XION: 일반화된 추상화 계층

Burnt Research

초안 배포, 2023년 12월 7일

초록

우리는 프로토콜 수준에서 사용자 경험 을 구현하는 일반화된 추상화 계층인 XION을 제안합니다. 이는 추상화된 계정, 서명, 수수료, 상호운용성 등에 관련된 프로토콜 수준의 구현을 통해 안전하고 직관적이며 매끄러운 사용자 경험를 가능하게 합니다. XION의 메타 계정의 모듈식 디자인, 서명에 구애받지 않는 구현, 그리고 XION의 매개변수화된 수수료 계층을 결합함으로써 조합 가능하고 미래에 대비한 인프라 계층을 제공합니다. XION은 개발자 경험을 단순화하고, 블록체인 기술의 탈중앙화 정신을 유지하면서도 주류 사용자들의 진입 장벽을 크게 낮추어 사용자 중심의 환경을 가능하게 합니다. 추상화된 상호운용성을 통해, 우리는 XION의 매끄러운 사용자 경험를 모든 연결된 체인으로 확장하는 솔루션을 추가로 제안하고, 그것이 가능하게 하는 여러 새로운 사용 사례를 탐구합니다.

1. 서론

기술적인 어려움이 블록체인 기술의 광범위한 채택을 방해하고 있습니다. 신규 사용자는 지갑 설정, 관리, 기기 간 사용, 구매, 가스 요금, 멀티체인 상호작용 등 혼란스러운 복잡성에 직면합니다. 블록체인은 엄청난 잠재력을 가지고 있지만, 이러한 복잡성으로 인해 광범위한 채택이 어렵습니다. 이러한 복잡성은 높은 사용자 이탈률과 낮은 사용자 관심도로 이어져, 사용자 친화적인 블록체인 인프라의 필요성을 제기합니다. 계정 추상화[1]의 도입과 같은 제안된 솔루션들은 이러한 문제를 완화하려고 시도했습니다. 그러나 컨센서스 레이어 변경을 피하는 구현은 단편화 문제[2][3], 상당한 배포 및 실행 비용, 중앙화 위험, 채굴자 추출 가능한 가치 포착[4], 그리고 검열[1]로 이어졌습니다. 현재 산업의 기술적 복잡성과 대중적 매력 사이의 격차를 해소할 수 있는 포괄적인 솔루션은 존재하지 않습니다.

본 논문은 XION의 새로운 아키텍처를 탐구합니다. 일반화된 추상화 계층의 기반은 계정, 서명, 수수료 관리, 상호운용성 등 복잡한 블록체인 기능들을 프로토콜 수준에서 직접 매끄럽게 통합하는 데 있습니다. XION은 신규 사용자들에게 큰 진입 장벽을 제거하는 한편, 개발자들에게는 단편화 문제를 피할 수 있게 합니다. 서명에 구애받지 않는 인프라는 기존의 다양한 암호학적 커브를 지원하며, 미래의 개발에도 쉽게 적응할 수 있어 시장 범위를 넓힐 뿐만 아니라 다양한 블록체인 프로토콜 간의 장기적인 생존 가능성과 상호운용성을 보장합니다. 추상화된 상호운용성을 통해 XION은 네이티브 애플리케이션뿐만 아니라 연결된 체인에서 구축된 애플리케이션에도 매끄러운 경험을 제공할 수 있습니다

본 논문의 나머지 부분은 다음과 같은 구조를 따릅니다: 2장에서는 XION이 의존하는 기술적 개념의 배경을 제시합니다; 3장에서는 일반화된 추상화을 소개하며, 여기에는 메타 계정, 서명 추상화, 기기 추상화, 매개변수화된 수수료 계층, 그리고 향상된 토큰 발행 역학이 포함됩니다; 4장에서는 추상화된 상호운용성을 제시합니다; 5장에서는 새로운 사용 사례 예시를 제시합니다; 그리고 6장에서는 결론을 내립니다.

2. 배경

2.1 외부 소유 계정

일반적으로, 블록체인은 두 가지 유형의 계정을 가지고 있습니다: 1) 외부 소유 계정, 그리고 2) 스마트 계약 계정[5]. 전통적으로 사용자는 비대칭 암호화를 사용하는 외부 소유 계정 (EOAs)를 통해 블록체인과 상호 작용합니다. 이러한 계정은 공개 키/개인 키 쌍을 가지며, 공개 키는 블록체인에 저장되고 개인 키는 사용자가 오프체인에서 보관합니다. 사용자만 알고 있는 개인 키는 거래에 서명하는 데 사용되며, 공개 키는 서명의 진위성을 확인하는 데 사용됩니다.

그러나 EOAs는 많은 단점을 가지고 있습니다. 추가적인 인증 메커니즘을 구현할 수 없고, 자율적인 작업이나 스마트 계약 실행을 수행할 수 없으며, 공개 키/개인 키 쌍을 변경할 수 없습니다. 그 결과, EOAs는 사용자에게 단일 실패 지점이 됩니다. 사용자가 개인 키에 대한 접근을 잃으면 계정에 완전히 접근할 수 없게 됩니다. 마찬가지로, 사용자의 개인 키가 손상되면 계정도 되돌릴 수 없이 손상됩니다.

2.2 스마트 계약 계정

두 번째 유형의 계정인 스마트 계약 계정 (SCAs)는 블록체인의 코드에 의해 관리됩니다. 이들의 생성은 EOA에 의해 시작된 거래를 통해 블록체인에 배포되는 것을 포함합니다. 배포되면 이 스마트 계약들은 블록체인의 특정 주소에 위치하며, 그들의 코드는 작동하는 규칙과 조건을 결정합니다. 이러한 규칙들은 특정 조건이 충족되거나 거래나 다른 스마트 계약에 의해 트리거될 때 자동으로 실행됩니다. 전통적으로, 개인 키의 부재로 인해 이들은 거래를 시작할 수 없습니다.

