

Arc: 안정코인 금융을 위해 설계된 오픈 레이어-1 블록체인

Gordon Y. Liao
gordon.liao@circle.com

Rachel Mayer
rachel.mayer@circle.com

Adrian Soghoian
adrian.soghoian@circle.com

Sanket Jain
sanket.jain@circle.com

Erik Tierney
erik.tierney@circle.com

2025년 8월

Abstract

Arc는 안정코인 금융과 토큰화를 선도하기 위해 설계된, EVM 호환 오픈 레이어-1 블록체인이다. Arc는 USDC를 원화(가스)로 사용하는 모델, 결정적 결제 최종성, 선택적(옵트인) 프라이버시, 그리고 안정적인 거래 수수료 아키텍처를 갖춘다. 글로벌 결제, 외환, 자본시장 등 안정코인 네이티브 활용 사례에 최적화되어 있으며, 인터넷 상의 프로그래머블 머니를 위한 기초 결제 레이어로 기능한다.

1 서론

현대 상업의 토대인 글로벌 금융 시스템은, 인터넷의 속도·개방성·프로그래머블성을 기준으로 보면 근본적으로 양립하기 어려운 레거시 인프라 위에 서 있다. 소비자 및 엔터프라이즈 소프트웨어의 수십 년 혁신에도 불구하고, 금융 접근성·포용성·실시간 자본 이동성은 여전히 제약을 크게 받고 있으며, 특히 국경 간과 신흥시장 영역에서 두드러진다. 국경 간 결제는 느리고 불투명하며 비용이 높고, 재무(트레저리) 운영은 관할권·중개기관·상호 비호환 금융 레일 전반으로 분절되어 있다. 자본시장은 수작업 프로세스와 여러 종의 중개로 인해 폐쇄적·분절적이다. 이러한 구조적 비효율은 경제적 비용을 초래하고, 체계적 성격의 거래상대방·운영 리스크를 유발한다 [Committee on Payments and Market Infrastructures, 2020].

블록체인 기술은 금융과 상거래에 프로그래머블성·투명성·검열저항을 제공하는 새로운 패러다임을 약속했으나, 현존 퍼블릭 체인은 제도권 및 엔터프라이즈 도입을 가로막는 근본적 제약을 보인다. 변동성 높은 네이티브 토큰을 가스로 사용하는 관행은 예측 불가능한 운영 비용과 회계 복잡성을 초래한다. 더 나아가 많은 체인에서 결제 최종성(settlement finality)에 대한 불명확성은 금융 리스크를 키우며, 트랜잭션 프라이버시의 부재는 민감한 상업 활동에 필수적인 요소가 빠져 있음을 의미한다. 완전히 개방·투명한 트랜잭션 제출은 특권적 참여자가 거래 순서를 악용해 이익을 취하는 최대추출가치(MEV) 현상을 낳아 시장 견전성을 훼손해 왔다 [Daian et al., 2019]. 마지막으로, 여러 블록체인에 걸친 안정코인 유동성과 앱의 단편화는 사용자와 개발자 모두에 마찰을 만든다.

이 라이트페이퍼는 이러한 핵심 공백을 해소하기 위해 안정코인 금융에 특화된 오픈 레이어-1 체인인 Arc를 소개한다. 우리는 미래의 금융과 상거래가 구체제를 전면 대체하는 것이 아니라, 새로운 것과 기성의 것을 결합하는 합성(synthesis)임을 전제로 한다. 즉, 스마트컨트랙트의 프로그래머블성과 법의 집행가능성(예: GENIUS Act),

블록체인의 효율성과 법정화폐 담보 통화의 안정성, 퍼블릭 원장의 투명성과 상업 거래에 필요한 프라이버시의 결합이다. EVM 호환 네트워크인 Arc는 친숙한 프로그래밍 환경을 제공하며, Tendermint(말라카이트)에 기반한 고성능 BFT 합의를 채택해 인터넷 스케일의 규제 금융 서비스를 위한 기관급 인프라를 제공한다. 이 설계는 허가형 검증자 집합에 의존하며, 바젤 은행감독위원회의 암호자산에 대한 전성 규제 프레임워크 등 신흥 규제 환경과도 정합적이다. 해당 프레임워크는 강건한 통제체계를 갖춘 네트워크의 안정코인이 은행의 자본 규제상 보다 우호적인 "그룹 1" 자산으로 분류될 수 있음을 시사한다 [Basel Committee on Banking Supervision, 2022].

본질적으로 Arc는 디지털 가치의 전송과 보안을 재정의 한다. Arc가 도입하는 세 가지 핵심 혁신은 다음과 같다.

- 안정적 수수료와 USDC의 원화(가스)화:** USDC를 트랜잭션 수수료의 원화 자산으로 채택해 수수료 변동성과 회계 복잡성을 크게 줄이며, 전용 페이마스터 통합을 통해 기타 현지 안정코인과 토큰화된 머니를 가스로 사용하는 것도 지원한다.
- 결정적 결제 최종성:** 1초 미만 시간 내 명확하고 확정적인 최종 결제를 제공하며, 금융시장 인프라 원칙(PFMI)과의 정합성을 갖춘다 [Committee on Payment and Market Infrastructures and International Organization of Securities Commissions, 2012].
- 옵트인 프라이버시:** 선택적 투명성을 가능하게 하는 프라이버시 보존 기술을 통합해 민감한 금융 워크플로우를 지원하고, 기관의 자체 컴플라이언스 이행을 뒷받침한다.

Arc는 인터넷 스케일 금융을 위한 인프라를 제공한다. Circle Internet Group(이하 Circle)은 USDC 운영, 체인 전반의 금융 프리미티브 구축, 기관·규제기관·개발자 커뮤니티와의 긴밀한 협업 경험을 바탕으로 이 노력을 주도할 독보적 위치에 있다. 안정코인 기반 금융의 고유 요구에 집중함으로써 Arc는 프로그래머블 머니를 위한 기초 결제 레이어이자 유동성 허브를 제공한다.

