

셀로(Celo)

해당 번역본은 이용자가 디지털자산 관련 정보를 편리하게 확인할 수 있도록 단순 참고용으로 번역된 것이며, 투자 권유를 목적으로 하지 않습니다.

그 내용이 정확하지 않을 수 있으므로 정확한 정보 습득을 위해서는 원문을 참고하시거나 원문 작성 주체 측에 문의하시기 바랍니다.

두나무는 해당 번역본 내용의 진실성 및 정확성을 보장하지 않고, 제공된 정보에 의한 투자 결과에 대하여 어떠한 책임도 지지 않으며, 투자 손실은 투자자에게 귀속됩니다.

Celo 프로토콜: 분산형 소셜 결제를 위한 다중 자산 암호 프로토콜

cLabs 팀
초안 버전 0.25

초록

지불 수단으로서 암호화폐의 대규모 채택을 가로막는 가장 큰 장벽 두 가지는 사용 편의성과 구매력의 변동성입니다. 우리는 이러한 문제들을 해결하기 위해 주소 기반 암호화 스킴과 안정적 가치 자산을 활용한 Celo 프로토콜을 소개합니다. 이 두 가지 속성이 결합되어 어떻게 전 세계 기준 통화, 지역 및 로컬 안정가치 통화, 사회배당을 포함하는 화폐 생태계를 형성하는 데 기여할 수 있는지를 설명합니다. 우리의 첫 번째 애플리케이션은 스마트폰을 중심으로 한 소셜 결제 시스템입니다.

서론

암호화폐는 지불 수단으로서 법정화폐에 비해 여러 가지 이점을 가지고 있습니다. 스마트폰만 있다면 누구나 접근 가능한 기술을 활용해, 은행 송금보다 훨씬 빠르고, 더 낮은 비용(특히 국제 송금의 경우)으로, 공개적으로 감사 가능하고 보안이 확보된 방식으로 가치를 전송할 수 있습니다. 또한 암호화폐는 프로그래밍이 가능하며, 금융 계약, 에스크로, 보험 등을 중개인 없이 실행할 수 있습니다.

그러나 현재로서는 암호화폐가 지불 수단으로서 주류로 채택되는 데에는 몇 가지 장벽이 존재합니다. 첫째, 결정론적 공급 규칙과 예측 불가능한 수요로 인해 성공적인 코인들은¹ 디플레이션 성향의 가격 불안정을 겪습니다. 그 결과, 사용자들은 이를 교환 수단보다는 가치 저장 수단으로 합리적으로 선호하게 됩니다. 둘째, 가격 변동성이 큰 암호화폐를 지불 수단으로 사용하고자 하더라도, 사용자는 지불을 받기 위해 개인/공개키 쌍을 생성하고, 지불을 보내기 위해 상대방의 공개키를 입력해야 합니다. 이러한 점들은 사소한 문제처럼 보일 수 있으나, 사용자 경험의 미세한 차이가 실제 사용률에 큰 차이를 불러온다는 것이 경험적으로 입증되었습니다.

암호 기반 소셜 결제 시스템이 성공하기 위해서는, 결제가 문자 메시지를 보내는 것만큼 쉬워야 하며, 통화의 변동성은 최소화되어야 합니다. 우리는 이러한 문제를 각각 해결하는 Celo 프로토콜을 설명합니다. 결제의 용이성을 높이기 위해, Celo 프로토콜은 주소 기반 암호화(address-based encryption)라는 암호화 스킴을 도입합니다. 이 방식에서 참여자들은 전화번호에서 공개키로의 매핑을 검증하며, 사용자는 친구의 휴대전화 번호를 공개키로 사용할 수 있습니다.

가치 안정성을 위해, Celo 프로토콜은 탄력적 공급 규칙을 갖춘 통화 정책과 가변 가치 준비금에 의해 안정화되는 자산을 도입합니다. 더 나아가, 이 프로토콜은 새로운 안정가치 코인을 지속적으로 도입할 수 있는 거버넌스 구조를 갖추고 있어, 지역적·광역적·유틸리티 용도의 안정가치 통화 패밀리를 구성할 수 있으며, 새로운 코인의 도입은 기존 코인의 안정성 특성을 강화하는 방식으로 설계됩니다.

마지막으로, Celo 프로토콜은 거래에 참여하는 모든 사용자가 검증에 참여할 수 있는 모바일 블록 보상 메커니즘을 도입하여, 참여자 기반을 넓히고 블록 보상을 일상 사용자에게 더 쉽게 접근할 수 있도록 합니다.

이 모든 요소는 함께 작동하여 설득력 있는 소셜 결제 프로토콜을 구성합니다.