위에서 언급한 EOA의 단점을 해결하기 위한 솔루션으로, 계정 추상화가 SCAs 거래를 시작할 수 있게 하는 방법으로 제안되었습니다[1]. 거래 인증이 상태 머신 수준에서 미리 정의된 규칙 세트에 의해 결정되는 대신, 계정 추상화은 이 작업을 SCAs에 위임합니다. 그렇게 함으로써 SCAs는 키 회전, 자율 작업 수행, 다중 요소 인증 통합 등 필요한 대로 맞춤형 인증 로직을 구현할 수 있습니다.

2.3 서명

암호학적 서명은 일련의 수학적 연산을 포함하는 디지털 서명 알고리즘을 사용하여 생성됩니다. Web3에서 가장 일반적으로 사용되는 서명 방식은 타원 곡선 디지털 서명 알고리즘 (ECDSA)[6]와 에드워즈 곡선 디지털 서명 알고리즘 (EdDSA)[7]입니다. Ethereum과 Bitcoin은 ECDSA를 사용하며, 특히 Secp256k1 curve[58]를 활용합니다. 반면 Solana는 EdDSA를 사용하며, 특히 Ed25519

curve[9]를 활용합니다. 또 다른 널리 인정받는 암호학적 곡선인 Secp256r은 Apple의 Secure Enclave[10]와 Android 디바이스[11]와 같은 대부분의 인기 있는 소비자 기기에서 사용됩니다.

2.4 거래

표준 Cosmos SDK[12] 내에서, 각 거래는 메시지로 구성됩니다. 거래가 블록에 포함되도록 설정되면, AnteHandler라고 불리는 고유한 컴포넌트를 거치게 됩니다. AnteHandler는 각 거래 전에 실행되는 함수들의 집합인 데코레이터를 통해 특정한 검사와 작업을 수행하는 역할을 합니다. 이는 거래 실행 전에 거래의 유효성, 서명, 수수료, 논스 검증 등을 보장합니다. 메시지가 실행된 후에는 자체적인 데코레이터 세트를 가진 PostHandler가 호출됩니다. 이 데코레이터는 거래가 처리된 후 블록에 커밋되기 전에 이벤트, 로그, 거래 후 로직 등을 실행하도록 설계되었습니다.

2.5 거래 수수료

거래 수수료는 종종 "가스"라고 불리며, 거래를 실행하는 데 필요한 계산 작업의 양을 측정하는 데 사용됩니다. 전통적으로 각 거래는 그 복잡성과 요구되는 계산 자원에 따라 일정량의 가스를 소비합니다. 거래를 확인하고 블록체인에 추가하는 역할을 하는 검증자들은 최소 가스 가격을 설정합니다. 자신의 거래가 처리되길 원하는 사용자들은 최소한 이 최소 가스 가격을 지불해야 합니다. 사용자가 거래에 대해 지불하는 총 수수료는 사용된 가스 양에 가스 가격을 곱하여 계산됩니다. 사용자들은 거래에 가스 수수료를 포함시키며, 이는 그들이 사용하는 블록체인의 네이티브 토큰으로 지불됩니다. 거래가 블록에 포함되면, 가스 수수료는 사용자의 계정에서 차감되어 해당 거래를 블록에 포함시킨 검증자에게 지급됩니다. 3.4장에서 다루었듯이, XION의 매개변수화된 수수료 계층는 최종 사용자들의 복잡성을 추상화하고, 마찰 없는 무가스 경험을 제공하며, 토큰에 구애받지 않는 결제 및 단위를 가능하게 하기 위해 상당한 변화를 구현합니다.

3. 일반화된 추상화

일반화된 추상화은 모든 사용자를 위한 내재된 암호화 복잡성을 제거하는 것을 목표로 하는 독특하고 포괄적인 인프라 솔루션입니다. 이 혁신의 핵심은 프로토콜 수준에서 직접 구현된 XION으로, 계정, 서명, 가스, 상호운용성, 가격, 디바이스, 결제 등을 매끄럽게 추상화합니다. 이렇게 전체적인 접근 방식을 통해 XION은 전 세계의 주류 사용자들에게 Web3의 약속을 전달할 차세대 프로젝트를 위한 견고한 기반을 마련합니다. 아래 섹션에서는 일반화된 추상화의 다양한 측면에 대해 자세히 설명합니다.

3.1 프로토콜 수준 계정 추상화: 메타 계정

XION은 스마트 계약 계정 (SCAs)와 상태 머신 변경[13]을 포함하는 프로토콜 수준의 구현을 통해 메타 계정를 도입합니다. 이러한 메타 계정는 기존의 개인-공개 키 모델을 분리하고, 전통적인 Web2 로그인 시스템과 일치하는 보다 직관적인 사용자 인터페이스의 생성을 가능하게 함으로써 사용자 상호작용을 간소화합니다. 사용자들은 이메일이나 생체 인증 방법과 같은 익숙한 방식으로 계정과 상호

작용하여, 직접적인 개인 키 관리의 필요성을 제거하면서도 완전히 비수탁성을 유지합니다.

XION의 모듈형 메타 계정 프레임워크는 키 가중치, 키 회전, 규칙 세트 및 다양한 인증 방법과 같은 고급 기능을 지원할 수 있는 고도로 적응적이고 안전한 권한 관리 시스템을 도입합니다. 이 시스템은 계정 관리에 상당한 유연성과 향상된 보안을 제공합니다:

• **키 회전**: 계정 키의 변경을 가능하게 함으로써 잠재적인 키 손상과 관련된 위험을 사전에 줄여 보안을 유지하는 데 필수적인 매개변수로, 키 노출 기간을 제한합니다.

• **규칙 세트**: 거래 한도에서 정기 결제에 이르기까지 계정을 관리하는 사용자 지정 규칙을 계정 소유자가 원하는 만큼 설정할 수 있게 하는 매개변수입니다.

• **키 가중치**: 각 키에 서로 다른 중요도나 권한 수준을 부여하여, 특정 작업에 더 높은 가중치의 키가 필요한 세밀한 계정 내 접근 제어 시스템을 가능하게 하는 매개변수입니다.

• **다양한 인증 방법**: 다양한 인증 방법을 지원함으로써 메타 계정은 다양한 기기와 플랫폼 간의 상호운용성을 달성하고, 진화하는 암호화 위협에 대한 탄력성을 가지며, 암호화 혁신에 대한 매끄러운 지원을 제공하고, 사용자 계정에 대한 강력한 보호를 보장합니다.

