korbit
Research

가상자산 커스터디의 미래

2025.09.26

테마

커스터디

관련 자산

가상자산

Cryptocurrency

작성자

최윤영 | Yoonyoung Choy

yoonyoung.choy@korbit.co.kr

김민승 | Minseung Kim

minseung.kim@korbit.co.kr

주요 자산 가격(2025.09.24)

BTC	
USD	$114,192
KRW	₩159,400,000
김치프리미엄	+2.18%

ETH	
USD	$4,240
KRW	₩5,919,000

가상자산 시대에 다시 쓰이는 커스터디의 정의

가상자산 커스터디는 전통 금융의 수탁 서비스와 유사하게 투자자 자산을 대신 보관·관리하지만, 자산의 본질과 소유권 증명 방식에서 뚜렷이 구별된다. 전통 금융자산은 중앙예탁기관(CSD)이나 명의개서대리인의 원장에 기명식으로 등록됨으로써 소유권이 보장되지만, 가상자산 커스터디의 핵심은 프라이빗 키 관리에 있으며 이를 위해 MPC·HSM·다중서명 등 다양한 보안 기술과 절차가 활용된다. 결국 가상자산 커스터디는 단순한 보관을 넘어 자산의 안전한 통제와 책임 구조를 설계하는 기반 인프라로 전통적 수탁과 성격이 상이하다.

가상자산 커스터디의 진화와 시장 재편

가상자산 커스터디는 기관 수요 확대에 따라 다이렉트 커스터디, 기술 제공자, 하이브리드 모델 등으로 발전해 왔다. Coinbase Custody는 규제 인가를 받은 적격 수탁 기관으로서 신뢰 기반의 전통적 수탁 서비스를 제공하며, Fireblocks는 MPC 인프라와 Wallet-as-a-Service를 통한 기술적 효율성을 제공한다. BitGo는 셀프 커스터디와 규제 수탁을 결합한 하이브리드 모델로 다중서명을 기반으로 안정성과 복구 가능성을 제공한다. 실제 서비스 영역에서는 경계가 점점 모호해지고 있으며, 전통 금융기관까지 가상자산 시장에 진입하면서 커스터디 시장은 점점 다양한 형태의 융합형 플랫폼으로 재편되고 있다.

가상자산 커스터디 시장의 네 가지 트렌드

가상자산 커스터디 시장은 디파이 연계 수익 창출, 크로스체인 자산 관리, RWA 편입에 따른 통합 역량, 전통 금융기관의 진입과 서비스 통합이라는 네 가지 축을 중심으로 진화하고 있다. Anchorage Digital, Coinbase Prime, Fireblocks 등은 스테이킹·온체인 접근·위협 탐지 등을 통해 디파이 게이트웨이 역할을 하고 있으며, 멀티체인 환경에서는 크로스체인 커스터디가 핵심 과제로 부상했다. 동시에 RWA 토큰화는 부동산·사모펀드 지분 등 실물자산의 디지털 권리를 기존 법률·등기·신탁 체계와 일치하도록 동기화해야 하는 복잡성을 수반한다. 전통 금융기관은 ETF 제도화와 기관 수요 확대를 계기로 M&A·합작법인 설립·플랫폼 개발을 통해 통합 관리 서비스를 구축하고 있다. 이 과정에서 시장은 전통 금융의 신뢰·규제 경험과 크립토 네이티브의 기술·민첩성이 결합되며 재편되고 있다. 궁극적으로 승자는 규제 준수·운영 안정성·신뢰와 투명성을 확보해 제도권 금융 인프라 수준으로 자리매김한 기업과 국가가 될 것이다.

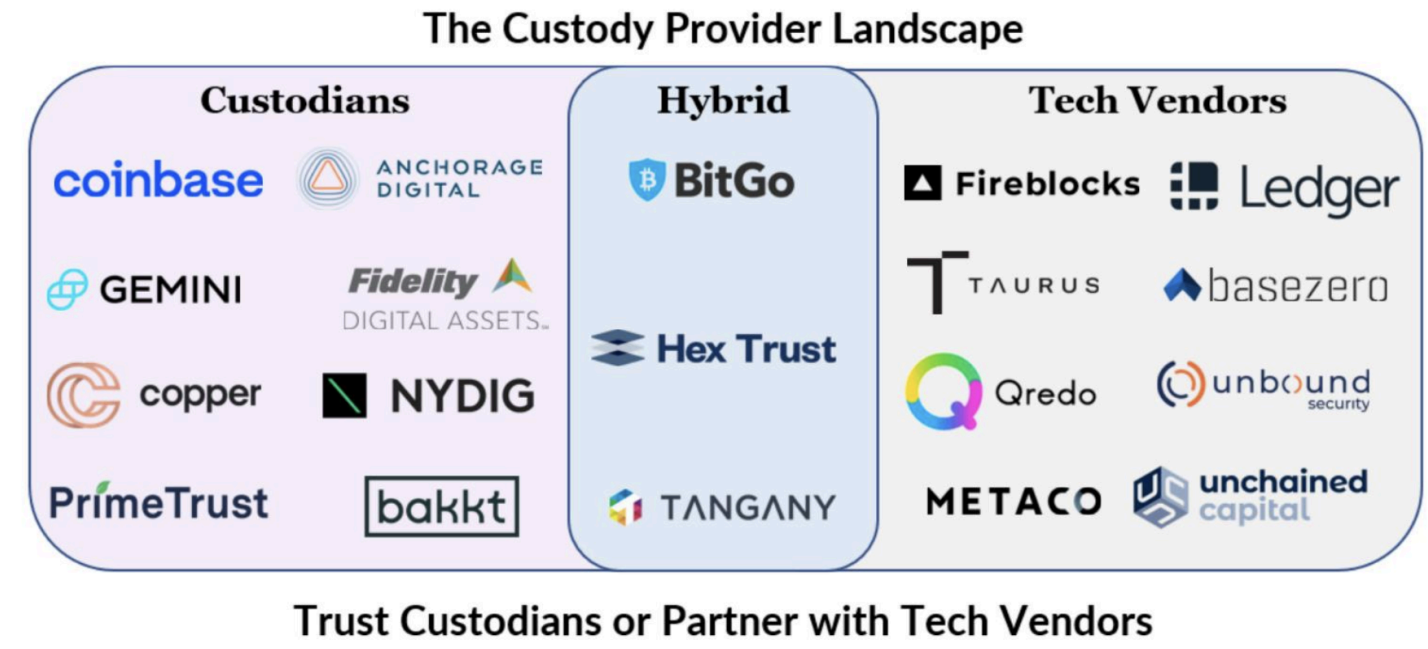
가상자산 시장이 본격적인 성장 궤도에 진입하면서 자산을 안전하게 보관하고 관리하는 '커스터디(custody)'의 중요성이 그 어느 때보다 부각되고 있다. 가상자산 커스터디는 단순히 전통 자산 수탁의 디지털 전환을 의미하지 않는다. 전통 자산과 가상자산 커스터디 간에는 근본적인 차이가 있으며, 커스터디는 단순한 보관 기능을 넘어, 기관투자자들이 가상자산 생태계에 안전하게 진입하고 다양한 온체인 활동을 수행할 수 있도록 지원하는 핵심 운영 인프라로 자리매김하였다. 이제 커스터디는 '디지털 금고'의 기능 뿐만 아니라 가상자산 생태계 전반의 신뢰·확장성을 지탱하는 인프라로 기능하고 있는 것이다.

이와 함께 시장의 수요가 고도화되면서 서비스 모델 또한 다변화되고 있으며, 이를 가능하게 하는 보안 기술과 운영 아키텍처 역시 고도의 전문성을 요구한다. 여기에 비트코인 현물 ETF 승인을 필두로 제도권과의 접점이 확대되면서 커스터디의 역할은 기술, 보안 인프라를 넘어 규제 신뢰 확보와 투자자 보호의 핵심 기제로도 재정의되고 있다.

본 보고서는 이러한 인식에 기반하여 가상자산 커스터디의 개념과 구조를 정리하고, 전통 커스터디와의 차별점, 산업 생태계의 변화 양상, 그리고 주요 사업자와 규제 환경의 상호작용을 다층적으로 고찰하고자 한다. 나아가 커스터디 산업이 향후 온체인 금융의 인프라로 자리잡기 위해 어떤 기술적, 제도적 조건이 요구되는지를 조망하여 미래 전략의 방향성을 제시하고자 한다.

Figure 1: 가상자산 커스터디 지형도

출처: The Block Research[1]



[1] Cahill, A. (2021). "An Evaluation of Digital Asset Custody Solutions". *The Block Research*.

가상자산 커스터디의 개념과 범위

한때 소수 개인투자자들의 영역으로 여겨졌던 가상자산은 이제 기관투자자들의 포트폴리오 구성에 본격적으로 편입되고 있다. 이에 발맞춰 전통 금융기관—은행, 자산운용사, 증권사, 브로커-딜러, 수탁기관, 핀테크 등—역시 이 흐름에 합류하며, 기관 수준의 크립토 상품과 서비스를 경쟁적으로 출시하고 있다. 이러한 변화는 가상자산을 기반으로 한 토큰화 경제(tokenized economy)의 부상을 가속화하고 있으며, 그 중심에는 커스터디라는 핵심 기반시설이 자리하고 있다.

전통 자산 커스터디 vs. 가상자산 커스터디

전통 금융시장에서 커스터디는 투자자의 금융 자산을 제3자인 수탁기관이 대신 보관하고 관리해주는 서비스를 의미한다. 주요 대상 자산은 주식, 채권과 같은 유가증권이며 수탁기관은 투자자의 대리인으로서 자산의 보관, 매매에 따른 수취 및 결제, 배당금 및 이자 수령과 같은 권리 보전, 의결권 행사 대리 등 광범위한 업무를 수행한다. 그리고 그 핵심은 중앙화된 기관이 신뢰를 바탕으로 투자자의 법적 권리를 안전하게 보호하고 관리하는 데 있다. 수탁기관은 신뢰할 수 있는 보관 시스템과 절차를 통해 자산을 보호하며, 투자자의 자산에 대한 접근과 관리를 제한된 범위 내에서 수행함으로써 보안과 안전성을 확보한다.