2 Arc의 코어 아키텍처

Arc의 아키텍처는 안정코인과 토큰화 자산 위에서 금융 서비스와 애플리케이션을 구축하기 위한 견고하고 기관급의 토대를 제공하도록 처음부터 설계되었다. Arc는 기존 블록체인의 핵심 한계를 극복하여, 규제 금융과 실물 상거래에 적합한 보안·성능을 갖춘 플랫폼을 제공한다. 그림 1과 같이 네트워크의 핵심은 말라카이트 합의 엔진을 구동하는 허가형 검증자 집합이며, 이는 Arc의 성능과

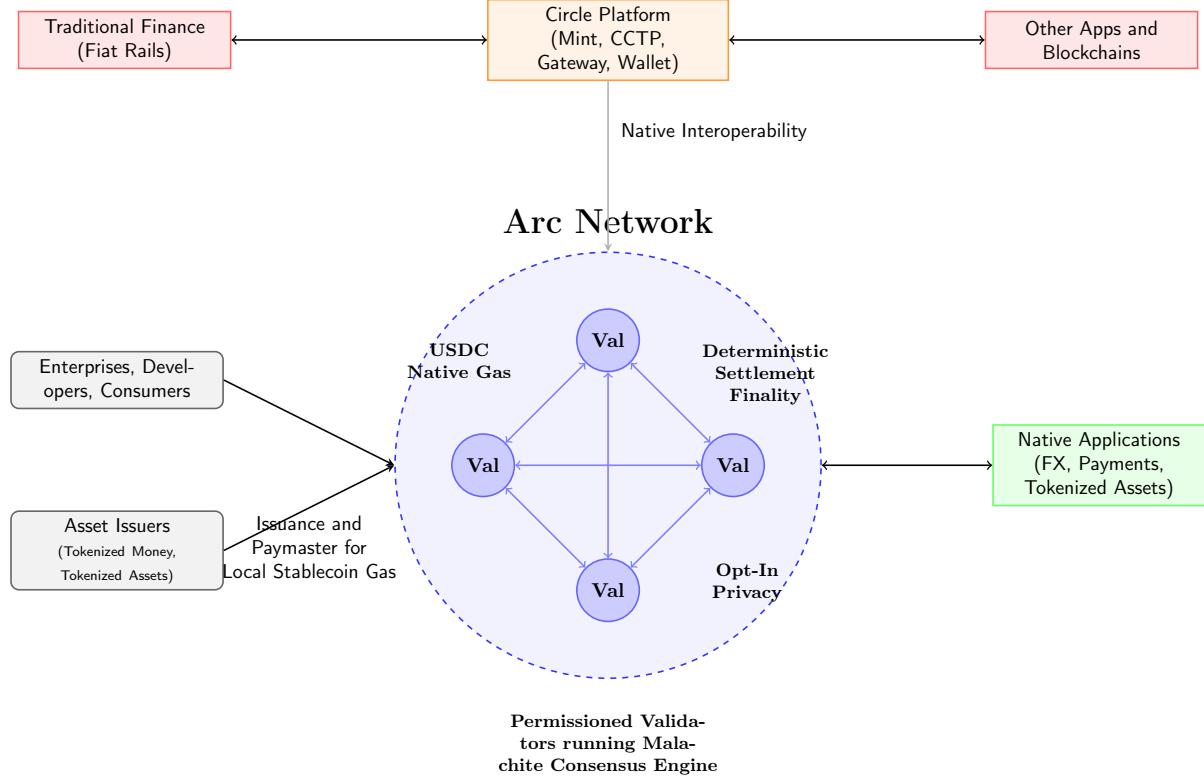


Figure 1: Arc의 아키텍처: 코어 구성요소, 네이티브 애플리케이션, 광범위한 금융 생태계와의 연결을 보여준다.

보안을 떠받치는 초석이다. 설계는 주류 금융 도입의 핵심 수요를 해결하는 세 가지 기둥 위에 서 있다.

첫째, 네트워크는 **안정코인 네이티브**로서 USDC를 가스로 사용해 수수료 변동성을 제거하고 운영을 단순화한다. 둘째, 고성능 합의 엔진을 통해 결제 최종성을 아(亞)초 단위로 결정적으로 제공함으로써 고가치 결제에 필요한 확실성을 보장한다. 셋째, **옵트인 프라이버시를 로드맵에 포함해** 잔액과 트랜잭션에 대한 선택적 투명성을 제공, 민감한 금융 정보를 보호하면서도 감사를 가능하게 한다. 이러한 코어 특성은 프로그래머를 FX, 결제, 기관 트레이딩 같은 안정코인 네이티브 애플리케이션을 뒷받침하고, Circle 플랫폼과 성장하는 안정코인 파트너 생태계를 통해 온체인·오프체인 금융 시스템과의 원활한 연결을 보장한다. 본 장에서는 Arc를 인터넷 네이티브 경제의 신뢰할 수 있는 결제 레이어로 자리매김하게 하는 이 세 가지 아키텍처 기둥을 상세히 설명한다.

2.1 USDC 원화(가스) 및 안정적 수수료 메커니즘

Arc의 기본 설계 원칙은 USDC를 모든 트랜잭션 수수료(가스)의 원화 자산으로 사용하는 것이다. 또한 전용 페이미스터 통합을 통해 현지 안정코인과 토큰화된 법정화폐를 가스로 사용하는 것도 지원한다. 가스를 법정화폐 가치에 연동하면, 투기성 네이티브 토큰을 운영 비용으로 쓰는 데에서 발생하는 변동성과 회계 복잡성이라는, 엔터프라이즈 도입의 핵심 장벽을 해소할 수 있다. 안정적인 계량 단위로 수수료를 책정함으로써 Arc는 사용자와 개발자에게 예측 가능하고 감사 가능하며 간소화된 재무 운영을 제공한다. 이는 가치 이전의 계량 단위와 트랜잭션 비용의 계량 단위를 일치시킨다.

