> <p>By using Verite , users will be able to manage their own ID information and present it in a trustworthy manner to service providers such as decentralized financial systems.</p> <p>Verite 's RegTech objectives are as follows:</p> <p>KYC and AML Streamlining :</p> <p>Automating the process of verifying user identities , enabling financial institutions and service providers to more effectively comply with KYC/AML regulations</p> <p>Enhanced data privacy and security :</p> <p>The Verite Protocol is a data privacy protocol that aims to securely manage users' personal information on a decentralized network.</p> <p>Increased transparency in regulatory compliance :</p> <p>Improving transparency of transactions and data management by utilizing blockchain technology</p> <p>Since the current aim is to achieve equality with traditional financial functions, it is thought that the RegTech functions of decentralized finance do not offer any particular advantages. However, if the use of blockchain-related technology in the future enables financial institutions to safely share KYC data with each other, it is expected that the issue of duplicate costs in KYC operations , which is a sharing challenge in the financial sector, will be reduced.</p>	See the column of Fireblocks.	Decentralized financial system using Verite	AML/CFT/CPF

3. Summary

In Chapter 2, Part 1, titled "RegTech/SupTech Verification Project Involving Authorities and Others," introduces the views of authorities and others regarding the potential of RegTech and SupTech. In particular, it was mentioned that regulated financial institutions or authorities could efficiently supervise token trading by using embedded supervision or supervisory nodes.

In Chapter 2, Part 2, titled "RegTech in Decentralized Finance," we introduced the examples covered in Chapter 1 (Fireblocks, Uniswap, Circle, and Verite) and their functions equivalent to RegTech, an innovative technology that can be used by trading entities in decentralized financial systems to support compliance with regulations, reporting obligations, and other laws. In addition, in light of IOSCO 's guiding principle of "same activities, same risks, same regulations and regulatory outcomes," we compared decentralized finance using blockchain technology with functions equivalent to RegTech in traditional finance that meets regulatory requirements, and considered the significance of RegTech in decentralized finance .

Therefore, in Chapter 3, we will examine the technical possibilities and challenges of RegTech and SupTech for cryptocurrency exchanges that are already actively engaged in token (cryptocurrency) trading.

Chapter 3 Desk-based verification of Regtech/Suptech utilizing the characteristics of blockchain

Chapter 3: Desk-based verification of RegTech/SupTech utilizing the characteristics of blockchain

The main technical terms used in Chapter 3 are defined as follows:

term	Definition
Deploy	In the system development process for web applications, etc., this refers to the series of tasks involved in placing and deploying the application's functions and services on a server and making them available for use. Deployment utilizes test and production environments to reflect executable files on the server and make it operational.
Validators	Generally speaking, this refers to a node that is responsible for verifying transactions and generating blocks in a blockchain network.
Off-Chain Data	This refers to data that is not recorded on the blockchain. Most of the data is managed in company databases or on paper documents.

Chapter 3: Desk-based verification of RegTech/SupTech utilizing the characteristics of blockchain

1. Elements of Supervision Scenario

Chapter 3 examines the technical possibilities and constraints of RegTech and SupTech based on a supervision scenario for cryptocurrency exchange operators.

In terms of the nature of token transactions handled by regulated financial institutions, we will follow "Table 1-7-1 Differences in the nature of Token Transactions Handled by Regulated Financial Institutions" summarized in Chapter 1, Section 7 and examine the following patterns.

Transaction Scenarios	explanation
Cryptocurrency transaction through cryptocurrency exchanges	Specifically, it envisages cryptocurrency transactions between cryptocurrency exchange operators and external mutual wallets. This scenario does not include off-chain cases in which customers trade cryptocurrencies with each other while their cryptocurrencies are held in safe custody within the cryptocurrency exchange.

This desk-based verification aims to verify the risk reduction effect of embedded supervision and supervisory nodes by assuming a simple scenario, taking into account the risks and vulnerabilities related to tokenization and decentralized finance mentioned in reports by international organizations such as the FSB. In particular, for the response by authorities (SupTech), a scenario is assumed in which the authorities themselves build supervisory nodes and perform data analysis, etc. Please note that this test was conducted on a limited scope with a bold hypothesis in order to verify the potential of RegTech / SupTech , and does not fully consider compliance with Japan's regulatory requirements.