• **다중 요소 인증 프레임워크**: 다중 요소 인증 프레임워크는 유연하고 견고한 보안 구조를 가능하게 하며, 거래를 실행할 때 사용자나 조직이 정의한 특정하고 사용자 지정 가능한 매개변수에 따라 계정 내 접근 및 제어가 이루어지도록 보장합니다.

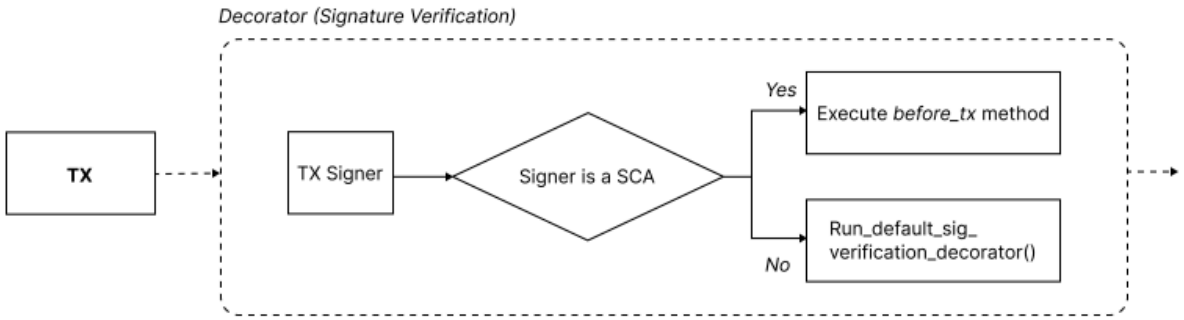

Figure 1: SCA Signature Verification Decorator

3.1.1 스마트 계약 계정 구현

스마트 계약 계정가 서명을 가능하게 하기 위해서는, 거래 인증의 책임이 상태 머신에서 스마트 계약 계정(SCAs)로 이동해야 합니다. 이는 SCAs에 두 가지 중요한 메서드인 before tx와 after tx를 통합함으로써 달성됩니다. 거래 실행 전에, 상태 머신은 before tx 메서드를 호출하며, 이는 SCA에게 상세한 거래 정보와 서명 인증 정보를 제공하여 서명 검증 및 기타 프로그래밍된 작업을 가능하게 합니다. 거래 실행 후, before tx 메서드와 모든 거래 메시지가 성공적으로 실행되었다면, after tx 메서드가 활성화되어 SCA가 추가적인 프로그래밍된 작업을 수행할 수 있게 합니다.

3.1.2 상태 기계 구현
상태 머신 업데이트는 SCA의 before tx와 after tx를 트리거하기 위해 두 가지 decorator 변경을 포함합니다. SigVerificationDecorator는 새로운 decorator로 업데이트되어 SCAs가 서명할 때 before tx 메서드를 트리거하거나, 기본 SigVerificationDecorator 로직을 단순히 진행합니다. 이는 그림 1에서 보여집니다. 추가적인 decorator가 PostHandler에 추가되어 after tx 메서드를 트리거합니다.

3.2 서명추상화
XION의 곡선 비종속적 구현은 SCA 기능을 확장하여 기존의 SCA 솔루션보다 상당한 이점을 제공합니다. 사용자의 메타 계정에는 최대 256개의 다양한 인증자를 추가할 수 있습니다. 사용자가 탈중앙화 애플리케이션에서 계정을 생성하거나 로그인할 때, 프로토콜에 하드코딩되는 대신, 서명 검증은 사용자의 계정으로 전송되는 동적 요청을 통해 구현됩니다. 이는 임의의 로직과 상태로 거래 검증을 가능하게 하여, XION을 미래에 대비한, 곡선 비종속적 프로토콜로 자리매김합니다. 거래 검증에 임의의 로직을 활용함으로써, XION은 특정한 검증 스키마에 제한되지 않습니다. 그 결과, XION은 특별한 적응이나 수정 없이도 다양한 암호학적 커브를 매끄럽게 지원합니다. 이는 기본 암호화 메커니즘을 사용자 인터페이스와 분리하는 XION의 독특한 추상화 접근 방식에서 비롯되며, 이를 통해 시스템은 다양한 암호학적 커브를 매끄럽게 채택할 수 있습니다.

XION의 일반화된 추상화 계층은 Ethereum의 Secp256K1과 Solana의 Ed25519와 같은 잘 확립된 것들을 포함하여, JSON Web Tokens (JWTs)에서 사용되는 Secp256R1 및 RS256과 같은 널리 채택된 표준을 포함한 다양한 범위의 커브를 지원합니다. 추가적으로, 향후 새롭게 등장하는 암호학적 curves도 지원할 수 있어, 새로운 트렌드와 발전에 적응할 수 있음을 보장합니다. XION 위에서 개발하는 개발자들은 암호학이 빠르게 발전함에 따라 그들의 스마트 계약 계정가 계속해서 호환되고 적응할 수 있을 것이라고 믿을 수 있습니다.

3.3 장치 추상화
위의 구현을 결합함으로써, XION은 사용자가 개인 키를 저장하고 관리할 필요성을 없앱니다. 이러한 접근 방식은 사용자가 여러 기기에서 계정을 사용하려 할 때 전통적으로 존재하던 안전 위험, 복잡성 및 마찰을 제거합니다. 따라서 XION의 독특한 접근 방식은 사용자들이 컴퓨터, 스마트폰 또는 태블릿을 포함한 다양한 기기에서 계정과 매끄럽게 상호작용할 수 있도록 함으로써 **기기 불가지론적(장치 비종속적)**이 됩니다. 이 보편적으로 접근 가능한 아키텍처는 사용자 경험를 크게 간소화하여 진입 장벽을 줄이고 XION에서 접근 가능한 모든 애플리케이션의 사용 편의성을 향상시킴으로써 광범위한 채택을 촉진합니다.

