JANE
Journal of Entrepreneurial Economics
JANE 3(1): 70–85
ISSN 3048-0213

Institute for Advanced Science, Social and Sustainable Future
MORALITY BEFORE KNOWLEDGE

A sandbox regulatory framework for bullion integration in the decentralised digital finance (DeFi) ecosystem

Aidatul Fitriyah[1,*], Beckham Napitupulu[2]
[1] *Department of English Language and Literature, Faculty of Humanities, Universitas Airlangga, Surabaya, East Java 60286, Indonesia.*
[2] *Public Sector Accounting, Accounting, Politeknik Keuangan Negara STAN, South Tangerang, Banten 15222, Indonesia*
*Correspondence: aidatul.fitriyah-2020@fib.unair.ac.id

Received Date: January 10, 2025 Revised Date: February 23, 2026 Accepted Date: February 25, 2026

ABSTRACT
Background: This research addresses regulatory friction and systemic risks arising from the integration of tokenised bullion into the Decentralised Finance (DeFi) ecosystem, focusing on how to balance investor protection with continued innovation. It outlines the context of DeFi's permissionless architecture, the sensitivity of bullion as a high value asset class, and the resulting challenges for regulatory certainty and market integrity. **Methods:** The study employs an analytical and conceptual approach based on a comprehensive literature review and the examination of international regulatory frameworks, including IOSCO principles and FATF recommendations. It develops an adaptive regulatory model by comparing existing rules on securities, commodities, and virtual assets with the specific risk profile of tokenised bullion in DeFi. **Findings:** The analysis identifies core conflicts between DeFi's borderless, permissionless protocols and jurisdiction bound AML/KYC requirements, as well as single point of failure risks arising from custodial bullion structures. To address these conflicts, the paper proposes a DeFi Bullion Specific Regulatory Sandbox Framework grounded in technology neutral and risk based principles, which embeds regulatory KPIs, capital adequacy thresholds, and RegTech enabled real time monitoring. **Conclusion:** The results indicate that the proposed sandbox model offers a viable pathway to mitigate systemic risk and enhance regulatory certainty by enforcing compliance at critical on chain and off chain interaction points, particularly physical redemption of bullion. The framework strengthens investor protection while preserving space for innovation in tokenised bullion markets. **Novelty/Originality of this article:** This research delivers a comprehensive and actionable regulatory blueprint tailored to tokenised bullion in DeFi, explicitly addressing jurisdictional arbitrage and dual asset integrity issues. Its original contributions include defining technical prerequisites for embedding AML compliance into DAO governance and outlining a cross border mandatory liquidation protocol as a theoretical roadmap for regulators and industry stakeholders.

KEYWORDS: sandbox regulatory; digital finance; bullion; regulator technology.

1. Introduction

Over the last decade, the global financial architecture has undergone fundamental disruption due to the adoption of Distributed Ledger Technology (DLT). One of the most significant manifestations of this disruption is the tokenisation of Real World Assets (RWA). This mechanism transforms ownership rights of physical assets into programmable digital representations, creating a market projected by the Boston Consulting Group (BCG) to reach US$16 trillion by 2030, representing approximately 10% of global GDP (Kumar et al., n.d.).

Cite This Article:
Fitriyah, A., & Napitupulu, B. (2026). A sandbox regulatory framework for bullion integration in the decentralised digital finance (DeFi) ecosystem. *Journal of Entrepreneurial Economics*, *3*(1), 70-85. https://doi.org/10.61511/jane.v3i1.2026.3397

Among the broad spectrum of assets, gold bullion has emerged as a primitive asset class attracting substantial market attention with a global market capitalisation estimated at US$28-30 trillion as of late 2025 (Kumar et al., n.d.). The urgency for gold tokenisation is driven not only by its intrinsic characteristic as a hedging asset (haven) against inflation and fiat volatility but also by persistent structural inefficiencies in conventional commodity markets.

High transactional frictions and exclusionary barriers burden traditional gold markets. Conventional trading often imposes wide spreads and significant barriers to entry, such as the standard "Good Delivery" bar weighing 400 troy ounces (approx. 12.5 kg), which requires a minimum capital outlay exceeding EU 600,000, effectively excluding the vast majority of retail investors (Marston, 2020). These economic inefficiencies are exacerbated by operational hurdles, specifically long, multi-layered custody chains. Traditional settlement cycles typically follow a T+2 (Trade plus two days) timeframe, requiring repeated physical verification and reconciliation across intermediaries (CITI, 2023). This centralized reliance introduces points of failure, operational delays, and high storage and insurance costs that erode investor net returns.

The integration of bullion into the Decentralised Finance (DeFi) ecosystem offers a radical solution through fractionalization. This democratisation enables micro-scale participation allowing investment entry as low as US$0.01, which was previously economically unfeasible (World Bank Group, 2024). Consequently, this has spurred the growth of tokenised gold assets, such as Tether Gold (XAUT) and Paxos Gold (PAXG), which now command a combined market capitalisation exceeding US$1 billion (Díaz et al., 2023).

Beyond accessibility, tokenisation transforms gold from a static asset into a dynamic financial instrument. Through smart contracts, the trading cycle is executed autonomously via atomic settlement, reducing settlement time from days to seconds and effectively eliminating counterparty risk. Furthermore, tokenised gold can be utilized within DeFi protocols for lending, borrowing, and liquidity pooling on a 24/7 basis, overcoming the limited operating hours of legacy commodity exchanges (Baur & Lucey, 2010).

However, the convergence between the heavily regulated physical commodity markets and permissionless, borderless DeFi protocols creates a multifaceted legal dilemma (Harvey et al., 2020). Physical gold trading is subject to strict national regimes regarding custody standards and purity audits, whereas DeFi protocols operate in a decentralized environment that often escapes the reach of single jurisdictions. This disparity raises the risk of "regulatory arbitrage," where market participants opportunistically exploit loopholes across jurisdictions to avoid compliance burdens (Riles, 2013). A critical concern is the enforceability of the legal rights represented by tokens. In the event of a protocol exploit or custodian bankruptcy, legal avenues for redeeming physical gold from digital tokens remain untested under conventional contract law. Moreover, ontological uncertainty regarding the legal status of tokens hinders adoption by mainstream financial institutions and increases exposure to systemic risks, including money laundering and terrorist financing (FATF, 2023)

Despite the growing market traction, existing academic literature remains bifurcated. Previous studies have predominantly focused either on the technical scalability of DLT architectures or the macroeconomic utility of asset tokenisation. There is a critical scarcity of socio-legal research that specifically addresses the "hybrid paradox", the legal friction between immutable on-chain ownership and the mutable, regulated nature of physical custody. Existing legal frameworks often treat digital assets as purely virtual, neglecting the custodial complexities unique to tangible commodities like gold. Furthermore, while the concept of a "Regulatory Sandbox" is widely discussed in fintech literature, no specific framework currently exists that tailors this mechanism to the unique volatility and settlement risks of tokenised commodities.

