Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.34, NO.4, Aug. 2024 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2024.34.4.811

가상자산 커스터디 서비스의 최신 동향 및 DeFi 프로토콜 커스터디 가능성 평가 가이드라인 제시

이 형 근,[1†] 주 문 호,[3] 임 지 훈,[1] 김 범 중,[1] 전 기 석,[1] 심 준 식,[1] 이 중 희[2‡]
[1,2]고려대학교 (대학원생, 교수), [3]개인정보보호위원회 (사무관)

Trends in Cryptocurrency Custody Services and Evaluation Guidelines for DeFi Protocols' Custody Potential

Hyunggeun Lee,[1†] Moonho Joo,[3] Jihun Lim,[1] Beomjoong Kim,[1] Kiseok Jeon,[1]
Junsik Sim,[1] Junghee Lee[2‡]
[1,2]Korea University (Graduate student, Professor),
[3]Personal Information Protection Commission (Deputy director)

요 약

본 논문은 1차 목적과 2차 목적을 가지고 작성됐다. 1차 목적은 가상자산 커스터디 서비스에 대한 종합적인 서베이와 글로벌 규제 동향 및 기술적 시사점을 탐구하는 것이다. 이를 위해 가상자산 커스터디 솔루션의 장단점, 분류 체계, 기술적 취약점 등을 다룬 기존 서베이 논문을 종합적으로 검토했다. 또한, 법률적 측면에서 최신 규제 흐름과 기존 규제 프레임워크의 적용 사례, 커스터디 업무 수행에 필요한 조건, 서비스 제공자의 의무사항을 분석했다. 2차 목적은 규제권 밖에서 운영되는 DeFi 프로토콜을 'Gray Area'로 식별하고, 이들의 기술적/거버넌스적 메커니즘을 분석하는 것이다. 최종적으로, 위 서베이 내용을 종합하여 DeFi 프로토콜의 탈중앙화 평가 기준 가이드라인을 제시하고, 이를 통해 제도권 내 통합 가능성을 제기함으로써, 업계 전문가, 규제 기관, 정책 입안자 등 이해관계자들에게 업계의 요구와 사회적 이익의 균형을 찾는 데 중요한 인사이트를 제공하고자 한다.

ABSTRACT

This paper has two main objectives. The primary objective is to conduct a comprehensive review of existing survey papers on the advantages, disadvantages, taxonomy, and technical vulnerabilities of cryptocurrency custody services. Additionally, we examined recent regulatory developments, the application of existing frameworks, conditions for performing custody services, and service providers' obligations. The secondary objective is to identify DeFi protocols in the regulatory 'grey area' and analyze their technical aspects and governance mechanisms. By synthesizing these findings, we propose guidelines for assessing DeFi decentralization and their potential for integration within the regulatory framework, providing insights for industry experts, regulators, and policymakers to balance industry needs with societal benefits.

Keywords: Custody, Blockchain, DeFi, Private Key

I. 서 론

유럽연합(EU)[1]의 가상자산 관련 활동을 규제하는 MiCA(Markets in Crypto Asset Regulation) 규정에 따르면, 커스터디 서비스는 고객을 대신하여 가상자산을 보관 및 관리하며, 특히

Received(05. 20. 2024), Modified(07. 24. 2024), Accepted(07. 25. 2024)

† 주저자, gudrms123@korea.ac.kr
‡ 교신저자, j_lee@korea.ac.kr(Corresponding author)

암호화폐의 개인 키(Private Key)를 안전하게 보관하거나 통제하는 역할을 포함한다. 현재 가상자산 커스터디 서비스 제공자들은 주문 접수, 주문 실행, 자산 전송 등 다양한 서비스를 제공하고 있다. 이 과정에서 가상자산 커스터디 서비스는 디지털 자산을 보호하고 관리하는 데 필요한 보안, 규정 준수 및 기술 인프라를 지속적해서 보완하고 있다. 규제 측면에서는 이용자의 자산 보호와 거래 투명성 향상을 위해 세밀한 규제들이 새롭게 제시되고 있으며, 이에 따라 가상자산 사업자들이 각국의 조건에 맞춰 운영되고 있다.

본 논문은 선행 연구를 통해 글로벌 가상자산 커스터디 서비스의 범위[1-3]를 정의하고, 관련된 가상자산 커스터디 서베이 페이퍼[5-6]를 활용하여 가상자산 관리에 관한 규제와 동향[7-9]을 포괄적으로 서베이하고자 한다. 이를 통해 특히 가상자산 보관 솔루션의 중요성, 안전한 관리와 보관에 대한 지침 제공, 법적 관할 구역의 중요성, 그리고 각 가상자산의 특성에 맞춘 맞춤형 가이드라인의 중요성을 강조한다.

가상자산의 본질적 특성을 고려할 때, 전통 금융 시스템과 구별되는 블록체인 기술의 활용은 자산 인식 및 처리 방식에 여러 차별점을 가져온다. 이는 암호화 메커니즘을 통한 자산 인식, 유형 자산의 부재에서 비롯된 변동성, 중개자의 부재로 인한 탈중앙화, 그리고 이러한 자산의 글로벌 접근성 향상 등을 포함한다. 이러한 차별점은 가상자산 시장의 특수성을 인정하고, 그에 맞는 조정된 규제 접근 방식을 제안하는 데 중요한 기반이 된다. 이에 가상자산과 DeFi의 본질적 특성을 활용하여 본질적으로는 커스터디 서비스이지만 규제 속에 포함되지 않은 DeFi를 Gray Area로 식별했다. 여러 특성을 고려하여 전통 금융과는 다른 접근 방식을 모색했으며, DeFi 프로토콜의 탈중앙화 평가 기준 가이드라인을 제시하고, 이를 통해 제도권 내로의 통합 가능성을 평가하고자 한다. 이를 통해 업계 전문가, 규제 기관, 정책 입안자 등 이해관계자들에게 업계의 요구와 사회적 이익을 모두 충족하는 균형을 찾는 데 중요한 인사이트를 제공하고자 한다.

결과적으로, 본 연구는 가상자산 커스터디 서비스를 체계적으로 이해하고, 이를 기반으로 한 정책과 규제가 더욱 효과적으로 구현될 수 있도록 지원하고자 한다. 이 과정을 통해, 가상자산 커스터디 산업의 지속 가능한 성장과 발전을 촉진하고, 더 나아가, 투자자 보호를 강화하고, 시스템의 투명성과 안정성을 향상시키며, 가상자산 커스터디 산업의 안전한 성장을 도모하는 데 중요한 역할을 할 것으로 기대한다.

II. Methodology(방법론)

MiCA Article 3번에 정의된 커스터디 서비스 제공자에 대한 정의는 이처럼 설명한다: '암호화 자산 서비스 제공자'란 전문적으로 고객에게 하나 이상의 암호화 자산 서비스를 제공하는 것을 직업 또는 사업으로 하는 법인 또는 기타 사업체로서, 제59조에 따라 암호화 자산 서비스 제공이 허용된 자를 의미한다. 여기서 '암호화 자산 서비스'란 암호화 자산과 관련된 다음 중 어느 하나에 해당하는 서비스 및 활동을 의미한다[1]:

1. 고객들을 대신한 암호자산의 위탁보관(custody) 및 관리(administration) 제공.
2. 암호자산 거래플랫폼의 운영.
3. 자금과 암호자산들의 교환.
4. 다른 암호자산과 암호자산들의 교환.
5. 고객들을 대신한 암호자산들에 관한 주문의 집행(execution).
6. 암호자산들의 모집 주선(placing).
7. 고객들을 대신한 암호자산들에 관한 주문의 접수 및 전송.
8. 암호자산들에 관한 자문 제공.
9. 암호자산들에 관한 포트폴리오 운용 제공.
10. 고객들을 대신한 암호자산들에 관한 이전(전송) 서비스 제공.

이 섹션에서는 다양한 가상자산 서비스 및 프로토콜에 대한 논의를 통해 본 서베이의 구체적 범위를 명확히 하고자 한다. Fig. 1은 큰 틀에서 서비스의 범위를 시각적으로 보여주며, 자산 보관과 관련하여 비수탁 지갑이나 계약 주소(CA)에 의존하는 기관을 의도적으로 배제했다는 점을 명시적으로 언급한다.

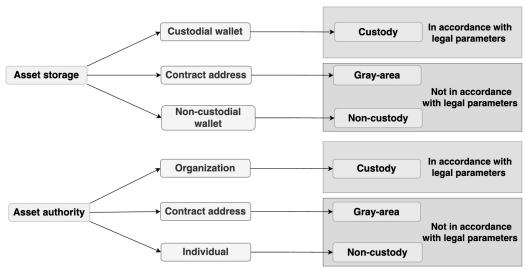

Fig. 1. Visualization of custodial scope.

2.1 자산 보관 방식

암호화폐 수탁기관은 암호화폐 운영에서 중추적인 역할을 해왔고 지금도 계속하고 있다. 지금까지 암호화폐 커스터디는 일반적으로 '핫(온라인)' 집단 커스터디의 형태를 취했는데, 이는 지갑 제공자가 고객의 모든 개인 키를 영구적으로 온라인 상태로 유지하며 분산 원장에 연결된 지갑에 함께 저장하는 것을 의미한다[2]. 여기서 정의하는 커스터디 서비스와 부합하는 서비스로는 중앙화 거래소(Centralized Exchange, CEX)나 비트고(BitGo), 앵커리지(Anchorage)와 같은 가상자산 위탁 보관 및 관리 전문 커스터디 업체가 대표적이다. 이러한 기관들은 다중 서명 지갑 및 콜드 스토리지와 같은 고도의 보안 기술을 사용하여 자산의 안전을 보장한다. 가상자산 커스터디 사업자나 가상자산 거래소에서는 고객 자산 수탁에 대한 통일된 관행이 존재하지 않지만, 일부 암호화폐 거래소나 서비스 제공업체는 커스터디 제공 정책을 매우 명확하고 구체적으로 규정한다. 예를 들어, 가상자산 거래소 Coinbase의 사용자 동의서에는 "디지털 자산 지갑에 보관된 모든 지원되는 디지털 자산은 아래에 자세히 설명된 대로 코인베이스가 회원의 이익을 위해 보관하는 수탁 자산이다[3]"라고 명시한다. 이러한 규정 속에서, 개인의 암호화폐를 보관하기 위한 블록체인 기반 솔루션은 크게 커스터디 지갑과 비커스터디 지갑 두 가지 유형으로 구분된다. 커스터디 지갑은 가상자산과 관련된 개인 키를 제3자 기관에 위탁하는 보관 솔루션으로, 이 경우 사용자는 개인 키에 대한 통제권을 서비스 제공자에게 맡기며, 서비스 제공자는 가상자산의 보안, 유지 관리 및 전반적인 관리에 관한 책임을 진다. 반면, 비커스터디 지갑에서는 사용자에게 개인 키에 대한 독점적인 소유권과 통제권이 부여되어, 사용자는 제3자의 개입 없이 자신의 자산에 액세스하고 전송할 수 있는 권한을 포함하여 암호화폐 보유에 대한 완전한 자율권을 갖게 된다. 이러한 맥락에서, 커스터디 지갑과 비커스터디 지갑의 주요 차이는 개인 키의 관리 방식에 있으며, 이는 사용자에게 매우 중요한 보안 및 자율성의 문제로 작용한다.

가상자산을 보관하는 또 다른 방식은 컨트랙트 주소(CA)에 의존하는 것으로, DeFi(Decentralized Finance, 탈중앙 금융)는 이러한 스마트 컨트랙트 로직에 따라 여러 사용자의 자산을 통합하고 운영하는 방식이다. 이 접근법은 가상자산을 지갑에 보관하는 기존의 방식에서 벗어나, 계약된 로직에 따라 운영되는 탈중앙화 모델을 수용함으로써, 기존의 외부 소유 계정(EOA) 개념을 넘어선다.

따라서, 본 논문에서는 가상자산 커스터디 서비스의 체계적인 분류 프레임워크를 구축하기 위해, 자산을 커스터디 지갑에 보관하는 경우를 '수탁(custodial) 영역', 비커스터디 지갑을 사용하는 경우를 '비수탁(non-custodial) 영역', 그리고 스마트 컨트랙트를 사용하는 경우를 'Gray Area'로 정의한다. 이 분류 방식은 각각의 커스터디 유형에 따른 법적 및 운영적 차이를 명확히 이해하고, 관련 규제 및 관리 접근법을 체계화하는 데 기여하고자 한다.

