big data and cognitive computing

MDPI

Article

Proposal of a Service Model for Blockchain-Based Security Tokens

Keundug Park [1] and Heung-Youl Youm [2,*]

[1] AI & Blockchain Research Center, Seoul University of Foreign Studies, Seoul 60745, Republic of Korea; jacepark926@gmail.com
[2] Department of Information Security Engineering, Soonchunhyang University, Asan 31538, Republic of Korea
* Correspondence: hyyoum@sch.ac.kr

Abstract: The volume of the asset investment and trading market can be expanded through the issuance and management of blockchain-based security tokens that logically divide the value of assets and guarantee ownership. This paper proposes a service model to solve a problem with the existing investment service model, identifies security threats to the service model, and specifies security requirements countering the identified security threats for privacy protection and anti-money laundering (AML) involving security tokens. The identified security threats and specified security requirements should be taken into consideration when implementing the proposed service model. The proposed service model allows users to invest in tokenized tangible and intangible assets and trade in blockchain-based security tokens. This paper discusses considerations to prevent excessive regulation and market monopoly in the issuance of and trading in security tokens when implementing the proposed service model and concludes with future works.

Keywords: blockchain; security token; asset tokenization; investment; anti-money laundering; exchange; trade; custody; asset-backed token

Citation: Park, K.; Youm, H.-Y. Proposal of a Service Model for Blockchain-Based Security Tokens. *Big Data Cogn. Comput.* **2024**, *8*, 30. https://doi.org/10.3390/bdcc8030030

Academic Editors: Ioanna Dionysiou, Oleg Basov, Elias Iosif and Christiana Ioannou

Received: 18 January 2024
Revised: 8 March 2024
Accepted: 11 March 2024
Published: 12 March 2024

1. Introduction

A security token is a type of cryptocurrency that is an asset-backed token representing the value and ownership of a tokenized tangible or intangible asset using blockchain and distributed ledger technology (DLT). Asset tokenization means logically segmenting the value of a tangible or intangible asset and assigning the value and ownership of the segmentation to asset-backed tokens.

There are online markets related to asset tokenization, such as tZERO [1], Securitize [2], INX [3], and the Security Token Market (STM) [4]. Users can invest in tokenized assets and trade security tokens on online markets. In Japan, a non-profit organization, JTSA [5], was established to promote an ecosystem for security tokens. According to [6], the market volume for tokenized assets is expected to grow to about $10 trillion by 2030.

Unlike cryptocurrencies (e.g., Bitcoin [7], Ether [8], etc.), it is necessary to establish a service model for security tokens representing the value and ownership of a tokenized asset. The service model must include the issuance, distribution, transfer, trade, storage, and revocation of security tokens and identify role-based key components. It is necessary to identify security threats to the service model and specify the security requirements countering the identified security threats in order to preserve the user's privacy and prevent money laundering involving security tokens.

The contribution of this paper is as follows. To the best of our knowledge, there has been no previous study on a service model for blockchain-based security tokens, so this paper proposes a service model for blockchain-based security tokens, including security threats and security requirements. The proposed service model provides a solution for investment in both tokenized tangible and intangible assets (e.g., buildings, art, movies,

music, etc.) and trading in security tokens. It improves user convenience for investment in and trading of assets compared to the existing investment service model.

This paper is organized into the following sections: Section 1 introduces security tokens and their trends. Section 2 describes related studies, including a problem in the existing investment service model. Section 3 proposes a service model to solve the problem identified in Section 2. Section 4 identifies security threats to the proposed service model and specifies security requirements countering the identified security threats. Section 5 discusses the results and concludes the paper.

2. Related Studies

This section describes the problem with investment in tangible and intangible assets, and examines other studies related to the problem.

2.1. Problem with Investment in Assets

It is easy for users to invest in tangible and intangible assets in the existing investment service model. For example, a user wishing to invest in a building worth $1 million would acquire ownership of the building after paying $1 million to the building owner.

However, it is difficult for users to invest in tangible and intangible assets in the existing investment service model. For example, a user wishing to invest in a building worth $1 million would not acquire partial ownership of the building, even after paying $1000 to the building owner. This problem arises because asset tokenization is not applied in the existing investment service model.

2.2. Other Approaches for Asset Tokenization including Security Tokens

Several organizations and studies have made proposals to solve the problem mentioned in Section 2.1, but their proposals differ from the proposed service model in terms of concept and concreteness.

The framework for security tokens was proposed in [9]. ERC-1400 is a specification for security tokens issued on the Ethereum blockchain. ERC means "Ethereum Request for Comments". The key features of ERC-1400 include partially fungible tokens, document management, issuance and redemption, dynamic token supply, and authorized operators.

A blockchain for security tokens based on ERC-1400 was proposed in [10]. Polymesh is a public and permissioned blockchain for security tokens. The key features of Polymesh include identity management, record storage, capital distribution, and stablecoin [11] support.

The protocol for asset tokenization was proposed in [12]. ERC3643 is designed to support the issuance, management, and transfer of permissioned tokens applicable to security tokens based on the Ethereum blockchain. The key features of ERC3643 include control and permission management for security tokens and blockchain-based decentralized identity management.

Real estate security token offerings and the secondary market were analyzed in [13]. This paper includes the process of real estate tokenization, the analysis of blockchain transactions, the analysis of security token offering (STO) success determinants, and the analysis of funding determinants.

The features of STO and STO success factors were analyzed in [14]. This paper includes the definition of the security token, the STO process, the need for the STO market as an essential part of corporate finance, an overview of the STO market, and the analysis of STO success factors.