This research bridges this gap by offering a novel techno-legal framework. Unlike normative legal studies that suggest static regulations, this study introduces a dynamic Regulatory Sandbox model specifically designed for tokenised bullion. The primary novelty lies in the proposed integration of algorithmic supervision directly into the governance

model, ensuring that compliance is not merely a retrospective legal obligation but a prospective element of the protocol code itself.

Given the complex issues outlined above, this research aims to develop a comprehensive analytical framework that bridges the gap between the acceleration of technological innovation and the need for legal certainty. Specifically, this research is designed to achieve three strategic objectives. First, to critically analyse the regulatory gap and potential legal conflicts arising in tradetokenised bullion. This identification is crucial for mapping specific friction points where current positive law fails to accommodate the hybrid and cross-border nature of decentralised digital assets.

Second, this study aims to develop a framework model. Regulatory Sandbox: adaptive and responsive. Adopting the experimental approach recommended by global institutions such as the modelsandbox. This framework is designed as a "safe testbed" with limited parameters (World Bank Group, 2020). The goal is to enable productive coexistence between DeFi protocol innovation and regulatory oversight mandates, enabling regulations to be empirically tested before widespread implementation.

Third, formulate governance recommendations for holistic risk mitigation. This recommendation includes integrating Anti-Money Laundering (AML) and Know Your Customer (KYC) standards directly into the protocol logic (on-chain compliance), as well as developing robust consumer protection mechanisms against price volatility and technical risks, such as a fault-tolerant, contractor-data-inaccuracy oracle. The significance of this research lies in its contribution to the emerging literature on the digital economy and capital market law. For regulators, it offers a blueprint for prudential supervision that balances financial stability with innovation. For industry players, it provides strategic compliance guidance to navigate the fragmented regulatory landscape. Macroeconomically, this research encourages the paradigm of responsible innovation, ensuring that the market efficiency offered by DeFi is realized without compromising market integrity or investor protection (Dias et al., 2022).

2. Methods

This research is categorised as a Comprehensive Literature Review and Conceptual Framework Development Study. Its primary focus is to present actionable theoretical solutions to the regulatory challenges arising from tokenised bullion in DeFi. The primary data used comes from a critical analysis of global policy and regulatory documents. The data sources for this research are divided into two main categories: Primary Data (Normative Documents) and Secondary Data (Academic and Industry Literature). Primary Data includes policy and regulatory documents from leading international institutions, such as the Financial Action Task Force (FATF) Guidelines and Recommendations, which are crucial for Anti-Money Laundering (AML) and Know Your Customer (KYC) requirements for Virtual Asset Service Providers (VASPs). Furthermore, Primary Data includes the Principles and Recommendations of the International Organisation of Securities Commissions (IOSCO), particularly those relating to investor protection and cross-border cooperation (Principles 13 and 14), as well as reports from the Financial Stability Board (FSB) addressing the systemic risks of crypto assets. These normative sources are reinforced by an analysis of relevant Regulations and regulatory proposals from major global jurisdictions (such as the European Union's MiCA and policies from Asian authorities) (FSB, 2017). Meanwhile, Secondary Data comes from academic and industry literature, including journals, legal articles, and reports specifically addressing DeFi governance, smart contract risks, physical asset custody issues, and jurisdictional arbitration dilemmas in blockchain technology.

The data collection technique used was systematic library research. This process involved as follows: use keyword combinations such as “tokenised bullion regulation,” “DeFi AML KYC,” “regulatory sandbox crypto,” “FATF VASP,” and “IOSCO principles”; focusing on documents published by international regulatory bodies and academic literature that have high relevance to the integration of physical assets (gold) into a decentralized financial framework. The data analysis for this research was executed

through two main phases. The first phase, Critical Normative Analysis, focused on deconstructing the existing regulatory framework to identify regulatory frictions unresolved by traditional provisions. Specifically, this analysis included Identifying Core Conflicts, comparing the basic philosophy of decentralization (permissionlessness) with the principles of sovereignty, territoriality, and legal accountability, and determining Regulatory Gaps related to fully decentralized entities (Decentralized Autonomous Organizations/DAOs) and assets that have a dual layer (physical and digital) that is inadequate in current guidance (e.g., FATF). Based on these findings, the research transitioned to the second phase: Conceptual Framework Development. This framework aims to formulate adaptive regulatory solutions using a Risk-Based Approach, where regulations are shaped by the level of risk posed (operational risk, liquidity, AML, smart contracts) rather than the technology used. This development resulted in the Adaptive Sandbox Model, a Bullion-specific DeFi Sandbox Regulatory Framework that requires key elements, including regulatory Key Performance Indicators (KPIs) and transition mechanisms (graduation/closure), as well as a Hybrid Solution Synthesis that integrates on-chain analytics with off-chain KYC at critical gateways (minting and redemption). Overall, the resulting conceptual framework represents a synthesis that links international regulatory requirements with the technical realities of DeFi operations, thus forming a coherent roadmap to achieve regulatory certainty.

3. Results and Discussion

3.1 Bullion regulatory challenges in the DeFi ecosystem

The implementation of tokenised bullion assets within the Decentralised Finance (DeFi) ecosystem offers significant capital efficiency and global liquidity, yet fundamentally generates unresolved regulatory frictions. The core issue stems from the deep discrepancy between borderless, permissionless, anonymous, and global technologies, and legal frameworks that are territorial, rigid, and historically grounded. This conflict inhibits the full integration of high-value physical assets into modern digital finance.