2.2 자산의 권한 할당

사실, Private Key를 넘겼다는 것은 자산의 통제권을 완전히 위임했음을 의미하기도 한다. 이러한 경우, 자산의 소유자는 더 이상 자산에 대한 직접적인 접근권을 가지지 않으며, 수탁자가 해당 자산을 관리하고 운용하는 전적인 권한을 갖게 된다. 이는 특히 사업자와 이용자의 계약에서 중요하게 작용한다. MiCA[1]에서 규정하는 바와 같이, 가상자산 서비스는 현물자산 및 가상자산 교환, 암호자산 간 교환, 고객을 대신한 주문 집행, 암호자산의 모집 주선, 주문의 접수 및 전송을 포함한다. Private Key의 위임은 단순한 자산 보관을 넘어, 수탁자가 자산을 적극적으로 운용하고 다양한 금융 서비스를 제공할 수 있는 기반을 마련한다. 이에 사업자와 이용자의 계약에서 수탁자와 위탁자 사이의 관계와 권한 배분이 더욱 유연하게 조정될 수 있다.

따라서, 본 논문에서는 자산 권한의 소유자가 개인일 경우를 '비수탁'으로, 어떠한 단체나 기업에 권한이 일부 혹은 전부 넘어갔을 경우를 '수탁'으로 분류하고자 한다. 마지막으로, 자산에 대한 권한이 개인에서 스마트 컨트랙트로 이전되었을 경우를 Gray Area로 정의하며, 이는 자산 권한의 이전과 관리의 복잡한 특성을 내포하며, 각 상황에 따른 법적 및 운영적 차이를 이해하는 데 중요한 기준점을 제공한다.

2.3 Gray Area

'Gray Area'라는 용어는 DeFi 프로토콜이 내재하고 있는 다양한 커스터디 특성을 지칭하며, 이는 DeFi 시스템에서 사용자의 자산이 개인 주소에서

해당 프로토콜의 스마트 컨트랙트로 이전되고, 프로토콜에 내장된 메커니즘에 따라 관리되는 과정을 포함한다. 주목할 점은, 자산이 다양한 컨트랙트 로직에 의해 특정 기간 동안 컨트랙트의 스토리지나 관리자의 EOA에 저장되며, 이는 전통적 금융 시스템에서 요구하는 명확한 커스터디 지침과 대비되는 DeFi 고유의 특성과 중앙화된 권한에 관한 문제를 제기한다.

현재 가상자산 업계에서는 중앙화 거래소(CEX) 및 디지털 자산 신탁 회사와 같은 특정 서비스가 명확히 커스터디 서비스로 분류되어 법적 규제를 받고 있으며, 이들은 이용자의 자산을 신탁 받아 보관하고 보호한다. 반면, DeFi로 분류되어 법적 규제를 받지 않으면서도 커스터디와 유사한 서비스를 제공하는 경우도 존재한다. 본 섹션에서는 전통 금융의 수탁 요소를 포함하여 현재 커스터디 서비스로 인식되지 않는 서비스들을 식별하는 것을 목표로 한다. 특히, DeFi 프로토콜 내 거버넌스적 기술적 메커니즘을 통해 특정 단체나 개인 지갑에 큰 영향을 미칠 수 있는 권한이 부여된 중앙화된 객체를 식별하여, DeFi가 가상자산 커스터디 서비스의 Gray Area를 형성하는 이유와 그 논리적 근거를 심도 있게 탐구하고자 한다.

III. 관련 연구

이번 선행 연구 세션에서는 가상자산 커스터디 솔루션에 관한 기존 서베이 논문들을 조사하고 분석했다. 각 논문은 커스터디 솔루션별 장단점을 종합적으로 평가하고, 분류 체계를 확립하며, 암호화폐 지갑의 취약점을 체계적으로 탐구한다. 또한, 자산을 보관함에 따르는 다양한 위협에 대한 커스터디 서비스의 취약성을 인식하면서 업계는 일관된 규제 프레임워크의 부재, 발전하는 규제 동향, 사고 발생 시 책임에 대한 불확실성 등 여러 미해결 과제에 직면해 있음을 지적한다. 이에 따라, 본 연구는 사전에 연구된 다양한 고려 사항을 통합하여 보다 정확하고 체계적인 분석을 제공하고자 한다.

3.1 가상자산 커스터디 솔루션 분석 및 평가

급성장하는 가상자산 업계에서는 사용자의 접근성과 자산 전송의 용이성을 보장하면서 동시에 암호화폐 자산을 안전하게 보호하는 것이 중요한 연구 과제로 자리 잡고 있다. Di Nicola[4] 등의 연구에서는 다양한 커스터디 솔루션들을 면밀히 조사하여 각각의 장단점을 비교 분석하고 있다. 특히, 보안, 사용자 편의성, 안전성이 조화를 이루는 블록체인 독립적인 솔루션을 제공하는 다자간 연산 기반 시스템(secure multiparty computation-based schemes)을 상세히 검토한다. 이 논문은 키 생성 과정에서 오프라인 참여자를 포함시켜 프로토콜의 실용성을 강화하는 데 중점을 둔다.

Jaroucheh와 Ghaleb[5]의 연구는 주요 가상자산 수탁 서비스를 심도 있게 검토하고, 수탁 방식의 다양성을 비교할 수 있는 분류법을 제시한다. 이 연구는 자산 감사와 관련된 문제, 향후 연구 과제, 그리고 커스터디 서비스 자체의 위험성을 강조한다. 또한, 책임, 분배, 연결성, 키 저장 등을 중심으로 커스터디 접근법의 장단점을 종합적으로 분석한다. 이러한 분석을 통해 연구자, 실무자, 정책 입안자가 특정 조건과 필요에 가장 적합한 커스터디 전략을 선택하는 데 있어 정보에 기반을 둔 의사결정을 내리는 데 중요한 기여를 하고자 한다.

3.2 비트코인 커스터디의 기술적 취약점

Vaddadi[6]등의 연구는 비트코인의 중앙집중식 기술 구조, 특히 머클 루트(Merkle Root), 채굴, 반감기, 키, 지갑을 중심으로 내재한 취약점을 철저히 분석한다. 이 연구에서는 커스터디형 지갑의 키 저장 문제를 포함하여, 핫 스토리지, 콜드 스토리지, 딥 콜드 스토리지 등 다양한 저장 기술의 취약점들을 깊이 있게 검토한다. 또한, 비트코인 거래와 관련된 암호화폐 거래소의 보안을 강화하기 위한 전략으로 거래 대기 시간 문제에 대응하며, 규제 감독의 강화 및 합법적인 암호화폐 채굴자 수 증가를 통해 이러한 보안 문제에 대한 방안을 제안한다. 이는 비트코인의 기술적 취약성에 대한 이해를 증진시키고, 보안 대책 및 규제 정책을 마련하는 데 기여하고자 했다.

IV. 법률 및 규제

법률 및 규제 섹션에서는 규제 동향, 제안된 프레임워크, 수탁자와 위탁자 사이의 책임 역학, 수탁 서비스 제공자의 의무 등을 다루며, 이를 통해 현재 전 세계 규제 환경의 미묘한 차이를 분석하고 제안된 규제 방향의 시사점을 도출한다. Table 1에 요약된

바와 같이, 가상자산 커스터디 업계의 규제 고려 사항은 정부의 조사 권한, 가상자산의 법적 확실성, 시장 거버넌스 문제 완화를 우선시하며, 강력한 재해 복구 계획, 자산 손실에 대비한 보험, 커스터디 절차 확립을 전제로 한다. 또한, 커스터디 서비스에 관한 주요 책임으로 규정 준수, 위험 완화, 투명한 공개를 강조하며, 이는 가상자산 커스터디 업계의 안정적 성장과 고객 자산 보호에 필수적인 요소로 작용한다.

Table 1. Crypto-asset custody: underlying rationales, prerequisites, and regulatory imperatives

Topic	Summary
Rationale for regulatory consideration	1) Preservation of the government's investigative authority for tax evasion is a key priority. 2) Affirmation of legal certainty surrounding asset contractual relationships is crucial for regulatory clarity. 3) Mitigation of challenges in establishing a voluntarily governed market framework is essential for fostering a stable crypto ecosystem.
Prerequisites for assessing custodial businesses	1) A comprehensive business continuity and disaster recovery plan is imperative. 2) Maintenance of insurance against hacking or unauthorized transfer of crypto assets is a foundational requirement. 3) Procedures for accessing the staking of cryptocurrency assets need to be established 4) Access to custody of newly issued coins with no existing custody solution is a necessary capability. 5) The implementation of audits and traceability of transactions is fundamental for ensuring transparency.
Obligations for custody services	1) Ensuring compliance with regulatory requirements and control procedures is paramount, involving the prevention of asset theft and misuse as well as safeguarding against unauthorized access or use. 2) Formulating response procedures for mitigating various risks, including the incorporation of mandatory insurance, is a key responsibility. 3) Transparent disclosure of custody policy guidelines to customers is necessary for clarity, elucidating customer rights and responsibilities through written contractual agreements.

4.1 가상자산 커스터디 관련 규제 동향

먼저, 가상자산 커스터디 관련 규제 동향을 조사하여 보다 심층적인 분석을 이어가고자 한다. Blandin, Apolline[7] 등은 가상자산 자산의 규제 환경과 관련 동향에 대한 종합적이고 체계적인 비교 분석 연구를 수행했다. 이 연구는 커스터디 서비스 제공자와 비커스터디 서비스 제공자 간의 규제 개입의 차이를 포함하여, 고객 자금 이체 및 계정 동결 권한을 조명한다. 일부 국가에서는 이미 수탁업체를 별도로 규제하기로 결정하거나 이러한 방안을 의사를 표명한 바 있다. 본 논문이 분석한 20개 국가 중 약 45%의 관할구역에서는 수탁 서비스 제공업체와 비수탁 서비스 제공업체를 구분하고 있으며, 이는 수탁 서비스 제공업체에 대한 추가적인 규제 요건이 적용될 수 있음을 시사한다.

Lekkas, Nikolaos[8]는 암호화 자산의 등장이 현행 법률 체계에 제기하는 과제를 분석하고 있으며, 이와 관련해 암호화 자산의 특성, 규제 당국의 구조, 그리고 이 새로운 자산 형태에 대한 접근 방법을 강조하고 있다.

Scharfman, Jason[9]은 커스터디 서비스와 관련하여 가상자산 및 가상자산 자산 펀드에 대한 기관 투자자들의 운영 실사(ODD)의 주요 동향을 분석한다. 이 연구는 특히 콜드월렛(cold wallet)의 한계를 넘어서는 커스터디 사업자의 성장과 가상자산 보관 계약에 대한 규제에 집중하는 관심을 다룬다. 이러한 연구를 통해 가상자산 자산에 대한 규제 흐름의 본격화와 동시에 커스터디 서비스의 특성을 반영한 새로운 규제의 필요성이 강조되고 있다는 점을 확인할 수 있다.

또한, 주요 국가들이 커스터디 서비스에 대해 새로운 규제 프레임워크를 도입하고 있는 것은 중대한 의미를 지닌다. 유럽연합은 가상자산 자산 시장에 대한 규제 프레임워크를 마련하면서 커스터디 사업자에게 의무와 책임을 부과하는 MiCA[1]를 제정했으며, 이는 2023년 6월 29일에 공식적으로 발효되었다. 독일은 2020년 1월 새로운 자금세탁방지법을 적용하면서 가상자산 커스터디를 새로운 금융 서비스 규제 체계에 포함했다. 미국에서는 2020년 7월 증권거래위원회가 연방 은행 및 금융 서비스 기관(FSA)이 고객에게 가상자산 수탁 서비스를 제공할 수 있음을 명확히 하는 해석을 발표했다. 이는 커스터디 서비스가 국가 규제 범위에 포함될 수 있다는 중대한

의미를 가진다.

4.2 기존 규제 프레임워크의 적용

Chu, Dennis[10]는 기존의 금융상품 커스터디 규정들이 가상자산 거래소를 포함한 가상자산 커스터디 서비스에 적용될 수 있음을 제안한다. 저자는 가상자산 커스터디가 현재 직면한 문제들과 1960년대 후반 전통 금융 브로커-딜러들이 직면했던 문제들 사이의 유사성을 강조한다. 당시 브로커-딜러들의 실패는 고객 자산의 부적절한 관리, 자본 부족, 그리고 파산 시 고객 자산의 불충분한 보호로 인해 발생하였다. 현재에도 마찬가지로, 가상자산의 적절한 수탁은 서비스 제공자에 의한 자산의 오용이나 잘못된 취급을 방지하는 데 필수적이며, 플랫폼 파산 시 고객 자산의 적절한 처리가 매우 중요하다. 따라서 저자는 1960년대 말 브로커-딜러의 실패에 대응하여 도입된 고객 보호 규칙, 순자본 규칙, 증권투자자보호법상의 파산 절차 등과 같은 유사한 규제 프레임워크를 가상자산 커스터디 플랫폼에 적용할 것을 제안한다.