이를 단순 모델로 설명하면, 사용자 관점에서의 트랜잭

션 비용 C_{USD} 은 다음과 같다. 변동성 네이티브 자산(예: ETH)을 사용하는 네트워크에서는, 달러 기준 비용이 세 변수의 곱이다: 소비된 가스 단위 g , 네이티브 자산 기준 단위 가스당 프로토콜 기본 수수료 b_{native} , 해당 자산의 시장가격 P_{native} . 즉 $C_{USD} = g \times b_{native} \times P_{native}$. 이 비용은 서로 다른 두 가지 변동성에 노출된다: 블록공간 수요에 따른 b_{native} 의 프로토콜 기인 변동성과, 투기에 따른 P_{native} 의 시장 기인 변동성이다. EIP-1559와 같은 수수료 안정화 메커니즘은 b_{native} 에는 영향을 미칠 수 있지만, 가스 토큰 가격 P_{native} 의 변동성은 제거하지 못한다. 후자는 종종 지배적 요소다. 따라서 프로토콜은 달러 단위에서 예측 가능한 트랜잭션 비용을 제공할 수 없다.

반면 Arc에서는 $C_{USD} \approx g \times b_{USDC}$ 로 볼 수 있는데, 이는 USDC 가격이 \$1로 안정적이기 때문이다. 시장 주도의 가격 변동성은 사실상 제거된다. 프로토콜은 따라서 b_{USDC} 를 조정함으로써 안정적인 계량 단위에서 트랜잭션 비용을 직접적이고 의미 있게 관리할 수 있다. 이와 같이 이중 변동성에서 프로토콜이 관리하는 단일 변동성으로의 전환은, 엔터프라이즈의 블록체인 사용을 근본적으로 디리스킹한다. 이는 예측 가능한 재무 기획과 견고한 비즈니스 모델을 가능하게 하여, 제도권 및 상업적 활용 사례에서 네트워크의 도입 잠재력을 높인다.

안정코인을 가스로 채택하는 선택은 단지 편의의 문제가 아니다. 이는 변동성 토큰으로는 불가능한 강력한 수수료 설계 공간을 연다. 예측 가능한 수수료 시장, 프로그램 가능한 수수료 리워드·보조금, 그리고 사용자가 다른 통화로 수수료를 지불할 수 있게 하는 전용 페이미스터 서비스를 가능하게 한다.

출시 시점에 Arc는 Ethereum의 EIP-1559 [Buterin et al., 2019]에서 영감을 받은, 안정성과 예측 가능성에 중점을

둔 수수료 시장을 구현한다. 핵심 강화점은 수수료 평활화 메커니즘이다. 프로토콜 기본 수수료는 블록 단위가 아니라 블록 활용도의 지수가중이동평균(EWMA)을 사용해 업데이트된다. 이 접근은 경계(bound)를 둔 기본 수수료와 결합되어 단기 변동성을 억제하고, 트랜잭션 비용을 지속적으로 낮게 유지한다. 초기 수수료는 온체인 Arc Treasury로 귀속되어 네트워크의 장기적 성장을 지원한다.

2.2 합의와 최종성

Arc의 보안 모델은 전통적 합의만으로 달성 가능한 수준을 넘어선 신뢰와 회복탄력성을 제공하도록 설계되었다. 이를 위해 Arc는 결정적 최종성을 제공하는 고성능 합의 엔진 말라카이트와, 높은 책무성과 운영 보증을 지닌 허가형 검증자 집합을 결합한다.

Arc의 목표는 기존 트랜잭션 블록을 두고 경쟁하는 것이 아니라, 필요한 고빈도 결제 보장을 제공함으로써 온체인으로 유입될 다음 수조 달러 규모의 결제와 기관 자본을 가능하게 하여 총잠재시장(TAM)을 확장하는 데 있다.

퍼블릭 블록체인이 글로벌 금융시장 인프라가 되는 데 있어 가장 큰 저해 요인 중 하나는 결제 최종성에 대한 명확한 정의의 부재다. 대부분의 기존 체인(지분증명·작업증명 포함)에서는 트랜잭션이 확률적 상태를 거치며, 최근 확정된 거래가 체인 리오그로 되돌려질 수 있다. 이러한 결제 모호성은 고가치 금융 워크플로우에 리스크와 자본 비효율을 초래한다. 극단적으로, 완전 무허가형 PoS 체인은 악의적 참여자가 스테이킹 토큰의 초과다수를 확보할 경우 "최종화 공격"으로 최종화된 블록을 되돌릴 위험도 있다. 스테이킹 토큰의 경제적 가치가 현재의 크립토 네이티브 스케일에는 충분할지라도, 수조 달러 규모의 토큰화 금융 자산을 보호하려면 훨씬 더 큰 담보가 필요하다. 또한 다수 체인에서 "정산"된 거래조차, 생태계 거버넌스에 의존한 사회적 조정 포크로 되돌려질 수 있다.¹ 레이어 1 위에 구축된 레이어 2 네트워크 역시 베이스 레이어의 동일한 최종성 리스크와 대기시간을 상속한다.

Arc의 기관급 성능과 보안의 기반은 말라카이트에 기반한 Tendermint BFT 프로토콜의 고성능 구현이다. 이는 초기 세대 체인의 확률적 최종성과, 최근 레이어 2의 중앙화된 시퀀싱 모델에서 의도적으로 벗어난 선택이다.

Arc는 소수의, 신원이 명확하고 신뢰성이 입증되었으며 지리적으로 분산된 기관으로 구성된 허가형 권한증명(PoA) 검증자 집합에 의존한다.² Arc는 규제된 자금 이동을 위한 기초 인프라로서, 전 세계적으로 분산된 금융 시스템을 지원하고자 한다. 블록체인에서의 "탈중앙화"가 전통적으로 기술적 회복탄력성과 겸연저항을 의미했지만, Arc는 더 넓은 관점을 취한다. Arc는 다수의 관할권과 체계적으로 중요한 기관들과의 전략적 협업에 뿌리를 둔 탈중앙화 모델을 그린다. 이러한 주체들이 네트워크 검증에 참여함으로써, 전 세계의 주권국과 엔터프라이즈의 미션 크리티컬 운영을 지원할 수 있는, 회복탄력적이고 규제 적합한 인프라를 제공하고자 한다. 검증자들은 블록 생산과 네트워크의 일상적 운영 무결성과 성능 보장에 책임을 진다. 실세계의 신원과 규제 의무(SOC 2 준수 등)는 악의적 행위에 대한 강력한 억지력을 제공한다.