3.1.1 Jurisdictional conflicts and regulatory arbitrage

The central conflict arises from DeFi's permissionless nature, which enables it to operate across sovereign boundaries. At the same time, the regulation of capital markets and gold assets has traditionally been tied to the geographic borders of nation-states. Tokenised bullion, which can be traded 24/7 on Global Automated Market Makers (AMMs), creates explicit potential for jurisdictional arbitrage, whereby issuers or users strategically seek regulatory loopholes in countries with the least stringent market oversight. This phenomenon risks triggering a "race to the bottom" in financial supervisory standards (Zetzsche et al., 2017).

Traditional legal frameworks, such as the principles embedded in Indonesia's Law on the Prevention and Eradication of Money Laundering/*Tindak Pidana Pencucian Uang* (UU TPPU), base law-enforcement authority on territoriality. Article 17 of the UU TPPU explicitly requires the implementation of Know Your Customer Principles/*Prinsip Mengenali Pengguna Jasa* (PMPJ) or Customer Due Diligence (CDD). The wording of Article 17 paragraphs (1) and (2) is as follows.

> Article 17 paragraph (1): *"Financial Service Providers must apply the Know Your Customer Principle."*
>
> Article 17 paragraph (2): *"The Know Your Customer Principle as referred to in paragraph (1) includes: a. identification of the Customer; b. verification of the Customer; and c. monitoring of the business relationship."*

These foundational principles are difficult to enforce on DeFi protocols that lack a physical headquarters or a clear legal entity within any single country, which contradicts FATF Recommendation 10, which requires CDD. The inability to determine which jurisdiction is responsible for tokenised gold allows protocol s to operate outside of this legal framework.

3.1.2 AML–KYC challenges and the core anonymity problem

The most significant challenge lies in harmonizing Anti-Money Laundering (AML) and Know Your Customer (KYC) standards. Although the Financial Action Task Force (FATF) has issued guidelines intended to accommodate Virtual Asset Service Providers (VASPs), DeFi protocols, especially those operating without centralised intermediaries, are inherently resistant to party identification and preserve user anonymity (Hou Sak, 2024). This creates significant opportunities for terrorism financing and money laundering.

Indonesia's Law on the Prevention and Eradication of Money Laundering/*Tindak Pidana Pencucian Uang* (UU TPPU) require the identification and verification of users. DeFi, through its anonymous design, fundamentally contradicts these obligations. Deficiencies in compliance with global standards further reinforce the failure of law enforcement. The basic principles of Customer Due Diligence (CDD) within the international AML framework include mandatory information transfers. FATF Recommendation 16 (Wire Transfers) specifically requires VASPs to obtain and retain necessary information such as the sender's name, account number, and physical address. The inability or refusal of DeFi protocols to comply with this recommendation directly violates global compliance principles and renders them high-risk in the eyes of regulators. If gold tokens are considered securities or high-risk instruments in certain jurisdictions, the originating jurisdiction must be able to enforce sanctions and financial crime prevention regimes. The failure to achieve a binding global consensus on digital identity significantly obstructs safe institutional adoption.

3.1.3 Asset integrity and the custodian challenge

The integrity of tokenised bullion depends entirely on the verification of the underlying physical asset, a dependency that contradicts the philosophy of decentralisation. This creates a significant custodian challenge. Although Proof of Reserve (PoR) mechanisms are employed, the verification and auditing of physical gold must be conducted periodically by independent third-party auditors. (Braband, 2024).

Inconsistent, non–real-time audits, or audits conducted using non-standardised methodologies, create a single point of failure (SPOF) for the physical asset and revive the problem of information asymmetry. The reliance of tokens on physical audits, which remain largely manual, reveals that decentralisation occurs only at the data-transaction layer, not at the primary asset-integrity layer. In conventional capital markets, the principle of custodian asset segregation is absolute. Securities laws establish that client assets must be separated from the custodian firm's own assets. For gold-backed tokens, this means custodians must guarantee that the underlying gold exists, is not rehypothecated, and is legally owned by token holders. The absence of strong legal assurances regarding ultimate ownership rights in the digital domain creates substantial risks to legal certainty.

3.1.4 Smart contract execution risk, oracle failure, and the implications of immutability

Smart contracts governing the issuance, redemption, and collateralization of tokens introduce unique execution risks. Although the principle of "code is law" is adhered to, vulnerabilities such as bugs, flawed contract design, or intentional exploitation may result in permanent and massive losses (Werbach, 2018). The immutability of smart contracts deployed on blockchain exacerbates these risks. Unlike traditional financial systems, which allow for patches or interventions, defective DeFi code is difficult to repair, and losses from

cyberattacks (e.g., re-entrancy exploits or flash loan attacks) are often irreversible. This exposes holders of gold-backed tokens to the potential for rapid and total loss.

These risks are compounded by oracle-related problems that may feed incorrect price data or recommendations to smart contracts, thereby triggering erroneous executions. Oracle failures, whether due to price manipulation or technical errors (downtime), directly threaten the fundamental function of gold tokens as collateralised assets. For instance, if an oracle fails to load the correct market price of gold or is manipulated to report significantly lower values, a smart contract may wrongfully liquidate a user's collateral even when the user remains solvent. The safe integration of real-world custodian audit data with digital smart contracts via oracles remains a major technical and regulatory challenge, creating layered risks that far exceed those in traditional custodian systems

3.1.5 Consumer protection and dispute resolution mechanisms

Within the DeFi framework, consumer and investor protection is significantly diminished due to the removal of centralised intermediaries. As a result, no institution is responsible for providing legally recognised dispute-resolution mechanisms. In cases of valuation disagreements, token-redemption failures, or clawbacks, investors have no access to traditional complaint channels that can enforce compensation (Grennan, 2022). Decentralised Autonomous Organisations (DAOs) that may govern gold tokens are often too dispersed and anonymous to be held legally accountable. Provisions on investor protection in traditional capital-market laws, such as those regulated under Law Number 21 of 2011 concerning the Financial Services Authority/*Undang-Undang Otoritas Jasa Keuangan* (UU OJK), guarantee avenues and rights to seek compensation. Article 28, paragraph (1)(f) of the UU OJK specifically grants authority to the OJK, which states:

> *"to conduct legal defence, including appointing another party to act as OJK's representative in court,"* as well as facilitating dispute resolution through mediation and facilitation.

In addition, Law Number 8 of 1995 concerning Capital Markets/*Undang-Undang Pasar Modal* explicitly regulates legal liability (Articles 104 and 107) and mandates the establishment of the Investor Protection Fund/*Dana Perlindungan Pemodal* (DPP). In the DeFi context, the disappearance of intermediary roles means there is no central body that can be sued or subject to OJK authority, effectively eliminating the statutory rights to compensation guaranteed by these laws.