또한, Hossain[11]의 연구는 국제 가상자산 시장의 규제 프레임워크에 대한 조사 및 분석을 다룬다. 이 논문은 기존 규제 프레임워크 내에서 가상자산을 기존 투자 상품과 함께 금융 상품으로 간주할 수 있도록 허용한 최근의 법적 변화를 강조한다. 이러한 통합을 통해 가상자산 커스터디는 새로운 금융 서비스로 인식되어 규제 감독을 받게 되었다.

Nabilou, Hossein[12]의 연구는 규제 설계가 전통 금융 시장, 기관, 인프라 내에서 커스터디에 미치는 영향을 분석하고, 최근 가상자산 시장의 커스터디 규제의 필요성 및 방향을 조망한다. 저자는 전통 금융 부문에서 커스터디 또는 고객 자산 관리에 관한 규칙이 금융 시장과 제도 형성에 중요한 역할을 했듯이, 가상자산 시장에서도 유사한 규칙의 적용이 가능하다고 주장한다. 이 논문은 특히 거래소나 가상자산 수탁기관과 같은 중앙화된 가상자산 자산 서비스 제공자가 제공하는 커스터디에 초점을 맞추고 있으며, 커스터디와 자산 분리에 관한 규칙이 향후 가상자산 산업 발전에 중요한 역할을 할 것으로 예상한다. 또한, 커스터디와 같은 서비스에 대한 명확한 정의와 함께, 기존 금융 시장의 커스터디 및 자산 분리 관련 규제에서 출발하여 기존 규제 프레임워크를 참조하여 기반을 다지는 것에 대한 중요성을 강조한다.

4.3 계약에 따른 책임성 문제

가상자산을 수탁할 때 발생하는 수탁자와 투자자 간의 책임과 권한 문제에 초점을 맞춘 일부 논문은, 커스터디의 형태가 가상자산 자산의 실제 소유권에 영향을 미칠 수 있으며, 규제 목적으로 이러한 권리 보유자를 명확하게 정의하는 것이 필수적임을 논한다.

Micheler, Eva[13]는 비트코인과 같은 가상자산 기반 기술의 출현과 관련하여 투자자와 수탁자 간의 관계를 국제적인 관점에서 연구를 진행했다. 이 논문은 수탁자와 체결한 계약에 따라 수탁 투자자의 권리가 결정되며, 수탁자와의 계약을 통해 구체적인 권리가 보장된다고 주장한다. 이는 수탁 계약에 따라 수탁자가 자산을 제3자에게 대여하거나 다른 증권 및 금융 거래에 사용할 수 있는지 여부도 결정하게 된다. 이 과정에서 커스터디 제공자는 커스터디 서비스 제공 중 발생할 수 있는 문제에 관한 책임을 지는 기준을 설정하며, 서비스를 제공하는 모든 하위 수탁자 간의 모든 계약에 의해 적용받는다는 점을 강조한다.

Malvagna, Ugo와 Filippo Sartori[14]는 이탈리아의 법적 프레임워크 내에서 가상자산에 대한 포괄적인 개요를 제공하고, 현재 규제 환경을 기반으로 주요한 규제 이슈를 검토한다. 특히, 가상자산과 관련된 자금세탁방지(AML) 규정의 변화를 상세히 분석하며, 커스터디 및 거래소 서비스 제공업체의 역할과 기능의 맥락에서 가상자산의 법적 지위와 관련된 이슈를 고려한다.

특히, 개인 키가 전자지갑에 보관될 때 가상자산의 법적 소유자가 누구인지에 대한 문제를 살펴본다. 콜드월렛의 경우, 수탁자가 개인키에 접근하거나 통제하지 않는 한 가상자산 보유자가 가상자산의 소유권을 유지한다. 따라서 수탁자가 소유자의 동의 없이 토큰을 사용하는 것은 기술적으로 불가능하며, 개인 키에 대한 독점적인 통제권을 보장한다. 반면, 핫월렛(hot wallet)에서는 수탁자가 개인 키를 관리하며, 가상자산 소유자는 인터넷을 통해서만 지갑에 접근할 수 있으며, 특정 거래를 수행하려면 수탁자를 통해 진행되어야 한다. 이러한 맥락에서, 개인 키를 관리자에게 전송하면 가상자산의 소유권이 자동으로 이전되는 것과 같은 결과를 초래한다. 이는 이러한 과정이 단순한 소유권 변경에 해당하는지, 또는 수탁자가 자산의 소유자가 되어 위탁자에게 동일한 수량과 가치의 자산을 반환할 의무를 부담하는지에 대한

의문이 제기되고 있다.

Cone, Geoffrey[15] 등은 수탁자가 위탁자에게 지급할 수 없게 된 경우 비트코인이나 기타 가상자산이 어떻게 보상되는지 검토하는 연구를 수행한다. 이 논문은 미국 Wyoming 주의 법률을 바탕으로 수탁기관과 거래소가 간과했던 문제에 관한 판례를 분석한다. Wyoming 주에서 발생한 Ruscoe v Cryptopia Ltd 사건 분석을 통해 전 세계적으로 유사한 사례에 대한 인사이트를 제공한다. 해당 사건은 수탁기관이 관리하는 가상자산을 채권자, 주주 또는 계정 소유자가 사용할 수 있는 회사의 자산으로 인정할 수 있는지에 관한 중요한 문제를 제기했다. 결론적으로, 수탁자가 고객의 가상자산에 대하여 수행한 기본적인 역할과 가상자산 잔액에 대한 재량권을 행사하지 않았다는 점이 핵심적인 결점으로 판결에 결정적인 영향을 미쳤다. 따라서 이는 단순한 소극적 수탁 계약만으로는 명시적인 신탁 관계가 형성되지 않는다고 해석하며, 수탁자의 역할은 계약에 정의된 의무의 범위에 따라 달라질 수 있음을 시사한다,

Lehmann, Matthias[16] 등은 가상자산의 안전한 거래 관행을 탐구하고 수탁자가 보유한 가상자산의 소유권에 적용되는 근본적인 법적 문제를 다룬다. 이 논문은 사실상 통제권을 가진 수탁자가 보유한 가상자산의 소유권에 우선 적용되어야 한다는 점을 주장하며, 투자자와 수탁자 간의 수탁 계약에 관한 법률 선택은 수탁자가 통제하는 가상자산의 보안 이익에 적용되는 법률에 따라 결정되어야 한다고 주장한다.

결론적으로, 본 논문은 커스터디 계약의 형태와 가상자산의 실제 소유권이 누구에게 귀속되어 있는지에 따라 커스터디 기관과 가상자산 투자자 간의 책임이 변동될 수 있음을 지적한다. 이는 커스터디 서비스의 구조적 다양성과 책임 분배의 복잡성을 반영하며, 가상자산 커스터디 분야의 규제 기관은 이러한 요소를 신중하게 고려해야 한다.

4.4 수탁자의 의무

커스터디 규제 영역에서는 커스터디 서비스 제공자를 어떻게 규제해야 하는지에 관한 수많은 학술 논문이 발표되고 있다. 특히, 수탁자의 법적 의무에 관한 논문이 주목을 받고 있다. 2020년 12월 23일 미국 증권거래위원회(SEC)가 공개한 Smith, Holly[17] 의 연구는 브로커-딜러가 가상자산 증권 투자 시 거래소법 규정 15c3-3(고객 보호 규칙)에 명시된 수탁 요건을 준수하는 방안에 대한 비전을 제시하며, 수탁 관련 비즈니스에서 요구되는 최소한의 의무 사항을 요약하고 있다.

Zetzsche, Dirk A.[18] 등은 유럽의 가상자산 시장 규정(MiCA; Markets in Crypto-Assets Regulation)의 주요 조항을 검토하고 개선 사항을 제안한다. 이 백서는 주로 커스터디 서비스에 중점을 두고 있으며, 커스터디 서비스 제공업체의 요건과 그 중요성을 상세히 설명한다.

Alkadri, Susan[19]은 주로 커스터디가 아닌 가상자산 규제에 초점을 맞추지만, 사용자 소유의 가상자산에 대한 '통제권' 또는 '보관권'을 보유한 기업이 포괄적인 법적 자격 요건을 충족하는 것의 중요성을 강조한다.

Zuckerman, Adam[20]은 커스터디 서비스 제공업체의 보험 가입 의무를 강조한다. 이 서비스는 주로 고액 자산가와 대규모 가상자산 자산 포트폴리오를 보유한 기관을 대상으로 제공되고 있으며, 리테일 커스터디 제공업체의 증가하는 추세를 지적한다.

V. Gray Area

탈중앙화 금융(DeFi)이라는 용어는 이더리움 블록체인 위에 구축된 대안 금융 인프라를 의미한다. 이 용어는 일반적으로 이더리움 블록체인과 같은 공개 스마트 계약 플랫폼에 구축된 개방적이고 비허가적이며 상호 운용성이 뛰어난 프로토콜 스택을 지칭한다[21]. DeFi는 기존 금융 서비스를 보다 개방적이고 투명한 방식으로 제공하며, 중개자나 중앙화된 기관에 의존하지 않는다. 서비스는 스마트 계약으로 정의된 코드에 의해 시행되며, 합법적인 상태 변경은 퍼블릭 블록체인에 기록된다. 이러한 아키텍처를 통해 투명성과 동등한 접근 권한을 제공하며, 수탁자, 중앙 청산소(clearing houses) 또는 에스크로(escrow, 결제대금예치제도) 서비스의 필요성을 최소화하는 상호 운용 가능한 금융 시스템을 구축할 수 있다[22].

현재 가상자산 업계에서는 중앙화 거래소(CEX)나 디지털 자산 신탁 회사와 같은 일부 서비스가 명확히 커스터디 서비스로 분류되어 법적 규제를 받으며 이용자의 자산을 대신 신탁 받아 보관하고 보호하는 반면, DeFi로 분류되어 법적 규제를 받지 않으면서 커스터디와 유사한 서비스를 제공하는 경우도

존재한다. DeFi 서비스가 앞서 정의된 것처럼 중앙화된 영역이나 중개자 없이 자산에 대한 권한이 사용자 개개인에게만 분배된다면 논란의 여지가 줄어들겠지만, 중앙화된 객체가 식별되고 있다. 또한, 여러 DeFi 프로토콜들을 사용자에게 "프로토콜 운영비"라는 명목으로 수수료가 부과하는데, 이 수수료는 프로토콜의 운영 자금으로 활용된다. 이러한 메커니즘은 특정 서비스를 제공하고 그에 따른 이용료를 지급하는 전통적인 커스터디 서비스 형태와 매우 유사하다. 따라서 이번 세션에서는 DeFi가 가상자산 커스터디 서비스의 Gray Area를 형성하는 이유와 그 논리적 근거를 탐구하고자 한다.

5.1 스테이블 코인 (Stablecoin)

스테이블코인은 법정화폐나 실물 자산에 연동되어 안정된 가치를 제공하는 암호화폐의 일종으로, 이번 서브섹션에서는 스테이블코인의 경제적 특성과 랩드 코인에 관한 연구를 포함하여 스테이블 코인 업계의 불투명한 측면과 그에 따른 시사점을 분석하고자 한다. 위 Fig. 2는 스테이블코인 프레임워크 내에서 법정화폐와 암호화폐 간의 연결 메커니즘을 개괄적으로 설명하는데, 정부 발행 화폐인 법정화폐는 그 안정성과 널리 인정받는 수용성을 바탕으로 가치의 교환 매체 역할을 하며, 암호화폐는 투명성과 추적성을 제공하며 즉각적인 국경 간 거래를 가능하게 한다. 스테이블코인은 이러한 법정화폐와 암호화폐의 가치를 안정적으로 고정해 변동성을 최소화하도록 설계되었으며, 블록체인 생태계 내에서 법정화폐와 암호화

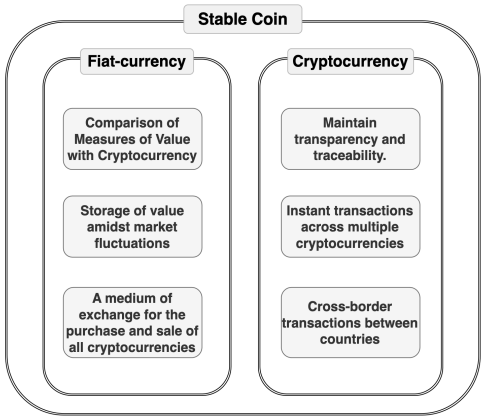

Fig. 2. Mechanism of stablecoin bridging fiat currency and cryptocurrency.