XION을 통해 앱과 상호 작용할 때, 사용자는 이메일, 소셜 계정, FaceId 등 여러 로그인 방법을 제공받으며, 고급 사용자들은 KeplR나 MetaMask 지갑과 같은 Web3 자격 증명을 사용하여 로그인할 옵션을 갖습니다. 따라서 XION은 비암호화(native) 사용자들을 위한 매끄러운 사용자 경험을 유지하면서 모든 사용자층에 서비스를 제공할 수 있습니다. 추가적으로, 그 메타 계정는 다중 요소 인증, 세션 키, 키 회전 등과 같은 추가적인 보안, 유연성 및 사용 편의성을 가능하게 합니다. 요약하면, XION의 프로토콜 수준의 계정 추상화과 서명 불가지론적 구현의 결합은 사용자가 안전하고 마찰 없는

방식으로 여러 기기에서 계정에 매끄럽게 접근할 수 있게 합니다.

3.4 매개변수화된 수수료 계층

원활한 사용자 경험을 창출하는 데 필요한 많은 기능을 가능하게 하기 위해, XION은 네트워크에서 수수료를 처리하는 새로운 접근 방식을 취합니다. 이는 다음을 포함합니다: 1) 글로벌 수수료 추상화(글로벌 수수료 추상화) 구현, 2) 새로운 유형의 수수료인 플랫폼 전송 도입, 그리고 3) 이것들을 수수료 승인의 사용과 결합하는것입니다.

3.4.1 수수료 추상화

XION은 글로벌 수수료 추상화를 통해 거래 수수료로 어떤 토큰도 사용할 수 있게 합니다. 이는 사용자들이 지불한 거래 수수료를 수수료 수집기에 모은 후, 이러한 비네이티브(비토착) 토큰들을 네이티브(토착) XION 토큰으로 교환하고, 생성된 네이티브 토큰들을 다시 수수료 수집기에 분배함으로써 달성됩니다. 이후의 3.5장에서 다루듯이, 수수료 수집기에 있는 생성된 네이티브 토큰들은 체인의 인플레이션을 결정하는 데 사용됩니다.

수집된 수수료를 네이티브 XION 토큰으로 교환하는 데에는 다양한 방법이 있으며, 이는 흥미로운 수수료 시장의 가능성을 열어줍니다. 한 가지 구현 방식은 원하는 탈중앙화 거래소(탈중앙화 거래소, DEX)로부터 주기적으로 데이터를 가져와 시간 가중 평균 가격(시간 가중 평균 가격, TWAP)을 사용하여 환율을 결정하는 것입니다. 그림 2에서는 비동기 상호체인 쿼리 모듈 (Async-ICQ)[14]를 사용하여 이를 시연합니다.

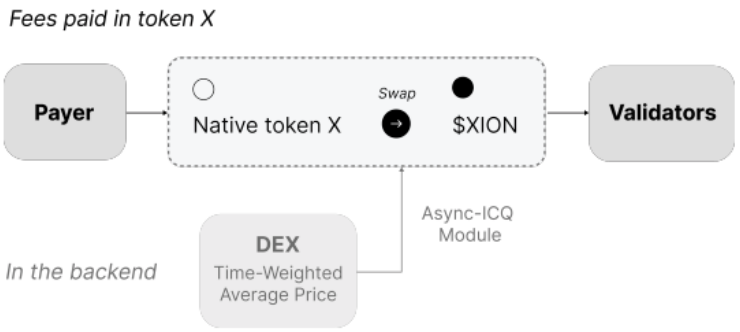

Figure 2: Fee Abstraction

3.4.2 플랫폼 전송 & 수수료 승인

네트워크상의 거래는 두 가지 주요 범주로 분류될 수 있습니다: 1) 가치가 교환되는 경우, 2) 가치가 교환되지 않는 경우. 첫 번째 범주의 거래가 네트워크에서 발생할 때, 플랫폼 전송가 실행됩니다. 참여자 간에 가치가 교환되기 때문에, 그 가치의 일부가 네트워크를 지원하고 시빌 공격을 방지하기 위한 수수료로 취해집니다. 가스 수수료가 네트워크 공격을 완화하는 방식과 유사하게, 플랫폼 전송 수수료는 교환된 가치에 비례하여 공격자가 지불해야 하는 비용 장벽입니다. 그림 3에서 보여지는 이 우아한 설계는 가스 토큰을 요구하지 않고도 사용자가 원하는 어떤 통화로 직접 거래할 수 있게 합니다. 그런 다음, Section 3.4.1에서 설명된 글로벌 수수료 추상화를활용하여, 수집된 수수료는

네이티브 토큰으로 교환되어 네트워크 인플레이션을 결정하고 네트워크 참가자들에게 보상합니다.

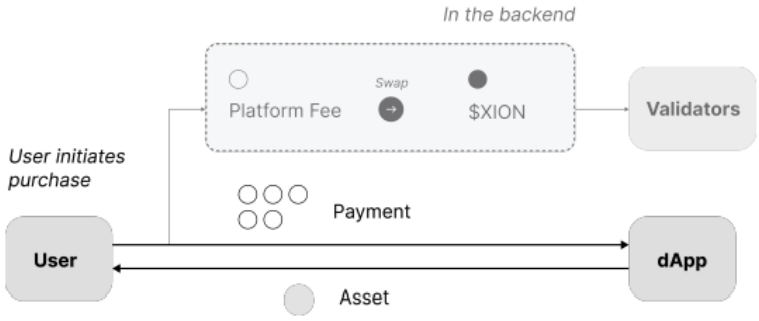

Figure 3: PlatformSend

두 번째 범주의 거래가 발생할 때, 네트워크 스팸을 방지하기 위해 일반적인 가스 수수료가 부과되며, 이러한 유형의 거래에 대해 XION은 수수료 승인을 구현합니다. 그림 4에서 보여지듯이, 이는 개발자들이 사용자들을 대신하여 거래를 매끄럽게 후원하고 무가스 경험을 제공할 수 있게 합니다. 추가로, 스폰서는 스테이킹 보상을 활용하거나 최소 거래 임계값을 적용하거나 기타 구성 가능한 매개변수를 사용하는 등 다양한 방식으로 수행할 수 있습니다.