가상자산 커스터디는 전통적인 커스터디의 개념을 비트코인, 이더리움과 같은 가상자산에 적용한 서비스이다. 그러나 대상 자산의 성격상 커스터디의 중심 기능은 전통적 수탁과는 다른 방식으로 정의된다.

자산의 본질과 소유권 증명 방식: 전통 금융과 가상자산 커스터디의 가장 큰 차이는 자산 그 자체의 본질과 소유권을 증명하는 방식에서 비롯된다. 이는 기술적인 특성 뿐만 아니라 리스크 관리와 규제 방향성까지 결정하는 핵심 요소로 작용한다.

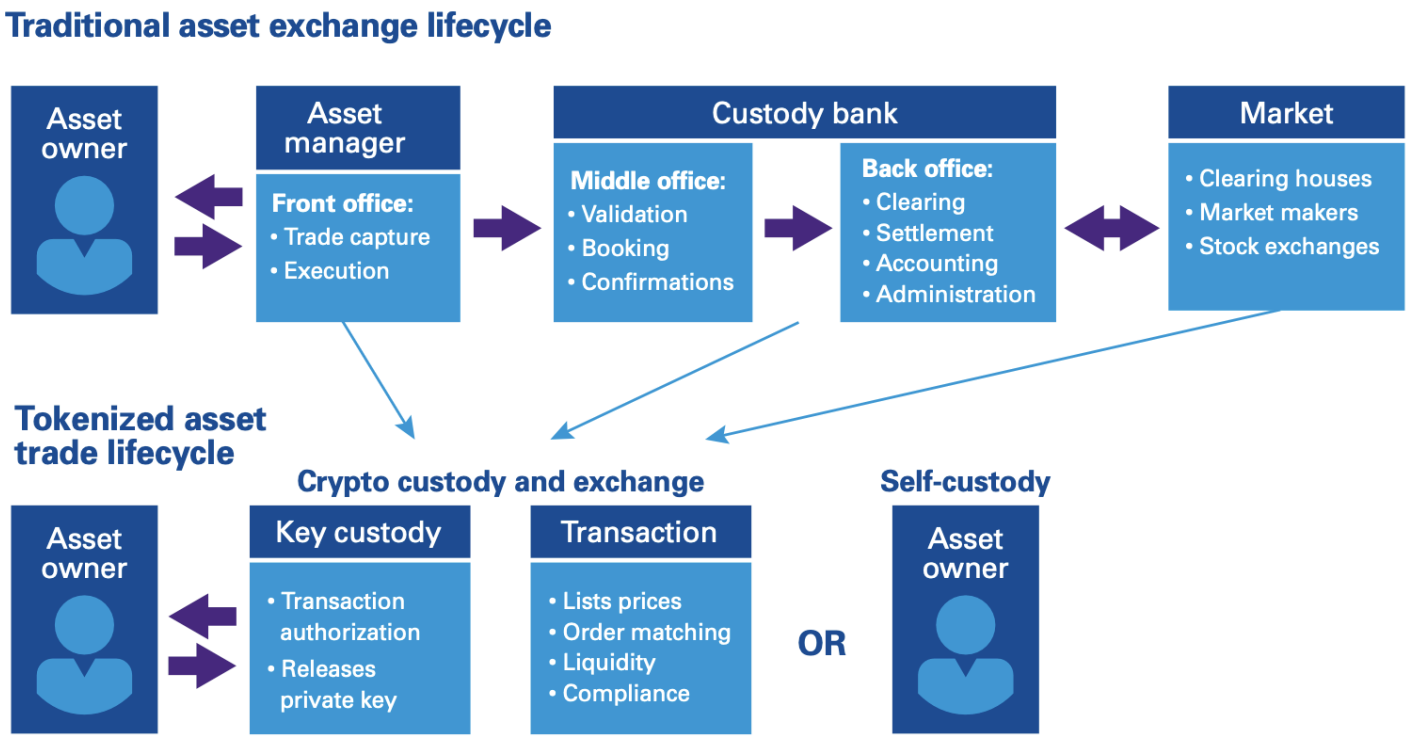
전통 금융자산, 예컨대 주식이나 채권은 '기명식 증권(registered securities)[2]'의 형태를 띤다. 자산의 소유권은 특정 개인이나 법인의 이름으로 중앙화된 원장(ledger)에 법적으로 등록됨으로써 효력을 갖는다. 한국예탁결제원(KSD)와 같은 중앙예탁기관(CSD)이나 명의개서대리인이 이 원장을 관리하며, 소유권 이전은 이들의 기록을 변경함으로써 완료된다. 즉, 전통 금융에서 '소유'란 법률 시스템과 신뢰받는 제3자(intermediary)에 의해 보장받는 법적 권리이다. 커스터디 서비스는 이러한 법적 권리를 고객을 대신하여 안전하게 관리하고 행정절차를 처리하는 역할을 수행한다.

[2] Keele, T., Krajecki, M., Ternullo, S., Wyner, S. (2020). "Cracking Crypto Custody". *KPMG*.

반면 비트코인이나 이더리움 같은 가상자산은 '디지털 무기명 증서(digital bearer instruments)'의 특성을 갖는다. 이는 실물 현금이나 무기명 채권과 같은 자산을 물리적으로 소지한 자가 소유권을 갖는 것과 유사한 원리가 디지털 환경에서 구현된 것이다. 가상자산의 소유권은 중앙화된 원장에 이름이 기록되는 것이 아니라, 해당 자산에 접근하고 거래를 승인할 수 있는 '프라이빗 키(private key)'를 누가 보유하느냐에 따라 결정된다.

Figure 2: 전통 금융자산 vs 가상자산의 거래 프로세스 비교

출처: KPMG



커스터디 관리 방법: 가상자산의 저장 및 전송은 암호화 키(cryptographic key)를 통해 구현된다. Figure 3에서 퍼블릭 키(public key)는 말 그대로 공개된 키로, 특정 퍼블릭 주소(public address)에 매핑된다. 이 주소는 영문자와 숫자가 조합된 문자열 형태이며, 이 주소를 알고 있는 누구나 해당 주소를 제어하는 개인 또는 기관에게 자금을 전송할 수 있다.

프라이빗 키(private key)는 비공개 키로, seed phrase[3]에서 파생되며 이를 통해 퍼블릭 키가 생성되고 다시 퍼블릭 주소(public address)로 변환된다. 중요한 점은 프라이빗 키를 통제하는 것이 곧 해당 퍼블릭 주소에 존재하는 가상자산을 통제하는 것과 동일하다는 사실("Your keys, your bitcoin. Not your keys, not your bitcoin.")이다.

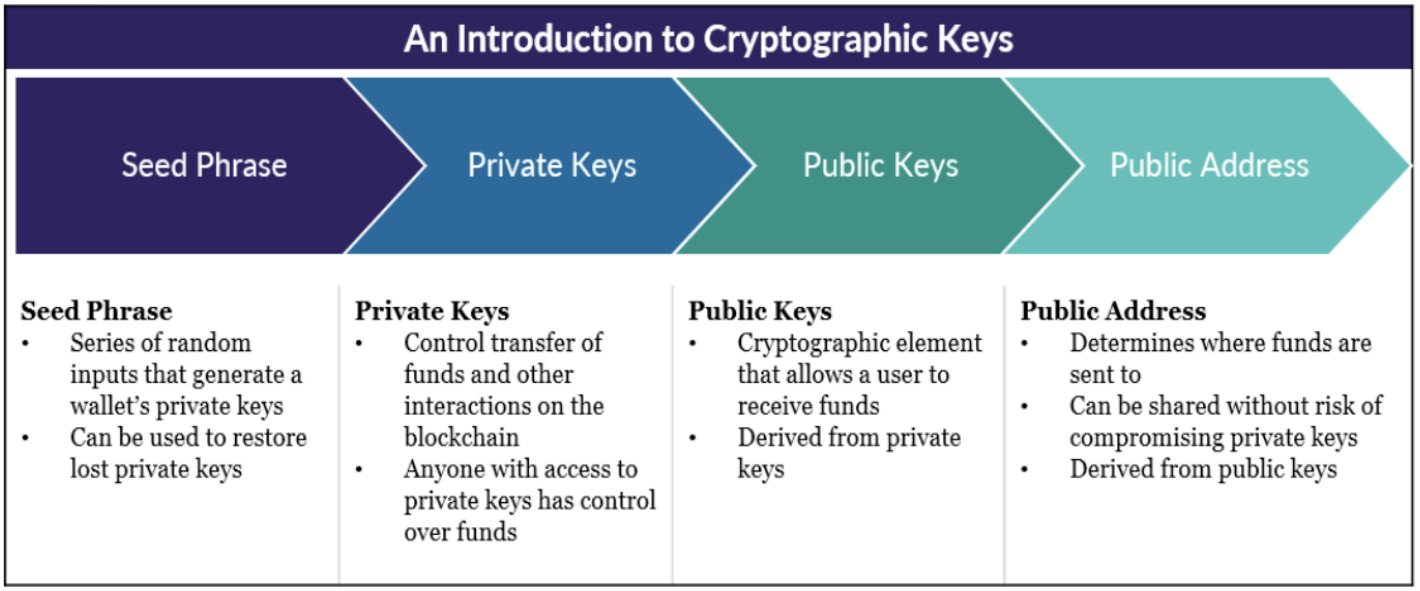
[3] 'seed phrase'는 지갑을 분실·손상하거나 복구가 필요할 때 접근을 되찾는 데 필수적인 복구 키이다. 일반적으로 무작위로 생성된 12개 이상의 단어로 구성되며, 지갑의 마스터 키 역할을 한다(출처: Fitzgerald, D., Brewin, P., Wang, L., Tao, J., Hayes, M., Clevenot, A. (2023). "State of Digital Asset Custody", *PwC*.).

따라서 프라이빗 키를 어떻게 관리하느냐가 무엇보다 중요하다고 볼 수 있다. 가상자산 산업의 모든 참여자는 정도의 차이는 있어도 프라이빗 키 관리와 관련된 리스크에 노출될 수 밖에 없다. 키 관리가 허술하면 최악의 경우 막대한 자산 손실로 직결될 수 있다.

가상자산 수탁 기관의 보안 체계, 운영 절차, 서비스 전반에 대한 지속적인 점검, 테스트, 개선이 중요한 이유가 바로 여기에 있다. 특히 지원하는 블록체인의 수가 늘어날수록 복잡성과 리스크도 함께 증가하므로 이를 완화하기 위해 MPC(Multi-Party Computation, 다자간 연산), HSM, 다중서명(multisig) 기술[4] 등이 활용되며, 접근 통제 등 다양한 보안 절차도 병행된다.