Arc에서 트랜잭션은 미확인 상태이거나 100% 최종이며 비가역적이다. 확률적 단계는 존재하지 않는다. 검증자

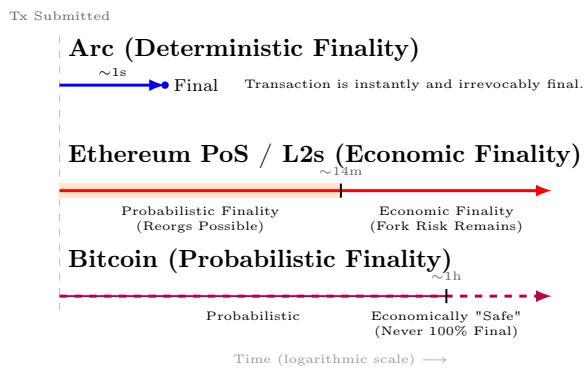


Figure 2: 서로 다른 최종성 모델의 타임라인 비교.

집합의 3분의 2를 초과하는 동의로 다라운드 투표 과정을 통해 블록이 커밋되면 즉시 최종화된다. 이는 명확하고 확정적인 최종 결제를 강조하는 PFMI 원칙 8과 부합한다 [Committee on Payment and Market Infrastructures and International Organization of Securities Commissions, 2012]. 최종성의 확실성은 금융 시스템 안정성에 필수적이며, 당사자 간 권리·관계를 명료히 하여 리스크 노출을 보다 효과적으로 관리할 수 있게 한다 [Cheng, 2022]. Arc에서는 이 프로세스가 1초 미만 내에 결제 보장을 제공한다. 이는 확실성과 속도가 모두 중요한 애플리케이션에 핵심적이다.

2.2.1 성능

Arc는 글로벌 금융시장 인프라의 엄격한 요구를 충족하기 위해 높은 처리량과 빠른 최종성을 제공하도록 기관급 성능으로 엔지니어링되었다. 지리적으로 분산된 20개 검증자 구성에서 Arc는 초당 약 3,000건(TPS)의 트랜잭션을 처리하고 350밀리초 미만의 사실상 즉시 최종성을 달성할 수 있다.³ 지리적으로 분산된 4개 검증자 구성에서는 TPS가 10,000건을 초과하고 최종성은 100밀리초 미만이 될 수 있다.⁴ 이러한 벤치마크는 범용 하드웨어로 달성되었으며, 프로덕션급 인프라에서는 더 큰 처리량이 가능함을 시사한다.⁵

이를 맥락화하면, 20 검증자 구성에서 Arc는 Fedwire Funds Service의 일일 평균 트랜잭션 수의 280배 이상을 처리할 수 있다.⁶ 이는 Arc가 전통적 실시간총액결제(RTGS) 시스템을 훨씬 능가하는 스케일에서 작동할 수 있음을 보여준다.⁷

말라카이트 합의 엔진의 계획된 개선에는 멀티 프로포저 지원(처리량 약 10배 증가 잠재)과 선택적 낮은 내결합성 구성(지연 약 30% 감소 잠재)이 포함된다.

¹ DAO 해킹과 포크에 관한 논의는 Dupont [2018] 참조.

² 검증자 선정 기준에는 운영 회복탄력성의 입증, 기동시간 보증, 규제 컴플라이언스, 보안 관행 등이 포함되나 이에 제한되지 않는다.

³ 20 검증자 구성은 10개 지역으로, 각 지역에 2개 검증자가 있다. 10개 지역은 뉴욕(두 데이터센터), 암스테르담, 프랑크푸르트, 런던, 샌프란시스코, 토론토, 싱가포르, 시드니, 맹갈루루이다.

⁴ 4 검증자 구성은 3개 지역으로, 뉴욕 2개, 샌프란시스코 1개, 토론토 1개 검증자다.

⁵ 해당 지역은 EVM 실행의 추가 오버헤드를 반영하지 않는다. 벤치마크는 합의에 초점을 두었다.

⁶ 2025년 6월 Fedwire Funds Service 데이터 기준 평균 일일 912,515건 이체.

⁷ 실시간총액결제에 대한 논의는 Liao et al. [2023] 참조.

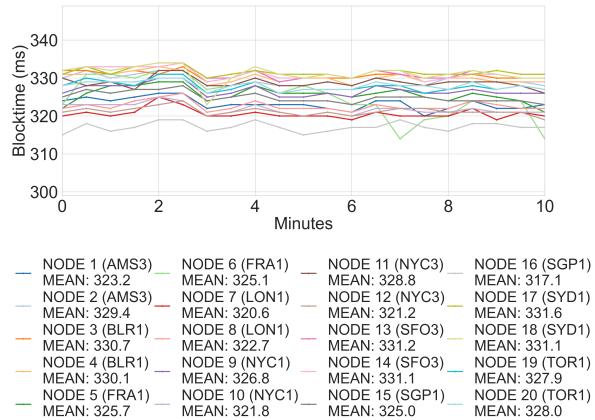


Figure 3: 20개 지리 분산 검증자에서 10분 구간 동안의 말라카이트 합의 엔진 블록 시간(밀리초, y축; 시간, x축).

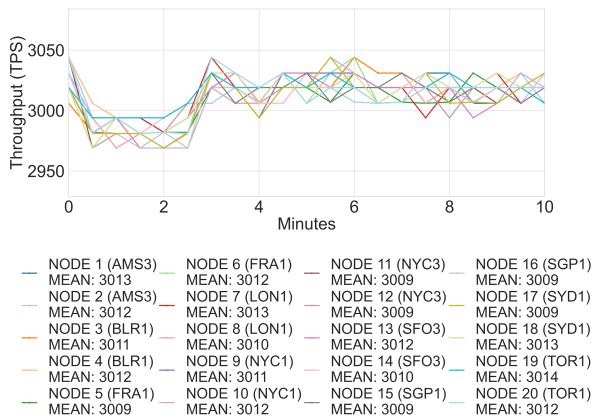


Figure 4: 20개 지리 분산 검증자에서 10분 구간 동안의 말라카이트 합의 엔진 처리량(TPS, y축; 시간, x축).