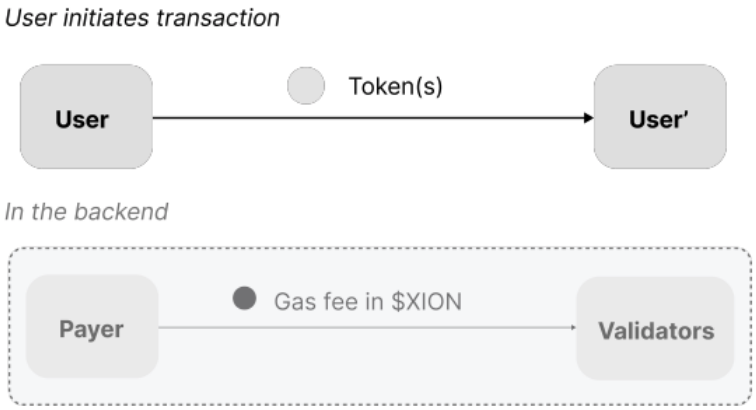

Figure 4: Fee Sponsoring

3.4.3 가격 및 결제 추상화

위에서 언급한 일반화된 추상화의 매개변수화된 수수료 계층을 통해, XION은 USDC, 완전하게 준비금이 보유된 디지털 달러를 주요 거래 통화로 사용할 수 있는 최초의 블록체인이 됩니다[15]. 그림 5는 수수료 수집기에서 USDC 수수료가 네이티브 토큰으로 자동 교환되는 동태를 보여주며, 이를 통해 XION 위에서 구축된 모든 제품이 단순히 USDC를 사용하여 사용자들에게 가격이 책정되고 결제될 수 있게 합니다. 이는 가스 토큰을 획득하는 전통적인 마찰을 제거하고, 사용자들이 익숙한 가격으로 매끄럽게 온보딩할 수 있게 하며, 동시에 원치 않는 변동성과 투기를 줄여줍니다.
추가적으로, 매개변수화된 수수료 계층를 통해 XION은 모든 연결된 생태계와 네이티브하게 상호운용

가능하며, 사용자는 원하는 어떤 토큰으로도 지불할 수 있습니다. 최종 사용자의 무가스(가스less) 경험과 결합하여, XION의 일반화된 추상화은 마찰을 줄이고 Web3의 대중적인 채택을 이끄는 능력에서 두드러집니다.

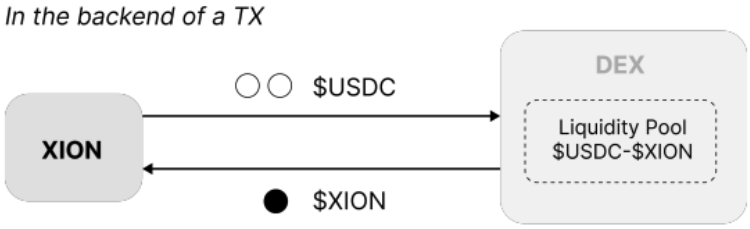

Figure 5: USDC Fee Swap

3.5 토큰 발행 동작

네트워크의 거시경제적 역학은 토큰 발행의 미묘한 차이에 의해 형성되며, 이러한 발행 파라미터는 시스템의 장기적인 생존 가능성에 매우 중요합니다. 일반화된 추상화의 매개변수화된 수수료 계층와 긴밀하게 연계된 XION의 설계는 네트워크 참여자들의 인센티브와 장기적인 지속 가능성의 균형을 맞추기 위해 토큰 발행 역학에 대한 제1원칙 접근 방식을 취합니다. XION은 발행 모듈에 두 가지 중대한 변경을 가합니다:

- 누적된 수수료는 가능할 경우 인플레이션을 상쇄하는 데 사용됩니다.
- 토큰 인플레이션은 스테이킹된 토큰에 대해서만 계산됩니다.

3.5.1 발행 모듈 개요

발행 모듈의 목표는 생태계 내에서 스테이킹된 토큰과 유동성 토큰의 사전에 결정된 비율을 유지하는 것입니다. 이는 세 가지 값을 설정함으로써 달성됩니다: 인플레이션의 상한선, 인플레이션의 하한선, 그리고 목표 스테이킹 비율입니다. 일단 인플레이션율이 결정되면, 모듈은 인플레이션 비율을 충족하기 위해 블록에서 생성되어야 하는 토큰 수를 계산합니다. 이는 시장 유동성과 스테이킹된 공급량 사이의 중요한 균형을 이루는 것으로, 이는 네트워크의 장기적인 보안과 성장에 영향을 미치며, 아래의 공식들이 이 균형을 보여줍니다.

만약 P_bonded < P_goal 이면 : IR = min(IR + ΔIR, IRmax)

이 시나리오에서, ΔIR은 P_bonded가 P_goal보다 낮을 때 인플레이션이 증가하는 비율입니다.

만약 P_bonded = P_goal 이면 : IR = 상수

이 시나리오에서, 결속 비율이 목표치에 도달하면 인플레이션율은 변하지 않습니다.

만약 P_bonded > P_goal 이면 : IR = max(IR − ΔIR, IRmin)

이 시나리오에서, ΔIR은 P_bonded가 P_goal을 초과할 때 인플레이션이 감소하는 비율입니다.

위에서, IR은 현재 인플레이션율을 나타냅니다. P_bonded는 현재 스테이킹된 토큰의 비율입니다. P_goal은 스테이킹된 토큰의 목표 비율입니다. IRmax는 허용되는 최대 인플레이션율이고, IRmin은 허용되는 최소 인플레이션율입니다.

이 공식들은 현재 결합된 토큰의 퍼센티지와 목표 결합 퍼센티지 사이의 관계, 그리고 최대 및 최소 인플레이션율의 제약을 기반으로 인플레이션율의 동적 조정을 효과적으로 포착합니다.

3.5.2 수수료로 인플레이션 상쇄

기본 발행 모듈은 현재 블록에서 누적된 수수료를 매 블록마다 발행되는 토큰에 더해 검증자들에게 전달합니다. 이는 다음과 같이 표현됩니다:

$$T\_net = T\_minted + F\_collected$$

여기서 T_minted는 T_total × IR이며, T_total은 현재 토큰의 총 공급량입니다.