Figure 3: 가상자산 저장·전송과 암호화 키

출처: The Block Research



거래의 완결성: 자산의 본질과 소유권의 차이는 거래의 특성에도 변화를 가져온다. 전통 금융 시스템에서는 거래 과정에 오류가 발생하거나 잘못된 거래가 일어났을 경우, 이를 되돌릴(reversibility) 수 있는 장치가 마련되어 있다. 예컨대 신용카드 부정 사용이 발생하면 카드사에 연락하여 거래를 취소하고 피해 금액을 보상받을 수 있다. 이는 은행, 카드사, 지급결제 중개기관 등 신뢰받는 중개자들이 거래 검증 및 취소 권한을 가지고 있기 때문에 가능하다.

[4] MPC(Multi-Party Computation)는 프라이빗 키가 한 번도 완성된 형태로 생성·보관되지 않고 각 참여자가 가진 부분 정보를 이용해 공동으로 연산을 수행하는 기술이며, HSM(Hardware Security Module)은 키 생성·저장·서명 작업을 전용 하드웨어 장치에서 수행해 외부 노출을 차단하는 장치, 다중서명(multisig)은 거래 승인 시 다수의 독립 서명을 요구해 단일 키 유출로 인한 자산 탈취를 방지하는 방식이다(출처: The block Research. (2021). "Institutional Custody for Digital Assets: A Primer").

그러나 블록체인 상에서 이루어지는 가상자산 거래는 한번 네트워크의 검증을 거쳐 블록에 기록되고 나면 사실상 되돌리는 것이 거의 불가능하다. 이러한 거래 완결성 또는 비가역성(immutability)은 블록체인 기술의 핵심 장점 중 하나로 거래의 신뢰도를 높이고 중개자의 필요성을 줄여주는 동시에, 단 하나의 실수나 보안상의 허점이 회복 불가능한 손실로 이어질 수 있다는 리스크를 내포하고 있다. 따라서 가상자산의 저장 방식과 거래 실행 방법을 통제하는 '가상자산 커스터디'는 산업 운영자에게 중요한 고려 사항이 될 수밖에 없으며, 거래의 비가역성과 키 기반의 소유권 구조는 프라이빗 키가 단순한 인증 수단이 아니라 자산 그 자체의 소유를 의미한다는 점을 명확히 한다. 이러한 구조는 커스터디가 단순 보관서비스를 넘어 자산을 안전하게 관리·통제할 권리에 대한 책임 구조를 설계하는 행위임을 보여주며, 가상자산 커스터디가 전통 수탁과 본질적으로 구별되는 핵심 이유로 작용한다.

Figure 4: 가상자산 커스터디 vs. 전통 자산 커스터디

출처: 코빗 리서치

구분	전통 자산 커스터디	가상자산 커스터디
자산의 본질	중앙화된 원장에 기록된 법적 권리 증서	분산원장에 기록된 암호학적 무기명 증서
소유권 증명	중앙화된 원장 기록	프라이빗 키의 배타적 보유
핵심 수탁 기능	법적 권리 대리 행사 및 보관	프라이빗 키의 기술적/물리적 보호
이전 및 결제	다수 중개자, 영업일 기준	P2P, 24/7 실시간
주요 리스크	거래상대방 리스크, 결제 리스크	기술적 리스크, 운영 리스크, 거래상대방 리스크[5]

[5] 가상자산 커스터디에서의 거래상대방 리스크는 자산을 보관·거래하는 과정에서 거래소·커스터디 업체·거래 파트너 등이 의무를 다하지 못하거나(결제 불이행, 고객 자금 운용), 보안 취약성으로 인해 자산 손실이 발생할 수 있는 위험을 의미한다. 전통 금융 커스터디 역시 결제 지연, 인프라 장애, 운영 실패 등 상대방 의존 위험을 안고 있다는 점에서는 유사하지만, 차이는 전통 금융이 중앙화된 시장 인프라에 기초한 위험이 큰 반면, 가상자산은 프라이빗 키 관리·스마트 컨트랙트·사이버 보안 같은 기술적 요인에 더 크게 노출된다는 데 있다(출처: Global Custody Pro, "Digital Asset Custody vs Traditional Global Custody", November 09, 2024.)

가상자산 커스터디 유형과 대표 사례

전통 금융에서 자산의 안전한 수탁(custody)은 투자자 신뢰의 핵심 기반이 되어왔다. 가상자산 영역도 초기에는 개인이 직접 키를 관리하는 셀프 커스터디(자체 보관)에서 출발했는데, 이는 하드웨어 지갑이나 소프트웨어 지갑을 통해 사용자가 seed phrase 등을 직접 보관하는 방식을 말한다. 셀프 커스터디는 사용자가 자산에 대해 완전한 통제권을 갖는다는 장점이 있으나, 반대로 키 분실·사이버 공격·보관 부주의와 같은 위험에 노출될 경우 복구가 불가능한 손실로 이어질 수 있다는 한계가 있다.

2016년 이후부터는 기관용 콜드월렛·보안 인프라를 갖춘 기관형 커스터디가 등장했다. 그리고 2020년부터는 디파이·메타버스·게임 등 웹3 확장과 함께 기관들이 다양한 온체인 활동(예: DeFi 참여)을 원스톱으로 지원받을 수 있는 단계로 진입하고 있다. 이러한 흐름 속에서 고액자산가와 패밀리오피스는 셀프 커스터디 대신 보안·거버넌스·보험이 갖춰진 제3자 커스터디를 선호하는 추세다. 더블록 리서치(각주 3 참조)에 따르면 제3자 커스터디는 크게 다이렉트 커스터디, 기술 제공자, 하이브리드로 구분된다[6].

다만 이러한 구분은 기업 유형을 기준으로 한 단순화된 틀에 가깝고 실제 서비스 제공 형태에서는 경계가 명확하지 않다는 한계가 있다. 특히 기술제공자와 하이브리드 모델은 기업에 따라 기능과 역할이 상당 부분 중첩되며 고객이 이용하는 서비스 관점에서는 양자를 정확히 구분하기 어려운 경우가 많다. 따라서 이하의 구분은 설명을 돕기 위한 틀로 이해할 필요가 있으며, 실제 시장에서는 경계가 훨씬 더 모호하다는 점을 감안할 필요가 있다.

Figure 5: 가상자산 커스터디 방식 비교

출처: PwC, 코빗 리서치

	제3자 커스터디		셀프 커스터디	
구분	**가상자산 수탁업체**	**거래소 지갑**	**하드웨어 지갑**	**소프트웨어 지갑**
거버넌스	MPC	거래소 정책에 따름	Seed phrase, 비밀번호	Seed phrase, 비밀번호
운영방식	24/7 기관급 MPC, REST API 제공, 정책 필터 적용	거래소가 관리	사용자가 직접 관리	사용자가 직접 관리
관리 수수료	있음	없음	없음	없음
리스크	거래상대방 리스크 (수탁기관 부실 등)	해킹, 규제 리스크	키 분실 (부적절한 보관시)	키 분실, 사이버 공격

[6] Reyes, C. (2021). “Institutional Custody for Digital Assets: A Primer”. *The Block Research.*

다이렉트 커스터디

다이렉트 커스터디(direct custody, 예: 코인베이스 커스터디)는 가장 전통적인 형태의 커스터디로 고객의 가상자산을 직접 보관하고 프라이빗 키를 관리하는 역할을 수행한다. 이들은 자산 안전 보관 및 운영상 통제에 책임을 지며, 수탁 자산 규모를 기준으로 일정 비율의 수수료를 부과하거나 거래 및 인출 수수료 등으로 수익을 창출한다. 이러한 구조는 전통 금융의 아웃소싱 모델과 유사하다. 즉, 기관이 자체적으로 인프라를 구축하고 전문 인력을 확보하여 관련 하드웨어와 소프트웨어를 직접 운용하는 대신, 이미 전문성을 갖춘 커스터디 업체에 위탁함으로써 초기 비용과 내부 리스크를 절감할 수 있다.

특히 일부 기관투자자는 규제에 따라 반드시 라이선스를 보유한 수탁기관(custodian)에게 자산을 보관해야 한다. 예컨대 미국의 「1940년 투자자문법(Investment Advisers Act of 1940)」은 고객 자금을 보관하는 자문사가 해당 자산을 브로커-딜러, 은행, 또는 적격 수탁 기관(qualified custodian)에게 위탁하도록 규정한다(Rule 206(4)-2). 이러한 구조는 규제 요건을 충족하는 동시에 내부 통제 리스크를 완화하고, 고객 자산을 자문사 자산과 명확히 분리하여 이해 상충이나 운영 리스크를 최소화하는 효과를 가진다.

가상자산 시장에 처음 진입하는 기관투자자에게는 다이렉트 커스터디가 유용한 선택일 수 있다. 초기에는 자산 규모도 작고, 직접 인프라를 구축하기에는 비용과 리스크 부담이 크기 때문에 이런 상황에서 외부 전문 커스터디 기관을 활용하면 초기 진입 단계에서의 불필요한 시스템 구축 비용과 운영 리스크를 피할 수 있어 경제적이고 효율적인 대안이 된다. 또한 통제 프레임워크가 이미 갖춰져 있다는 점에서 안정적이기도 하다.

다만 다이렉트 커스터디 모델에도 한계는 존재한다. 일부 대형 기관의 경우, 상대적으로 작은 규모의 핀테크 스타트업에 해당 자산을 위탁하는 것이 오히려 위험 요소로 작용할 수 있다. 이들은 내부적으로 인력과 시스템을 구축해 리스크를 직접 관리하는 편이 더 안정적이라고 판단할 수 있으며, 특히 고빈도 거래(high-frequency trading)나 초저지연 실행 속도가 핵심인 전략을 구사하는 기관 입장에서는 외부 커스터디를 거치며 발생하는 자산 전송, 보안 승인 절차 등의 지연(latency)이 제약으로 작용할 수 있다[7].

[7] TechMag. (2025) “The Function of Latency in Cryptocurrency Data”.