2.2.2 MEV 완화 로드맵

Arc 설계 철학의 핵심 요소는 최대추출가치(MEV)를 완화하는 접근이다. 많은 퍼블릭 체인에서 MEV는 네트워크 혼잡, 불안정성, 약탈적 행위의 주요 원인이 되었지만 [Daian et al., 2019], Arc의 로드맵은 모든 MEV가 해로운 것은 아님을 전제한다. 안정코인 네이티브 결제 맥락에서 Arc는 MEV를 크게 "건설적"과 "유해"로 구분한다. 건설적 MEV에는 안정코인의 동일성(fungibility)을 높이고 온체인 시장의 환율을 긴밀히 정렬시키는 크로스 베뉴 차익거래가 포함된다. 이는 원활한 결제 경험에 필수적이다. 예컨대 다양한 유동성 venue 간 USDC/EURC 가격을 수렴시키는 차익거래는 상거래에서 안정코인의 신뢰성을 직접적으로 뒷받침한다. 반면 유해한 MEV에는 샌드위치 공격 등, 결제 의도와 최종 결제 사이에 독성 흐름을 삽입해 거래 예측가능성을 훼손하고 신뢰를 약화시키는 행위가 포함된다. 이는 POS나 B2B 결제처럼 저지연이 중요한 환경에서 특히 문제다. 따라서 네트워크 설계는 약탈적 선행매수(front-running)를 억제하면서, 가격발견과 시장 효율성에 기여하는 유익한 백러닝(back-running) 활동은 보존하는 것을 목표로 한다. 이를 위해 암호화된 멤풀, 배치 트랜잭션 처리, 멀티 프로토콜 등 고도화된 완화 기술을 도입해, 기관급 금융 결제에 최적화된 공정하고 질서 있는 시장을 조성할 계획이다.

2.3 프라이버시: 규제 적합 금융을 위한 로드맵

금융 서비스가 온체인으로 이전되기 위해 프라이버시는 선택이 아니라 전제다. 급여 지급부터 무역금융 상세, 기업 재무에 이르기까지 민감한 상업·개인 데이터가 완전 투명한 퍼블릭 원장에서 노출될 수는 없다. 과제는 프라이버시를 제공하면서도 규제기관·감사인·허가된 제3자에게 완전한 감사 가능성을 보장하고, 기관이 자체 규제 의무를 완전히 이행할 수 있도록 하는 것이다. Arc는 모듈식이고 미래지향적인 아키텍처를 바탕으로, 옵트인 프라이버시를 단계적으로 제공하는 실용적 로드맵을 따른다.

Arc의 프라이버시 로드맵은 **기밀 송금(confidential transfers)**으로 시작한다. 이는 온체인 결제를 유지하면서도 거래 금액을 공중에 숨긴다. 주소까지 가리는 완전 익명성과는 구분해야 한다. 1단계에서는 거래 당사자 주소는 퍼블릭 원장에 보이되, 전송 금액은 암호화된다. 이 설계는 민감한 상업 데이터에 대한 기밀성을 제공하는 동시에, 주소 추적을 위한 기존 블록체인 분석·모니터링 도구와의 호환성을 유지한다.

글로벌 금융은 규제 환경 하에서 작동하므로, Arc의 프라이버시 모델은 처음부터 기관 내부의 컴플라이언스 프로그램을 지원하도록 설계되었다. "뷰 키(view keys)"와 같은 메커니즘을 통해 선택적 공개를 허용하여, 감사인이나 규제기관 등 허가된 제3자에게 특정 거래 데이터에 대한 읽기 전용 접근을 제공한다. 더불어, 기관은 항상 자사 고객이 수행한 거래(상·하류 거래 포함)에 대한 완전한 가시성을 유지한다. 이는 트랜잭션 모니터링과 Travel Rule 같은 규제 의무 이행에 필수적이다.

이는 전용 EVM 프리컴파일을 통해 스마트컨트랙트가 암호화적 백엔드와 상호작용하는 모듈식 아키텍처로 구현된다. 해당 백엔드는 TEE(신뢰 실행 환경)와 같은 기술을 활용해 암호화된 데이터 위에서 연산을 수행한다. 다수의 프라이버시 솔루션이 성능 제약을 겪는 반면, Arc의 TEE 기반 기밀 송금은 빠르고 감사 가능한 은닉(shielded) 트랜잭션을 제공한다. 모듈식 설계는 또한 신규 암호 백엔드가 성숙함에 따라 통합을 허용하여, 기관이 기대하는 지연·UX를 훼손하지 않고 기밀 금융을 제공하도록 한다.

앞으로 로드맵은 단순 송금을 넘어 **프라이빗 상태와 기밀 연산**으로 확장된다. 이는 프라이빗 주문서 상태, 무역 금융 계약, 자동화된 재무 운영 같은 복잡한 금융 로직을 프라이빗하게 관리할 수 있게 한다. 이 단계적 전개는 모듈식·미래지향적 설계에 의해 뒷받침된다. TEE는 성숙하고 성능이 우수한 기밀 연산의 출발점이지만, Arc의 아키텍처는 단일 기술에 종속되지 않는다. 플러그형 백엔드는 MPC(다자간 보안 연산), FHE(완전동형암호), 영지식증명 등, 생산 스케일 금융 시스템에 적용 가능한 성숙 단계에 이르면 다른 PETs(프라이버시 강화 기술)의 통합을 허용한다.

3 네이티브 애플리케이션과 활용 사례

Arc는 개발자가 정교한 금융 제품을 구축할 수 있도록 일련의 네이티브 애플리케이션과 서비스를 제공하는 금융 운영체계로 설계되었다. 이 통합적 접근은 복잡성을 줄이고 혁신의 기반을 제공한다. Arc는 Circle 제품만을 위해 구축된 것이 아니라—기관, 개발자, 기업가에게 신뢰·보안·스케일을 전제로 차세대 금융 혁신을 함께 구축하자는 개방형 초대다.