The tokenization of assets was analyzed in [15]. This paper includes the definition of tokenization, the key advantages of tokenization (e.g., greater liquidity, faster and cheaper transactions, greater transparency and accessibility), the obstacles to tokenization, and the considerations for tokenization (e.g., business model, platform integration, cybersecurity, compliance, and jurisdiction).

The blockchain-based open asset protocol (OAP) was proposed in [16]. This paper includes the framework of OAP on a blockchain, the specification of asset-backed tokens, the conversion of real and virtual objects to asset-backed tokens, the discussion of a new method for data utilization and privacy protection, and the introduction of policy-backed tokens as use cases.

Tokenized assets and securities were proposed in [17]. This paper includes the analysis of tokenized securities, the benefits of tokenizing assets and securities based on blockchain (e.g., increased efficiency, reduced cost, increased transparency and security, better compliance, improved liquidity, and facilitated innovation), the tokenization process, the introduction of tokenization platforms (e.g., tZERO, ConsenSys Codefi, Securitize, and Polymath), and the use cases of assets and securities tokenization.

Based on studies and analyses in other literature, the conclusion was that no previous study exists of a service model for blockchain-based security tokens. The main objective of this paper is to propose a new service model for investment in tokenized assets and trading in blockchain-based security tokens, identify potential security threats to the proposed service model, and specify the security requirements countering the identified security threats. The proposed service model focuses on trading and investing based on asset-backed tokens, such as security tokens.

3. A Service Model for Blockchain-Based Security Tokens

This section proposes a service model for blockchain-based security tokens to facilitate investment in tokenized tangible and intangible assets.

The proposed service model is partially similar to the existing cryptocurrency service model. The main difference between the proposed service model and the cryptocurrency service model comes from asset collateralization and tokenization. Since blockchains for cryptocurrencies, cryptocurrency wallets, and cryptocurrency exchanges are well known and used to provide many services, this section does not address the implementation evaluation of the proposed service model.

3.1. Service Model

The proposed service model includes holders with security token wallets, custodians with security token wallets, tokenization service providers (TSPs), investors, asset owners, issuers, exchanges with security token wallets, traders, anti-money laundering (AML) regulators, and the blockchains for security tokens.

The proposed service model expands investment products and increases the convenience of asset investment compared to existing investment systems. Through the proposed service model, users can invest in tokenized tangible and intangible assets (e.g., buildings, art, music, movies, etc.) with a small amount, even $5–10, and receive dividends of profits after asset management (e.g., sales, etc.) is fulfilled. Additionally, if asset management is not fulfilled, users who hold security tokens can make a profit by selling the security tokens.

Holders, custodians, TSPs, issuers, exchanges, AML regulators, and blockchain providers are the stakeholders in the proposed service model. There are requirements for each stakeholder to make the proposed service model successful. The holder should prevent the loss and theft of security tokens. The custodian should prevent the embezzlement and theft of security tokens owned by the holders. The TSP should guarantee the value of tokenized assets and prevent embezzlement and theft of investments. The issuer should guarantee that the amount of issued and revoked security tokens matches the amount of investment. The exchange should prevent the embezzlement and theft of security tokens owned by traders. The AML regulator should administer and supervise exchanges to prevent money laundering involving security tokens in accordance with AML laws. The blockchain provider should guarantee the storage and maintenance of a ledger for the issuance, transfer, and revocation of security tokens.

In Figure 1, the role-based entities of the proposed service model are described as follows:

- The holder with security token wallets is the owner of security tokens issued by issuers, bought from exchanges, or transferred from other entities. Holders transfer security tokens on the blockchain and entrust their private keys or security tokens to custodians.
- The custodian with security token wallets stores and maintains the holder's private keys, which are used to transfer the holder's security tokens. If the holder is a legal person, a child, an elderly person, or a digitally disabled person, the custodian transfers the holder's security tokens on the blockchain on behalf of the holder. The custodian stores and maintains the security tokens received from the holders.
- The tokenization service provider (TSP) registers tangible assets (e.g., real estate, art, agricultural products, fishery products, livestock products, etc.) or intangible assets (e.g., music, movies, copyrights, intellectual property rights, etc.) and provides tokenized assets for investment. The TSP requests the issuer to issue and revoke security tokens and retrieves the issuance and revocation information of the security tokens from the blockchain.
- The asset owner registers his/her tangible and intangible assets with the TSP and receives payment from the TSP for investments in the registered assets. The asset owner provides the price for the registered asset to the TSP.
- The investor pays the TSP for investments in tokenized assets and receives the profit from the asset management of the TSP.
- The issuer issues and revokes security tokens in accordance with the request of the TSP. The issuers store issuance and revocation information for the security tokens on the blockchain.
- The exchange with security wallets provides trading in security tokens (for details, see Figures 2 and 3). The exchange transfers security tokens on the blockchain and retrieves the issuance and revocation information of the security tokens from the blockchain.
- The trader buys and sells security tokens at the exchanges (for details, see Figures 2 and 3).
- The anti-money laundering (AML) regulator administers and supervises exchanges to prevent money laundering involving security tokens.
- The blockchain stores and maintains information on the issuance, transfer, and revocation of security tokens. Since the proposed service model does not require the mining of security tokens, the type of blockchain can either be private or permissioned. The consensus algorithm can be either Proof of Stake (PoS) or Delegated Proof of Stake (DPoS). TSPs, issuers, exchanges, and AML regulators can participate as nodes on the blockchain.