기술제공자 및 하이브리드 제공자

기술제공자(Technology Providers)는 고객이 프라이빗 키를 제3자에게 넘기지 않고도(i.e. 비수탁형 구조) 자산을 안전하게 보관할 수 있도록 소프트웨어·하드웨어 솔루션을 제공한다. MPC나 다중서명을 활용해 고객과 공동으로 자산을 관리할 수 있도록 설계되며, 단일 장애점(single point of failure)을 줄이는 특징이 있다[8]. 법적 수탁자가 아니기 때문에 엄격한 규제 의무에서는 비교적 자유로우나, 자산 보호의 최종 책임은 고객에게 있다. 다만 고객 편의를 위해 백업 키, 재해 복구 기능, 보험 연계 등 보조적 안전장치를 제공하기도 한다. 광범위한 자산 지원, 보안 네트워크, 구독료·서비스 이용료(outgoing transaction amount) 기반 수익 모델 등을 통해 경쟁력을 확보하지만, 멀티체인 환경에서는 운영 복잡성이 증가할 수 있다.

하이브리드 제공자(Hybrid Providers)는 기술 기반 솔루션에 다이렉트 커스터디를 결합한 모델이다. 기술제공자와 마찬가지로 하이브리드 중 일부는 고객과 커스터디 업체(custodian)가 각각 서명 권한을 보유해 특정 조건에서만 트랜잭션이 실행되도록 설계된다. 평상시에는 고객이 직접 통제하되 비상 상황에서만 커스터디 업체가 복구를 지원하는 경우도 있다. 또한 고객은 필요에 따라 비수탁 모드(직접 키 관리)와 수탁 모드(규제·보험 체계 활용) 중에서 선택할 수 있어 기술제공자 대비 더 높은 제도적 안전망을 확보할 수 있다. 기술제공자와 마찬가지로 하이브리드 또한 멀티체인 환경에서는 복잡성이 증가하는 한계가 존재한다.

두 모델은 모두 자산 통제권을 유지하면서도 운영 효율성을 높이고자 하는 기관에 적합하다. 기술제공자는 비수탁형 구조를 기반으로 고객에게 키 관리 및 운영 효율성을 제공하는 반면, 하이브리드 제공자는 여기에 제한적 수탁 기능과 제도적 안전망을 결합한다는 점에서 차이가 있다. 다만 실제로는 두 모델의 기능과 역할이 상당 부분 중첩되어 경계를 명확히 나누기 어렵다. 최근에는 기술제공자이면서 동시에 다이렉트 커스터디 솔루션도 제공하는 기업들이 늘어나면서 다이렉트 커스터디·기술제공자·하이브리드 제공자 간의 전통적 구분이 점차 사라지고 있다. 더 나아가 전통 은행과 글로벌 금융사 계열이 가상자산 시장에 본격 진입하면서 전통 금융 인프라와 가상자산 커스터디가 결합된 융합형 모델 역시 빠르게 확산되는 추세다.

[8] CCData Research Team. (2023). "Crypto Custody: An Institutional Primer." Commissioned by Zodia Custody. *AYU Technologies Limited*.

Figure 6: 세가지 주요 커스터디 모델의 특징(미국 기준) 출처: PwC, 코빗 리서치

특징	다이렉트 커스터디	기술제공자	하이브리드 제공자
라이선스 외 추가 규제 충족 필요 여부	Yes	면제(exempted)	경우에 따라 다름
라이선스 보유 여부	Yes	No	Yes
고객 자산 이동 권한	Yes	No	개별 플랫폼은 없지만 커스터디 기관은 있음
대표 기업	Coinbase Custody	Fireblocks	Bitgo

대표 사례 1: Coinbase Custody

Coinbase Custody는 규제 준수와 신뢰를 기반으로 하는 다이렉트 커스터디 모델의 대표 사례다. 미국 상장사이자 규제 기관의 감독을 받는 기업이라는 점은 Coinbase Custody의 보안 체계, 서비스 모델, 리스크 관리 전반을 뒷받침하는 핵심 기반이 되고 있다.

비즈니스 모델 및 시장 포지셔닝: Coinbase Custody Trust Company, LLC는 뉴욕 금융감독국(NYDFS)으로부터 제한 목적 신탁회사(limited purpose trust company) 인가를 받아 '적격 수탁 기관'으로서의 지위를 확보하고 있다. 이는 상기한 1940년 투자자문법의 요건을 충족하는 것으로, 헤지펀드, 자산운용사, ETF 발행사 등 기관 고객에게는 필수 조건이다.

그래서인지 Coinbase Custody의 주요 고객은 규제 준수와 리스크 완화를 최우선으로 하는 기관이 많다. 연기금, ETF 발행사, 헤지펀드, 패밀리 오피스 등은 Coinbase의 미국 상장사로서의 감사 체계, 딜로이트를 통해 획득한 SOC 1 및 SOC 2 인증[9] 등을 높은 신뢰 요인으로 본다. Coinbase Custody는 "규제 기관의 감독을 받는 전문가에게 커스터디를 위임해 기관이 보안·운영·규정 부담을 덜 수 있다"는 명확한 가치를 제시하며, 단순 기술회사가 아닌 '신뢰와 규제 준수를 서비스화한 금융 인프라'로 포지셔닝하고 있다.

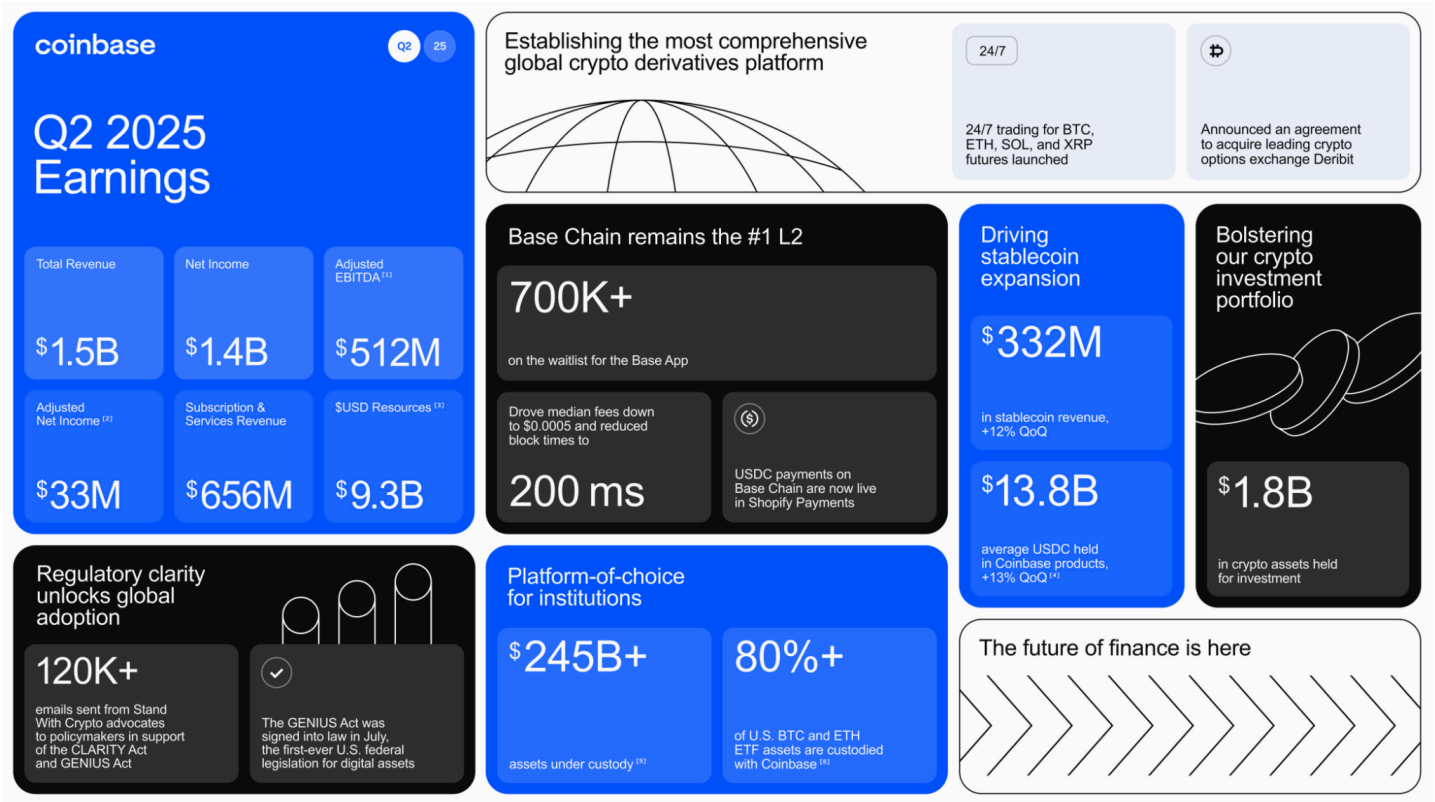
또한 Coinbase의 기관용 플랫폼인 Coinbase Prime은 트레이딩, 파이낸싱, 커스터디, 스테이킹, 리스크 관리와 같은 주요 기능을 통합한 프라임 브로커리지 솔루션으로 설계돼 있다. 기관 투자자는 이 플랫폼을 통해 분기 기준 약 1,940억 달러 규모의 거래를 실제로 수행했으며, 수탁 자산 규모(AUC)는 약 2,450억 달러에 이른다. 특히 커스터디 서비스는 플랫폼 내 자산을 예치하면 자연스럽게 트레이딩, 스테이킹, 파이낸싱 등으로 고객

[9] SOC(System and Organization Controls) 보고서는 미국공인회계사협회(AICPA)가 제정한 서비스 기관 내부통제 검증 기준으로, SOC 1은 재무보고 관련 내부통제, SOC 2는 보안·가용성·무결성·기밀성·프라이버시의 5대 신뢰 서비스 기준을 평가한다. Coinbase는 2020년 딜로이트를 통해 SOC 1 및 SOC 2 보고서를 획득하였다.

활동을 확장할 수 있는 핵심 접점으로 작용한다. 이러한 구조는 선순환(flywheel) 효과를 생성하며, 고객의 플랫폼 체류 기간을 늘리고, 수익 다변화 및 경쟁 우위 강화에 크게 기여하고 있다.