XION이 구현한 첫 번째 변경 사항은 블록에서 수집된 수수료를 사용하여, 해당 블록에서 발행해야 할 토큰의 수를 이 누적된 수수료로 상쇄하는 것입니다. 이는 다음과 같이 나타납니다:

$$T\_net = T\_minted - F\_collected$$

F_collected가 충분히 크다면, T_net을 줄일 수 있으며, 이는 수집된 수수료를 사용하여 새로 발행되는 토큰을 상쇄함으로써 효과적으로 인플레이션 영향을 감소시킵니다.

체인 사용량이 증가하면, 수수료의 누적이 새로운 토큰의 발행을 지속적으로 상쇄하기 때문에 인플레이션이 감소하게 됩니다. 수수료 누적이 스테이커들에게 분배하는 데 필요한 블록당 토큰 수를 초과하면, 초과된 토큰은 소각되어 토큰 공급량이 감소하게 되고, 자연스럽게 디플레이션이 발생합니다.

3.5.3 스테이킹된 토큰의 토큰 인플레이션

토큰 인플레이션과 관련하여, 기본 발행 모듈은 모든 기존 토큰에 대해 인플레이션을 계산합니다. 이는 다음과 같이 표현될 수 있습니다:

$$T\_minted = IR \times T\_total$$

여기서 T_minted는 발행될 총 토큰 수이며, IR은 인플레이션율, T_total은 총 토큰 공급량입니다.
그 결과, 스테이커를 위한 연간 수익률(APY)은 다음과 같이 표현될 수 있습니다:

$$APY = IR \div P\_bonded$$

여기서 APY ≥ IR이며, 이는 P_bonded의 함수입니다. 이는 모든 토큰이 스테이킹되지 않기 때문에, 실제로 인플레이션율보다 더 높은 스테이킹 연간 수익률(APY)을 초래합니다.
XION의 민트 모듈은 중요한 변화를 구현합니다. 모든 토큰을 기준으로 계산하는 대신, 스테이킹된 토큰을 기준으로 계산합니다.

$$T\_minted\_x = IR \times T\_bonded$$

T_bonded가 T_total보다 작기 때문에, 동일한 IR에서 총 인플레이션 영향인 T_minted_x는 T_minted보다 작거나 같습니다.

그 결과, 인플레이션 영향은 감소하고 스테이커들은 항상 APY = IR을 보게 됩니다. 이 변화는 장기 참여자를 유치하여 네트워크의 안전성을 보장함으로써 훨씬 더 안정적인 환경을 조성합니다.

4. 추상화된 상호 운용성

XION의 추상화된 상호운용성은 일반화된 추상화의 핵심 측면으로, 크로스체인 사용자 경험를 크게 향상시킵니다. 이는 XION과 같은 컨트롤러 체인에서 어떤 호스트 체인에서도 작업을 수행할 수 있게 해주는 패키지 전달 미들웨어[16][18]의 사용을 통해 달성됩니다. 이 미들웨어를 기존의 일반화된 추상화 프레임워크와 통합함으로써, 간소화된 프로토콜 수준의 인터페이스가 만들어집니다. 그림 6에서 보여지듯이, 이는 XION과 채널을 구축한 어떤 체인에서도 사용자가 작업을 수행할 수 있게 하며, 동시에 XION의 매끄러운 사용자 경험를 즐길 수 있게 합니다.

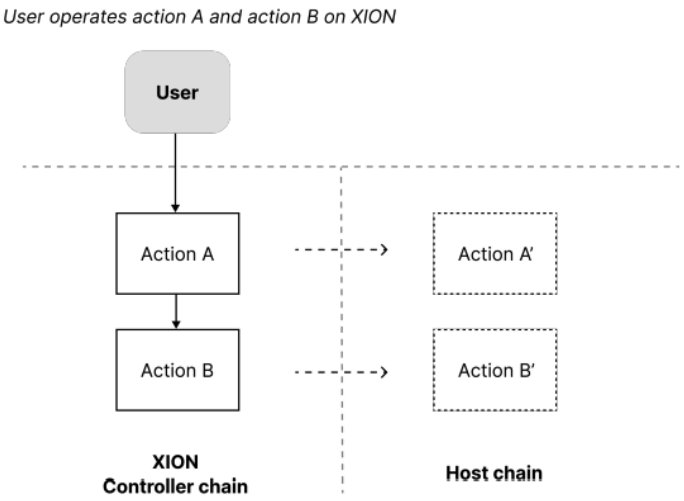

Figure 6: Multi-Interaction to Host Chain

XION의 상호운용성 접근 방식은 멀티체인 환경에서 흔히 발생하는 계정 분산 문제를 해결합니다. 사용자는 여러 체인에 걸쳐 소유한 계정들을 자신의 *XION 메타 계정*에 연결하여, 하나의 중앙 계정에서 자산을 관리할 수 있는 매끄러운 방법을 제공합니다. 각 계정은 소스 체인의 식별자와 원래 계정의 주소를 결합한 고유 식별자를 가지며, 이는 연결된 체인 간에 독특한 매핑을 보장합니다. 따라서 사용자는 단일 XION 인터페이스를 통해 멀티체인 계정을 제어할 수 있습니다.

XION은 여러 구현 방법[17–18]을 통해 대칭적 통신을 활용하여 이를 달성합니다. 이는 별도의 블록체인들 사이에 신뢰할 수 있고, 순서가 있으며, 인증된 통신 채널을 구축합니다. 그런 다음, 패키지 전달 미들웨어 컴포넌트는 계정 인터페이스의 추상을 통해 다양한 체인에서 실질적인 사용자 계정 제어 및 관리를 제공하는 데 중요하며, 그림 7에서 볼 수 있듯이 XION과 연결된 어떤 체인과도

매끄러운 상호작용을 가능하게 합니다.