In Figure 2, Exchange-1 includes security token wallets, cryptocurrency wallets, central bank digital currency (CBDC) wallets, and a trade ledger containing personally identifiable information (PII). If Exchange-1 does not include CBDC wallets, traders can trade security tokens with traditional fiat currencies, such as USD, EUR, etc. The fact that Exchange-1 includes security token wallets means that Exchange-1 can hold security tokens. Exchange-1 identifies and authenticates traders before trading. Exchange-1 provides traders with trading between security tokens and fiat currencies, including CBDCs, between security tokens and cryptocurrencies (e.g., Bitcoin, Ether, etc.), and between security tokens. Exchange-1 stores and maintains the trade ledger containing the PII of the traders. The AML regulator administers and supervises Exchange-1 to prevent money laundering involving security tokens.

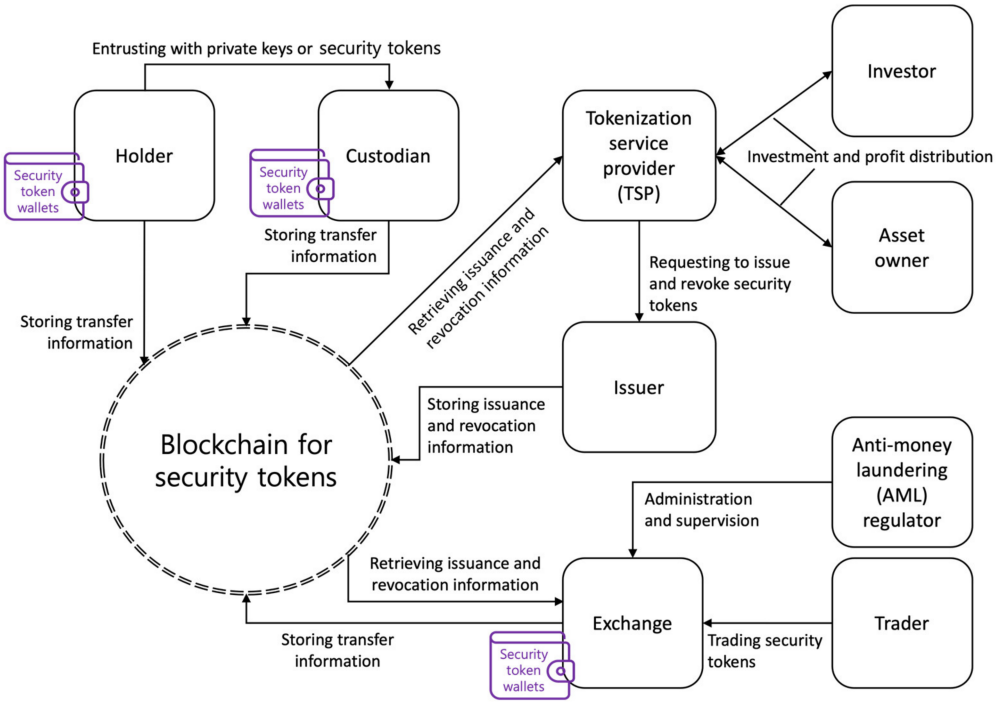
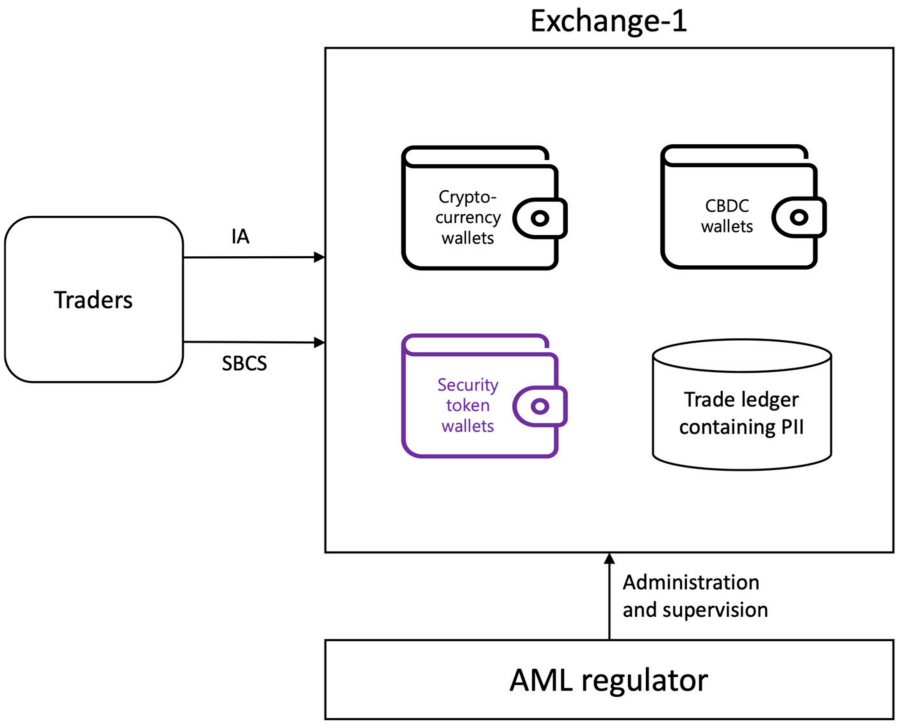


Figure 1. The service model for blockchain-based security tokens.



* AML: anti-money laundering
* CBDC: central bank digital currency
* IA: identification and authentication
* PII: personally identifiable information such as name, the date of birth, address, etc.
* SBCS: selling and buying cryptocurrencies and security tokens

Figure 2. The service model for trading in security tokens on a single exchange.