Figure 7: 코인베이스의 2025년 2분기 실적

출처: Coinbase Shareholder Letter



기술 및 보안 아키텍처: Coinbase는 고객 자산의 98% 이상을 에어갭(air-gapped) 콜드 스토리지[10]에 보관한다. 이 시스템은 은행 금고 수준의 물리적 보안, 지리적으로 분산된 인프라, 감사 가능한 관리 프로세스를 결합해 온라인 해킹 위험을 원천적으로 차단한다. 또한 2018년 약 50억 달러 규모의 자산을 차세대(Generation 3 → Generation 4) 콜드 스토리지로 온체인 이관하며 보안 인프라를 업그레이드하였고 이 사례는 Coinbase의 대규모 운영 역량을 보여준 대표적 이벤트로 평가된다.

콜드 스토리지의 보안성과 운영 효율 간의 상충 문제[11]를 해결하기 위해, Coinbase는 MPC 기반 기술을 도입했다. 이 기술은 프라이빗 키를 여러 환경에 분산 저장함으로써 단일 장애점(Single Point of Failure)을 제거하고, 더 빠른 출금 처리, 24/7 가용성, 유연한 운영을 가능하게 한다. 즉, 대부분의 자산은 콜드 스토리지에 안전하게 보관하되, 운영에 필요한 자산은 MPC 기반 지갑으로 관리하는 하이브리드 보안 모델을 구현한 것이다. 이러한 접근은

[10] 에어갭 콜드 스토리지란 인터넷 및 무선 통신망뿐 아니라 USB 등 외부 연결까지 차단된 오프라인 환경에서 가상자산 프라이빗 키를 저장하는 방식으로, 온라인 해킹을 원천적으로 방어할 수 있는 보안 구조를 말한다.

[11] 콜드 스토리지의 보안성과 운영 효율 간 상충 문제란, 오프라인 환경에 키를 보관해 해킹 위험을 줄이는 대신(보안성 ↑) 자산 이동·출금 속도가 느려지고, 상시 운영이 어렵다는 점(효율성 ↓)을 의미한다.

현재 업계에서 널리 인정받는 모범 사례로 평가된다.

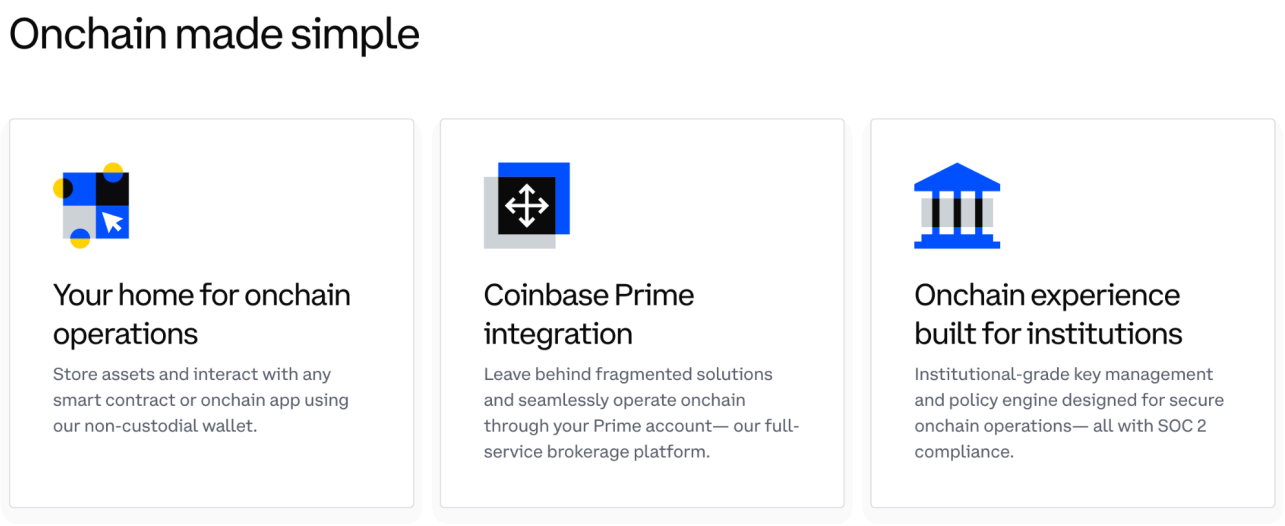
핵심 서비스 및 부가 가치: Coinbase Custody는 420종 이상의 가상자산을 안전하게 보관하며 고객 자산을 회사 자산과 철저히 분리해 관리한다. 이는 파산 상황에서도 법적으로 보호될 수 있는 구조로 기관투자자에게 신뢰를 제공하는 점 중 하나이다.

스테이킹 서비스는 커스터디와 직접 통합된 대표적 부가 기능이다. 고객은 Coinbase Custody에서 ETH, SOL, ADA, DOT 등 주요 네트워크 자산을 별도의 이전 없이 스테이킹할 수 있으며, Coinbase는 약 200억 달러 이상의 스테이킹 자산(AUM)을 관리하고 있다. 이를 통해 기관은 유휴 자산으로 수익을 창출할 수 있고, Coinbase는 수수료 기반의 신규 수익원을 확보한다.

또한 Coinbase는 단순 보관과 스테이킹을 넘어, 기관 고객이 직접 온체인 활동을 수행할 수 있도록 서비스를 확장하고 있다. 그 대표적인 사례가 Prime Onchain Wallet이다. Prime Onchain Wallet은 정책 엔진과 보안 인증을 갖춘 온체인 게이트웨이로, DeFi와 Web3 활동을 기관 등급 환경에서 수행할 수 있게 한다. 이를 통해 리테일 솔루션에 의존하지 않고도 규제 준수·내부통제·보안 요건을 충족하는 기관 전용 인프라를 제공하며, 코인베이스가 전통적 수탁 모델에 머물지 않고 비수탁형 영역까지 사업을 넓혀가고 있음을 알 수 있다.

Figure 8: 코인베이스의 Prime Onchain Wallet

출처: Coinbase Prime



이처럼 Coinbase Custody는 단순 보관 기능을 넘어 가상자산 관리 및 운용 최적화 플랫폼으로 진화하고 있다. 규제와 감사 체계가 보장된 환경에서 스테이킹·DeFi 등 부가 서비스를 결합함으로써, Coinbase는 커스터디를 비용 중심이 아닌 수익 창출 중심의 사업 영역으로 재정의하고 있다.

대표 사례 2: Fireblocks

비즈니스 모델 및 시장 포지셔닝: Fireblocks는 가상자산 인프라 제공업체로, 자체 MPC-CMP 기술을 활용해 프라이빗 키가 한 번도 완성된 형태로 드러나지 않고, 고객과 Fireblocks 보안 인클레이브(SGX) 등 분산된 환경에서 공동 연산을 수행하는 구조를 제공한다. 이 방식 덕분에 Fireblocks는 고객의 자산을 직접 보관하거나 단독으로 이동시킬 수 없으며, 고객은 자산 소유권과 통제권을 유지한 채 Fireblocks의 보안·운영 효율성을 활용할 수 있다. 즉, Coinbase Custody가 전통적인 '수탁(custody)' 모델이라면, Fireblocks는 지갑 인프라(Wallet-as-a-Service) 제공자로서 고객이 자체 커스터디 역량을 구축할 수 있게 해주는 기술 제공자라는 점에서 차별화된다.

Fireblocks의 핵심 서비스는 대규모 지갑 생성 및 관리 플랫폼이다. Fireblocks는 'embedded wallet'과 'direct custody WaaS'를 통해 수많은 MPC 지갑을 보호하고 있으며, 핀테크·거래소·게임사 등 커스터디 기반 인프라가 필요한 기업들에게 서비스를 제공한다.

Fireblocks는 자산을 직접 보관하지 않고 고객이 자산 이동 권한을 유지하는 구조이기 때문에 전통적인 커스터디 업체에 적용되는 일부 규제 요건에서 벗어나 있다. 그 결과 빠른 혁신이 가능하지만, 키 관리·백업·복구와 같은 책임은 전적으로 고객에게 남는다. Fireblocks는 이를 보완하기 위해 재해 복구 메커니즘과 백업 키 관리, 보험 연계 등의 기능을 제공하고 있으며, 고객은 필요 시 "break-glass recovery tool"을 통해 Fireblocks 서비스가 불능 상태일 경우에도 자산을 복구·이동할 수 있도록 설계되어 있다.

Fireblocks는 금융 기관, 결제사, 게임사, Web3 기업 등 산업 전반에서 가상자산 키 관리와 토큰화를 제공하는 기반 인프라로 기능한다. 100개 이상의 블록체인을 지원하고 다양한 자산 유형을 동일 플랫폼에서 처리할 수 있어, 특정 산업에 국한되지 않는 수평적 플랫폼 구조라는 점에서 차별화된 비즈니스 모델로 평가된다.