Chapter 3: Desk-based verification of RegTech/SupTech utilizing the characteristics of blockchain

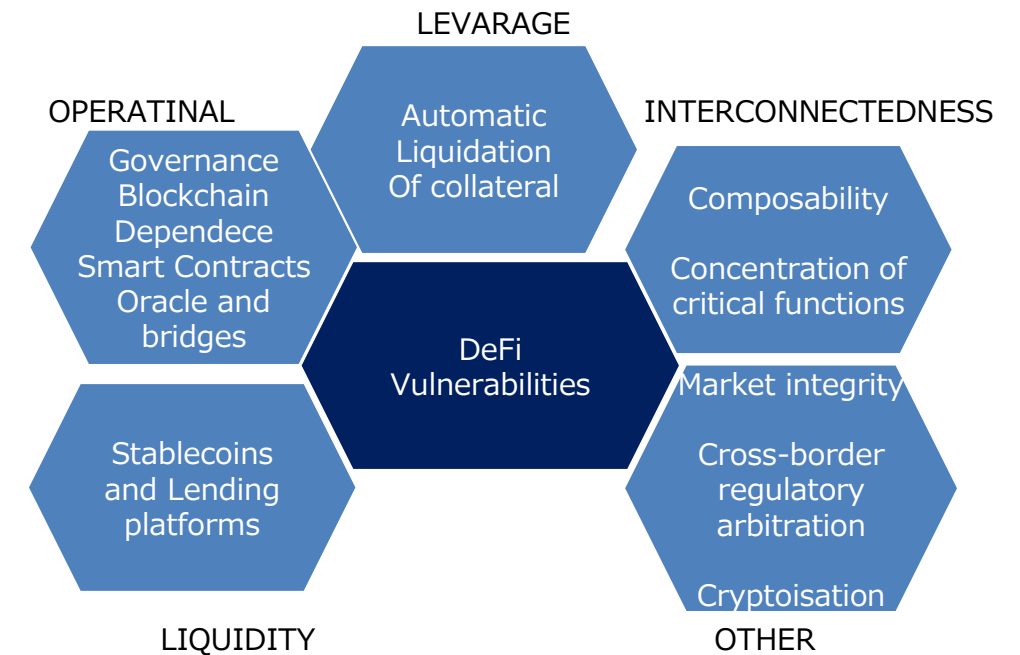
1. Elements of Supervision Scenario

According to the FSB report, the risks and vulnerabilities of Multi-Functional Cryptocurrency Intermediaries (MCI) to financial stability are shown in Table 3-1-1 , and the characteristics and vulnerabilities of DeFi are shown in Figure 3-1-1 . The cryptocurrency-related supervision scenarios in this document will be created with reference to these risks and vulnerabilities.

Table 3-1-1 MCI Financial Stability Risks and Vulnerabilities

Risks and Vulnerabilities
Misappropriation of clients' funds
Fraud
Market manipulation through speculative activities on their own investment tokens or through nontransparent supply management activities
Price manipulation/volatility
Wash Trading
Front Running
MCI's trading against or ahead of their customers
Conflict of interests
Excessive leverage (e.g. reusing one's investment tokens as collateral)
Liquidity
Credit risk
Supply-reserve mismatch (e.g.misappropriation of reserves and/or fractional reserves without appropriate safeguards)
Interconnection - concentration risks exacerbated by anticompetitive practices
Interconnection - interdependence (e.g. on oracles)
Technical and operational vulnerabilities

Figure 3-1-1 Summary of DeFi characteristics and vulnerabilities



Source: FSB report "Financial Stability Risks of Decentralized Finance"

Table 3-1 Appendix 1 of the FSB report "Impact of Multifunctional Cryptocurrency Intermediaries on Financial Stability"
: Created by Kunie from the risks and vulnerabilities associated with the combination of functions in an MCI