3.1.6 Transparency and information asymmetry

Transparency for gold tokens must extend beyond mere ledger transactions on the blockchain. Comprehensive risk disclosures must include highly specific details on the physical location of the gold, insurance policies, vault storage fees, and explicit statements clarifying that the token represents a digital claim on the asset (debt), not direct physical ownership. The technical complexity and governance structures of DeFi often create severe information asymmetry, which may cause retail investors to misunderstand the de jure relationship between the digital token and the physical gold held by custodians(Muradyan, 2023).

Furthermore, Goforth (2021) States That Regulators play a crucial role in establishing minimum disclosure standards to ensure that stakeholders fully understand smart-contract risks, custodian risks, and redemption rights. This Principle of Information Disclosure is supported by Article 8 of Law Number 8 of 1995 concerning Capital Markets*/Undang-Undang Pasar Modal*, which explicitly regulates disclosure responsibilities. The article states:

> *"Any Party engaged in the Capital Market shall ensure the absence of incorrect and/or misleading information regarding material facts related to the Securities being offered or guaranteed."*

This provision requires every issuer or any functionally equivalent party in DeFi to disclose all material information, including custodian risk details, storage fees, and the legal status of token claims, to ensure transparent investment decision-making.

3.2 Bullion-DeFi sandbox regulatory framework model

3.2.1 General principle of sandbox

In response to the regulatory complexity and systemic risks outlined in the previous discussion, Bullion-DeFi proposed a Regulatory Sandbox, designed as a crucial intermediary solution for innovation. This framework aims to facilitate safe, controlled innovation experiments, enabling regulators to assess risks in real time and develop supervisory expertise before integrating this technology into the broader market regulatory framework (FSB, 2017). This Framework sandbox approach must be based on adaptive, outcome-oriented principles, not on process-oriented ones.

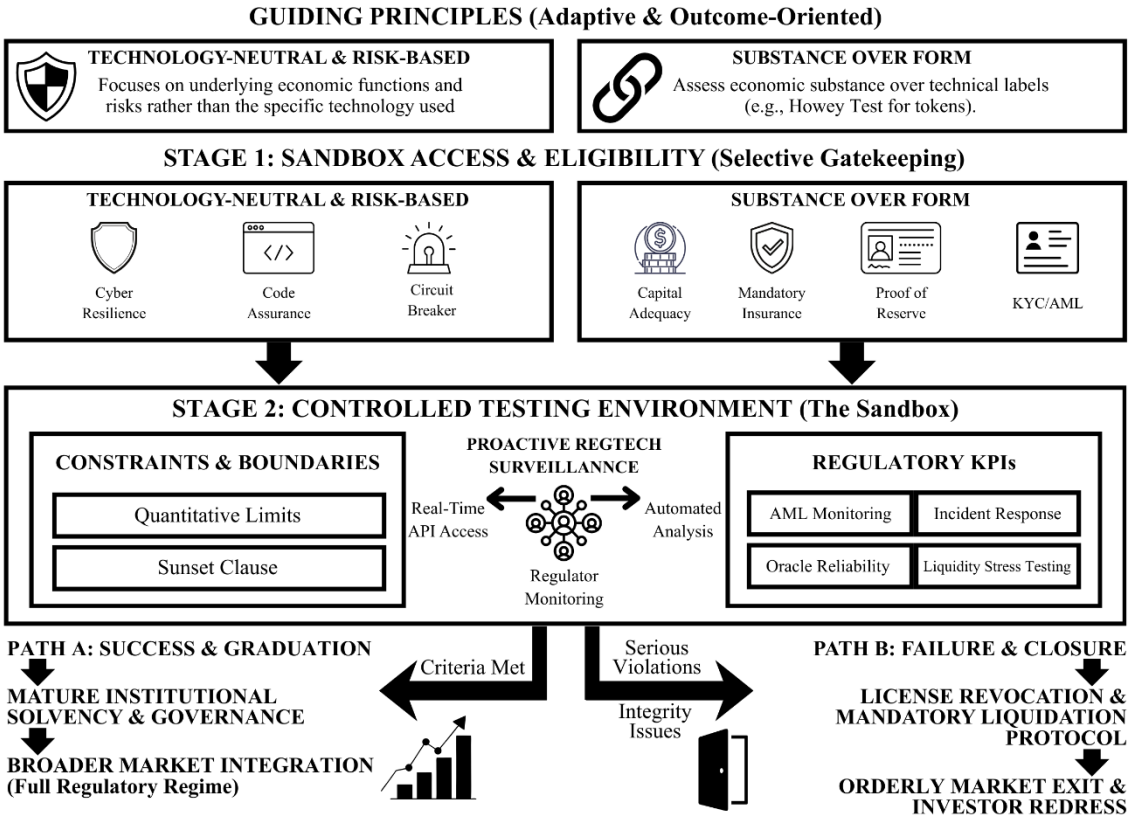

Fig. 1 Bullion DeFi sandbox regulatory framework

First, the Technology-Neutral and Risk-Based approach is fundamental. Regulation should not focus on platforms or types of blockchain used (technological neutrality), but rather on the economic function, systemic risk, and consumer risks arising from the activities carried out. For example, custodial functions and settlement. Second, the overriding principle should be Substance over Form (Zetzsche et al., 2020). Regulators should ignore technical labels like "token" or "coin" and assess their economic substance. If tokenised bullion meets the criteria as an investment contract or security under the Howey test, then it must be regulated by capital market standards applicable to securities (Rohr & Wright, 2017). This principle is crucial to prevent regulatory arbitrage that exploits

technical terminology. The application of this principle ensures that the protection offered by the sandbox is proportional to the financial activity's inherent risk. Access to the Bullion-DeFi Sandbox must be selective, prioritising fiduciary duties and high-risk mitigation, making it the first line of defence for market integrity. Eligibility criteria must carefully address both the physical asset risks and the digital execution risks inherent in the operational model of tokenised bullion.