Figure 9: 산업별 Fireblocks 활용 분야

출처: developers.fireblocks.com

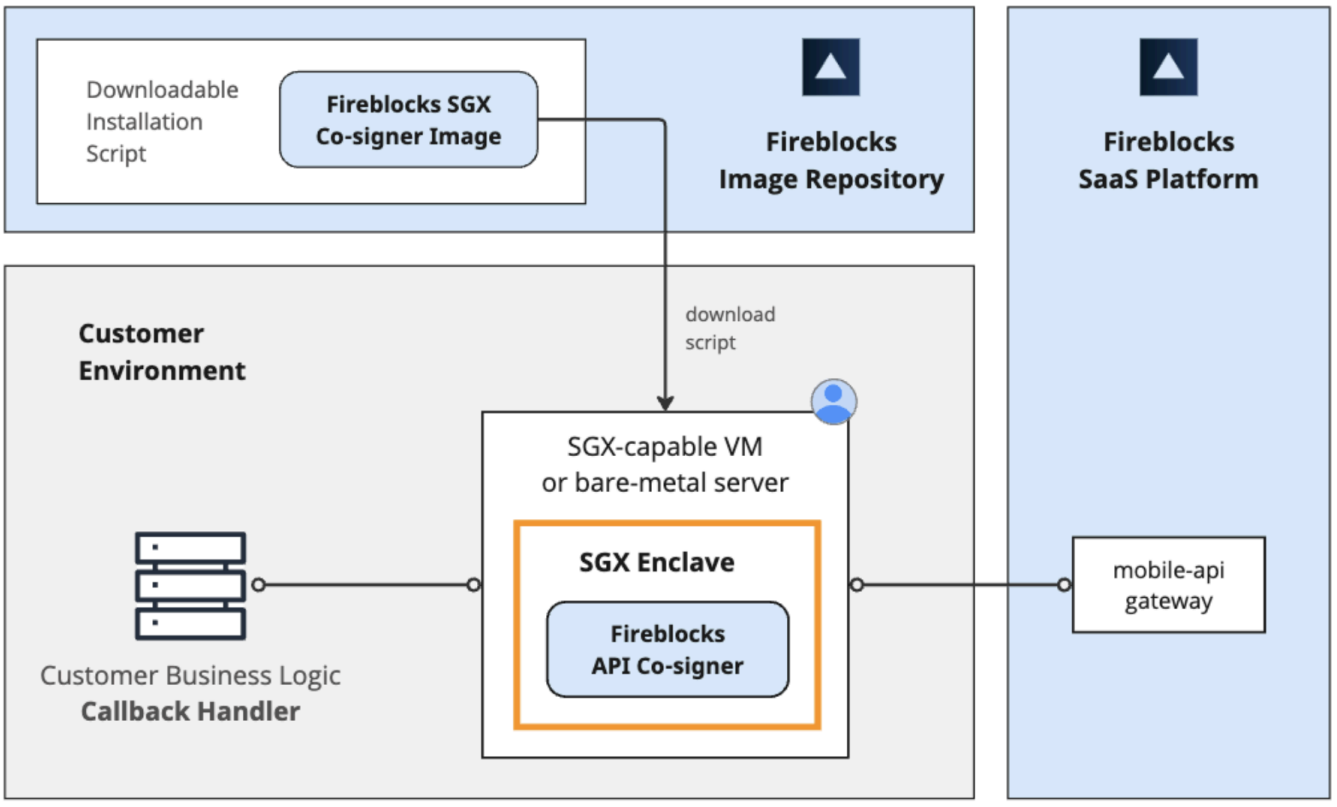
산업	유형
금융기관	은행, 헤지펀드, 자산운용사, 대출 데스크, OTC 데스크, 프라임 브로커, 마켓메이커, 패밀리 오피스
Web3 기업	NFT 마켓플레이스, DAO, 디파이프로토콜, 게임파이, Web3 인프라 제공업체, 프로토콜 재단, B2B Web3 서비스
리테일 서비스	거래소, 일반 기업, 핀테크, 투자 플랫폼
B2B 서비스	결제 서비스 제공업체, BaaS 제공업체

기술 및 보안 아키텍처: Fireblocks 플랫폼은 MPC 방식을 통해 프라이빗 키가 한 번도 완성된 형태로 드러나지 않고, 각 참여자가 가진 부분 정보를 활용해 공동으로 연산이 수행되도록 설계되어 단일 장애점 리스크(single point of failure)를 낮춘다. 자체 개발한 MPC-CMP 프로토콜은 기존 MPC보다 최대 8배 빠른 서명 속도를 제공하며, Fireblocks는 이를 기반으로 100개 이상의 블록체인과 다양한 가상자산을 효율적으로 지원하는 인프라를 제공한다.

또한 Fireblocks의 보안 구조는 MPC, Intel SGX, AWS Nitro, Google Cloud Confidential Space 하드웨어 인클레이브(hardware enclave)[12], 세분화된 정책 엔진, 보안 전송 네트워크를 결합한 다층 보안 체계로 설계되어 있다. 덕분에 고객들은 다중 승인, 거래 한도 설정, 화이트리스트 제어 등 맞춤 거버넌스 규칙을 자동화·정책화할 수 있으며, 사실상 고객 스스로 운영하는 '수탁사(custodian)' 수준의 제어가 가능하다. 또한, 이 시스템은 SOC 2 Type II 및 ISO 27001/27017/27018 등의 국제 보안 인증을 획득함으로써 높은 수준의 신뢰성을 갖추었다. 참고로 Fireblocks가 다중서명(multi-sig) 대신 MPC를 채택한 이유는 MPC가 프로토콜에 구애받지 않고 단일 표준 서명을 생성해 체인별 개발 부담을 줄이면서도 운영 유연성과 확장성을 제공하기 때문이다. 온체인 투명성 측면에서는 다중서명보다 다소 제한적일 수 있으나, 고객에게는 확장성과 운영 효율을 보장할 수 있다.

Figure 10: Fireblocks SGX Co-signer 아키텍처

출처: developers.fireblocks.com



[12] 하드웨어 인클레이브(hardware enclave)란 컴퓨터나 스마트폰 같은 기기 안에 별도로 격리된 보안 공간을 말한다.

Figure 11: MPC vs. Multi-sig

출처: Fireblocks

핵심 서비스 및 부가가치: Fireblocks는 강력한 API와 SDK를 통해 토큰화, 지갑, 거래 자동화 등 다양한 기능을 자체 인프라 위에서 구현할 수 있는 '개발자 우선' 플랫폼이다. 특히 Fireblocks Network는 기관 간 정산(settlement) 워크플로우로 네트워크 참여자와의 거래에서 주소를 일일이 화이트리스트에 등록할 필요 없이 빠르게 전송할 수 있도록 지원한다. 자동 주소 인증 기능(Automated Address Authentication)을 통해 입금 주소 위·변조 리스크를 효과적으로 억제하는 동시에 지원되는 자산에 대해서는 보안 주소를 주기적으로 자동 교체(automatically rotating secure addresses)해 관리하고, 모든 거래를 상대 기관에 매핑(maps transactions to counterparties)하여 정확한 리포팅까지 가능하다. 현재 Fireblocks Network는 2,400개 이상의 기관을 연결[13]하고 있다. 이러한 네트워크는 참여 기관이 많을수록 거래 편의성과 신뢰성이 향상되는 자기 강화적 구조를 갖추고 있으며, 고객이 플랫폼 위에 보안·컴플라이언스·결제 네트워크를 일체화한 이후에는 다른 기반으로 이전하기가 어렵기 때문에 강력한 전환 장벽이 형성된다. 결과적으로 Fireblocks는 네트워크 효과와 높은 전환 비용을 바탕으로 기관용 가상자산 인프라 시장에서 견고한 해자를 구축하고 있다.

[13] 스테이킹 연계 기능 역시 Galaxy Digital과의 제휴를 통해 기관 고객이 Fireblocks 내 자산을 외부로 이동시키지 않고도 스테이킹에 안전하게 참여할 수 있도록 지원하지만, 이는 Fireblocks만의 독점적 기능이라기보다 최근 대부분의 커스터디 플랫폼에서 제공하는 서비스이기도 하다.

대표 사례 3: BitGo

비즈니스모델 및 시장 포지셔닝: BitGo는 2013년 설립된 가상자산 커스터디 기업으로 다중서명 기반 지갑 기술을 최초로 상용화하며 기관 시장에 진입했다. 2018년 미국 South Dakota 금융당국의 인가를 받아 BitGo Trust Company를 설립하면서 Qualified Custodian 지위를 확보했으며, 이를 통해 셀프 커스터디(self-custody)와 규제된 적격 수탁(qualified custody)을 결합한 하이브리드 모델을 제공하고 있다. 이러한 구조 덕분에 기관 고객은 자산 통제권을 유지하면서도 규제 준수와 보안을 동시에 확보할 수 있다. BitGo는 현재 2,000개 이상의 기관 고객을 보유하며, 자체 집계 기준으로 온체인 비트코인 거래액의 약 8~20%를 처리한다고 밝히고 있다.

BitGo는 초창기부터 다중서명 기술을 선도해 왔다. 셀프 커스터디 지갑은 일반적으로 2-of-3 다중서명 구조를 사용하며, 고객이 두 개의 키를 직접 보유하고 BitGo가 하나의 키를 보관함으로써 공동 서명 및 복구가 가능하다. 최근 시장에서 MPC(Multi-Party Computation) 기술이 부상했음에도, BitGo는 다중서명이 제공하는 온체인 투명성과 신뢰성을 강조한다. 회사 측은 보안이 단일 기술에 의존해서는 안 되며, 운영상 안전장치를 갖춘 구조가 필수적이라고 주장한다.

BitGo Trust Company는 South Dakota 인가에 이어 뉴욕 한정 목적 신탁 라이선스도 보유하고 있다. 이를 통해 고객 자산은 파산 절연(bankruptcy remote)[14]이 가능하며, SEC 투자자문 규정의 수탁 요건(Custody Rule)을 충족하는 규제 커스터디 서비스를 제공한다. 이러한 인프라는 기관 고객에게 법적 안정성과 신뢰성을 보장하는 핵심 기반이 된다.

BitGo의 하이브리드 모델은 시장 불확실성에 대한 전략적 헤지 역할을 한다. 규제가 강화되는 국면에서는 적격 수탁 서비스의 수요가 확대되고, 반대로 기관이 직접 통제나 DeFi 연동을 중시하는 국면에서는 셀프 커스터디 서비스가 성장한다. 기관 고객은 단일 파트너십 내에서 단기적·활발한 거래에 적합한 셀프 커스터디 핫월렛과 장기 보유 및 규제 준수에 적합한 적격 수탁 콜드월렛을 병행할 수 있어 보안과 효율성, 규제 대응을 동시에 확보할 수 있다.

기술 및 보안 아키텍처: BitGo의 적격 수탁 서비스는 은행 등급 금고, 분산형 오프라인 저장소, 하드웨어 보안 모듈(HSM)을 기반으로 구축되어 있으며, 다중서명 구조와 결합해 단일 장애점을 제거한다. 이를 통해 기관이 요구하는 수준의 보안 표준과 일치하는 인프라를 제공한다.

또한 주소 화이트리스팅, 거래 속도 제한, 역할 기반 접근 제어(RBAC) 등 정책적 제어를 포함한 심층 방어 전략을 운영한다. Deloitte 감사 기반 SOC 1

[14] 파산 절연(bankruptcy remote)은 특정 자산이나 법인을 모회사의 파산 위험으로부터 격리하는 구조를 뜻한다.

Type 2 및 SOC 2 Type 2 인증을 정기적으로 획득하고 있으며, 2013년 설립 이후 자사 인프라에서 보안 침해 사례가 없었다고 강조한다.