3.1 안정코인, 프로그래머블 FX, 토큰화 자산

Arc의 핵심 역량 중 하나는 다양한 형태의 토큰화 머니 발행에 대한 네이티브 지원이다. Circle이 발행한 USDC·EURC와 토큰화된 머니마켓펀드 USYC는 출시 시점부터 지원되지만, Arc는 이외의 토큰화 머니 발행자(법정화폐 담보 안정코인에서 토큰화 은행 예금, 중앙은행 화폐에 이르기까지)도 지원하는 개방형 플랫폼이다. 이를 통해 미 달러 이외 통화에 페깅된 안정코인 및 토큰화 상품을 발행할 수 있으며, 보다 포괄적인 글로벌 금융 시스템을 구현한다. 향후 내장 페이마스터 추상화를 결합하면, 사용자는 현지 안정코인으로 수수료를 지불할 수 있어 비-달러 중심 애플리케이션의 사용성을 크게 개선한다.

Arc는 또한 토큰화된 수익형 자산의 프리미어 venue로 설계되었다. 출시 시점에 네트워크는 Circle의 USYC를 지원한다. 이는 단기 미 국채로 담보화된 규제된 이자지급 형 토큰이다.⁸ 이를 통해 기관, 엔터프라이즈, 적격 DeFi 프로토콜은 안전하고 규제 적합한 환경에서 자본을 생산적으로 활용할 수 있는 저위험 온체인 수익원을 확보한다. USYC와 같은 자산의 통합은 Arc를 강력한 온체인 트레저리 관리, 담보 대출, 신규 자본시장 인프라의 기반으로 변모시킨다.

다중 통화 기반 위에서 Arc 로드맵에는 기관급 외환(FX) 엔진이 포함된다. 이 엔진은 심사된 거래상대방 간 24/7 프로그래머블 PvP(지급 대 지급) 결제를 가능케 하며, 온체인 스마트컨트랙트를 활용해 거래 등록, 구성 가능한 결제 윈도우, 담보 관리를 수행한다. 또한 오프체인 RFQ 실행 레이어를 통합해 기관 테이커가 마켓메이커 네트워크로부터 FX 호가를 소싱할 수 있게 한다. 초기에는 규제 적합성, 시장 진전성, 핵심 통로의 심층 유동성을 보장하기 위해 허가형 시스템으로 운영된다. 장기 로드맵에는 기관급 FX 유동성에 대한 접근을 민주화하는 무허가형 프로토콜도 포함된다.⁹

마지막으로 Arc는 고품질 토큰화 금융자산의 다음 진화를 지원하도록 설계되었다. 안정코인과 토큰화 현금성 자산을 넘어, 규제된 실물자산(RWA)—토큰화 주식, 채권, 사모 신용, 사모 펀드, 기타 기관급 증권—의 발행, 결제, 조합가능성을 가능하게 한다. 이는 규제된 자산 발행사, 커스터디언, 펀드 관리자와의 파트너십을 통해 달성되며, 토큰화 표현이 법적으로 견고하고, 적절히 담보화되며, 실물 금융 의무와 통합되도록 한다. Arc에서 발행된 토큰화 자산은 차입·대출 프로토콜, 거래·스왑 venue, 스테이킹 메커니즘, 수익 전략 등 DeFi 프리미티브 전반과 네이티브하게 조합될 수 있다. 이를 통해 자본 배분자, 펀데크, 자산운용사는 투명하고 자동화되며 글로벌하게 접근 가능한 차세대 금융 상품을, 실물 세계의 규제 준수에 앵커링된 상태로 구축할 수 있다.

오프체인 금융 시스템을 온체인으로 가져옴으로써, Arc는 지리·인프라·라이선스 제약에 의해 역사적으로 제한되었던 금융 도구에 대한 접근을 변화시킨다. Arc는 전 세계 투자자가 자산에 지속적으로 접근·거래·결제할 수 있는 통합 환경을 조성하며, 프로토콜 레벨의 옵트인 프라이버시 컨트롤을 통해 컴플라이언스 의무를 충족한다. Arc는 단순한 디지털 자산 블록체인을 넘어, 자본시장을 근본부터 재구성하는 플랫폼이다.

이러한 안정코인 발행, 고품질 토큰화 자산, 프로그래머

⁸USYC 이용 가능성에 대한 면책은 문서 말미 참조.

⁹온체인 FX와 국경 간 결제에 대한 논의는 Adams et al. [2023] 참조.

블 FX 역량은 네트워크를 차세대 글로벌 금융 애플리케이션—국경 간 결제 솔루션에서 자동화 해징, 온체인 자본시장, 엔터프라이즈 트레이딩의 환리스크 관리 도구에 이르기까지—구축을 위한 강력한 플랫폼으로 만든다.

3.2 크로스체인 유동성과 결제 허브

Arc는 안정코인 유동성과 애플리케이션의 허브로 기능하도록 설계되었다. 빠른 최종성과 USDC 가스를 바탕으로, Arc 사용자는 Circle의 CCTP와 Gateway를 통해 수십 개 이상의 블록체인 전반의 어느 애플리케이션에도 즉시 접근할 수 있다. 이러한 연결성을 통해 사용자는 기저 체인을 의식하지 않고 USDC와 애플리케이션을 사용할 수 있으며, 크로스체인 활동을 통합되고 직관적인 경험으로 단순화한다. Arc, USDC, Circle의 상호운용 제품은 마찰 없는 금융 생태계의 토대를 함께 이룬다.

이 역량은 다음의 네이티브 통합 Circle 제품군에 의해 가능해진다:

- **Mint:** Circle 고객은 법정화폐 은행 예치금을 Arc 상의 USDC 및 EURC로 직접 무증단·무신용 의존·무선유동성으로 민팅할 수 있어, 전통 금융에서 온체인 자본으로의 가장 빠른 온램프를 제공한다.
- **CCTP(Cross-Chain Transfer Protocol)¹⁰:** USDC의 네이티브 발행 체인으로서 Arc는 CCTP를 활용해 연결된 어느 블록체인으로든 안정코인 유동성을 무허가·안전·신속하게 이전한다. 이를 통해 자본은 지체 없이 가장 필요한 곳으로 이동한다.
- **Gateway:** Arc는 Gateway를 통해 체인 추상화된 USDC 잔액을 지원하여, 기업이 선입금이나 리밸런싱 없이도 체인 간 안정코인 유동성 수요를 즉시(<1초) 충족할 수 있게 한다. 앱과 지갑은 통합된 USDC 잔액과 생태계 간 조합가능성을 기반으로 매끄러운 UX를 제공할 수 있다.