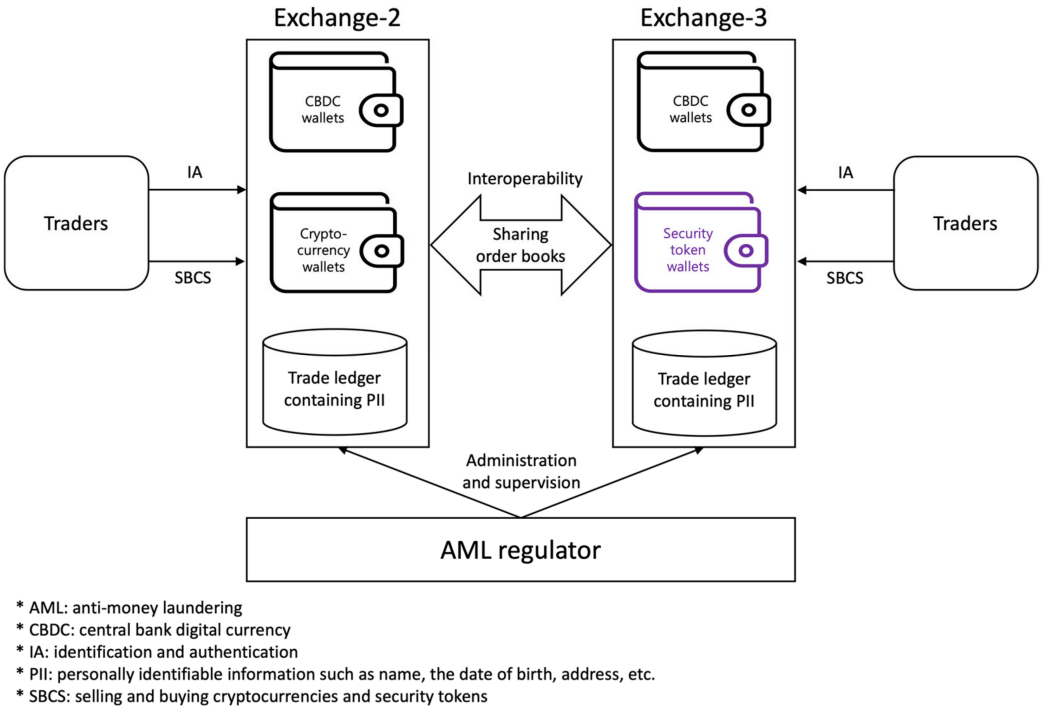


Figure 3. The service model for trading in security tokens on multiple exchanges.

In Figure 3, Exchange-2 includes cryptocurrency wallets, CBDC wallets, and a trade ledger with PII. Exchange-3 includes security token wallets, CBDC wallets, and a trade ledger with PII. If Exchange-2 and Exchange-3 do not include CBDC wallets, traders can trade security tokens with traditional fiat currencies, such as USD, EUR, etc. Exchange-2 and Exchange-3 identify and authenticate traders before trading. Although Exchange-2 does not include security token wallets, through interoperability between Exchange-2 and Exchange-3 (e.g., sharing order books, etc.), Exchange-2 and Exchange-3 can enable traders to trade between security tokens and fiat currencies, including CBDCs, between security tokens and cryptocurrencies (e.g., Bitcoin, Ether, etc.), and between security tokens. The fact that Exchange-2 does not include security token wallets means that Exchange-2 does not hold security tokens. Exchange-2 and Exchange-3 store and maintain a trade ledger containing the PII of the traders. The AML regulator administrates and supervises Exchange-2 and Exchange-3 to prevent money laundering involving security tokens.

As shown in Figure 4, the life cycle of security tokens includes issuance, distribution, usage, storage, and revocation phases. Unlike the life cycle of cryptocurrencies (e.g., Bitcoin, Eth, etc.), the life cycle of security tokens has a revocation phase. Since security tokens are used to tokenize tangible and intangible assets, the security tokens must be revoked when the tokenized assets are destroyed or tokenized asset management is fulfilled. The issuance phase occurs when issuers issue security tokens. The next phase of issuance is the distribution phase, which occurs when the issuers distribute the security tokens to the investors. The next phase of the distribution can be a usage, storage, or revocation phase. The usage phase occurs when the holders transfer their security tokens to other holders and trade their security tokens on exchanges. The next phase of the cycle can be either the storage or the revocation phase. The storage phase occurs when the holders keep their security tokens for a certain period. The holders can entrust custodians with their security tokens during the storage phase. The next storage phase can be either the usage or revocation phase. The revocation phase occurs when the issuers revoke the issued security tokens. Since security tokens are asset-backed tokens, security tokens that have fulfilled asset management must be revoked. The issuers can revoke the issued security tokens by transferring them to a predefined revocation wallet. The history of the issuance, distribution, usage, storage, and revocation of security tokens can be stored and maintained

on the blockchain. The trading history of security tokens can be stored and maintained by the exchanges.

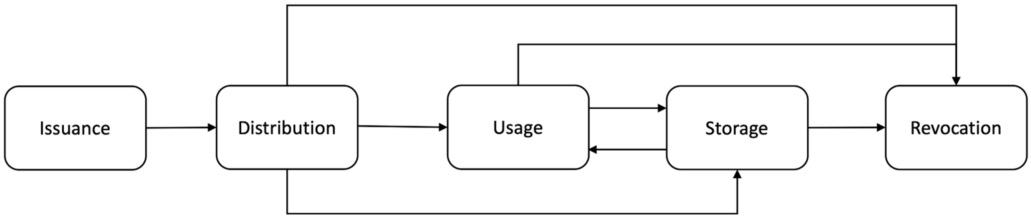


Figure 4. The life cycle of security tokens.

3.2. Service Scenarios and Data Flows

The service scenarios include investing in tokenized assets and trading in security tokens. The service scenario for trading in security tokens includes trading between security tokens and fiat currencies, including CBDCs, between security tokens and cryptocurrencies (e.g., Bitcoin, Ether, etc.), and between security tokens.