Table 2. Integrated reference across sub-sections

Projects	Categories	Explanation
UST FEI FRAX	Algorithmic stablecoin (Decentralized stablecoin)	Algorithmic stablecoins maintain their value by incentivizing market speculation through their own protocols. The key advantage lies in their uncollateralized mechanism, allowing for increased capital utilization. However, there is a risk of price deviation from the anchor if market arbitrage doesn't align with the protocol's design expectations.
DAI MIM LUSD	Over-collateralization stablecoin (Decentralized stablecoin)	Overcollateralized stablecoins generate $1 worth of stablecoins by pledging collateral exceeding the value of $1. This collateral may consist of various tokens, including non-stable assets such as ETH, protocol tokens, and LP tokens. These stablecoins operate on the same blockchain as the collateral, and the primary risk stems from collateral value fluctuations.
Tether USDC BUSD	Centralized	Centralized stablecoins, often collateralized by fiat off-chain, are closely linked to third-party administrators, resembling traditional banking structures. Their reliability is attributed to the backing of trusted entities and regulatory oversight, making them more stable than decentralized counterparts. Typically, these stablecoins are backed by fiat reserves held in off-chain accounts, or they may peg their value to alternative assets. Trust in the custodian is crucial, although technologies like Chainlink Proof of Reserve enhance transparency through automated verification.

폐 간의 가교 역할을 수행한다.

Table.2의 다양한 프로젝트를 통해 볼 때, 각각의 운영 아키텍처에 따라 분류된 여러 종류의 스테이블코인을 확인할 수 있다. 여기서 탈중앙화 알고리즘 스테이블코인은 담보가 없어도 고유한 프로토콜을 통해 시장 투기를 유도함으로써 자체적으로 가치를 유지하나, 초과 담보(Over-collateralization) 스테이블코인은 발행량보다 많은 담보를 요구함으로써 가치의 안정성을 보장한다. 이러한 코인들은 같은 블록체인 위에서 운영되며, 담보 자산의 가치 변동에 따른 위험성을 내포하고 있다. 다른 한편으로, 중앙화된 스테이블코인은 법정화폐를 오프체인 담보로 사용하고, 신뢰할 수 있는 기관의 감독을 받으며 전통적인 은행 시스템과 유사한 구조로 운영된다. 이러한 중앙화된 스테이블코인의 안정성은 수탁자의 신뢰성에 의존하며, 체인링크 예치 증명과 같은 기술을 통해 투명성을 강화하는 경우가 많다.

초과 담보 스테이블코인을 보다 상세히 살펴보면, 1달러의 가치를 초과하는 담보를 활용하여 1달러 상당의 스테이블코인을 창출한다. 해당 담보로는 이더리움과 같은 변동성이 높은 자산, 프로토콜 토큰, LP[23](유동성 공급) 토큰 등 다양한 형태가 포함될 수 있다. 이러한 스테이블코인은 담보 자산과 동일한 블록체인상에서 운영되며, 담보 가치의 변동성으로 인해 발생하는 위험을 주요한 관리 대상으로 삼는다. 예를 들어, 에이브와 컴파운드와 같은 플랫폼에서는, 담보 가치가 대출액보다 떨어질 경우, 제3자가 할인된 가격에 담보를 구입할 수 있는 청산 메커니즘을 통해 리스크를 관리하고 수익을 창출할 수 있다.

중앙 집중식 스테이블코인은 자산이 인증된 기관에 보관되어 예치금과 같은 역할을 한다. 법정화폐 기반으로 오프체인에서 담보화되며, 제3자 관리자가 이를 관리하여 기존 은행 시스템과 유사한 신뢰성을 확보한다. 테더(Tether), 트루 USD(True USD), USDC, 디직스(Digix), 글로브코인(Globecoin), AAA 등은 중앙화된 모델을 채택하고, 단일 기관이 아닌 컨소시엄에 의존한다. 예를 들어, 테더(Tether)는 유통되는 각 테더 단위를 Tether 유한회사에 예치된 법정화폐 단위와 1:1 비율로 뒷받침하며, 비트코인 블록체인 기반 최초의 법정화폐 연동 암호화폐로, 시장 변동성에 독립적으로 운영된다. 사용자가 Tether Limited에 법정화폐를 예치하면 해당 금액에 상응하는 TetherUSD가 발행된다. 이후 사용자가 테더를 반환하고 법정화폐로 교환하면, 회사는 반환된 테더를 소각하고 법정화폐를 이체한다. 이러한 구조는 테더가 안정적인 가치 저장 수단으로 기능하도록 하여 높은 유동성과 거래 편의성을 제공하며, 법정화폐와 암호화폐 간의 다리 역할을 한다.

이처럼 다양성을 품고 빠르게 성장하는 디파이 생태계는 다수의 보안 위협을 내포하고 있다. Werner[24] 등은 디파이 시장의 보안 위험을 기본 요소, 운영 프로토콜, 보안 측면에서 분석하고, 기술적 보안과 경제적 보안을 구분하여 경제학과 컴퓨터 과학의 통합적인 지식 체계를 제시하였다. 스테이블코인의 주요 우려 사항 중 하나로 기초 자산의 중앙 집중식 관리와 이에 따라 발생할 수 있는 문제들이 분명히 존재함을 강조했다. 이때 스테이블코인의 안정성과 시장 가치는 중앙화된 커스터디언(custodian)에 크게 좌우되며, 이러한 문제에 대한 고찰이 필요하다. 사용자는 스테이블코인을 법정화폐로 전환할 수 있으며, 커스터디언은 이 과정에서 스테이블코인의 가치를 신뢰성 있게 유지하는 역할을 한다.

앞선 연구들은 스테이블코인의 경제적 의미, 위험 분류, 경험적 분석 및 금융에서의 역할을 깊이 있게 조명했다. 본 논문에서는 스테이블코인의 주요 우려 사항 중 하나로 기초 자산의 중앙 집중식 관리를 강조하며, 이에 따른 문제들을 다룬다. 암호화폐는 희소성, 유용성, 채택, 보안, 시장 수요, 네트워크 효과 및 탈중앙화 등을 통해 가치를 창출하지만, 중앙화된 스테이블코인은 담보 자산의 관리에 의존하여 가치를 창출한다. 이는 전통 금융의 수탁 서비스와 유사한 메커니즘으로, 스테이블코인의 안정성과 신뢰성을 보장하면서도 중앙 집중화의 리스크를 내포한다. 따라서, 중앙화된 스테이블코인을 가상자산 환경 내의 Gray Area로 분류하며, 스테이블코인의 운영 메커니즘에 관한 지속적인 연구와 철저한 검토의 중요성을 강조한다.

5.2 브릿지 (Bridge)

Caldarelli[25]의 연구에 따르면, 블록체인 간의 토큰 전송을 용이하게 하는 메커니즘으로 체인 간 상호운용성을 달성하기 위해 브리지는 핵심적인 역할을 수행한다. 브리징 프로세스는 일반적으로 원본 토큰을 해당 네이티브 블록체인에 보관하고 대상 블록체인에서 해당 토큰의 사본을 생성하는 과정을 포함한다. 이러한 토큰 사본은 대상 블록체인에서 원본 토큰의 대표로 기능하며, 이를 통해 탈중앙화된 애플리

케이션 및 스마트 컨트랙트에서 활용될 수 있다. 랩드 토큰 브리지, 시크릿 브리지, 레이어 2 브리지 등 다양한 유형의 브리지가 존재하며, 이들 중 랩드 토큰 브리지는 WBTC와 RenBTC와 같은 프로젝트를 통해 구현되는 것이 특징이다. 이러한 프로젝트들은 스마트 컨트랙트 내에서 원본 토큰을 캡슐화하고 대상 블록체인에서 동등한 양의 랩드 토큰을 발행하는 과정을 포함한다.

Lyons[26]는 비트코인과 연계된 스테이블코인, 특히 랩드 비트코인(WBTC)의 생성 메커니즘을 심도 있게 연구한다. WBTC는 비트코인을 스마트 컨트랙트에 예치하고 그에 상응하는 양의 WBTC를 발행하는 구조로 설계되어 있다. 이를 통해 비트코인은 'Wrapping' 처리되어 이더리움 블록체인에서 효과적으로 활용될 수 있다. WBTC는 탈중앙화된 금융 생태계에서 서로 다른 체인 간에 다리 역할을 하며 여러 DeFi 서비스에서 유용하게 이용되고, 여러 가상자산 거래소에서도 거래가 가능하다. 대부분의 브리지 서비스는 Lock&Mint와 Burn&Mint 모델을 모두 포함하는 하이브리드 메커니즘을 채택하여, 다양한 블록체인 생태계 간의 양방향 자산 전송을 가능하게 한다[26].

특히 주목할 부분은 WBTC의 랩핑(Wrapping) 및 언랩핑(Unwrapping) 프로세스를 가능하게 하는 수탁자 컨소시엄의 존재이다. 이 수탁자들은 블록체인 및 암호화폐 네트워크에서 금융 거래의 보안성과 투명성을 유지하는 중추적인 역할을 한다. 이들은 WBTC를 지지하는 비트코인의 보유량을 관리하고, WBTC를 비트코인으로 교환하며, 소각 과정을 통해 비트코인을 상환한다. 이러한 과정은 거래의 무결성을 검증하고, 특정 거래를 승인하며, 관련 자산을 안전하게 관리함으로써 시스템의 무결성을 보장하고 사용자들에게 신뢰를 제공한다. 수탁자들의 이러한 역할은 WBTC DAO에 의해 규정된다. WBTC DAO는 WBTC 생태계의 주요 의사결정을 내리는 거버넌스 기구로, 수탁자들의 활동을 감독하고 필요한 규칙과 절차를 설정한다. 예를 들어, WBTC DAO는 수탁자들의 추가 및 제거, 비트코인 보유량의 감사, 스마트 계약의 수정 등을 관리한다. 이는 전체 시스템의 안정성과 신뢰성을 보장하는 중요한 요소이다

Bridge 프로토콜의 중요한 요소인 검증자는 DeFi 네트워크의 보안과 무결성을 유지하는 핵심 역할을 한다. 이들은 디지털 서명, 해시 함수, 공개키 암호화 등 고도의 암호화 기술을 사용해 거래를 엄격히 인증하고, 블록체인에 유효한 트랜잭션만 포함되도록 감독한다[27]. 특히 서로 다른 블록체인 간 자산 이동을 안전하게 관리하며, 트랜잭션의 무결성을 보장한다. 한편, Qasse[28]에 따르면 현대 산업의 블록체인 프로젝트에서 검증자가 광범위하게 사용되면서도 외부 공격에 취약한 한계가 존재한다. 검증자에게 보안 위반이나 침해가 발생하면 네트워크의 신뢰 기반이 위험에 처하게 되며, 이는 네트워크 전체의 신뢰성과 공신력을 크게 약화시킬 수 있다. 따라서 개발자는 단일 장애 지점에 의존하지 않는 대안을 찾아 블록체인 네트워크의 보안과 신뢰성을 보장해야 한다.

자산에 대한 권한 범위는 브리지 프로토콜에 따라 다양하게 나타나며, 이는 브리지 운영 구조와 밀접하게 연관되어 있다. 이러한 구조에서는 중앙화된 권한을 가진 중개자(수탁자 또는 검증자)가 운영을 책임지는 형태이다. DAO를 통과하고 영향력 있는 중개자가 담당하더라도, 외부 위협이나 중앙화된 권한의 존재는 변하지 않는다는 점이 핵심 취약점이다. 이러한 자산에 대한 권한 위임은 전통 금융의 커스터디 개념과 유사하게 해석될 수 있으며, 이는 승인된 역할을 수행하는 특정 개인에게 자산 관리가 위임되었음을 의미로도 해석할 수 있다. 이에 따라, 가상자산 커스터디 서비스 제공의 구조와 규제에 대한 깊이 있는 분석과 재평가가 필요하다.