3.2.2 Technical and operational requirements

Participants must have strong, tested proof of Cyber Resilience. This is not limited to a firewall; it must include a mandatory, comprehensive audit by an independent third-party cybersecurity auditor. This audit must include a comprehensive coverage of all critical functions (minting, redemption, and transfer) and requires periodic certification (at least quarterly), especially after major code updates (Tao et al., 2018). The platform must provide technical assurance that the code is executed correctly and securely, as well as implement emergency mechanisms, or 'circuit breaker', which can be activated by the authorities' sandbox (or multisig approved) to temporarily suspend operations in the event of a critical attack or bug (Werbach, 2018). The existence of this mechanism is a legal recognition that the principle of code is law must be subject to investor protection in the event of a systemic emergency.

3.2.3 Custodian financial and integrity requirements

From an economic perspective, the physical gold custodian entity that partners must meet the Capital Adequacy Requirements (Capital Adequacy Requirements), which are tight, functions as a buffer against primary financial risk from uninsured operational losses and must be proportionately adjusted to liquidity risk and gold price volatility. In addition, Argue that adequate insurance policies against operational risks, loss, or theft of the McLaughlin & Pecchenino (2022) underlying are mandatory. Token issuers are also required to demonstrate a legally binding protocol for Proof of Reserve (PoR) that is routinely audited by independent parties in accordance with LBMA standards and supported by on-chain cryptographic evidence. Finally, clear user identification procedures for AML/KYC compliance are imperative, especially at the point of physical redemption. It is at this point, when a digital claim is converted into a physical asset, that digital anonymity must be de-anonymised into a legitimate, verified physical identity, ensuring compliance with global sanctions and financial crime prevention measures. Testing within the sandbox must be designed to evaluate systemic impacts and operational integrity under stress, a crucial stage in the risk-based framework

3.2.4 Testing within the sandbox

3.2.4.1 Volume and market value restrictions

Regulators must establish strict and dynamic Quantitative Limits. These limits include a limit on the total value locked (Total Value Locked/ TVL) of gold tokens issued and limits on the number of retail investors allowed to participate (OECD, 2024). These limits are not only designed to prevent potential systemic risks from remaining isolated within the environmentsandbox, but also to ensure that the data generated during the testing period is representative and sufficient for in-depth analysis (FSB, 2017). For example, regulators could limit the initial market capitalisation to 10% of the custodian's authorised physical gold reserves, and limit the maximum transaction value per wallet in 24 hours to mitigate the risk of market manipulation.

3.2.4.1 Regulatory time and KPIs

The test period should be determined by a sunset clause(e.g., 12 to 24 months), ensuring that entities do not operate indefinitely under a lenient supervisory regime. Regulatory Key Performance Indicators (KPIs) should focus on critical compliance metrics that directly measure risk mitigation. The effectiveness of real-time AML monitoring, which includes the accuracy of suspicious transaction (STR) detection and reporting, as well as the blocking of wallets associated with sanctions lists. The frequency and response time of smart contract security incidents, including the platform's ability to perform regulator-approved emergency upgrades. The reliability of the oracle linking the gold market price to the smart contract valuation, measured by the average price deviation (slippage) between the on-chain price and the global gold market price (e.g., LBMA).

Platforms must also undergo comprehensive liquidity stress testing, simulating simultaneous mass redemption requests. This stress test scenario should test the physical custodian's ability to process redemptions (both physical and fiat equivalents) within a specified timeframe, as well as the robustness of smart contract mechanisms to prevent unfair digital bank runs. The results of this testing should serve as the primary basis for evaluating eligibility for graduation. Surveillance within the sandbox must be proactive, utilising Regulatory Technology (RegTech) tools to monitor on-chain data and anticipate risks rather than just react. ImplementationRegTech. This ensures that supervision does not become a barrier but an enabler for detecting anomalies in real time (Hou Sak, 2024).

3.2.5 Surveillance and RegTech implementation

3.2.5.1 Monitoring system real-time

Participants are required to provide a standardised, secure Application Programming Interface (API) that allows regulators to retrieve and analyse transaction data in real time. This API should include not only trading volume and market capitalisation, but also health metrics and smart contract metrics (for example, the number of gas fees, changes in pool liquidity, and consistency of the oracle feed). Periodic reporting, supported by tools, RegTech, and automated metrics, should include operational risk, smart contract risk, and AML compliance status metrics, allowing for rapid intervention if established risk thresholds are breached. A legal framework should support the legality of this mandate for API access. The sandbox itself stipulates that data access is a prerequisite for participation. This allows regulators to conduct transaction flow analysis (transaction flow analysis) to detect complex money laundering patterns automatically.

3.2.5.2 Transition procedure (graduation) and withdrawal of permit (closure)

Integrity lies in its ability to manage the transition to full regulation and, more importantly, manage failures in an orderly manner. Graduation, transition to a full regulatory regime (graduation) is only awarded if the participant not only successfully meets all KPIs, but also maintains consistent compliance and demonstrates Mature Institutional Solvency and Governance (Zetzsche et al., 2017). This mature governance includes the establishment of an independent board of directors structure, the implementation of a strong internal audit function, and adjustments to the capital buffer, which is proportional to their market size after exiting the sandbox. This is a positive signal to the global market and regulators about the maturity of the technology being tested.

Closure, in the event of serious violations of the KPI, repeated consumer protection failures, or fundamental issues with the custodian's integrity, the regulator should have the authority to revoke the operating license forcibly. License revocation must be followed by the implementation of a Mandatory Liquidation Protocol that has been agreed upon and rigorously tested before operation. This protocol should include a clear sequence of actions: asset freezing on-chain, assignment of a reserve custodian (escrow agent), and the orderly

and protected redemption of physical gold assets held by custodians. Legal innovation is needed to ensure that this protocol can be effectively enforced against DAO assets or smart contracts that may be resistant to traditional legal orders, providing a fast and clear redress mechanism for retail investors (Guillaume & Riva, 2022).

3.3 Governance and risk mitigation recommendations

3.3.1 Digital custody standardisation

To achieve a safe coexistence among innovation, tokenised bullion DeFi, and traditional financial stability, a series of recommendations is needed, focused on technical standardisation, strengthening AML compliance, and cross-border regulatory harmonisation Monitoring the integrity of physical assets is a top priority. Therefore, it is necessary to create global standards for Proof of Reserve (PoR), Verified On-Chain, and Verified Off-Chain. Auditing physical gold reserves is no longer sufficient to be merely periodic; it must adopt cryptographic audit elements that mimic the transparency of blockchain (Grieves, 2015). This standard requires custodians to use consistent audit methodologies (e.g., LBMA standards) and engage credible third-party auditors (Braband, 2024).