2. RegTech and SupTech Supervision Scenarios

The supervisory scenarios prepared for the transaction scenario are as follows:

Table 3-2-1 RegTech and SupTech Supervision Scenarios

Requirement Type	RegTech (embedded supervision)	SupTech (Supervisory Node)
Transaction Monitoring	<p>① A mechanism to verify that the wallet is an authenticated wallet before a token transaction is completed. If the wallet is not authenticated, the transaction will not be processed. An authenticated wallet here is what has been authenticated by a VC/DID provider or can be confirmed as a cryptocurrency transfer by a cryptocurrency exchange operator (and its KYC-certified customers).</p>	<p>The contents of the report will be verified based on data obtained from nodes set up by the authorities on the blockchain.</p>
	<p>② The system extracts token transaction data that matches predefined suspicious transaction patterns, adds additional information such as customer KYC and attributes, and reports the results to the designated authorities, with the aim of reporting in accordance with the obligation to notify suspicious transactions.</p>	
Reporting	<p>In order to respond to requests for reports from authorities (regular and occasional) , various data regarding tokens will be stored and reported to authorities.</p>	<p>The contents of the report will be verified based on data obtained from nodes set up by the authorities on the blockchain.</p>

3. System functions required by Supervision scenario

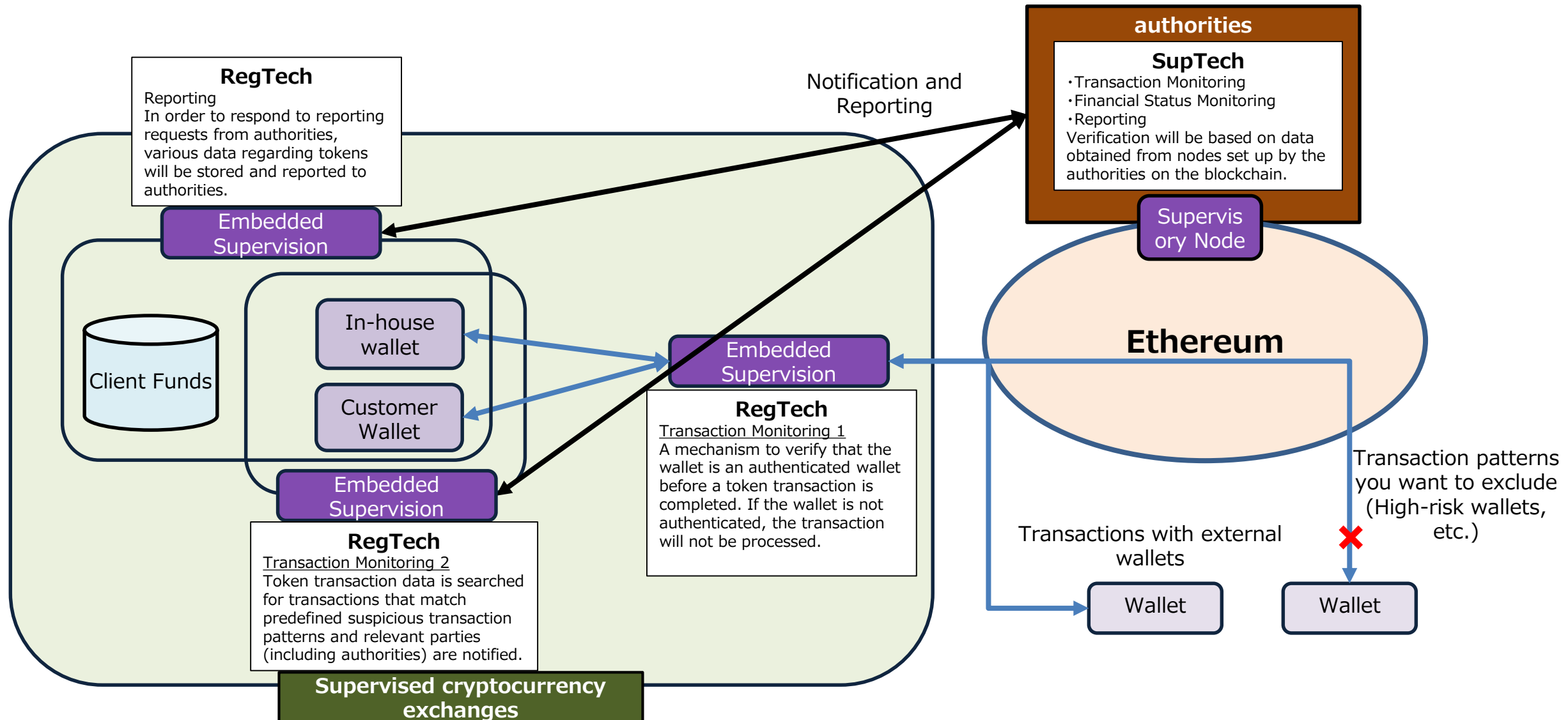
The main system functions required for each requirement type scenario are shown below.