5.3 유동성 스테이킹 (Liquid Staking)

유동성 스테이킹은 지분 증명(PoS) 블록체인의 스테이킹 개념에서 발전한 혁신적인 스테이킹 파생상품으로 간주된다. Lehmann[29]의 연구에 따르면, 스테이킹은 PoS 합의 메커니즘과 밀접하게 연관된 복잡한 과정으로, 검증자 또는 검증 노드가 제안된 블록에 대한 네트워크 전체의 합의를 형성하는 데 중요한 역할을 한다. 다수 검증자들은 하나의 검증 풀을 형성하고, 이 풀 내에서 무작위로 선정된 한 명이 새로운 블록을 생성하는 제안자의 역할을 맡게 된다. 제안된 블록은 네트워크 내의 다른 검증자들에게 전파되며, 블록에는 제안자가 수집한 트랜잭션들이 포함되어 있다. 검증자들은 블록을 검증하고 생성하는 데 대한 보상을 받으며, 이는 PoS 블록체인 네트워크의 안정성과 보안을 유지하는 인센티브로 작용한다. 이러한 과정은 PoS 블록체인의 기본 원리에 기

반을 두고 있으며, 유동성 스테이킹이라는 개념을 도입함으로써 PoS 스테이킹의 유연성이 크게 향상되었다. 이는 PoS 블록체인 기술의 발전에 중요한 역할을 하며, 더욱 포괄적이고 누구나 참여 가능한 디지털 금융 생태계 구축을 가능하게 한다. 본 서브세션에서는 PoS 스테이킹의 유연성을 확장시키는 과정에서 발생하는 권한 위임과 검증자의 역할, 그리고 권한 집중화에 대해 깊이 있게 논의한다.

John[30]의 연구에 따르면, 스테이킹은 암호화폐를 일정 기간 확보하고 약속하는 과정을 중심으로 이루어지며, 금전적 보상에 대한 기대는 투자자를 스테이킹 활동으로 유도하는 주요 동기로 작용한다. 유동성 스테이킹의 핵심 요소는 투자자의 참여와 네트워크의 안정성 사이의 균형을 맞추는 것이다. 스테이킹 모델은 네트워크의 분산화와 안정성을 강화하며, 경제적 보상을 통해 참여자들이 네트워크 유지에 기여하도록 독려한다. 이는 스테이킹은 암호화폐 생태계에서 중요한 역할을 하며, PoS 합의 메커니즘의 발전과 함께 더욱 복잡하고 다양한 형태로 발전하고 있다.

Bhambhwani[31]의 연구에 따르면, Lido 파이낸스와 같은 유동성 스테이킹 서비스는 이더리움의 PoS 스테이킹의 진입 장벽을 완화하는 데 필수적인 역할을 수행한다. Lido는 사용자들이 원하는 양의 이더리움을 예치하여 개별적인 하드웨어 관리 없이도 스테이킹에 참여할 수 있는 대안을 제공하며, 비론 체인에 대신 스테이킹을 수행한다. 이로써 검증자들은 이더리움을 스테이킹한 보상으로 stETH를 받게 된다. stETH는 탈중앙화 거래소에서 거래하고, 유동성 풀에 예치하거나, DeFi 플랫폼에서 담보로 사용할 수 있으며, 보유자는 지속해서 스테이킹 보상을 받을 수도 있다. 유동성 스테이킹은 커스터디 서비스의 중추적인 역할을 하며, 개별 스테이커들의 자산을 통합해 32 이더리움의 임계값을 달성함으로써 PoS에 참여하는 데 필요한 최소한의 32 이더라는 금전적 장벽에서 벗어나게 한다. 또한, 이를 통해 재정적 요건을 충족시키면서 자산에 대한 권한을 프로토콜로 이전한다. 이 과정에서 참여자들은 스테이킹에 필요한 하드웨어의 직접적인 관리와 유지의 부담에서 벗어나며, 대신 Lido 노드 운영자와 프로토콜이 필요한 하드웨어 인프라를 감독 및 유지 관리한다.

한편, 위처럼 32 이더리움이라는 임계치를 충족시키는 과정에서 토큰의 위임이 발생하며, 이는 토큰 보유자가 자신의 재정적 속성을 유지하면서 다른 당사자에게 자산에 대한 권한을 이전하는 과정을 의미한다. 예를 들어, Lido 노드를 운영하는 운영자는 사용자로부터 자산을 위임받아 PoS 스테이킹에 참여한다. 스테이킹에 참여하는 사용자와 운영자는 보상과 슬래싱(지분 삭감)의 책임을 공동으로 부담하기 때문에, 누구에게 자신의 자산을 위임할 것인가는 자산 손실의 가능성을 내포하여 중요한 결정이다[32]. 이처럼 위임된 자산을 책임지는 노드 운영자들은 스테이킹 보상의 일부를 보상으로 수령한다. 그러나 이러한 메커니즘에는 자산 위탁과 수익 창출 과정에서 발생할 수 있는 리스크와 책임 소재에 대한 법적 정의가 부재한 상태이다. 따라서 이러한 Gray Area에 대한 재검토가 필요한 시점이다. 이는 투자자 보호를 강화하고 시스템의 투명성과 안정성을 제고하는 데 목적이 있다.

VI. 최종 논의

DeFi는 정통 금융 중앙화된 금융 시스템과 여러 가지 근본적인 차이점을 지니고 있다. 이 시스템은 중앙화된 중개자 없이 분산된 형태로 운영되며, 스마트 계약을 통해 자동으로 실행된다. 따라서 누구나 별도의 승인 없이 서비스를 이용할 수 있으며, 사용자가 자신의 자산을 직접 관리한다. 또한, 국경 없이 전 세계에서 접근 가능하며, 각 사용자가 익명성을 유지함에 따라 규제 적용이 어렵다는 특징을 가진다.

따라서, DeFi라는 정의에 부합한 프로토콜을 개발하려면 기술적 측면과 거버넌스적 측면 모두에서 진정한 탈중앙화를 달성해야 한다. 그러나 일부 기존 DeFi 프로토콜은 탈중앙화를 표방하며 규제를 받지 않지만, 실제로는 부분적으로 중앙화된 서비스를 제공하는 경우가 존재한다. 진정한 탈중앙화를 이루기 위해서는 전통 금융의 중앙화된 형태에서 벗어나 다양한 분야에서 탈중앙화를 실현해야 한다. 이를 위해 중앙화된 객체를 없애고, 최대한 많은 영역에서 권한을 분산해야 하며, 충분한 분산을 위해서는 이용자의 적극적인 참여가 필요하다. 따라서 이번 최종 논의 세션에서는 DeFi 프로토콜의 특성에 맞춰 탈중앙화 수준을 평가하기 위한 4가지 지표(표 형태)와 세부 평가 항목을 제시하고자 한다. 이를 통해 탈중앙화 금융 서비스의 규제 필요성을 검토하고, 가상자산 이용자의 자산을 보호하며, 중앙화된 프로토콜에는 가상자산 커스터디 서비스 제공자 수준의 규제를 적용하여 시장의 건전성을 확보하고자 한다.

6.1 참여 장려 요소의 중요성

Table 3 평가 가이드라인 항목 1에 따르면, DeFi 프로토콜의 성공적인 탈중앙화를 위해서는 사용자의 적극적인 참여가 필수적이다. 사용자의 참여는 의사결정 과정에서 권력 집중을 방지하고, 네트워크 검증과 운영에 다양한 사용자가 참여함으로써 보안을 강화하며, 커뮤니티의 신뢰를 형성하여 프로토콜의 안정성을 높인다. 높은 참여도는 결국 프로토콜의 탈중앙화를 촉진하며, 더 많은 사용자와 커뮤니티 구성원이 프로토콜의 의사결정과 운영에 기여하게 된다.

먼저, 사용자 보상 구조의 존재 여부를 평가해야 한다. 유동성 공급자에게 인센티브를 제공하는 구조나 참여자에게 보상을 제공함으로써 사용자 참여를 유도할 수 있다. 예를 들어, 에어드롭은 몇 가지 자격 기준에 따라 활동 중인 서비스 이용자에게 신규 토큰을 지급하는 마케팅 전략이다. 이는 초기 사용자나 소셜 미디어를 통해 프로젝트의 인지도를 높이는 데 도움을 준 사람들에게 보상을 제공하여 사용자의 참여를 장려하는 효과적인 방법이다. 2010년 비트코인 개발자 개빈 안드레센은 비트코인에 대한 관심과 인지도를 높이기 위해 5개의 비트코인을 나눠주는 스레드를 레딧에서 시작한 것이 그 시초였다[33]. 이후 2016년경 이더리움이 등장하면서 에어드롭은 주류가 되었고, 주로 소셜 미디어 플랫폼에서 프로젝트 홍보나 사용자 참여를 유도하는 대가로 점점 더 많이 제공되었다. 그러나, 에어드롭은 특정 주소나 개인에게 집중될 위험이 있어 'Yield Farmer(이자 농사꾼)'에 의해 악용될 수 있으므로 이에 대한 대책도 간구해서 에어드롭을 기획해야 한다.

Rocha[34]는 소셜 네트워크의 몇 가지 특징으로 상호작용성, 세분화된 대상으로 제공하는 서비스, 새로운 형태의 데이터 관리를 가능하게 하는 기술, 더 나은 비용 대비 효율성, 그리고 효과적인 커뮤니케이션 결과 측정 등을 꼽았다. 이처럼 DeFi 프로토콜은 공식 포럼, Discord, Telegram, Reddit 등의 커뮤니티 채널을 운영하여 참여자들이 자유롭게 의견을 나누고 논의할 수 있는 공간을 제공함으로써 커뮤

Table 3. [Evaluation guidelines Topics 1] The importance of incentivising engagement

Evaluation Criteria	Evaluation Parameter	Evaluation Details	Remarks
Existence of User Incentive Structures	Providing incentives to highly active users / liquidity providers for example airdrops.	Assess whether incentives are provided to encourage participation of highly active users and liquidity providers within protocols.	It is also essential to examine whether there are countermeasures in place to address Yield Farmers.
Provision of Community Participation Spaces	Operation of community channels such as official forums, Discord, Telegram, Reddit	Assess whether spaces are provided for users to freely express opinions and participate in discussions, thereby promoting community engagement.	The activity level of the channel is also an important checkpoint.
Provision of Educational Materials and Promotion	Providing user guides, tutorials, webinars, AMA (Ask Me Anything) sessions	Assess whether educational materials and promotional activities are provided to help users easily participate in the protocol.	The continuity of educational materials and AMAs (Ask Me Anything sessions) is also an important checkpoint.

Table 4. [Evaluation guidelines Topics 2] Governance measures for decentralisation of authority

Evaluation Criteria	Evaluation Parameter	Evaluation Details	Remarks
Distribution and Use of Governance Tokens	Governance token voting, transparent proposal process	Assess whether decision-making processes using governance tokens are transparent and fair.	As with all voting systems, there is a risk of individuals or groups obtaining a majority of votes. The initial developers may hold or reserve a significant portion of the governance tokens when creating the network. There is also a risk of token distribution to multi-account users resulting in an individual holding a majority. It is crucial to recognize this and take appropriate measures.
Use of Multisignature Wallets and Various Governance Models	Multisignature for decisions, diverse governance models (Quadratic Voting, Liquid Democracy)	Assess whether multiple signatures are required for making governance decisions to ensure decentralization of authority, and whether diverse governance models like Quadratic Voting and Liquid Democracy are adopted to mitigate imbalances in voting power.	
Operation of DAOs	Operation by Decentralized Autonomous Organizations (DAOs), use of smart contracts	Assess whether DAOs operate autonomously through smart contracts, and whether rule changes are made through democratic voting.	

Table 5. [Evaluation guidelines Topics 3] Technical measures for decentralising authority

Evaluation Criteria	Evaluation Parameter	Evaluation Details	Remarks
Assignment of 'Roles' to Specific EOA Addresses	Existence of roles like validators and guardians	Assess whether roles like validators or guardians('PAUSE ROLE', 'MANAGE FEE', 'SLASHER ROLE', 'REWARDS RATE ROLE'') are assigned to specific EOA addresses.	Such control authority can be distributed in various ways, including to a single user, a small group (multi-signature), or a large group (governance token voting). Additionally, if the authority is granted to a specific EOA (Externally Owned Account), the process by which this authority was granted must also be evaluated.
Use of Proxy Patterns	Existence of proxy contracts that dynamically reference addresses of logic contracts	Assess whether proxy patterns are used to enhance flexibility and provide improved functionality without interruptions.	