The need for this rigorous audit is crucial, considering the structure, tokenised bullion, functionally similar, stablecoin asset-backed gold, where reserve transparency is a key determinant of market confidence(Adrian & Mancini-Griffoli, 2019). PoR standards must not only ensure a 1:1 ratio between tokens and physical reserves, but must also include metrics on the asset's physical location and quality. This means that each token must be transparently linked to a specific physical gold bar serial number and a verified vault location, not just a collective claim. This increased transparency effectively reduces information asymmetry, which allows for the misuse of funds and practices, and fractional reserve (Dhali et al., 2024).

Furthermore, the results of the physical audit (off-chain) must be hashed and published on the blockchain (on-chain), allowing real-time public verification that the pledged assets have been audited and that the data has not been manipulated. This process requires the development of a protocol, specifically PoR, with decentralised governance (e.g., multisig among auditors and regulators) to bridge sensitive physical data into a smart contract without introducing a new SPOF. The mechanism oracle must be resistant to censorship and data manipulation.

This standardisation should explicitly include protocol-custodial disaster recovery, which ensures that, in a default or liquidation scenario, a binding legal mechanism allows physical assets to be accessed and redeemed by token holders in a predetermined priority order, mitigating the risk of a single point of failure (SPOF) in the physical asset system. An agreement, escrow, and trust must support this recovery protocol. A legally recognised cross-jurisdictional agreement designates an independent legal entity with the right and authority to take custody of physical assets on behalf of token holders in the event of the issuing entity's failure. This effectively separates the operational risk of the token issuer from the risk of the physical gold custodian (Adhami & Guegan, 2020). This careful legal design is a prerequisite for building the institutional trust needed to integrate real assets into the DeFi ecosystem.

3.3.2 Enhanced anti-money laundering (AML) mechanisms in DeFi

The anonymous nature of DeFi poses a significant threat to global AML objectives. A realistic solution is to implement a hybrid AML solution that combines decentralised capabilities with regulatory requirements. This approach integrates analytics. On-Chain, where the device RegTech monitors the flow of funds and automatically identifies suspicious transaction patterns (Suspicious Transaction Reports/STR) with KYC; Off-Chain, centred on the gateway, is critical. The use of on-chain Analytics in this hybrid model must

be expanded. This analytics not only tracks wallet addresses, but uses machine learning algorithms (machine learning) which are trained to recognise the complex and anomalous fund transfer patterns that are characteristic of layering(layers) in money laundering, such as mixing services, peel chain, and transactions that are suddenly fragmented or concentrated to high-risk addresses (Islam et al., 2025). Analytics on-chain-generated intelligence data should be a mandatory input to the gateway Centralised KYC/CDD.

These critical points are where gold tokens interact with the real world: when they are first minted (issued) from fiat or physical gold, and when they are redeemed for physical gold. At the point of redemption, KYC/CDD procedures (Customer Due Diligence) must be strictly enabled, changing anonymity on-chain to a verified identity on-chain, in accordance with the FATF guidelines for VASPs (Hou Sak, 2024). In addition, to meet FATF standards, the gateway must also implement the Travel Rule, ensuring that the information of the sender and recipient of gold tokens is transferred and stored securely when exceeding certain value limits, especially when interacting with third-party VASPs.

Furthermore, the biggest challenge of the hybrid mechanism lies in integrating compliance into the DAO Governance itself. Decentralised governance (DAO governance) must be forced to integrate mechanisms that are activated. This centralised mechanism is used to block sanctioned addresses, which can improve the functional integrity of the system while reducing the pure autonomy of DeFi (Biais et al., 2018). This should be designed as an emergency function accessible by a multisig managed by the regulator and representatives' gateway, only activated after a valid and verified legal order (e.g., OFAC sanctions or a court order related to money laundering). This integration must be done via an updated smart contract agreed to by DAO governance, making compliance a technical prerequisite, not just a legal promise, even though this is philosophically at odds with the ethos of decentralisation.

This hybrid design recognises that anonymity can be permitted at the intra-protocol transaction layer. However, legal compliance must be enforced at the interaction layer with the traditional financial system (TradFi) chokepoint. Effective KYC/AML on the interface, on-chain and off-chain. This tokenised bullion will remain a high-risk instrument that traditional financial institutions, bound by regulations, cannot adopt (Zetzsche et al., 2017). The ultimate solution must be a globally recognised Decentralised Digital Identity (DID) Standard that allows users to prove their KYC/AML compliance (as issued credentials) without revealing their personal identity on every transaction, on-chain, while maintaining privacy and ensuring regulatory accountability.

3.3.3 Cross-jurisdictional regulatory approach

Considering the global reach of tokenised bullion, separate territorial regulations will not be effective and will only encourage jurisdictional arbitration. Therefore, strong, formal cooperation between regulators (Regulatory Colleges) is needed. Regulatory colleges should be established by the primary regulatory body (e.g., SEC, FCA, MAS, OJK) to focus exclusively on asset tokenised bullion traded across borders (Zetzsche et al., 2017). The goal is to create a Global Regulatory 'Passport' that would allow token issuers that comply with standards in one major jurisdiction to gain easier recognition in other jurisdictions.

The legal basis for this cooperation is firmly rooted in existing international frameworks, particularly those that support the cross-border exchange of information and law enforcement assistance. Fundamentally, this initiative is underpinned by the Financial Action Task Force (FATF) Recommendations, which explicitly call for effective international cooperation among authorities to combat Money Laundering and the Financing of Terrorism (AML/CFT). Recommendation 40 on International Co-operation States that:

> *"Countries should ensure that their competent authorities can rapidly, constructively and effectively provide the widest range of international cooperation in relation to money laundering, terrorist financing and financing of proliferation, and to the underlying predicate offences."*

In the context of digital assets, this mandate emphasises the importance of sharing information on-chain and of identifying VASPs across borders to ensure regulatory responses remain adaptive to evolving risks. This international framework is reinforced by the IOSCO principles, which provide guidelines for mutual recognition and legal assistance between capital market regulators. Principle 13 concerns cooperation, expressly states that:

> *"The regulator should have the authority to share information, including enforcement documents, with domestic and foreign authorities."*

This principle is the foundation for the development of formal cooperation schemes, such as Mutual Recognition Agreements (MRAs) and Multilateral Memoranda of Understanding (MoUs) between regulators. Model Global Regulatory Passport. This is a concrete manifestation of the mechanism's implementation, enabling more efficient cross-jurisdictional regulatory recognition and the exchange of law enforcement information in accordance with the principles established by IOSCO. Thus, the FATF and IOSCO frameworks jointly ensure that international cooperation in digital asset oversight is comprehensive, structured, and aligned with global standards.