In Figure 5, the service scenario for investing in tokenized assets is described as follows:

1. The asset owner registers his/her assets with the tokenization service provider (TSP). The asset owner provides the TSP with minimally required data, such as the identity information of the asset owner, the identifier of the asset, and the price of the asset (AP). The TSP tokenizes the registered asset at the price of a security token (SP). If the AP is $100,000 and the SP is $100, the asset will be tokenized into 1000 security tokens.
2. The investor invests in the tokenized assets on the TSP. The investor provides the TSP with minimally required data, such as the identity of an investor, the identifier of an asset, and the amount of the security token. If the AP is $100,000 and the asset is tokenized into 1000 security tokens, the investor can even invest in the tokenized asset by purchasing one security token worth $100.
3. The TSP requests the issuer to issue security tokens. The TSP provides the issuer with minimally required data, such as the identifier of an asset, the price of a security token, the issue date of security tokens, the expiry date of security tokens, and the amount of security tokens to be issued.
4. The issuer stores the transaction to issue security tokens on the blockchain. The transaction contains minimally required data, such as the identifier of a security token, the identifier of an asset, the price of a security token, the name of an issuer, the issue date of security tokens, the expiry date of security tokens, and the amount of security tokens to be issued.
5. The issuer issues and distributes the security tokens to investors in proportion to the investment.
6. The TSP verifies, through the blockchain, whether the amount of issued security tokens and the amount of security tokens requested for issuance are the same. The TSP retrieves the ledgers on the blockchain containing the issuance information for the security tokens.
7. The TSP pays the investment to the asset owner, and the investor owns the asset in proportion to the investment.
8. If profits are made from the TSP's asset management, the TSP distributes the profits to the investor in proportion to the amount of security tokens held.
9. Once asset management is fulfilled, the TSP requests the issuer to revoke security tokens. The TSP provides the issuer with minimally required data, such as the identifier of a security token, the identifier of an asset, the price of a security token, the name of an issuer, the issue date of security tokens, the expiry date of security tokens, and the amount of security tokens to be revoked.
10. The issuer stores the transaction to revoke security tokens on the blockchain. The transaction contains minimally required data, such as the identifier of a security token,

the identifier of an asset, the price of a security token, the name of an issuer, the issue date of security tokens, the expiry date of security tokens, and the amount of security tokens to be revoked.

11. The TSP verifies, through the blockchain, whether the amount of revoked security tokens and the amount of security tokens requested for revocation are the same. The TSP retrieves the ledgers on the blockchain containing the revocation information for the security tokens.

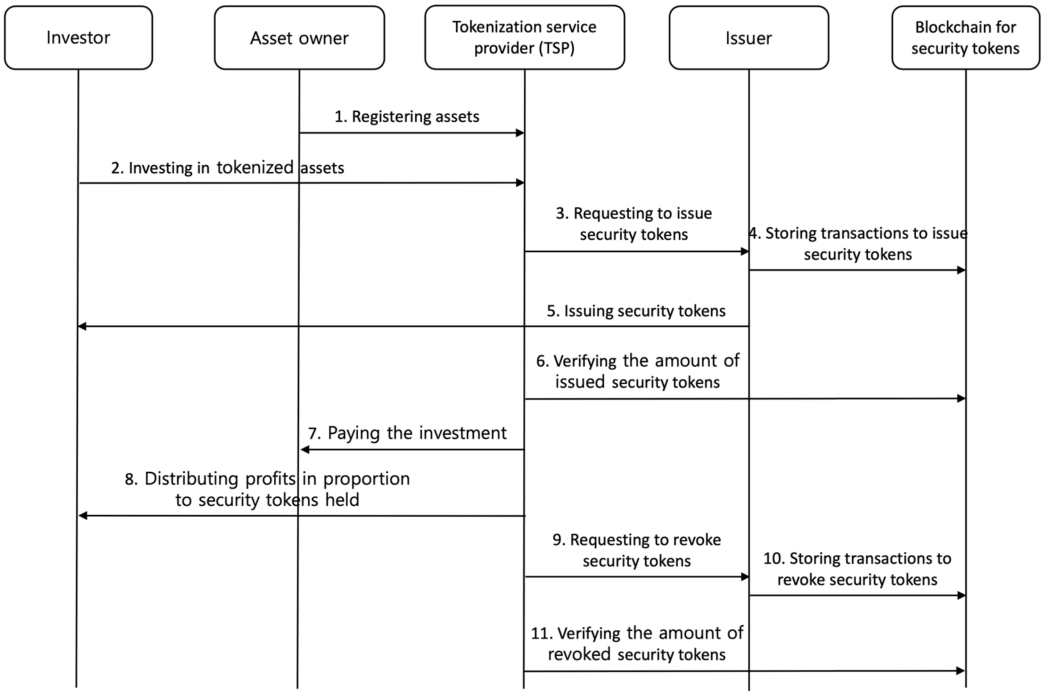


Figure 5. The service scenario for investing in tokenized assets.

In Figure 6, the service scenario for trading in security tokens is described as follows:

1. The AML regulator administers and supervises the exchange to prevent money laundering involving security tokens. The regulator enforces the exchange with the policy for anti-money laundering (AML), and the exchange complies with the policy.
2. The exchange retrieves the issuance and revocation information for security tokens on the blockchain. Issued security tokens can be listed on the exchange, and revoked security tokens must be delisted from the exchange.
3. The trader is identified and authenticated by the exchange. The trader provides the exchange with his/her identity information, and the exchange provides the trader with the wallet addresses for transferring security tokens.
4. The trader buys and sells security tokens on the exchange. The exchange provides the trader with trading between security tokens and fiat currencies, including CBDCs, between security tokens and cryptocurrencies (e.g., Bitcoin, Ether, etc.), and between security tokens.
5. The exchange stores and maintains the ledgers containing trade information for security tokens using a database management system (DBMS). The exchange provides the DBMS with minimally required data, such as the date of trade, the identifier of a security token, the identifier of a seller, the identifier of a buyer, and the amount of traded security tokens.
6. The exchange provides the AML regulator with trade ledgers retrieved from the DBMS in accordance with AML policy. The trade ledger includes minimally required data, such as the date of trade, the identifier of a security token, the identifier of a seller, the identifier of a buyer, and the amount of traded security tokens.