Table 6. [Evaluation guidelines Topics 4] Transparency and democracy in financial management

Evaluation Criteria	Evaluation Parameter	Evaluation Details	Remarks
Financial Management by Community Voting	Introduction of community treasury, blockchain recorded fund usage, community voting for major financial decisions	Assess whether financial management is determined by community voting, and whether fund usage is recorded on the blockchain to ensure transparency.	Throughout this process, it's crucial to evaluate if budget allocation is fair and transparent, as outlined in the project proposal and whitepaper. The proposal submission and evaluation should be transparently disclosed, and budget decisions made through community voting to ensure fairness.
Transparency of Circulation and Holdings	Real-time information on total supply, circulation, and holdings of tokens	Assess whether real-time information on token circulation and holdings is provided to clearly understand inflation or deflation situations such as dash board.	
Disclosure of Financial Reports	Regular financial reports on fund usage, revenue, expenses	Assess whether the project's financial status is regularly reported and whether fund usage, revenue, and expenses are transparently disclosed.	
Reward and Incentive Structures	Defined reward/incentive structures	Clearly define the reward and incentive structure for token holders, including the reasons for any incentives given, and disclose all reward details to enhance transparency.	

니티 참여를 촉진할 수 있다. 예를 들어, Discord에 접속하면 첫 번째로 보게 되는 것은 프로토콜에 대한 간략한 설명과 FAQ, 포럼, 문서 링크 등이 포함된 프레젠테이션이다. Discord는 여러 채널로 구성되어 있으며, 'Announcements' 채널에서는 프로젝트의 뉴스와 업데이트를 빠르게 팔로우할 수 있다. 다른 채널로는 커뮤니티, 개발자, 지원 섹션 등이 있으며, 각 섹션 내에는 'General', 'DeFi', 'NFT', 'Complaints' 등 주제별 채널에서 기술적 주제와 프로젝트 관련 문제를 논의하고 질문할 수 있다. Reddit에서는 사용자가 포스트에 대해 투표할 수 있는 시스템이 있어 커뮤니티의 관심사와 의견을 쉽게 파악할 수 있다. 우수한 아이디어는 많은 Upvote를 받아 프로젝트 개발자들의 주목을 받을 수 있으며, 높은 수준의 참여를 통해 의견을 표현하고, 콘텐츠와 아이디어를 제공하며 브랜드 팔로워들 간의 토론을 촉진한다. 이러한 채널은 사용자들 간의 정보 공유와 협력을 증진하며, 프로토콜의 개선에 대한 집단지성을 활용할 수 있게 한다.

마지막으로, 프로토콜에 대한 이해를 돕고 사용자 참여를 장려하기 위해 다양한 교육 자료와 홍보 활동이 필요하다. 사용자 가이드, 튜토리얼, 웨비나(Webinar), AMA(Ask Me Anything) 세션 등을 통해 교육 자료를 제공하고, 홍보 활동을 강화함으로써 사용자들이 프로토콜에 보다 쉽게 참여할 수 있도록 도울 수 있다. AMA는 주로 YouTube에서 진행되며, 개발자와 커뮤니티가 직접 소통할 수 있는 라이브 이벤트로, 기술적인 이슈를 다루고 시청자의 질문에 답변하며 프로젝트의 향후 전망에 대해 논의한다. 이러한 AMA 세션은 개발자들이 커뮤니티와 직접 대화할 중요한 기회이며, 커뮤니티는 이러한 경로를 통해 투자 여부에 관한 결정을 내리기도 한다[35].

사용자의 적극적인 참여는 DeFi 프로토콜의 성공과 지속 가능성에 필수적이며, 중요한 평가 기준이 된다. 이를 위해 보상 구조, 커뮤니티 참여 공간, 교육 자료와 홍보 활동을 통해 사용자 참여를 촉진함으로써 프로토콜의 탈중앙화와 안정성을 높일 수 있다.

6.2 거버넌스 측면의 권한 분산을 위한 조치

Table 4 평가 가이드라인 항목 2에는 DeFi를 거버넌스 측면에서‘ 권한’이라는 관점으로 논의하고 있다. 이는 모든 노드가 데이터에 동등한 접근권을 가지고 거버넌스 권한과 기술적 권한을 갖는 탈중앙화된 금융서비스를 뜻한다. 이는 사용자들이 직접 의사결정 과정에 참여해 프로토콜의 운영과 발전 방향을 결정하는 탈중앙화라는 블록체인의 본질을 반영한다.

탈중앙화 금융 애플리케이션은 일반적으로 거버넌스 토큰을 사용하여 의사결정 과정을 기술적으로 구현한다. 애플리케이션 개선 제안이 있을 경우, 거버넌스 토큰 보유자는 투표 시스템을 통해 제안을 결정할 수 있으며, 채택된 제안은 코드 수정 및 업데이트로 반영된다. 여기서 모든 거버넌스 토큰을 동일시해서는 안 된다. 가) 해당 토큰에 따라 어떤 결정이 내려지는지, 나) 토큰이 어떤 기준으로 할당되는지, 다) 토큰의 발행 및 소각에 따라 각 거버넌스 토큰의 탈중앙성의 차이가 발생한다[36]. Uniswap 프로토콜은 웹사이트에서 UNI 토큰 보유자 커뮤니티가 Uniswap을 관리한다고 설명한다. 사용자는 거버넌스 포럼에서 개선 제안을 찾고, 투표 기간 자신의 UNI 토큰을 위임하여 투표권을 행사할 수 있다. 또한, MakerDAO 프로토콜에서는 MKR 토큰 보유자는 공동으로 거래 수수료를 설정할 수 있는 권리를 가진다. 이는 이자 지급, 청산 수수료, ETH-USD 비율에 따라 MKR 토큰은 소멸하거나 생성되어 할인된 가격으로 판매된다[37]. 이처럼 거버넌스 토큰의 유형은 변칙적이며, 각 프로토콜에서 제공하는 서비스에 따라 다양성을 가지고 있기에, 획일적인 기준을 가지고 평가하기보다는 각 서비스를 개별적으로 평가하여 기준표에 부합하는지 여부를 판단하는 것이 옳은 방법일 것이다. 여기서, 모든 투표 시스템에서는 개인이나 그룹이 과반수를 획득할 위험이 존재한다. 최초 개발자가 많은 거버넌스 토큰을 보유하거나, 다계정을 사용하는 유저가 과반수를 차지할 위험도 있다. 이러한 위험을 인지하고 적절한 조치를 취했는지 여부도 중요한 평가지표가 된다.

다중서명 지갑을 도입하여 중요한 자산 관리와 의사결정에 여러 명의 서명이 필요하도록 설정하거나, Quadratic Voting, Liquid Democracy와 같은 다양한 거버넌스 모델을 도입하여 투표 권한의 불균형을 완화할 수 있다. 신세틱스(SNX)가 좋은 예시라고 볼 수 있다. 다른 프로젝트가 토큰과 투표권을 일대일로 연결하는 방식을 채택한 반면, 신세틱스의 Quadratic 투표 메커니즘은 주소의 투표권을 해당 주소가 보유한 토큰화된 투표권 수의 제곱근으로 계산한다. 이는 상당한 수의 SNX 토큰을 보유한 주소의 투표권을 제한하도록 설계되었으며, 예를 들어 10,000개의 SNX 토큰을 보유한 주소는 100표만 투표할 수 있는 권한을 가진다. 또한, 투표권의 감소율은 주소가 보유한 SNX 토큰 수에 비례하여 증가한다. 그러나 중요한 주의 사항은, 이차 투표는 civil 저항성이 없으므로 개인이 SNX 토큰을 여러 지갑 주소에 분산하여 단일 지갑 주소에 모든 SNX 토큰을 보유할 때보다 더 큰 투표권을 얻을 수 있다는 것이다. 이를 적용했을 때 2021년 8월 15일 기준, SNX 의결권의 50% 이상을 통제하기 위해서는 4,400개 이상의 주소(SNX를 보유한 총 주소 수의 약 5%)가 필요하게 된다[38]. SNX를 제외하고 조사된 의결권 토큰의 분포는 모두 매우 높은 수준의 중앙 집중도를 보였으며, 100개 미만의 주소가 의결권의 50% 이상을 통제하는 것으로 나타났다[38].

마지막으로, 탈중앙화 자율조직(DAO)은 스마트 컨트랙트에 의해 운영되어, 조직의 결정과 제안을 자동으로 실행하며, 규칙 변경은 민주적인 투표를 통해서만 가능한 탈중앙화 거버넌스 방식이다. 여기서 사용되는 스마트 컨트랙트는 다양한 블록체인에 배포되어 DAO의 규칙을 설정하고 있으며 이는 중앙화된 계층적 구조를 제거하고 민주적이고 평등한 거버넌스를 목표로 한다. 또한, DAO는 이익 분배, 합의, 자동 실행, 그리고 모든 구성원의 권한 분배라는 메커니즘을 통해 더욱 안정적인 커뮤니티를 구축한다[39]. 현재 금융 프로토콜 DAO(예: MakerDAO, Uniswap), NFT 구축 DAO(예: Root), 미디어 및 소셜 DAO(예: Bankless) 등 다양한 분야에서 활동하는 DAO가 있으며, 예를 들어, Loot DAO는 예술적 창의력과 상상력을 발휘해 콘텐츠를 구축함으로써 더 많은 투자를 유도하고 큰 수익을 얻는 공정한 보상 시스템을 갖추고 있다[38]. DAO 회원은 특정 토큰을 담보로 투표권을 획득하여 가치 정의와 규칙 제정에 참여하는 ‘입법권’을 보유하지만, 이러한 구조는 의결권의 중앙 집중화로 이어져 소수 이익에 부합하는 결과를 초래할 수도 있다. 따라서, 각 서비스 별 목적과 이해관계에 따라 다양한 투표 메커니즘이 존재하며, DAO의 성공적인 운영을 위해서는 이러한 메커니즘들이 평가되고 구현되어 보다 민주적이고 평등한 거버넌스 구조를 유지하고, 커뮤니티 구성

원의 공정한 참여와 자율성 증진을 통해 개인과 커뮤니티의 이익을 극대화해야 한다.

탈중앙화 금융(DeFi)의 권한 구조를 분석할 때, 데이터 접근권과 거버넌스 권한의 분배는 중요한 평가 요소이다. 거버넌스 토큰을 통한 의사 결정 과정은 블록체인의 탈중앙화 본질을 반영하며, 프로토콜마다 고유한 방식으로 구현되고 있다. 따라서, 각 프로토콜의 거버넌스 구조를 개별적으로 평가하고, 커뮤니티의 공정한 참여와 자율성을 증진시키는 것이 중요하다. 이는 궁극적으로 개인과 커뮤니티의 이익을 극대화하고, 안정적이고 민주적인 이익 커뮤니티를 구축하는 데 기여할 것이다.

6.3 기술적 측면의 권한 분산을 위한 조치

Table 5 평가 가이드라인 항목 3에 명시된 대로 탈중앙화 프로토콜의 기술적 측면에서 권한 분산 정도는 핵심 평가 요소이다. 불가성과 자동화는 스마트 컨트랙트의 핵심 특성으로, 이를 이용하는 DeFi는 중개자 없이 컨트랙트 로직만으로 작동하는 서비스를 통해 탈중앙화 금융의 정의에 부합해야 한다. 그러나 현실에서는 이와 다르게 나타나는 경우가 많다. 특히 현물 자산과 연계되거나 거래 검증 및 중앙화된 거래 처리가 필요한 서비스에서는 중개자의 완전한 제거가 현재로서는 어렵다. 또한, 특정 서비스는 스마트 컨트랙트의 프록시 패턴을 이용해 계약의 전체 기능을 업그레이드할 수 있는 유연성을 제공한다. 이러한 통제 권한은 단일 사용자, 소규모 그룹(다중 서명), 대규모 그룹(거버넌스 토큰 투표) 등 다양한 방식으로 분산될 수도 있으며[40], 이를 고려하여 그에 맞는 검토가 필요하다.

EOA 주소에 할당되는 'Role'에는 '검증자' 또는 '가디언(Guardian)'이라는 운영자의 개입이 존재한다. 이 역할은 프로토콜 내에서 사용자 활동을 검증하고 트랜잭션의 정확성을 보장하며, 우발적 상황을 관리하거나 주요 운영 로직을 조작할 수 있는 권한을 가진다. Fig.3을 보면, DeFi 스마트 계약 내에서 'Role'이라는 특정 권한을 가진 사용자들이 탈중앙 금융 프로토콜의 운영과 관리에 중추적인 역할을 담당한다. 'PAUSE ROLE'과 'RESUME ROLE'은 프로토콜의 핵심 기능을 제어하여 긴급 상황에 대응하고, 'MANAGE FEE' 역할은 특정 주소에 수수료 설정 권한을 위임한다. 'SLASHER ROLE'은 위반 행위 발생 시 스테이킹된 토큰을 차감하며,

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

abstract contract Roles is TokenStorage {
    //1. Rolls for operating DeFi Protocols.