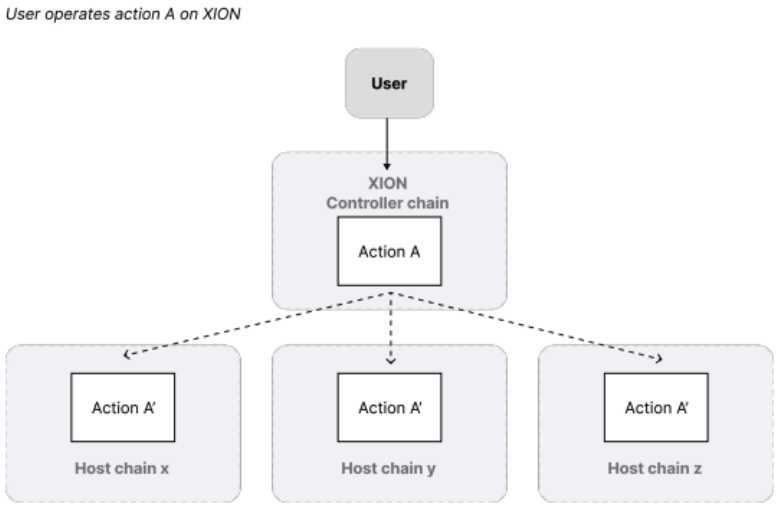

Figure 7: Multi-Chain Interactions from XION

XION의 일반화된 추상화 계층과 결합하여, 추상화된 상호 운용성는 모든 프로토콜 수준의 추상을 확장하여 이전에는 달성할 수 없었던 새로운 크로스체인 가능성과 매끄러운 사용자 경험를 촉진합니다.

5. 일반화된 추상화 애플리케이션

XION의 일반화된 추상화 계층은 기존 애플리케이션의 사용자 경험를 크게 향상시킬 뿐만 아니라, 다양한 새로운 애플리케이션도 가능하게 합니다. 아래에서는 XION의 일반화된 추상화으로 가능해진 몇 가지 예시적인 사용 사례를 제공합니다. 그다음으로, 추상화된 상호운용성을 활용하여 혁신적인 크로스체인 사용 사례를 가능하게 하는 애플리케이션의 추가적인 예를 제시합니다.

5.1 활성화 사용 사례

5.1.1 디지털 뱅킹

디지털 뱅킹 애플리케이션은 일반화된 추상화을 활용하여 고객들이 제한된 시간 동안 접근할 수 있는 임시 세션 키를 설정할 수 있게 함으로써 거래의 보안을 높이는 동시에 사용자들이 자신의 거래 한도와 조건을 정의할 수 있도록 합니다. 이러한 사용자들은 대규모 거래에 대해 다중 인증 방법 요구 사항을 설정할 수 있으며, 특정 인증 방법에 대한 접근을 잃을 경우 계정 정보를 복구할 수 있는 능력도 갖추게 됩니다.

5.1.2 글로벌 Venmo 메신저

탈중앙화된 메시징 서비스는 일반화된 추상화를 활용하여 사용자가 스마트폰, 태블릿 또는 데스크톱을 사용하더라도 동일한 계정으로 메시지 채팅에 안전하고 매끄럽게 접근할 수 있게 합니다. 사용자들은 익숙한 법정 통화를 사용하여 메시징 앱 내에서 직접 원활한 무가스 거래를 통해 국경 간

자산을 송금하여 전 세계적으로 거래할 수 있습니다.

5.1.3 크리에이터 경제 애플리케이션

탈중앙화된 콘텐츠 스트리밍 서비스는 일반화된 추상화을 활용하여 구독 기반의 계정을 생성합니다. 사용자는 수동으로 갱신할 필요 없이 스마트 계약 트리거를 통해 매월 자동으로 청구됩니다. 모든 연령의 크리에이터와 그들의 팬들은 마찰 없이 이러한 계정을 생성하고, 모든 기기에서 콘텐츠에 접근할 수 있습니다.

5.1.4 향상된 게임 경험

온체인 게임은 일반화된 추상화을 활용하여 세션 키의 매끄러운 사용, 거래의 배치 처리, 무가스(가스less) 거래를 가능하게 함으로써, 사용자의 자산을 위험에 빠뜨리지 않으면서도 부드럽고 안전한 게임 플레이를 제공하고, 동시에 지연 시간을 감소시킵니다.

5.1.5 사용자 친화적 DAO

온라인 협업 플랫폼은 일반화된 추상화을 활용하여 구성원들이 서로 다른 권한 수준을 가진 탈중앙화된 조직을 구축합니다. 이를 통해 비기술적 사용자들도 직관적이고 익숙한 Web2 인터페이스를 통해 거버넌스나 의사 결정 과정에 참여할 수 있습니다.

5.1.6 클라우드 스토리지 서비스

탈중앙화된 클라우드 스토리지 플랫폼은 일반화된 추상화을 활용하여 가족이 여러 기기에서 매끄럽게 콘텐츠에 접근할 수 있게 합니다. 계정 권한을 통해 가족 구성원들은 서로 다른 수준의 접근 및 편집 권한을 갖게 됩니다.

5.2 추상화된 상호 운용성

5.2.1 전 세계적으로 연결된 애플리케이션

추상화된 상호운용성을 통해 XION은 모든 기존 Web3 애플리케이션에 접근할 수 있습니다. 예를 들어, 사용자가 FriendTech 앱을 사용하여 Base 네트워크에 자금을 보유하고 있습니다. 이 사용자는 이제 Solana의 피트니스 앱인 StepN을 사용하고 싶어 하며, FriendTech 자금을 사용하여 디지털 신발을 구매하려고 합니다. XION을 사용하여, 그들은 Base와 Solana 모두의 계정을 제어하는 XION 메타 계정을 통해 StepN과 매끄럽게 상호작용하고 사용할 수 있습니다. 백그라운드에서 사용자의 Base 자금은 전송되고 변환되어 Solana 마켓플레이스에서 디지털 신발을 구매하는 데 사용됩니다. 최종 사용자에게 이것은 직관적이고 매끄러운 경험이며, 복잡한 크로스체인 상호작용을 사용자 친화적으로 만드는 XION의 능력을 보여줍니다.

5.2.2 글로벌 분산형 마켓플레이스

사용자들은 여러 블록체인에 걸쳐 있는 탈중앙화된 마켓플레이스에 참여하여 다양한 암호화폐로 상품이나 서비스를 사고 팔 수 있으며, 일반화된 추상화의 추상화된 상호 운용성를 활용하여 통합된 보안 정책과 크로스체인 결제 기능을 가진 단일 계정으로 모든 것을 관리할 수 있습니다.