이들 제품은 또한 기타 안정코인으로의 유틸리티 확장을 모색해, 크로스체인 유동성의 비전을 실현할 것이다.

이 모델의 초석은 Arc의 결정적 최종성이다. 트랜잭션이 단일 블록 내에서 (아초 단위로) 최종화되므로, Arc의 유동성은 소각 후 대상 체인에서 거의 즉시 검증 가능하게 재민팅될 수 있다. 이는 확률적 또는 경제적 최종성에 의존하는 체인에서 브리지들이 결제 보장을 위해 기다려야 하는 긴 대기시간을 제거한다. 결과적으로 Arc는 법정화폐→안정코인 온램프에 가장 빠른 체인이다, 광범위한 블록체인 전반으로 해당 유동성을 배포하는 데 가장 효율적인 분배 레이어로 기능한다.

3.3 엔터프라이즈 결제와 정산

안정적인 계량 단위, 예측 가능한 수수료, 신속한 정산, 기밀성이 결합되면 Arc는 엔터프라이즈 결제와 정산에 이상적인 플랫폼이 된다. 네트워크의 네이티브 특성은 단순한 가치 이전을 넘어, 복잡하고 프로그래머블한 결제 워크플로우를 지원하도록 설계되었다.

Arc는 개발자와 기업에, 강력한 애플리케이션으로 조합될 수 있는 핵심 결제 모듈군을 제공한다(Arc 로드맵 상에 반영 및 순차 제공):

- **인보이스 연계 결제:** 트랜잭션에 인보이스 상세나 메시지 같은 구조화 데이터를 첨부하는 네이티브 지

¹⁰CCTP에 대한 세부사항은 Mayerchak et al. [2025] 참조.

원.¹¹ 이는 대사를 단순화하고 매출·매입 프로세스를 자동화한다.

- **환불 및 분쟁 프로토콜:** 환불 관리와 결제 분쟁 해결을 위한 온체인 메커니즘. 이는 주류 채택에 필수적인 소비자·가맹점 보호 수준을 제공하나, 많은 기존 블록체인 시스템에선 결여되어 있다.
- **스마트 트레저리 에이전트:** 자율적이며 AI 네이티브 인 에이전트를 생성하여, 기업 트레저리를 관리하고 프로그래머블 지출 정책을 집행하며 실시간으로 운전자본을 최적화할 수 있다. 이는 확장 가능한 실시간 재무 운영을 가능케 하여 수작업 부담을 줄이고 자본 효율을 개선한다.

이러한 역량은 Circle Payments Network(CPN)과 함께 활용되어 국경 간 결제의 운영 효율을 높이는 한편, 글로벌 공급망 금융과 로열티 분배의 자동화에서 완전 규제 적합한 온체인 금여 시스템 및 자본시장 인프라 구축에 이르기까지 폭넓은 중요 활용 사례를 가능케 한다. 이러한 도구를 네이티브 프리미티브로 제공함으로써, Arc는 기업이 블록체인 상에서 안전하고 고성능이며 규제 적합한 금융 솔루션을 구축·배포하는 데 필요한 진입 장벽을 크게 낮춘다.

4 로드맵

Arc의 공개 테스트넷은 2025년 가을로 예상된다. Arc의 메인넷 베타 출시는 안정 수수료 아키텍처, 아초 단위의 결정적 최종성, FX 엔진 로드맵과 같은 코어 컴포넌트를 포함한다. 또한 Circle의 플랫폼 제품군(CPN, USDC, EURC, USYC, Mint, Wallets, Contracts, CCTP, Gateway, Paymaster 등)과 서드파티 생태계 인프라 지원이 제공될 예정이다.

프라이버시 향상 기능은 네트워크의 후속 업그레이드에서 제공될 것이며, 기밀 송금으로 시작해 완전히 프로그래머블한 프라이버시로 발전한다. 프라이버시 외에도, 암호화 멤풀, 배치 트랜잭션 처리, 멀티 프로포저 등 기관급 금융 결제에 최적화된 공정하고 질서 있는 시장 조성을 위한 MEV 완화 방안이 로드맵에서 탐색된다.

마지막으로, Arc의 추가 보장 로드맵에는 선택된 검증자 집합 내에서 허가형으로 구현되는 지분증명(PoS) 메커니즘으로의 전환이 포함된다. 해당 업그레이드는 더 넓은 검증자 탈중앙화와 거버넌스 유연성을 가능케 하여, Circle의 장기적 목표와 정합적으로 네트워크의 견고성을 담보한다. 또한 초기 검증자 집합을 넘어 Arc가 Circle과 독립적으로 가능할 수 있도록 하여, 운영 회복탄력성을 보강한다. 말라카이트 로드맵에는 성능 향상을 위한 새로운 멀티 프로포저 설계와, 2-페이즈 Tendermint 변형을 통한 지역 감소 등 합의 스택 전반의 최적화가 포함된다.

5 결론

Arc는 금융과 상거래를 위한 블록체인 인프라가 어떠해야 하는지에 대한 근본적 재구성을 제시한다. Arc는 인터넷 상에서 글로벌하고 규제 적합하며 효율적인 금융 시스템을 구축하는데 필요한 현실적 조건을 이해하는 데 기반하며, 기관·플랫폼·엔터프라이즈의 실제 요구를 충족한다. 수수료 변동성, 결제 불확실성, 프라이버시와 규정 준수

의 동시 달성 문제라는 핵심 한계를 해결함으로써, Arc는 프로그래머블 머니 시대를 위한 맞춤형 토대를 제공한다.

본 문서가 제시한 핵심 혁신—USDC를 가스로 하는 안정코인 네이티브 아키텍처, 고성능·결정적 결제 최종성, 규제 적합 프라이버시에 대한 약속—은 고립된 기능이 아니다. 이는 현대 경제를 위한 기초 신뢰 레이어를 창출하려는 일관된 비전의 통합된 구성요소들이다.