    // Role: OWNER_ROLE - Allows address to add or remove members from any of the roles below.
    bytes32 public constant OWNER_ROLE = keccak256("OWNER_ROLE");

    // Role for pausing operations in the DeFi Protocol.
    bytes32 constant public PAUSE_ROLE = keccak256("PAUSE_ROLE");

    // Role for resuming operations in the DeFi Protocol.
    bytes32 constant public RESUME_ROLE = keccak256("RESUME_ROLE");

    //2. Rolls for managing DeFi Protocols.

    // Role for managing fees in the DeFi Protocol.
    bytes32 constant public MANAGE_FEE = keccak256("MANAGE_FEE");

    // Role: SLASHER_ROLE - Empowers an entity to slash staked token balances and withdraw associated funds.
    bytes32 public constant SLASHER_ROLE = keccak256("SLASHER_ROLE");

    // Role: REWARDS_RATE_ROLE - Provides the authority to set the emission rate of rewards.
    bytes32 public constant REWARDS_RATE_ROLE = keccak256("REWARDS_RATE_ROLE");

    // Role: CLAIM_OPERATOR_ROLE - Permits claiming rewards on behalf of a user.
    bytes32 public constant CLAIM_OPERATOR_ROLE = keccak256("CLAIM_OPERATOR_ROLE");
}
```

Fig. 3. Roles implementation in smart contracts

'REWARDS RATE ROLE'은 보상 지급 비율을 조절한다. 이러한 권한 구조는 탈중앙화 금융의 본질적인 문제를 야기하며, 각 역할은 외부 공격이나 특정 개인 또는 그룹에 의해 악용될 가능성을 증가시킨다. 일반 사용자가 가질 수 없는 권한을 가진다는 점에서 탈중앙성을 해치지만, 차선책으로 다중 서명(multisignature)과 같은 기술을 통해 권한을 분산시키는 것이 이상적이다. 이는 여러 명의 승인이나 검토가 필요하게 하여 프로토콜의 투명성과 안정성을 높이고 사용자에게 가해질 수 있는 위험을 축소 시킬 수 있다.

스마트 계약의 기술적 고려 사항에는, Fig.4에서 볼 수 있듯이 스마트 계약의 프록시 패턴을 이용한 업그레이드 가능성이 포함된다. 일반적으로 스마트 계약은 배포 후 불변성을 유지하는 것이 원칙이지만, 운영상의 필요에 따라 계약의 내부 로직을 수정해야 할 경우가 종종 발생한다. 이러한 필요에 대응하기 위해 스토리지와 논리적 기능을 분리하는 설계가 채택된다. 프록시 계약은 사용자 인터페이스 역할을 하며, 실제 서비스 로직을 담은 계약은 독립적으로 운영된다. 프록시 계약은 로직 계약의 주소 값을 동적으로 참조하여, 새로운 로직 계약을 배포하고 업데이트된 주소를 프록시에 전달함으로써, 클라이언트는 코드를 변경할 필요 없이 새로운 로직으로 전환하여 서비스를 지속할 수 있다. 이 과정에서 프록시 계약은 항상 최신 로직을 참조하도록 설정되어, 사용자들은 중단 없이 향상된 기능을 이용할 수 있다. 이러한 구조는 스마트 계약의 유지 보수와 확장성을 크게 향상시키며, 빠르게 변화하는 요구사항에 유연하게 대응할 수 있게 한다. 그러나 이러한 프록시 패턴의 사용은 프로토콜의 유연성을 높여주는 반면, 중요한 로직에 대한 수정 권한을 프로토콜이 갖게 됨으로써 탈

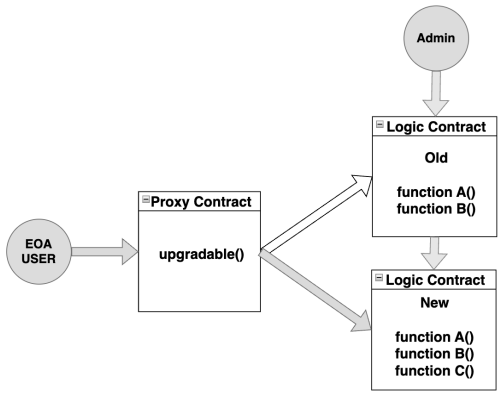

Fig. 4. Architectural framework of the proxy pattern

중앙성이 침해될 수 있다. 특정 개인이나 그룹이 계약의 핵심 기능을 변경할 수 있는 권한을 가지게 되면, 이는 운영자에 대한 지나친 의존성을 초래하고, 외부의 공격이나 내부의 악의적 행위에 대한 취약성을 증가시킬 수 있다.

탈중앙화 금융 서비스의 환경이 빠르게 발전하고 있음에도, 이러한 시스템을 뒷받침하는 복잡한 메커니즘으로 인해 완전한 탈중앙화를 달성하기는 여전히 어려운 일이다. 따라서 명확한 기준을 토대로 각 프로토콜의 기술적 탈중앙성을 평가하는 것도 핵심 평가 기준이 된다

6.4 재무 관리의 투명성과 민주성

Table 6 평가 가이드라인 항목 4에 관한 내용으로, 기존 전통 금융 시스템의 대부분은 신뢰 기반이며 중앙화된 기관에 의존하지만, 탈중앙 금융은 이러한 신뢰 요건 중 일부를 스마트 컨트랙트로 대체한다. 스마트 컨트랙트는 수탁자, 에스크로(escrow) 에이전트, 중앙 집중식 자금 조달 기관(CCP)의 역할을 맡을 수 있다[37]. 따라서, 탈중앙화 프로토콜의 재무 관리가 투명하고 민주적으로 이루어지는지 평가하는 것이 중요하며, 이는 재무 관리의 커뮤니티 투표 여부와 프로젝트 제안서 및 예산 배분의 공정성을 포함한다.

먼저, 재무 관리가 커뮤니티의 투표에 의해 결정되는지를 평가해야 한다. 커뮤니티 트레저리를 도입하고, 자금 사용 내역을 블록체인에 기록하여 투명성을 확보하며, 중요한 재무 결정은 커뮤니티 투표를 통해 진행하여, 재무 관리 과정에서의 투명성과 신뢰성을 확보할 수 있다. 이를 위한 방법으로는 토크노믹스(Tokenomics)가 가장 대표적이 예시이다. 토크노믹스는 가치를 거래 가능한 토큰이나 코인으로 캡슐화하여 토큰 설계자가 설정한 규칙에 따라 자율적인 경제 시스템을 만드는 과정을 말한다[41]. 이는 이해관계자 사이의 인센티브 구조를 시스템의 목표와 일치시키기 위해, 경제적 관점에서 토큰 할당을 분석하여 결정한다. 이러한 토큰 기반 경제 시스템은 투자자 풀 확대, 거래 효율성, 투명성을 통해 자산 유동성을 개선하고, 인프라 자금 조달 시 자금세탁방지법을 준수할 수 있다.

다음은 탈중앙화 프로토콜에서 투명하고 공정한 재무 관리를 위한 구체적인 방안이다:

1. 토큰 배포 계획 공개: 토큰 배포 일정과 비율, 초기 배포량, 팀 할당, 투자자 할당 등을 명확하게 공개한다. 이는 사용자가 토큰 배포의 공정성을 평가할 수 있도록 돕는다.
2. 유통량 및 보유량 투명성: 토큰의 총 공급량, 유통량, 보유량에 대한 실시간 정보를 제공하는 대시보드나 웹사이트를 운영한다. 이는 토큰의 인플레이션이나 디플레이션 상황을 명확히 파악할 수 있게 한다.
3. 재무 보고서 공개: 프로젝트의 재무 상태와 관련된 정기 보고서를 발행하여 자금 사용 내역, 수익, 비용 등을 공개한다. 이는 프로젝트의 재정 건전성을 확인할 수 있게 한다.
4. 리워드 및 인센티브 구조: 토큰 보유자에게 제공되는 리워드나 인센티브 구조를 명확히 정의하고, 모든 보상 내역을 공개하여 투명성을 높인다.

이를 위해 DUNE과 같은 블록체인 분석 플랫폼을 활용할 수 있다. 이 플랫폼은 프로토콜의 거래 내역, 유동성 풀, 대출 및 차입, Yield Farming, NFT 거래 및 발행, 소유권 및 시장 데이터를 시각화하여 제공함으로써 이용자의 편의를 증진하고 투명성을 높일 수 있다.

위와 같은 방안들은 커뮤니티 구성원들이 프로토콜의 재무 관리에 적극 참여할 수 있게 하며, 투명한 재무 관리를 통해 커뮤니티의 신뢰를 강화할 수 있다.

Table 7을 보면, 네 가지 평가 가이드라인을 각 탈중앙화 금융(DeFi) 프로토콜에 적용한 결과를 1~5점 척도로 표시했다, 점수가 높을수록(5점) 탈

Table 7. Applying the Four Evaluation Guidelines to Each DeFi Protocol, the results are represented on a 1 to 5 scale, where higher scores (5 points) indicate closer to decentralization and lower scores (1 point) indicate further from decentralization:

Evaluation guidelines Topics	Evaluation Criteria	Evaluation Parameter	FEI	DAI	Tether	WBTC	Lido	Uniswap	Synthetix
1. The importance of incentivising engagement	Existence of User Incentive Structures	Providing incentives to highly active users / liquidity providers for example airdrops.	4	5	3	3	4	5	5
	Provision of Community Participation Spaces	Operation of community channels such as official forums, Discord, Telegram, Reddit	5	5	3	2	3	5	4
	Provision of Educational Materials and Promotion	Providing user guides, tutorials, webinars, AMA (Ask Me Anything) sessions	5	5	5	3	5	5	5
2. Governance measures for decentralisation of authority	Distribution and Use of Governance Tokens	Governance token voting, transparent proposal process	0	5	1	5	5	5	5
	Use of Multisignature Wallets and Various Governance Models	Multisignature for decisions, diverse governance models (Quadratic Voting, Liquid Democracy)	5	5	5	5	5	5	5
	Operation of DAOs	Operation by Decentralized Autonomous Organizations (DAOs), use of smart contracts	5	5	1	5	5	5	5
3. Technical measures for decentralising authority	Assignment of 'Roles' to Specific EOA Addresses	Existence of roles like validators and guardians	1	1	1	1	1	5	5
	Use of Proxy Patterns	Existence of proxy contracts that dynamically reference addresses of logic contracts	5	1	3	3	1	5	1
4. Transparency and democracy in financial management	Financial Management by Community Voting	Introduction of community treasury, blockchain recorded fund usage, community voting for major financial decisions	4	5	1	5	5	5	5
	Transparency of Circulation and Holdings	Real-time information on total supply, circulation, and holdings of tokens	2	5	5	5	4	5	5
	Disclosure of Financial Reports	Regular financial reports on fund usage, revenue, expenses	2	5	5	5	4	5	5
	Reward and Incentive Structures	Defined reward/incentive structures	2	5	5	5	4	5	5
Total			40	52	38	47	46	60	55

중앙화 수준이 높고, 점수가 낮을수록(1점) 탈중앙화 수준이 낮음을 나타낸다. 저자는 가능한 한 객관적으로 각 항목을 조사하여 점수를 부여했지만, 이러한 평가는 주관적일 수 있으므로 각 프로토콜에 해당 항목에 대한 증빙을 요청하고 이를 바탕으로 객관적인 평가 요소를 세분화하여 평가하는 것이 적절하다. 또한, 각 평가 요소의 중요도에 따라 점수를 차등 배정하는 것도 필요하지만, 본 논문의 목적은 DeFi 프로토콜의 탈중앙화 여부를 판단하는 데 있지 않기 때문에 이를 적용하지 않았다.

평가 결과, Tether와 같은 중앙화 스테이블코인은 가장 낮은 탈중앙성을 보였으며, Uniswap과 Synthetix 같은 DEX는 가장 높은 탈중앙성을 보였다. 특히, Uniswap은 중앙화된 객체나 컨트랙트의 업그레이드 가능성이 없는 DeFi의 정의와 가장 적합한 프로토콜로 평가됐으며, Synthetix는 동일한 DEX 프로토콜로 분류되지만 프록시 패턴을 이용한 컨트랙트 업그레이드 기능을 제공함으로써 탈중앙성을 일부 포기하고 편의성을 택했다.

이처럼 다양한 DeFi 프로토콜은 각자의 특성과 차별성을 가지고 운영되며, 미세한 차이도 향후 이용자에게는 큰 위협이 될 수 있다. 따라서 이러한 평가 가이드라인을 규제에 적용하여 각 프로토콜을 평가함으로써, 탈중앙화 금융 서비스의 규제 필요성을 검토하고자 한다. 이를 통해 가상 자산 이용자의 자산을 보호하고, 중앙화된 프로토콜에는 가상 자산 커스터디 서비스 제공자 수준의 규제를 적용하여 시장의 건전성을 확보하고자 한다.

VII. 결 론

본 논문은 현재 시점에서 가상자산 커스터디 서비스를 분석하고, 관련 법률적 트렌드를 조사하여 커스터디 서비스와 유사하지만 규제의 적용을 받지 않아 이용자 자산 보호가 불분명한 영역을 DeFi(탈중앙화 금융)로 식별했다. 이를 통해 가상자산 커스터디 서비스의 규제적 측면, 가상자산의 특성, 그리고 DeFi 서비스의 특수성을 비교 분석하여, 가상자산

커스터디 서비스와 DeFi의 잠재적 커스터디 서비스 가능성을 평가하는 것을 본 논문의 결론으로 삼고자 한다.

이를 위해 가상자산 커스터디 서비스 평가 가이드라인을 작성하고, 서비스의 탈중앙화 정도를 파악할 수 있도록 했다. 평가 가이드라인을 통해 DeFi 서비스가 본래의 정의와 맞지 않게 운영되는 경우, 그에 대한 추후 규제 가능성에 대한 의문점을 제기하고 그 허점을 밝혀내는 것을 목표로 한다.

이 연구는 가상자산 커스터디 서비스와 DeFi 서비스의 안전성을 강화하고, 규제와 탈중앙화의 균형을 맞추는 데 기여하고자 한다. 이는 시장의 무결성을 유지하고 윤리적 비즈니스 관행을 강화하며, 가상자산 수탁 환경에 내재한 허점을 식별하는 데 도움이 될 것이다. 궁극적으로, 이러한 노력이 디지털 자산 생태계의 신뢰성과 안정성을 높이고, 투자자와 사용자 모두에게 보다 안전한 금융 환경을 제공하는 데 기여할 것으로 기대된다.

References

[1] EUR-Lex, MiCa Regulation 2023/1114, https://eur-lex.europa.eu/eli/reg/2023/1114/oj, Sep. 2023.