7. The exchange stores transfer information for security tokens on the blockchain. The transfer information includes minimally required data, such as the date of transfer, the identifier of a security token, an originator's wallet address, a beneficiary's wallet address, and the amount of transferred security tokens.
8. The exchange provides transfer information for the security tokens. The transfer information includes minimally required data, such as the date of transfer, the identifier of a security token, the identifier of an originator, an originator's wallet address, the identifier of a beneficiary, a beneficiary's wallet address, and the amount of transferred security tokens.
9. The AML regulator retrieves the transfer ledgers for security tokens from the blockchain. The transfer ledger includes minimally required data, such as the date of transfer, the identifier of a security token, an originator's wallet address, a beneficiary's wallet address, and the amount of transferred security tokens. The AML regulator verifies whether the transfer information provided by the exchange and the transfer information retrieved from the blockchain are the same.

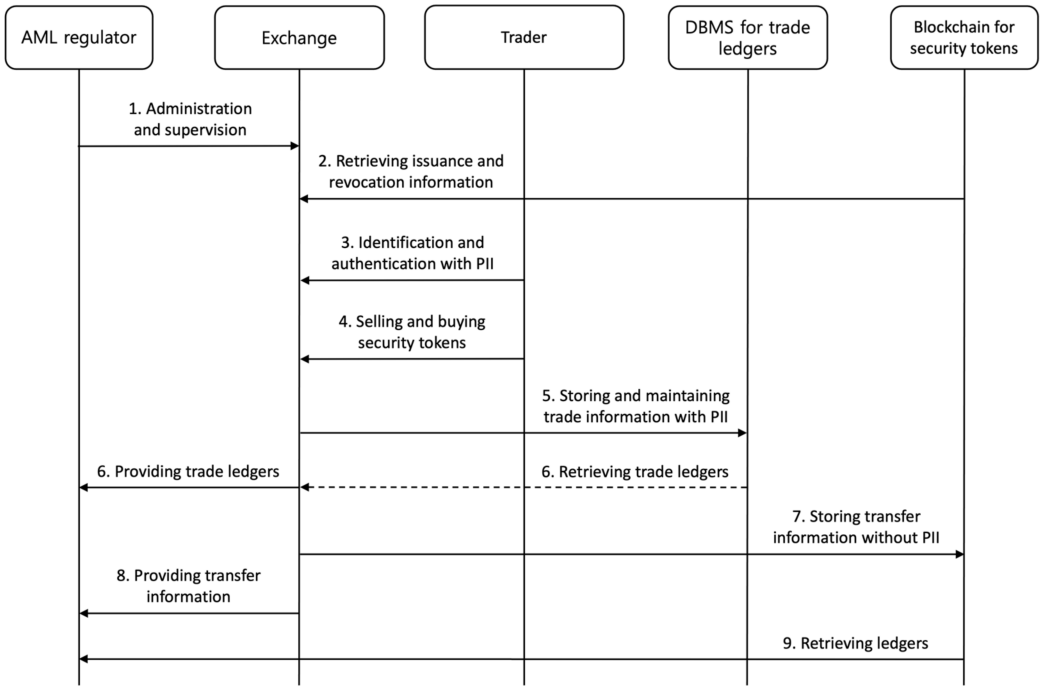


Figure 6. The service scenario for trading in security tokens.

4. Security Threats and Requirements

The security threats to the proposed service model for blockchain-based security tokens are identified and the security requirements countering the security threats are specified in this section.

4.1. Security Threats

The security threats (STs) to the proposed service model for blockchain-based security tokens are identified as follows:

- (ST-1) Deception involving the amount of issued security tokens: An issuer can falsify the amount of issued security tokens. The issuer can issue security tokens for more or less than the investment. This threat can cause money laundering involving security tokens and the embezzlement of investments.
- (ST-2) Deception involving the amount of revoked security tokens: An issuer can falsify the amount of revoked security tokens. The issuer can revoke security tokens for less

than the amount of issued security tokens. This threat can cause money laundering involving security tokens.

- (ST-3) Unauthorized transfer of security tokens: A custodian can transfer security tokens without the holder's permission. This threat can cause money laundering and embezzlement involving security tokens.
- (ST-4) Leakage of PII from a TSP: The massive PII of investors and asset owners can be leaked from a TSP that has stored and maintained the identity information of investors and asset owners. This threat can cause privacy issues related to investors and asset owners.
- (ST-5) Leakage of PII from an exchange: The massive PII of traders can be leaked from an exchange that has stored and maintained the identity information of traders and the trade ledger. This threat can cause privacy issues related to traders.
- (ST-6) Malicious behavior: An asset owner can falsify the price of his/her asset to be registered in a TSP. An asset owner can register other people's assets in a TSP through identity theft. An employee or employer of a TSP can embezzle investments. This threat can cause financial issues related to the TSP.

The security threats are specific to the proposed service model for blockchain-based security tokens; they are not related to general IT services, including existing cryptocurrency services such as issuance, transfer, payment, trading, etc.