5.2.3 크로스체인 게임

추상화된 상호 운용성를 통해 게이머들은 하나의 통합된 게임 계정 아래에서 자산과 업적을 한 블록체인 게임에서 다른 체인의 게임으로 사용하거나 거래할 수 있는 크로스체인 게임 경험에 참여할 수 있습니다. 이 게임 계정은 모든 기기에서 쉽게 접근할 수 있으며, 다양한 수준의 접근 제어가 가능하고, 계정 손실의 가능성을 제거하기 위한 안전 조치를 구현할 수 있습니다.

5.3 DAOs

탈중앙화 자율 조직 (DAO)는 일반화된 추상화과 **추상화된 상호운용성**을 활용하여 여러 블록체인에서 매끄럽게 운영할 수 있습니다. 이는 다양한 애플리케이션, 더 넓은 사용자 기반, 더욱 유연하고 효율적인 거버넌스에 효과적으로 접근할 수 있게 하며, 일반적인 Web2 방법을 통해 주류 사용자 참여를 가능하게 합니다.

5.4 글로벌 프로필

크로스체인 신원 인증 시스템을 구축할 수 있으며, 이를 통해 사용자는 동일한 자격 증명과 평판을 사용하여 여러 블록체인에서 상호 작용할 수 있습니다. 이는 인식 가능한 평판을 통해 하나의 검증 가능한 신원으로 다양한 서비스에 접근할 수 있게 함으로써 수많은 가능성을 열어주며, 모든 생태계를 더 가깝게 만듭니다.

6. 결론

XION은 일반화된 추상화 레이어를통해 주류 채택을 방해해온 주요 과제들을 해결합니다. XION은 사용자 경험를 단순화하여 블록체인 기술을 더 넓은 대중이 접근할 수 있게 합니다. 이는 계정 생성, 상호 작용, 거래 수수료, 상호운용성과 관련된 복잡성을 제거하고, 익숙한 상호 작용으로 대체합니다. 추가로, 이는 이 매끄러운 사용자 경험를 크로스체인 상호 작용까지 확장합니다. 일반화된 추상화은 XION 생태계의 역량을 강화할 뿐만 아니라, 매끄러운 연결성과 광범위한 채택을 결합함으로써 블록체인 산업의 전반적인 성장에 기여합니다. 다각적인 일반화된 추상화 레이어를 통해, XION은 지속 가능하고 유연하며 사용자 중심적인 블록체인 인프라 패러다임을 제공하여 산업을 혁신과 광범위한 수용의 새로운 시대로 이끌 수 있습니다.

References

1. V. Buterin, and Y. Weiss. “ERC-4337: Account Abstraction Using Alt Mempool [Draft].” 29 Sept. 2021. [Online]. Available: https://eips.ethereum.org/EIPS/eip-4337

2. N. Mudge, “EIP-2535: Diamonds, Multi-Facet Proxy.”Ethereum Improvement Proposals, Ethereum Foundation.[Online]. Available: https://eips.ethereum.org/EIPS/eip-2535.

3. F. Giordano, et al., “EIP-1271: Standard Signature Validation Method for Contracts.” Ethereum Improvement Proposals, Ethereum Foundation. [Online]. Available: https://eips.ethereum.org/EIPS/eip-1271.

4. P. Daian, S. Goldfeder, et al., ”Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges,” in 2020 IEEE Symposium on Security and Privacy (SP), 2020, pp. 914-931.

5. V. Buterin, “A next-generation smart contract and decentralized application platform,” Whitepaper, 2014. [Online]. Available: https://ethereum.org/en/whitepaper/.

6. D. Johnson, A. Menezes, & S. Vanstone, “The Elliptic Curve Digital Signature Algorithm (ECDSA).” IJIS 1, 36–63 (2001). [Online]. Available: https://doi.org/10.1007/s102070100002

7. I. Liusvaara, and S. Josefsson. “RFC 8032 Edwards-Curve Digital Signature Algorithm (EdDSA).” Internet Engineering Task Force, Jan. 2017. [Online]. Available: https://rfc-editor.org/rfc/rfc8032.

8. S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System.” Bitcoin. [Online]. Available: https://bitcoin.org/bitcoin.pdf.

9. A. Yakovenko, “Solana: A new architecture for a high-performance blockchain v0.8.13.” Solana Foundation. [Online]. Available: https://solana.com/solana-whitepaper.pdf.

10. Apple Inc., “Secure Enclave,” Apple Support Guide. [Online]. Available: https://support.apple.com/guide/security/secure-enclave-sec59b0b31ff/web

11. A. Hamlin, “Secure Multiparty Computation.” Comp 116, Tufts University. [Online]. Available: www.cs.tufts.edu/comp/116/archive/ahamlin.pdf.

12. J. Kwon, E. Buchman, “A Network of Distributed Ledgers.” Tendermint. [Online]. Available: https://v1.cosmos.network/resources/whitepaper.

13. L. Lyu, “abstract-account,” GitHub repository. [Online]. Available: https://github.com/larry0x/abstract-account

14. A. Raja, E. Saradar, “Asynchronous Interchain Query Module (Async-ICQ),” GitHub repository, August 30, 2022. [Online]. Available: https://github.com/strangelove-ventures/async-icq

15. J. Allaire, S. Neville, “Introducing USD Coin (USDC) a Fully Reserved Stablecoin,” Circle Blog, Sept. 26, 2018. [Online]. Available:

https://www.circle.com/blog/introducing-usd-coin

16. T. Yun, S. King, J. Lee, “Cosmos/ibc ICS-027: Interchain Accounts Specification,” GitHub repository, [Online]. Available: https://github.com/cosmos/ibc/tree/main/spec/app/ics-027-interchain-accounts

17. C. Goes, “The Interblockchain Communication Protocol: An Overview,” Interchain GmbH. [Online]. Available: https://arxiv.org/pdf/2006.15918.pdf

18. Abacus Works, “Hyperlane v3 Docs,” Abacus Works, 2023.[Online]. Available: https://docs.hyperlane.xyz/