[2] Dirk A. Zetzsche et al. The Markets in Crypto-Assets regulation (MiCA) and the EU digital finance strategy, European Banking Institute Working Paper Series, no. 2020/77, Nov. 2020.

[3] Coinbase, User Agreement(Coinbase), https://www.coinbase.com/legal/user_agreement/united_states, July 2024.

[4] Vincenzo Di Nicola et al. Resilient Custody of Crypto-Assets, and Threshold Multisignatures, Mathematics 8, no. 10, Oct. 2020.

[5] Zakwan Jaroucheh and Baraq Ghaleb, Crypto Assets Custody: Taxonomy, Components, and Open Challenges, 2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), pp. 1-6, May 2023.

[6] Vasudha Rani Vaddadi et al. Exploiting Cyber Threats And Protecting Cryptocurrencies Toward Bitcoin Exchanges. 2023 5th Bienn. Int. Conf. Nascent Technol. Eng. Oct, pp. 1-6, Jan. 2023.

[7] Apolline Blandin et al. Global cryptoasset regulatory landscape study, University of Cambridge Faculty of Law Research, no. 23/2019, Sep. 2019.

[8] Lekkas, Nikolaos, Legal Aspects of the Custody of Digital Assets, International Hellenic University, Jun. 2020.

[9] Jason Scharfman, Operational Due Diligence on Cryptocurrency and Digital Asset Funds, The Journal of Alternative Investments, vol. 24, no. 3, pp. 44-50, 2022.

[10] Dennis Chu, Broker-dealers for virtual currency: Regulating cryptocurrency wallets and exchanges, Columbia Law Review, vol. 118, no. 8, pp.2323-2359, Dec. 2018.

[11] Mohammad Belayet Hossain, Acquiring an awareness of the latest regulatory developments concerning digital assets and anti-money laundering, Journal of Money Laundering Control, vol. 26, pp. 1261-1268, Jan. 2023.

[12] Hossein Nabilou, The Law and Macroeconomics of Custody and Asset Segregation Rules: Defining the Perimeters of Crypto-Banking, Amsterdam Law School Research Paper, no. 2022-09, Apr. 2022.

[13] Eva Micheler, Custody chains and asset values: why crypto-securities are worth contemplating, The Cambridge Law Journal, vol. 74, pp. 505-533, Aug. 2015.

[14] Ugo Malvagna and Filippo Sartori, Cryptocurrencies as' Fungible Digital Assets' within the Italian Legal

System: Regulatory and Private Law Issues, Italian LJ, vol. 8, no. 1, pp. 481-502, Sep. 2022

[15] Geoffrey Cone, et al. Digital assets and property rights in insolvency. Trusts & Trustees, vol. 27, no. 5, pp. 406 - 413, Oct. 2021.

[16] Matthias Lehmann and Matthias Haentjens. The Law Governing Secured Transactions in Digital Assets. Blockchain and Private International Law. Brill, Feb. 2023.

[17] Holly Smith, SEC guidance on broker-dealer custody of digital asset securities, Journal of Investment Compliance, vol. 22, no. 2, pp. 189-194, Jun. 2021.

[18] Dirk A Zetzsche, el al. The Markets in Crypto-Assets regulation (MiCA) and the EU digital finance strategy, Oxford University Press, vol. 16, pp. 203-225, Nov. 2020.

[19] Susan Alkadri, Defining and Regulating Cryptocurrency: Fake Internet Money or Legitimate Medium of Exchange? Duke L. & Tech. Rev., vol. 71, no. 1, pp. 71-98, Dec. 2018.

[20] Adam Zuckerman, Insuring crypto: The birth of digital asset insurance, U. Illinois. JL Tech. & Policy, Dec. 2020.

[21] Ethereum, Ethereum Whitepaper, https://ethereum.org/en/whitepaper/, Mar. 2024.

[22] Fabian Schär, Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets, Federal Reserve Bank of St. LouisReview, pp.153-174, Apr. 2021.

[23] Lennart Ante, et al. A Systematic Literature Review of Empirical Research on Stablecoins. FinTech, vol. 2, no. 1, pp. 34 - 47, Jan. 2023.

[24] Sam Werner, et al. SokDecentralized finance (defi), In Proceedings of the 4th ACM Conference on Advances in Financial Technologies (AFT '22), pp. 30-46, Sep. 2022.

[25] Giulio Caldarelli, Wrapping trust for interoperability: A preliminary study of wrapped tokens, Information, vol. 13, no. 1, Dec. 2021.

[26] Richard K. Lyons and Ganesh Viswanath-Natraj, What keeps stablecoins stable? Journal of International Money and Finance, vol. 131, Mar. 2023.

[27] Babu Pillai et al. Cross-Blockchain Technology: Integration Framework and Security Assumptions, IEEE Access, vol. 10, pp. 41239 - 41259, Apr. 2022.

[28] Ilham A. Qasse, et al. Inter Blockchain Communication: A Survey, ArabWIC 2019: Proceedings of the ArabWIC 6th Annual International Conference Research Track, no. 2, pp. 1-6, Mar. 2019.

[29] Matthias Lehmann, et al. Staking Your Crypto: What are the Stakes?, J. Bus. & Tech. L., vol. 19. no. 3, pp. 53-103, Jan. 2023.

[30] Kose John, et al. Equilibrium Staking Levels in a Proof-of-Stake Blockchain, SSRN, Nov. 2021.

[31] Siddharth Bhambhwani, Governing Decentralized Finance (DeFi), SSRN, Jul. 2023.

[32] Hyoungsung Kim, et al. Perpetual Contract NFT as Collateral for DeFi Compos-ability, IEEE Access, vol. 10, pp. 126802-126814, Dec. 2022.

[33] Makridis, Christos A. et al. The rise of decentralized cryptocurrency exchanges: Evaluating the role of airdrops and governance tokens, Journal of Corporate Finance, vol. 79, Apr. 2023

〔34〕 Rocha, M. D. A., and Trevisan, N. M., Marketing nas mídias sociais sociais, Saraiva Educação, Feb 2020.
〔35〕 Gontijo, L. H. O., and D'Leon de Almeida, I., Decentralized Finance (DeFi) A study of how decentralized finance positions itself in marketing in the eyes of users, International Journal of Business Marketing, vol. 8, no. 2, pp. 4-14. Feb. 2024.
〔36〕 Anker-Sørensen, Linn and Zetzsche, Dirk Andreas, From Centralized to Decentralized Finance: The Issue of 'Fake-DeFi', SSRN, Dec. 2021.
〔37〕 Fabian Schär, Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets, Federal Reserve Bank of St. Louis Review 2021, pp. 153-174, Feb. 2021.
〔38〕 Barbereau, Tom et al. Decentralised Finance's timocratic governance: The distribution and exercise of tokenised voting rights, Technology in Society, vol. 73, May 2023.
〔39〕 Chao, Chian-Hsueng, et al. The Study of Decentralized Autonomous Organization (DAO)in Social Network, MISNC '22: Proceedings of the 9th Multidisciplinary International Social Networks Conference, pp. 59-65, Nov. 2022.
〔40〕 Our Network, Governance Extractible Value, https://ournetwork.substack.com/p/our-network-deep-dive-2, Apr. 2021.
〔41〕 Taherdoost, Hamed, Non-Fungible Tokens (NFT): A Systematic Review, Information, vol. 14, no. 1, Dec. 2022.

〈저자소개〉

이 형 근 (Hyunggeun Lee) 정회원
2019년 12월: Baruch, City University of New York 정보 시스템&통계학과 학사
2022년 9월~현재: 고려대학교 금융보안학과 석사과정
2023년 9월~현재: 온더 Blockchain Engineer
〈관심분야〉 블록체인, Layer 2 솔루션, 개인정보보호, 침해사고대응

주 문 호 (Moonho Joo) 종신회원
2014년 8월: 고려대학교 정보통신대학 컴퓨터공학과 공학학사
2014년~2017년: 고려대학교 정보보호연구원(사이버보안정책센터) 책임연구원
2017년~2020년: 고려대학교 정보보호연구원(사이버보안정책센터) 전문연구요원
2020년 8월: 고려대학교 정보보호대학원 정보보호학과 공학박사
2020년~2021년: 고려대학교 정보보호대학원(정보보호연구원) 연구교수
2021년 8월~현재: 개인정보보호위원회 사무관
〈관심분야〉 개인정보보호정책, 정보보안, 융합기술보안, 사이버법률

임 지 훈 (Jihun Lim) 학생회원
2016년 3월: Waseda University 법학부 법학사
2020년 8월: 고려대학교 정보보호대학원 정보보호학과 공학석사
2024년 8월: 고려대학교 정보보호대학원 정보보호학과 공학박사
〈관심분야〉 인공지능 보안, 데이터 보안

김 범 중 (Beomjoong Kim) 학생회원
2014년~2021년: 고려대학교 물리학과
2021년 3월~현재: 고려대학교 정보보호대학원 정보보호학과 석박사통합과정
〈관심분야〉 디지털 자산 보안, 블록체인, 프라이버시

전 기 석 (Kiseok Jeon) 학생회원
2017년 6월: Shanghai jiaotong University Media and Editing 학사 졸업
2021년 9월~현재: 고려대학교 정보보호대학원 정보보호학과 통합과정
〈관심분야〉 정보보호, 시스템 소프트웨어 보안, 블록체인 마이닝 소프트웨어

심 준 식 (Junsik Sim) 정회원
2004년 12월: 오클라호마대학교 경제학 학사
2017년 7월: 고려대학교 정보보호대학원 빅데이터 응용 및 분석 석사
2020년 12월: 고려대학교 일반대학원 사이버국방학과 박사과정 수료
2015년~2019년: 딜로이트 안진회계법인 스타트업자문그룹 이사
2019년~2021년: 삼정KPMG 디지털금융본부 Director
2021년~2024년: 온더 대표이사
2024년~현재: 비온미디어 대표이사
2023년~현재: 고려대학교 정보보호대학원 겸임교수
〈관심분야〉 빅데이터, 블록체인, 정보보호

이 중 희 (Junghee Lee) 종신회원
2000년 2월: 서울대학교 컴퓨터공학과 공학학사
2003년 2월: 서울대학교 컴퓨터공학과 공학석사
2003년~2008년: 삼성전자, 연구원
2013년 2월: 조지아공과대학교 전자공학과 공학박사
2014년~2019년: University of Texas at San Antonio 교수
2019년~현재: 고려대학교 정보보호대학원 교수
〈관심분야〉 하드웨어 보안