Table 3-3-1 System functions required by the supervisory scenario

Requirement Type	RegTech / SupTech	Main System Features
Transaction Monitoring	RegTech	<ul style="list-style-type: none"> • Real-time monitoring of financial transaction data • Detecting inappropriate financial transactions • Control of financial transactions under specific rules (stopping certain transactions) • KYC for trading participants
	SupTech	<ul style="list-style-type: none"> • Financial transaction data verification • Shielding regulatory oversight and data analysis from outsiders
Reporting	RegTech	<ul style="list-style-type: none"> • Reporting on transaction monitoring and financial status monitoring
	SupTech	<ul style="list-style-type: none"> • Verification of transaction monitoring and financial status monitoring

4. System configuration of trading scenario

The system configuration (permissionless chain: Ethereum) for each supervision scenario is shown below.



Chapter 3: Desk-based verification of RegTech/SupTech utilizing the characteristics of blockchain

5. Verification items and results for system requirements

Trading scenario: Trading of crypto assets through a cryptocurrency exchange

We verified whether embedded supervisors and supervisor nodes can function effectively.

Supervisory Scenario	System Requirements	Verification Content	RegTech (embedded supervision)
			Ethereum
RegTech Transaction Monitoring	Real-time monitoring of financial transaction data	Is real-time anomaly detection possible?	Embedded oversight allows for on-chain data monitoring, enabling real-time anomaly detection.
	Detecting inappropriate financial transactions	What kind of outliers can be detected?	Embedded oversight can automatically detect suspicious transaction addresses and quantities by monitoring on-chain data (block number, source address, destination address, transaction amount, token type, transaction fee, timestamp).
	Control of financial transactions in trading rules (stopping certain transactions)	Can a cryptocurrency exchange stop a transaction after cryptocurrency has been transferred to an external cryptocurrency address?	In Ethereum, for example, the draft ERC-1644 defines the forced transfer of security tokens, which can be used for reversals, etc., and there is room for implementing a transaction suspension function depending on the configuration of the smart contract.
	Counterparty KYC	Can I check the KYC status of the sender and recipient?	Addresses (generated from public keys) alone cannot prove identity. As a premise, between domestic cryptocurrency exchanges, KYC customer attributes and addresses are linked and managed, so the KYC status of the sender and recipient can be confirmed. On the other hand, there are cases where overseas cryptocurrency exchanges have not completed KYC, or where the wallet address was generated by an individual, making it impossible to confirm.
RegTech Reporting	Transaction monitoring report	Is the report comprehensive and traceable?	If appropriate transaction monitoring and financial status monitoring are implemented, comprehensive and traceable reporting can be expected.