4.2. Security Requirements

The security requirements (SRs) countering the security threats identified in Section 4.1 are specified as follows:

- (SR-1) Separation between an issuer and a TSP: The issuer of security tokens and the TSP should be two physically separate entities. The TSP should verify whether the amount of issued security tokens and the amount of security tokens requested to be issued are the same, as well as whether the amount of revoked security tokens and the amount of security tokens requested to be revoked are the same. This requirement can mitigate the ST-1 and ST-2 identified in Section 4.1.
- (SR-2) Separation between an issuer and an exchange: The issuer of security tokens and the exchange should be two physically separate entities. The exchange should verify whether the amount of issued security tokens and the amount of revoked security tokens are the same. This requirement can mitigate the ST-2 identified in Section 4.1.
- (SR-3) Wallet separation and audit logs: A custodian should create and maintain a security token wallet for each holder and allow each holder to transfer security tokens only through that wallet. The custodian should store and maintain the audit logs for the transfer of security tokens and inform the holders of the transfer history of security tokens in real time. The transfer information of security tokens should include the custodian's digital signature for nonrepudiation. This requirement can mitigate the ST-3 identified in Section 4.1.
- (SR-4) Data encryption: A TSP should use secure encryption algorithms (e.g., AES-128 [18], SHA-256 [19], etc.) to encrypt the PII related to the identity information of investors and asset owners when storing the PII. An exchange should use secure encryption algorithms (e.g., AES-128, SHA-256, etc.) and secure cryptographic protocols (e.g., TLS [20,21]) to encrypt the PII related to the identity information and trade ledgers of traders when storing and transmitting the PII. This requirement can mitigate the ST-4 and ST-5 identified in Section 4.1.
- (SR-5) Decentralized identification: An investor and an asset owner should present their identity certificates to a TSP using decentralized identity (DID) [22,23]. A trader should present his/her identity certificate to an exchange using DID. DID allows a TSP and an exchange not to store and maintain the PII related to identity information of investors, asset owners, and traders. This requirement can mitigate the ST-4 and ST-5 identified in Section 4.1;

- (SR-6) Investment protection: A TSP should assess the assets to be registered by asset owners. The TSP should verify, through an assessment, whether the asset price provided by an asset owner is reasonable. The TSP can conduct the assessment via a trustworthy third party. A TSP should entrust financial companies (e.g., banks, securities companies, etc.) with investments. This requirement can mitigate the ST-6 identified in Section 4.1.

5. Discussion and Conclusions

The proposed service model provides users (i.e., investors, holders, traders) with investment in and trading of tokenized tangible and intangible assets. Through the proposed service model, investors can invest small amounts (e.g., $10, $100, $1000, etc.) in expensive assets (e.g., $1 million building, art, etc.) and make a profit. The holders and traders can also sell security tokens (i.e., the ownership of tokenized assets) and make a profit.

Based on many studies in the literature, recommendations to prevent excessive regulation and market monopoly in the issuance and trade of security tokens are as follows:

- Separation between issuance and trade of security tokens: To prevent money laundering and market monopoly, it is necessary to strictly separate the issuer and exchange of security tokens. The issuer cannot provide a trading service for security tokens, and the exchange cannot issue security tokens. The issuers and exchanges, as stakeholders, can mutually monitor the amount of security tokens issued and transferred through the blockchain.
- Prohibition of excessive administration of security tokens: Since the amount of issued and revoked security tokens can be monitored through the blockchain (i.e., a decentralized distributed ledger system), if the regulator operates the nodes of the blockchain, it is unnecessary for the regulator to administer the amount of issued and revoked security tokens. The history of the issuance, distribution, usage, storage, and revocation of security tokens can be stored and maintained on the blockchain. Holders can entrust their security tokens to custodians. Financial companies (e.g., banks, etc.) can be custodians of security tokens.
- Prevention of monopoly in security token trading and expansion of the trading market: Rather than trading security tokens only on specific exchanges, through interoperability (e.g., sharing order books, etc.) between exchanges that list and do not list security tokens, trading between security tokens and fiat currencies, including CBDCs, between security tokens and cryptocurrencies (e.g., Bitcoin, Ether, etc.), and between security tokens must be allowed. The trade of security tokens must be allowed on cryptocurrency exchanges complying with AML regulations.
- There is no need for the restriction of assets to be tokenized. The increase in sales of TSPs, which tokenize tangible and intangible assets, is the most important element in the virtuous cycle structure that leads to the increased sales of issuers and exchanges due to the increased issuance and trading volume of security tokens. In addition to investing in already created assets (e.g., buildings, art, music, movies, etc.), there is no need to restrict the assets to be tokenized to make a profit by investing in creating assets. For example, this can include building construction and renovation, the production of agricultural, fishery, and livestock products, including processed products, and the creation of intellectual property (e.g., webtoons, music, movies, etc.).

Recommendations for evaluating the proposed service model include the following:

- Feature of security token wallet: Private keys for security tokens must be securely stored and maintained where the Internet is not connected.
- Feature of security token revocation: Once asset management is fulfilled, the security tokens must be permanently revoked. The revoked security tokens must not be transferred.
- Feature of privacy preservation: The PII of users must be securely stored and maintained where the Internet is not connected, and must be securely transmitted even over the Internet.

- Feature of investment management: The entire amount of the investment must be separated into TSP's funds and entrusted to financial companies, such as banks, securities companies, etc. The investment system must be assessed for compliance with requirements under AML laws.
- Feature of AML: AML systems involving security tokens must be assessed for compliance with requirements under AML laws.