This cooperation should not only include sharing information andbest practicessupervisionon-chain, but also agreed on a protocolsettlementsynchronized emergency procedures, to ensure that if a gold token platform is liquidated in one country, supervisory authorities in other countries have the authority and agreed protocols to freeze the associated assets and facilitate redemptions for their citizens, thereby reducing systemic risk and protecting investors settlement (Zetzsche et al., 2020). This emergency must be governed by the Cross-Border Settlement Agreement (Cross-Border Resolution Agreement), which establishes the priority of claims for gold token holders across jurisdictions in the event of the liquidation or insolvency of the token issuer. This framework should specifically emulate global efforts to address crypto assets that may pose systemic risks, ensuring consistent regulatory treatment based on risk rather than geography(Dewi & Kurniawan, 2025). The strong legal basis provided by this Multilateral MOU provides a Legal Assistance Clause, which strengthens the extraterritorial authority of authorities to freeze or seize digital assets (gold tokens) identified as proceeds of crime in different jurisdictions.

4. Conclusions

Integrating tokenized gold into the Decentralized Finance ecosystem represents a significant innovation opportunity, yet the sector faces real headwinds from regulatory constraints. The core tension emerges between permissionless DeFi protocols and the territorial requirements of AML/KYC regulations coupled with capital market laws. This research proposes a Bullion-DeFi Regulatory Sandbox as a viable pathway forward, grounded in technology-neutral and risk-based principles. The framework combines stringent capital adequacy requirements with custodial disaster recovery protocols to address systemic risks while safeguarding investors without suppressing technological advancement. Critically, RegTech implementation becomes mandatory for real-time monitoring and enforcement across on-chain and off-chain interaction points, particularly during physical redemption transactions.

The contribution here addresses a genuine gap in existing literature by developing a comprehensive framework aligned with IOSCO Principles and FATF Recommendations. The sandbox model tackles jurisdictional arbitrage and dual asset integrity problems through an innovative mechanism: embedding AML compliance directly into DAO Governance as a technical requirement rather than relying on legal promises alone. The Cross-Border Mandatory Liquidation Protocol mitigates single point of failure risks in custody operations, providing both regulators and DeFi developers with concrete guidance toward regulatory certainty. These design choices reflect an understanding that hybrid physical-digital assets demand novel approaches that conventional regulatory frameworks alone cannot address.

The research operates within defined boundaries as analytical and conceptual work grounded in literature review and existing regulatory architecture. The most significant limitation remains the absence of real-world empirical testing. The proposed sandbox model has not been deployed in an actual operational environment, which constrains our ability to validate performance assumptions and identify unforeseen complications. This gap creates both a limitation and an opening for future investigation.

Future research should prioritize empirical validation through case studies and simulations designed to measure actual impacts on liquidity, transaction costs, and market volatility for tokenized bullion under rigorous oversight. Developing quantitative economic models to determine optimal Capital Adequacy Requirements across different risk profiles and oracle configurations would ground the framework in concrete financial data. Additionally, investigating legal enforcement mechanisms for activating circuit breakers and mandatory liquidation protocols in smart contract DAOs across both civil and common law jurisdictions deserves careful attention, since traditional court orders may not function effectively against decentralized entities operating across borders.

Acknowledgement
The authors would like to express their sincere appreciation to the editorial team and anonymous reviewers for their constructive comments and suggestions, which have significantly improved the quality and clarity of this article. The authors are also grateful to the institutions and regulatory bodies whose publicly available reports, guidelines, and datasets have provided essential empirical and policy foundations for this research. Any remaining errors or omissions are solely the responsibility of the authors.

Author Contribution
Conceptualization, A. F., B.N.; Methodology, A. F.; Formal analysis, A. F.; Investigation, A. F.; Data curation, A. F.; Writing – original draft preparation, A. F.; Writing – review and editing, B. N., A. F.; Visualization, B. N.; Supervision, B.N.

Funding
PT Pegadaian funded this research and fully covered the article processing charge (APC) as part of the joint Call for Papers program.

Ethical Review Board Statement
Not available.

Informed Consent Statement
Not available.

Data Availability Statement
The study relies on secondary data from publicly available reports and academic literature. No new datasets were generated or analyzed in this study.

Conflicts of Interest
The authors declare no conflict of interest.

Declaration of Generative AI Use
During the preparation of this work, the authors used DeepL to assist in translating parts of the manuscript, Grammarly to assist in improving grammar, clarity, and academic tone, and Perplexity AI to assist in reviewing structure and consistency. After using these tools, the authors reviewed and edited the content as needed and take full responsibility for the content of the publication.

References

Adhami, S., & Guegan, D. (2020). Crypto assets: the role of ICO tokens within a well-diversified portfolio. *Journal of Industrial and Business Economics*, *47*(2), 219–241. https://doi.org/10.1007/s40812-019-00141-x

Adrian, Tobias., & Mancini-Griffoli, Tommaso. (2019). *The rise of digital money*. International Monetary Fund. https://www.imf.org/-/media/files/publications/ftn063/2019/english/ftnea2019001.pdf

Baur, D. G., & Lucey, B. M. (2010). Is Gold a Hedge or a Safe Haven? An Analysis of Stocks, Bonds and Gold. *Financial Review*, *45*(2), 217–229. https://doi.org/10.1111/j.1540-6288.2010.00244.x

Biais, B., Bisiere, C., Bouvard, M., & Casamatta, C. (2018). The Blockchain Folk Theorem. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3108601

Braband, S. (2024). *<p>The role of Proof of Reserves in enhancing trust and transparency in Digital Currency and Digital Asset Systems</p>* https://doi.org/10.2139/ssrn.4997049

CITI. (2023). *Future of Cross-Border Payments: Who Will Be Moving $250 Trillion in the Next Five Years?* https://www.citigroup.com/global/insights/future-of-cross-border-payments-