BitGo는 다중서명을 "투명하고 입증된 공유 통제 모델"로 규정하며, 업계가 확장성과 유연성을 이유로 MPC 채택을 확대하는 가운데, MPC가 오히려 과도하게 중앙화된 신뢰 지점을 형성할 수 있다고 지적한다. 이에 따라 BitGo는 온체인 투명성과 독립적 키 소유권을 내세워, 보수적인 기관 투자자에게 안정성과 신뢰성에 기반한 대안적 선택지로 자리매김하고 있다.

핵심 서비스 및 부가 가치: BitGo는 기관 수요를 만족시키는 다양한 월렛 옵션—핫 월렛, 규제 수탁형 월렛, 셀프 관리 콜드 월렛을 제공한다. 또한 BitGo는 약 480억 달러 규모의 자산을 스테이킹하고 있고, 원클릭(one-click) 스테이킹과 자체 또는 파트너 Validator 선택 기능을 통해 유연한 스테이킹 경험을 제공한다.

프라임 서비스(Prime Services)는 규제된 수탁 환경 하에서 거래, 자금조달, 담보관리, 정산 등 기관형 서비스 전반을 통합 제공한다. Go Network는 이러한 프라임 서비스의 핵심 인프라로, USD 및 가상자산의 실시간 오프체인 정산(DvP[15] 포함)을 지원하여 거래상대방 리스크를 최소화한다.

전반적으로 BitGo의 전략은 다양한 서비스를 단일 플랫폼 내에서 연계 제공함으로써 기관 고객이 초기 셀프 커스터디에서 스테이킹·수탁·정산까지 부담 없이 성장 경로를 확장할 수 있도록 설계되었으며, 이러한 업그레이드 경로는 운영 마찰 최소화와 고객 고착 효과를 극대화하는 기반을 제공한다.

결국 Coinbase, Fireblocks, BitGo 간의 선택은 어느 곳이 '최고'인가의 문제가 아니라, 각 기관의 정체성, 리스크 선호도, 그리고 가상자산 전략의 장기적 목표에 따라 달라지는 전략적 결정이다. 시장은 이제 다양한 기관 철학에 부합하는 구체적이고 실행 가능한 모델들이 자리 잡을 만큼 성장했다. 전통 금융기관과 자산운용사는 규제 명확성과 운영 리스크 최소화를 최우선 가치로 두기 때문에 Coinbase 모델을 선호할 가능성이 크다. 반면, 가상자산 네이티브 트레이딩 기업이나 Web3 애플리케이션을 구축하는 핀테크 스타트업은 속도·개발 유연성·직접 통제를 중시해 Fireblocks 모델에 더 적합하다. 패밀리 오피스나 헤지펀드처럼 가상자산 친화적이면서도 기관 투자자들의 요구를 충족해야 하는 주체들은 BitGo의 하이브리드 모델을 통해 리스크와 통제의 균형을 추구할 수 있다. 따라서 세 회사는 단일 시장에서의 경쟁자가 아니라, 기관 타겟 가상자산 서비스라는 큰 틀 안에서 각기 다른 하위 시장을 대표하는 선도 사업자들이다. 이들의 성장은 곧 세 가지 가치 제안 모두에 실질적 수요가 존재함을 보여주며, 기관의 가상자산 채택이 얼마나 다원적 양상으로 전개되고 있는지를 잘 반영한다.

[15] DvP(Delivery vs. Payment)는 자산 인도와 대금 지급이 동시에 이루어지도록 설계된 결제 방식으로, 한쪽이 자산만 받고 대금을 지급하지 않거나 반대로 대금만 지급하고 자산을 받지 못하는 상황을 원천적으로 차단한다. 전통 증권결제에서 사용되는 원칙을 가상자산 결제에 적용한 개념이다.

Figure 12: 기관용 커스터디 대표 3사 비교

출처: 코빗 리서치

구분	Coinbase Custody	Fireblocks	BitGo
모델	다이렉트 커스터디	기술 인프라 제공	하이브리드
규제 인가	NYDFS 신탁 인가 (Qualified Custodian)	없음 (비수탁형 기술 업체)	South Dakota, NYDFS 신탁 인가 (Qualified Custodian)
주요 고객	전통 금융기관 (연기금, ETF, 운용사 등)	핀테크, 거래소, 웹3 기업	패밀리 오피스, 헤지펀드 등 혼합형
보안 아키텍처	콜드 스토리지 + MPC 하이브리드	MPC-CMP + 정책 엔진	다중서명 + 오프라인 금고/HSM
서비스 확장	Prime 플랫폼 (트레이딩, 스테이킹, 디파이)	Waas, Fireblocks Network(기관 연결)	Staking, Prime Services, Go Network(DvP 정산)

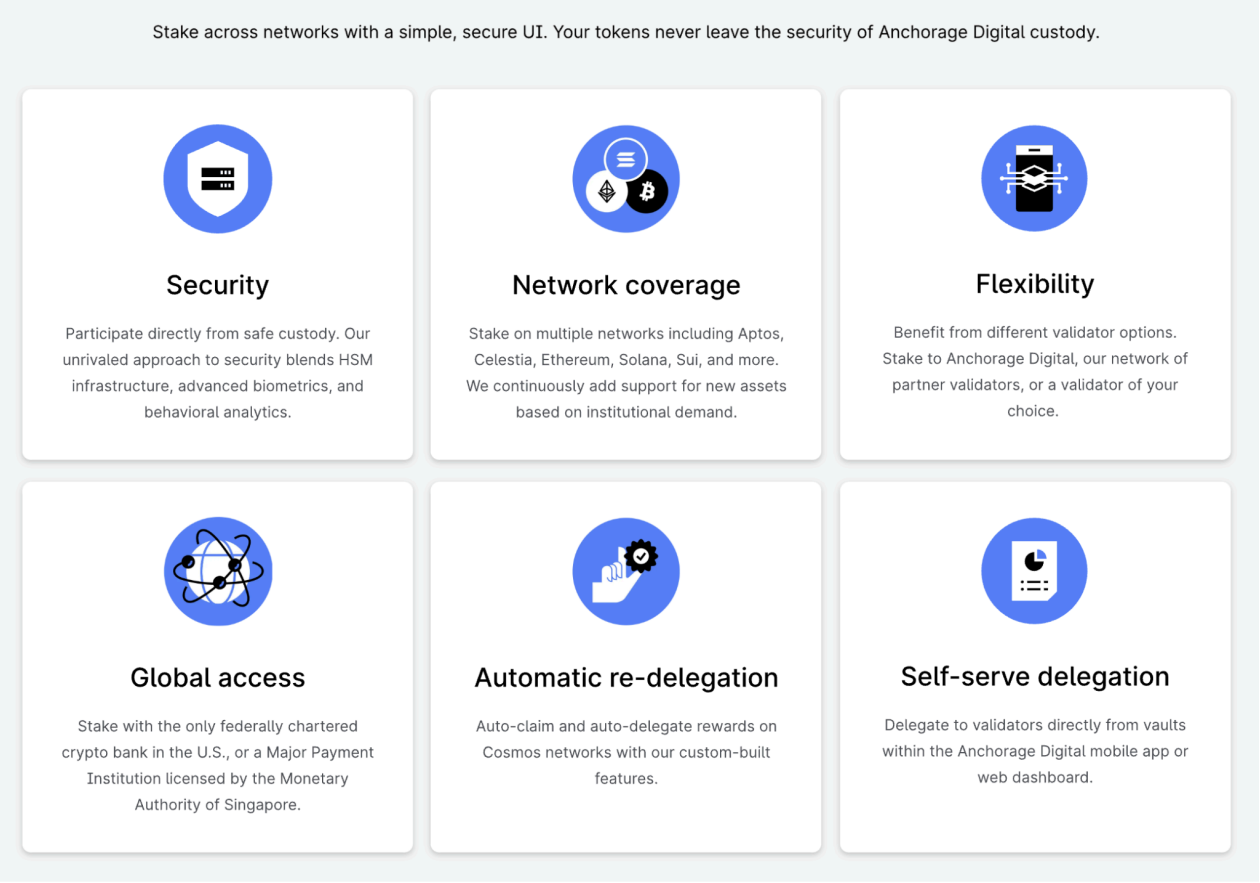
향후 전망과 시사점

4대 트렌드

가상자산 커스터디 시장은 더 이상 정적인 '보관소(vault)' 역할에 머무르지 않는다. 블록체인 기술의 발전과 기관 투자자들의 정교한 요구에 부응하기 위해, 커스터디 서비스는 능동적이고 다기능적인 금융 허브로 진화하고 있다. 그리고 이러한 변화를 주도하는 핵심 혁신 트렌드는 크게 4가지이다.

디파이 연계 수익 창출: 전통적인 커스터디의 핵심 가치가 '안전한 보관(secure storage)'에 있었다면, 향후 커스터디는 보관 자산을 안전하게 활용하여 '수익을 창출(yield generation)'하는 기능(예: 스테이킹, 유동성 공급, 렌딩)까지 포괄하는 방향으로 진화하고 있다. 실제로 Anchorage Digital, Coinbase Prime 등 주요 사업자는 기관 고객에게 수탁 연계 스테이킹, 온체인 접근을 제공(Figure 13) 하고 있으며, Fireblocks 등 인프라 사업자는 위협 탐지, 트랜잭션 시뮬레이션 등으로 디파이 접근을 통제, 자동화하고 있다.

Figure 13: Anchorage Digital Custody 기반 멀티네트워크 스테이킹 출처: Anchorage



이에 따라 커스터디 제공업체들은 보안을 최우선으로 유지하면서도 다양한 DeFi 생태계에 안전하게 접근할 수 있는 '관문(gateway)' 역할을 수행해야

한다. 이는 단순히 자산을 DeFi 프로토콜로 전송하는 차원을 넘어 거래 전 시뮬레이션을 통한 리스크 분석, 스마트 컨트랙트/상대주소 화이트리스팅, 정책 기반 승인(policy engine), 비정상 패턴 탐지 등 정교한 리스크 관리를 플랫폼 내에 통합하는 것을 의미한다.

다만 DeFi와의 융합은 새로운 기회인 동시에 고유 리스크(예: 스마트 컨트랙트 취약점, 오라클 조작, 거버넌스 공격 등)를 수반한다. 커스터디 제공업체는 자체·제3자 스마트컨트랙트 감사, 위협 탐지·모니터링 등의 체계를 통해 이러한 위험을 선제적으로 식별·완화해야 한다. 결국, '수익을 창출하는 커스터디'의 성공 여부는 DeFi가 제공하는 수익 기회와 내재된 위험 사이에서 얼마나 정교한 균형을 맞출 수 있느냐에 달려있다.