Arc는 인터넷의 속도와 개방성, 그리고 규제된 금융의 신뢰와 신뢰성이 만나는 지점이다.

전 세계 결제와 송금에서 토큰화 자본시장과 자율적 기업 트레저리에 이르기까지, 적용 가능성은 광범위하다. Arc는 인터넷 상의 금융 서비스와 애플리케이션이 구축될 안전·투명·고성능 결제 레이어가 되도록 설계되었다. 우리는 전 세계 선도 금융기관, 엔터프라이즈, 혁신가들을 초대한다. 인터넷 스케일로 금융과 상거래의 미래를 함께 구축하자.

References

Austin Adams, Mary-Catherine Lader, Gordon Y. Liao, David Puth, and Xin Wan. On-chain foreign exchange and cross-border payments. *SSRN Electronic Journal*, 2023. doi: 10.2139/ssrn.4328948. URL <https://ssrn.com/abstract=4328948>. Accessed August 2025.

Basel Committee on Banking Supervision. Prudential treatment of cryptoasset exposures. Technical report, Bank for International Settlements, December 2022. URL <https://www.bis.org/bcbs/publ/d545.pdf>.

Mira Belenkiy. Recibo: Encrypted messages for erc-20 transactions. <https://www.circle.com/blog/recibo-encrypted-messages-for-erc-20-transactions>, January 2025. Accessed July 2025.

Vitalik Buterin, Eric Conner, Rick Dudley, Matthew Slipper, Ian Norden, and Abdelhamid Bakhta. EIP-1559: Fee market change for eth 1.0 chain. <https://eips.ethereum.org/EIPS/eip-1559>, April 2019. Ethereum Improvement Proposal 1559.

Juliet M. Cheng. How to build a stablecoin: Certainty, finality, and stability through commercial law principles. *Berkeley Business Law Journal*, 19(1):129–170, 2022. URL <https://scholarship.law.berkeley.edu/bblj/vol19/iss1/5/>.

Committee on Payment and Market Infrastructures and International Organization of Securities Commissions. Principles for financial market infrastructures. Technical report, Bank for International Settlements, April 2012. URL <https://www.bis.org/cpmi/publ/d101.htm>.

Committee on Payments and Market Infrastructures. Enhancing cross-border payments: building blocks of a global roadmap - technical background note. Technical report, Bank for International Settlements, July 2020. URL <https://www.bis.org/cpmi/publ/d194.pdf>.

Philip Daian, Steven Goldfeder, Tyler Kell, Yunqi Li, Xueyuan Zhao, Iddo Bentov, Lorenz Breidenbach,

¹¹ "Recibo: Encrypted Messages for ERC-20 Transactions"에 대해서는 Belenkiy [2025] 참조.

and Ari Juels. Flash boys 2.0: Frontrunning, transaction reordering, and consensus instability in decentralized exchanges. *arXiv preprint arXiv:1904.05234*, 2019.

Quinn Dupont. Experiments in algorithmic governance: A history and ethnography of 'the dao,' a failed decentralized autonomous organization. In Malcolm Campbell-Verduyn, editor, *Bitcoin and Beyond: Cryptocurrencies, Blockchains, and Global Governance*, pages 169–187. Routledge, 2018.

Gordon Y. Liao, Thomas Hadeed, and Ziming Zeng. Beyond speculation: Payment stablecoins for real-time gross settlements. *SSRN Electronic Journal*, June 2023. doi: 10.2139/ssrn.4476859. URL <https://ssrn.com/abstract=4476859>. Accessed August 2025.

Walker Mayerchak, Mike Grant, Jonathan Lim, Chase McDermott, Elim Poon, Adrian Soghoian, Kaili Wang, and Gordon Y. Liao. Cross-Chain Transfer Protocol (CCTP) V2. https://github.com/circlefin/evm-cctp-contracts/blob/master/whitepaper/CCTPV2_White_Paper.pdf, March 2025. Accessed July 2025.

면책공고 본 문서는 일반적 정보 제공만을 목적으로 한다. 투자 자문을 구성하지 않으며, 어떠한 투자에 대한 매수·매도를 권유하거나 권장하지 않는다. 투자 의사 결정의 타당성을 평가하는 데 사용되어서는 안 된다. 또한 회계·법률·세무 자문이나 투자 권고로 의존되어서는 안 된다. Arc는 Circle Technology Services, LLC("CTS")가 제공한다. CTS는 소프트웨어 제공업체이며 규제된 금융 또는 자문 서비스를 제공하지 않는다. 본 문서에 기술된 모든 제품 기능은 사전 고지 없이, 언제든, CTS의 단독 재량으로 수정·지연·취소될 수 있다. 귀하는 사용자에게 제공하는 서비스에 대해 전적으로 책임을 지며, 필요한 라이선스·승인을 취득하고, 관련 법령을 준수하여야 한다. 본 문서는 작성자의 현재 의견을 반영할 뿐, Circle Internet Group 또는 그 계열사의 입장을 대변하지 않으며, 그들과 관련된 개인의 의견을 반드시 반영하지 않는다. 본 문서의 의견은 사전 통지 없이 변경될 수 있다.

USYC는 디지털 자산 토큰이다. 각 USYC 토큰은 Hashnote International Short Duration Fund Ltd.(펀드)의 1주식을 디지털로 표현한다. 펀드는 베리다 통화당국(BMA) 라이선스를 보유한 디지털 자산 사업자인 Circle International Bermuda Limited("CIBL")를 토큰 관리자(토큰 운영 책임자)로 지정하여, 펀드를 대신해 USYC를 관리하도록 하였다.

펀드 지분과 USYC는 1933년 증권법(개정 포함)상 "비 미국인(Non-U.S. Persons)"에게만 제공된다. 추가 적격성 제한이 적용될 수 있다. 본 문서는 교육·정보 제공 목적일 뿐이며, 어떠한 증권·금융상품·그 밖의 제품의 매도 제안이나 매수 청약으로 해석되어서는 안 된다.