FATF. (2023). *TARGETED UPDATE ON IMPLEMENTATION OF THE FATF STANDARDS ON VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS*. www.fatf-gafi.org

Dewi, K. N., & Kurniawan, I. G. A. (2025). Cryptocurrency and Digital Asset Regulation. *Pena Justisia: Media Komunikasi Dan Kajian Hukum*, *24*(1), 7896–7912. https://doi.org/10.31941/pj.v24i2.7141

Dhali, M., Hassan, S., & Zulhuda, S. (2024). The regulatory puzzle of decentralized cryptocurrencies: Opportunities for innovation and hurdles to overcome. *Journal of Infrastructure, Policy and Development*, *8*(6). https://doi.org/10.24294/jipd.v8i6.3377

Dias, R., Pereira, J. M., & Carvalho, L. C. (2022). Are African Stock Markets Efficient? A Comparative Analysis Between Six African Markets, the UK, Japan and the USA in the Period of the Pandemic. *Naše Gospodarstvo/Our Economy*, *68*(1), 35–51. https://doi.org/10.2478/ngoe-2022-0004

Díaz, A., Esparcia, C., & Huélamo, D. (2023). Stablecoins as a tool to mitigate the downside risk of cryptocurrency portfolios. *The North American Journal of Economics and Finance*, *64*, 101838. https://doi.org/10.1016/j.najef.2022.101838

FSB. (2017). *Financial Stability Implications from FinTech: Supervisory and Regulatory Issues that Merit Authorities' Attention*. www.fsb.org/emailalert

Goforth, C. R. (2021). Regulation of Crypto: Who Is the Securities and Exchange Commission Protecting? *American Business Law Journal*, *58*(3), 643–705. https://doi.org/10.1111/ablj.12192

Grennan, J. (2022). FinTech Regulation in the United States: Past, Present, and Future. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4045057

Grieves, M. (2015). *Digital Twin: Manufacturing Excellence through Virtual Factory Replication*. https://www.3ds.com/fileadmin/PRODUCTS-SERVICES/DELMIA/PDF/Whitepaper/DELMIA-APRISO-Digital-Twin-Whitepaper.pdf

Guillaume, F., & Riva, S. (2022). Blockchain Dispute Resolution for Decentralized Autonomous Organizations: The Rise of Decentralized Autonomous Justice. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4042704

Harvey, C. R., Ramachandran, A., & Santoro, J. (2020). DeFi and the Future of Finance. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3711777

Hou Sak, M. (2024). *KYC/AML Technologies in Decentralized Finance (DeFi)*. Stern NYU. https://www.stern.nyu.edu/sites/default/files/2024-07/Glucksman_Sak_2024.pdf

Islam, M. Z., Islam, M. S., Das, B. C., Reza, S. A., Bhowmik, P. K., Bishnu, K. K., Rahman, M. S., Chowdhury, R., & Pant, L. (2025). Machine Learning-Based Detection and Analysis of Suspicious Activities in Bitcoin Wallet Transactions in the USA. *Journal of Ecohumanism*, *4*(1). https://doi.org/10.62754/joe.v4i1.6214

Kumar, S., Suresh, R., Liu, D., Kronfellner, B., & Kaul, A. (n.d.). *Relevance of on-chain asset tokenization in "crypto winter."* ADDX. https://addx.co/insights/bcg-addx-report-asset-tokenisation-to-grow-50x-into-us-16-trillion-opportunity-by-2030/

Marston, R. (2020). *Gold hits record high as investor jitters spread*. BBC. https://www.bbc.com/news/business-53555771

McLaughlin, E., & Pecchenino, R. (2022). Fringe banking and financialization: Pawnbroking in pre-famine and famine Ireland. *The Economic History Review*, *75*(3), 903–931. https://doi.org/10.1111/ehr.13132

Muradyan, S. V. (2023). Digital Assets: Legal Regulation and Estimation of Risks. *Journal of Digital Technologies and Law*, *1*(1), 123–151. https://doi.org/10.21202/jdtl.2023.5

OECD. (2024). *The Limits of DeFi for Financial Inclusion*. OECD Publishing. https://doi.org/10.1787/f00a0c7f-en

Riles, A. (2013). Managing Regulatory Arbitrage: A Conflict of Laws Approach. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2335338

Rohr, J., & Wright, A. (2017). Blockchain-Based Token Sales, Initial Coin Offerings, and the Democratization of Public Capital Markets. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3048104

Tao, F., Cheng, J., Qi, Q., Zhang, M., Zhang, H., & Sui, F. (2018). Digital twin-driven product design, manufacturing and service with big data. *The International Journal of Advanced Manufacturing Technology*, *94*(9–12), 3563–3576. https://doi.org/10.1007/s00170-017-0233-1

Werbach, K. (2018). *The Blockchain and the New Architecture of Trust*. The MIT Press. https://doi.org/10.7551/mitpress/11449.001.0001

World Bank Group. (2020). *Global Experiences from Regulatory Sandboxes*. World Bank Group.

World Bank Group. (2024). *The Middle Income Trap*. World Bank Group.

Zetzsche, D. A., Arner, D. W., & Buckley, R. P. (2020). Decentralized Finance. *Journal of Financial Regulation*, *6*(2), 172–203. https://doi.org/10.1093/jfr/fjaa010

Zetzsche, D. A., Buckley, R. P., Arner, D. W., & Barberis, J. N. (2017). From FinTech to TechFin: The Regulatory Challenges of Data-Driven Finance. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2959925

Biographies of Authors

Beckham Napitupulu, a Public Sector Accounting student specializing in Information Systems at Politeknik Keuangan Negara STAN, integrates financial expertise with technological proficiency.

- Email: beckham_4131230349@pknstan.ac.id
- ORCID: N/A
- Web of Science ResearcherID: N/A
- Scopus Author ID: N/A
- Homepage: N/A

Aidatul Fitriyah, affectionately known as Afriya, is an award-winning researcher and distinguished alumnus of Universitas Airlangga. With a strong background in English Language and Literature, she has established expertise in interdisciplinary research covering linguistics, media studies, and environmental sustainability..

- Email: aidatul.fitriyah-2020@fib.unair.ac.id
- ORCID: 0000-0003-0195-372X
- Web of Science ResearcherID: ACQ-1958-2022
- Scopus Author ID: 59419339100
- Homepage: N/A