크로스체인 커스터디: 블록체인 생태계는 솔라나, 폴카닷, 코스모스 등 각기 다른 특성과 장점을 지닌 L1 체인이 활성화되면서, DeFi, NFT, RWA를 포함한 가상자산이 여러 체인에 분산되는 멀티체인 파편화 상황이 심화되고 있다. 이러한 환경은 투자자에게는 기회를 확산하지만, 자산 관리는 복잡성을 대폭 증가시킨다.

이같은 맥락에서 크로스체인 커스터디(Cross-Chain Custody)는 다양한 블록체인에 존재하는 자산을 통합 플랫폼상에서 안전하게 관리할 수 있는 솔루션으로 부상하고 있다. 이는 여러 종류의 자산을 지원하는 것을 넘어 체인 간 자산 이동을 가능하게 하는 브릿지(Bridge) 기술과의 안전한 연동을 포함한다.

하지만 크로스체인 브릿지는 블록체인 생태계에서 가장 취약한 공격 지점 중 하나로 꼽힌다. 실제로 2022년에 발생한 DeFi 관련 해킹 피해액의 64%가 크로스체인 브릿지에서 발생했을 정도로 보안 리스크가 상대적으로 높다. 자산이 하나의 체인에서 다른 체인으로 이동하는 과정에서 발생하는 기술적 복잡성과 취약점은 해커들에게 매력적인 공격 표적이 되기 때문이다. 따라서 크로스체인 커스터디 제공업체는 브릿지 보안에 대한 엄격한 실사(due diligence), 지속적 모니터링, 사고 대응 체계를 갖춰야 한다.

RWA와 같은 새로운 자산군 확대: 가상자산의 범위는 고변동성 자산을 넘어 실물 경제에 기반한 자산으로 빠르게 확장되고 있으며, 그 중심에 RWA(Real-World Assets)가 있다.

그러나 RWA 커스터디는 단순한 디지털 토큰 보관을 넘어서는 복잡한 도전 과제라 할 수 있다. 토큰이 표상하는 실물 자산의 법적 권리가 온체인에서 정확히 반영·동기화되어야 하기 때문이다. 예를 들어, 토큰화된 부동산의 경우 블록체인상 소유권 이전은 실제 등기부상의 권리 이전과 일치해야 한다. 따라서 RWA 커스터디는 법률·등기·신탁·자산 실사까지 아우르는 정교한 전문성과 통합 관리 역량을 필요로 한다.

전통 금융기관의 본격 진입과 서비스 통합: 가상자산 커스터디 시장은 전통 금융기관(TradFi)의 본격적인 진입과 서비스 통합(프라임 브로커리지) 모델의 부상이라는 구조적 변화를 맞이하고 있다. 과거 가상자산을 변방적 실험으로 치부하던 글로벌 은행과 자산운용사들이 이제는 커스터디를 새로운 성장 동력으로 인식하며 적극적으로 참여하는 모습이다. 이는 가상자산이 더 이상 대안적 투자 수단이 아닌, 제도권 금융의 핵심 인프라로 편입되고 있음을 보여준다.

또한 미국 SEC의 비트코인 현물 ETF 승인과 유럽 ETP 제도화는 커스터디 시장을 폭발적으로 성장시키는 기폭제가 되었다. BlackRock, Fidelity 등 글로벌 자산운용사들이 수십억 달러 규모의 비트코인을 Coinbase Custody나 Fidelity Digital Assets에 위탁하면서 제도권 자금이 대거 유입되는 구조적 변화가 일어나고 있다. ETF는 "가상자산이 제도권에서 투자 가능한 자산군"이라는 강력한 신호를 제공하며, 직접 투자 수요까지 견인하고 있다.

이러한 환경 변화 속에서 전통 금융기관의 시장 진입은 세 가지로 설명할 수 있다. 첫째, 고객 수요 대응 측면에서 ETF를 통한 기관 자금 유입은 전통 금융기관이 무시할 수 없는 구조적 트렌드를 만들었다. 둘째, 새로운 수익원 창출을 위해 BNY Mellon이 Fireblocks와 협력해 커스터디 서비스를 개시하거나 Citi가 Metaco를 인수하는 사례처럼 기술 파트너십 및 M&A 전략을 적극 활용하고 있다. 셋째, 금융 디지털화 전략의 일환으로 J.P. Morgan은 Onyx 플랫폼을 직접 개발했고, Standard Chartered와 Northern Trust는 합작법인 Zodia Custody를 설립해 장기적 경쟁력을 내재화했다.

이처럼 각기 다른 동기를 바탕으로 다양한 전략을 취하고 있지만, 전통 금융기관들이 지향하는 방향은 같다. 단순히 가상자산을 보관하는 수준을 넘어, 전통 자산과 디지털 자산을 아우르는 통합 관리 플랫폼을 구축하려는 것이다. 이는 커스터디가 제도권 금융에서 단순 수익 사업을 넘어 미래 금융 인프라의 핵심 축으로 자리 잡아가고 있음을 방증한다.

특히 기관 투자자들은 파편화된 시장 구조에서 발생하는 비효율성을 극도로 경계한다. 자산 보관은 A사, 거래 체결은 B사, 대출은 C사, 청산 및 결제는 D사로 나뉘는 구조는 비용과 리스크를 가중시킨다. 따라서 기관들은 커스터디, 거래, 대출, 스테이킹, 시장 데이터, 리서치까지 모든 기능을 하나의 원스톱 샵(one-stop-shop) 플랫폼에서 제공받기를 원한다. 이는 전통 금융시장의 프라임 브로커리지(prime brokerage) 모델과 유사하며, 가상자산 영역에서도 Fidelity Digital Assets, Coinbase Prime 등이 이러한 통합 모델을 구축하고 있다. 이들은 기관급 보안을 갖춘 커스터디를 기반으로 스마트 오더 라우팅(SOR), 담보 대출, 규제 준수 리포팅 등 통합 서비스를 제공하며 시장을 선도한다. 커스터디는 이 모든 서비스의 핵심 기반(anchor)로서, 고객 자산을 확보하고 이를 바탕으로 다른 서비스 이용을 자연스럽게 유도하는 전략적 출발점이 된다.

이러한 변화 속에서 경쟁 구도는 전통 금융 vs. 크립토 네이티브라는 양극 구도로 재편된다. 전통 금융은 브랜드 신뢰·자본력·규제 경험을 무기로 보수적 기관 고객을 흡수하는 반면, 크립토 네이티브는 기술 우위와 민첩성을 무기로 혁신을 선도한다. 단기적으로는 이들 간에 협력과 융합이 두드러질 수도 있겠으나, 장기적으로는 기술·규제·운영 안정성·통합 서비스 제공 역량을 모두 갖춘 소수의 플랫폼 중심 과점 구조가 형성될 가능성이 높다.

종합 시사점

향후 가상자산 커스터디 산업의 승패는 더 이상 단순한 기술력이나 초기 진입 속도에 달려 있지 않다. 시장이 성숙할수록 중요한 것은 제도권 금융의 눈높이에 맞춘 규제 준수 능력, 운영 안정성, 그리고 신뢰 확보 역량이다. MPC 또는 다중서명 기반 키 관리, 안전한 크로스체인 상호운용성, 법적 복잡성이 높은 RWA 관리와 같은 기술적 과제는 점차 표준화되겠지만, 이를 안정적으로 운영하고 규제 환경에 적응하는 능력은 기업의 존속과 성장을 가르는 핵심 분수령이 될 것이다.

기업 차원에서 보면, 규제 준수 역량을 경쟁 우위의 기반으로 삼고, 기술적 우위를 지속적으로 발전시키며, 커스터디를 중심으로 거래·대출·스테이킹·회계 보고까지 통합적으로 제공할 수 있는 플랫폼을 구축하는 능력이 요구된다. 더불어 신뢰와 투명성을 확보하기 위한 인증, 보험, 자산 증명 체계는 기관 고객이 안심하고 자산을 위탁할 수 있는 최소 조건으로 자리 잡고 있다.

정책 차원에서는 글로벌 주요국의 사례가 중요한 시사점을 제공한다. 미국은 입법과 규제 당국의 허용으로 은행의 커스터디 참여를 제도화했고, 유럽연합은 MiCA를 통해 규제 명확성과 단일 시장을 동시에 확보하며 커스터디 허브로 도약할 기반을 마련했다. 일본은 엄격한 고객 자산 보호 규제를 시행하며 높은 신뢰를 확보했고, 싱가포르는 리테일 규제를 강화하면서도 기관 투자자에게는 다양한 기회를 열어주는 방식으로 균형을 추구하고 있다.

한국이 글로벌 경쟁에서 뒤처지지 않으려면 금산분리 원칙의 유연한 적용 등을 통해 제도권 금융기관이 커스터디 시장에 진입할 수 있도록 기회를 열어주어야 한다. 동시에 글로벌 기관이 신뢰할 수 있는 수준의 AML과 투자자 보호 체계를 강화하고, 표준화와 보험시장을 육성하여 제도권 수준의 신뢰성을 확보해야 한다.

궁극적으로 가상자산 커스터디는 단순한 산업 영역이 아니라 미래 금융 인프라의 핵심 축이다. 산업의 진정한 승자는 화려한 기술이나 자본 규모가 아니라, 규제와 시장을 동시에 아우르는 제도권 수준의 운영 능력을 확보한 국가와 기업이 될 것이다.

작성자

최윤영 | Yoonyoung Choy

2022년 코빗 입사. (現)코빗 리서치센터장.
(前)삼성경제연구소, 하나금융경영연구소, 서울대 증권금융연구소 근무. 서울대 경영학 박사(Finance 전공). 미시간 대학교, 스미스여대 졸업.

김민승 | Min Seung Kim

2021년 코빗 입사. (現)코빗 리서치센터장.
블록체인과 가상자산 생태계에서 벌어지는 복잡한 사건과 개념을 쉽게 풀어 알리고, 다른 관점을 가진 사람들이 서로를 이해하도록 돕는다. 블록체인 프로젝트 전략 기획, 소프트웨어 개발 등의 경력 보유.

법적 고지서