The proposed service model will be developed as an international standard by ISO/TC 307 (blockchain and distributed ledger technologies), and the security guideline for the proposed service model will be developed as a Korean ICT standard by TTA (Telecommunications Technology Association) PG502. Private companies will be able to implement the proposed service for investment in tokenized assets based on the blockchain for security tokens by technology transfer in the future. In addition, as blockchain and security token technologies develop, studies on service models and security and privacy requirements can be enhanced accordingly.

Author Contributions: Conceptualization, K.P.; methodology, K.P.; validation, K.P. and H.-Y.Y.; formal analysis, K.P.; investigation, K.P.; writing—original draft preparation, K.P.; writing—review and editing, K.P. and H.-Y.Y.; supervision, H.-Y.Y.; project administration, H.-Y.Y. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Acknowledgments: This research was implemented as part of the project "Standardization Lab. for Next-generation Cybersecurity" (Project Number: 2021-0-00112) supported by MSIT (the Ministry of Science and ICT) and IITP (Institute of Information & Communications Technology Planning & Evaluation).

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. tZERO. Democratizing Markets Through Innovation. Available online: https://www.tzero.com (accessed on 29 December 2023).
2. Securitize. Accessed the Most Exclusive Asset Class in the World—Private Markets. Available online: https://securitize.io (accessed on 29 December 2023).
3. INX. Trade & Invest in Digital Assets. Available online: https://www.inx.co (accessed on 29 December 2023).
4. Security Token Market (STM). Security Tokens. Available online: https://stomarket.com (accessed on 29 December 2023).
5. JSTA. A Non-Profit Organization That Consolidates the Knowledge of Security Tokens and Promotes the Sound Development of the Security Token Ecosystem. Available online: https://securitytoken.or.jp/en/ (accessed on 29 December 2023).
6. CoinDesk. Tokenized RWAs Could Grow to a $10T Market by 2030 as Crypto Converges to TradFi: Report. Available online: https://www.coindesk.com/markets/2023/10/17/tokenized-rwas-could-grow-to-a-10t-market-by-2030-as-crypto-converges-to-tradfi-report/ (accessed on 29 December 2023).
7. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 30 December 2023).
8. Ethereum. Ethereum White Paper. Available online: https://ethereum.org/en/whitepaper/ (accessed on 30 December 2023).
9. GitHub. ERC 1400: Security Token Standard. Available online: https://github.com/ethereum/EIPs/issues/1411 (accessed on 27 December 2023).
10. Dossa, A.; Moore, G.; Lancaster, J.; Buchanan, M.; Ruiz, P. Polymesh Whitepaper v1.2. Available online: https://assets.polymesh.network/Whitepaper.pdf (accessed on 28 December 2023).
11. Arner, D.; Auer, R.; Frost, J. Stablecoins: Risks, Potential and Regulation. Available online: https://www.bis.org/publ/work905.pdf (accessed on 28 December 2023).
12. Lebrun, J.; Falempin, L.; Thizy, K.; Malghem, T.; Aznal, X.; Bousselin, T.; Croiseaux, F. Whitepaper, ERC3643, The T-REX Protocol (Token for Regulated EXchanges), The Token Standard for Real-World Asset Tokenization. Available online: https://www.erc3643.org (accessed on 27 December 2023).

13. Kreppmeier, J.; Laschinger, R.; Steininger, B.; Dorfleitner, G. Real Estate Security Token Offerings and the Secondary Market: Driven by Crypto Hype or Fundamentals? *J. Bank. Financ.* **2023**, *154*, 106940. [CrossRef]
14. Lambert, T.; Liebau, D.; Roosenboom, P. Security token offerings. *Small Bus. Econ.* **2022**, *59*, 299–325. [CrossRef]
15. Laurent, P.; Chollet, T.; Burke, M.; Seers, T. The Tokenization of Assets is Disrupting the Financial Industry. Are You Ready? Inside Magazine Issue 19 2019. Available online: https://www.wyoleg.gov/InterimCommittee/2019/S3-20190506TokenizationArticle.pdf (accessed on 28 December 2023).
16. Li, X.; Wu, X.; Pei, X.; Yao, Z. Tokenization: Open Asset Protocol on Blockchain. In Proceedings of the 2019 IEEE 2nd International Conference on Information and Computer Technologies (ICICT), Kahului, HI, USA, 14–17 March 2019. [CrossRef]
17. Benedetti, H.; Rodríguez-Garnica, G. Tokenized Assets and Securities. In *The Emerald Handbook on Cryptoassets: Investment Opportunities and Challenges*; Emerald Publishing Limited: Bingley, UK, 2023. [CrossRef]
18. Dworkin, M. Advanced Encryption Standard (AES). Available online: https://www.nist.gov/publications/advanced-encryption-standard-aes-0 (accessed on 30 December 2023).
19. Internet Engineering Task Force (IETF). US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF). Available online: https://datatracker.ietf.org/doc/html/rfc6234 (accessed on 30 December 2023).
20. OpenSSL Software Foundation. Vulnerabilities. Available online: https://www.openssl.org/news/vulnerabilities.html (accessed on 30 December 2023).
21. Internet Engineering Task Force (IETF). The Transport Layer Security (TLS) Protocol Version 1.3. Available online: https://datatracker.ietf.org/doc/html/rfc8446 (accessed on 30 December 2023).
22. Sporny, M.; Longley, D.; Sabadello, M.; Reed, D.; Steele, O.; Allen, C. Decentralized Identifiers (DIDs) v1.0 Core Architecture, Data Model, and Representations. Available online: https://www.w3.org/TR/did-core/ (accessed on 31 December 2023).
23. Sporny, M.; Longley, D.; Chadwick, D.; Steele, O. Verifiable Credentials Data Model v2.0. Available online: https://www.w3.org/TR/vc-data-model-2.0/ (accessed on 31 December 2023).