Chapter 3: Desk-based verification of RegTech/SupTech utilizing the characteristics of blockchain

5. Verification items and results for system requirements

Director's Scenario	System Requirements	Verification Content	Validation of SupTech (supervisory node)
			Ethereum
SupTech Transaction Monitoring	Financial transaction data verification	Is it possible to verify the authenticity of data provided by financial institutions in the event of a suspicious transaction, and what methods are available for doing so?	<p>By building their own nodes, authorities can increase their self-reliance in that they can access the Ethereum network without relying on external services or providers. For example, they will not be affected if Etherscan goes down or imposes restrictions.</p> <p>However, when operating, although it is not necessary to participate in block validation, it is necessary to have access to the entire history of the network, so it is thought that the operation of archive nodes will be a prerequisite.</p> <p>When operating an archive node, the entire history of the network can be accessed, but the data capacity becomes very large. Although this is technically possible, operation incurs costs such as server fees in addition to labor costs for regular maintenance. Specifically, the storage capacity required to operate an archive node is estimated to be about 12 TB as of October 2023 , and is increasing year by year. If a cloud service is used, the server costs for storing and operating this scale of data are expected to be about several hundred thousand yen per month. In addition, labor costs are incurred for ongoing maintenance such as hardware maintenance, software updates, and security measures. Considering these costs, it may be realistic to use a third-party service from a cost-effectiveness perspective .</p>
	Concealment of activities	Can the authorities maintain confidentiality by not disclosing to the public that they are monitoring transactions?	The existence of a supervisory node cannot be concealed from third parties, but it is impossible to determine whether or not it is a supervisory node, and it is possible to keep the content of monitoring confidential.
SupTech Reporting	Transaction monitoring content verification	Can the contents of a report be kept confidential from third parties?	If one were to operate the nodes themselves, the data volume would be extremely large, and in addition to the labor costs for regular maintenance, the costs for servers, etc. would make it unlikely to be feasible.

Source: <https://ethereum.org/ja/developers/docs/nodes-and-clients/archive-nodes/>

Chapter 3: Desk-based verification of RegTech/SupTech utilizing the characteristics of blockchain

6. Summary

The results of a desk-based study on whether embedded supervision and supervisory nodes by regulated financial institutions and authorities can be used as RegTech/SupTech in the context of tokenization in traditional financial institutions are summarized below.

Chapter 3, Section 1 lists risks and vulnerabilities to financial stability, as well as the characteristics and vulnerabilities of DeFi , as “Elements of Supervision Scenario ”.

Chapter 3.2 presents a supervisory scenario for RegTech and SupTech that takes into account the factors considered in Chapter 3.1 .

In Chapter 3.3, we presented the system functions of embedded supervision and the supervision node as “System functions required by the supervision scenario.”

In Chapter 3, Section 4, “System configuration for trading scenario,” we illustrated the configuration of embedded supervision and supervisory nodes in each trading scenario.

In Chapter 3, Section 5, “Verification items and results for system requirements”, we examined whether embedded supervision and supervision nodes are effective as

The SBI Financial and Economic Research Institute pointed out that "It is expected that transactions on public chains will make it difficult to respond to leaks and will increase AML/CFT risks. If it is assumed that individual investors will manage the wallets that control private keys, risks will remain to a certain extent. (Omitted) Since KYC will be critical for reducing AML / CFT risks and capturing taxes on interest/dividend payments and trading profits, KYC will be relied upon by regulated financial institutions . (Omitted) It is thought that measures will be needed, such as allowing transactions only through whitelisted wallets."

According to the FSB report, blockchain /DLT applications were listed as the next tool expected to be introduced in SupTech, following AI and cloud computing (see page 61 of this document). The report examined the effectiveness of embedded supervision and supervisory nodes as manifestations of blockchain technology (DLT). The scenarios in which this document found particular effectiveness were embedded supervision by cryptocurrency exchanges conducting transactions on permissionless chains and supervisory nodes assumed to be operated by authorities over traditional financial institutions conducting transactions on permissioned chains. The FSB report also indicated that areas where blockchain technology could be used as RegTech include KYC verification and risk management (see page 60 of this document).

This report indicates that embedded supervision and supervisory nodes could be used as RegTech/SupTech in some of the areas identified in the FSB report. However, as the study findings show, there are constraints, and further consideration will be required before implementation.

We hope that this document will serve as a reference for the conditions for the effectiveness of embedded supervision and supervisory nodes, and provide an opportunity to advance further operational and institutional consideration.

Source: Security Token Latest Situation and Future Outlook: Summer 2024 https://sbiferi.co.jp/report/20240725_1.html