¹ 학계, 규제 기관, 기업가 등은 분산 원장에 고유한 디지털 자산을 지칭하기 위해 "코인"과 "토큰"을 혼용하여 사용합니다. 본 문서에서는 '디지털 자산', '코인', '암호화폐', '토큰'을 일반적으로 상호교환 가능하게 사용합니다.

경량 신원 기반의 사용 용이성

암호화폐가 지불 수단으로서 주류 채택에 이르지 못하는 중요한 장애물 중 하나는 직관적이고 탈중앙화된 공개키 인프라의 부재입니다. 그 결과, 오늘날의 탈중앙화 시스템에서 지불을 보내기 위해 사용자는 수신자의 공개키를 반드시 알아야 합니다(중앙화된 게이트웨이를 사용하지 않는 이상). 또한 지불을 받기 위해서는 먼저 개인/공개키 쌍을 생성하고 이를 브로드캐스트해야 합니다. 이메일 주소나 전화번호로 직접 지불을 보내고, 별도의 지갑을 설정하지 않고도 지불을 받을 수 있다면 훨씬 더 간편할 것입니다.

Identity-based encryption(신원 기반 암호화) [18]은 이러한 문제를 해결할 수 있는 가능성을 보여줍니다. 이 방식에서는, 예를 들어 Alice가 bob@company.com으로 암호화된 메시지를 보내고자 할 때, Bob의 공개키 인증서를 별도로 획득할 필요 없이 단순히 bob@company.com이라는 문자열을 공개키로 사용하면 됩니다. 신원 기반 암호화에 기반한 암호화폐 시스템은 훨씬 매끄러운 사용자 경험을 제공할 수 있지만, 원래의 제안과 후속 구현들 [4, 6]은 모두 개인키를 생성하기 위한 신뢰된 제3자인 private-key generator를 필요로 한다는 점에서 제한을 받습니다. 그 결과, 이러한 방식은 개방형이고 허가가 필요 없는

시스템에서는 유용성이 떨어집니다.

주소 기반 암호화

우리는 신원 기반 암호화의 변형 방식으로 주소 기반 암호화(address-based encryption)를 제안합니다. 이메일 주소나 전화번호를 공개키로 직접 사용하는 대신, 신뢰된 개인키 생성자에 의존하지 않고 사용자가 기존 방식으로 자신만의 개인/공개키 쌍을 생성하게 합니다. 그런 다음 사용자는 자신의 공개키를 [address -> public key] 형태의 튜플로 저장하는 공개적인 append-only 데이터베이스에 등록합니다. 이 데이터베이스는 기능적으로는 탈중앙화되어 있어 중앙 관리 주체 없이 저장·관리·유지됩니다. 하지만 논리적으로는 통합되어 있어 누구나 언제든지 데이터베이스의 모든 항목을 확인할 수 있습니다. 핵심적으로, [address -> public key] 튜플은 P2P 네트워크에 의해 검증됩니다. 검증을 수행하기 위해, 네트워크 내 무작위로 선택된 검증자들이 서명되고 보안이 유지된 메시지를 등록자에게 보내면, 등록자는 해당 메시지에 자신의 개인키로 서명한 뒤 이를 Attestations 스마트 계약에 반환합니다. Attestations 계약은 메시지를 보낸 검증자가 실제로 존재하는지 확인하고, 서명이 수신자의 공개키와 일치하는지도 검증합니다.

이 프로토콜은 이메일 주소뿐만 아니라, 휴대전화 번호, IP 주소, 은행 계좌 및 라우팅 번호 등 안전한 메시지를 보낼 수 있는 모든 채널에 대해 동작합니다. 또한, 주소 키에 임의의 문자열을 추가할 수 있도록 허용함으로써, 각 주소에 대해 서로 다른 애플리케이션에 사용할 수 있는 다수의 공개키를 저장할 수 있습니다. 그 결과, 이 암호화 방식은 신뢰된 제3자에 의존하지 않고도 이중 인증부터 탈중앙형 소셜 네트워크에 이르기까지 다양한 암호화 애플리케이션을 지원할 수 있습니다.

소셜 결제의 사용 사례에 있어, 이 방식은 두 가지 중요한 기능을 제공합니다. 첫째, 사용자는 친구의 휴대전화 번호를 공개키로 사용하여 Celo 통화를 간편하게 전송할 수 있어 연락처 기반의 손쉬운 결제가 가능합니다. 둘째, 친구가 아직 Celo 지갑을 설치하지 않았더라도 Celo 통화를 전송할 수 있습니다.

단일 노드 주소 기반 암호화

설명을 위해, 우리는 시스템의 상태를 단일 노드가 유지하는 단순화된 주소 기반 암호화 스키ムの 버전부터 소개합니다. 이 단일 노드는 validator node(검증자 노드)라고 불립니다.

검증자 노드의 핵심 역할은 [address -> public key] 매핑을 저장하는 공개적이고 append-only한 데이터베이스를 유지하는 것입니다. 단일 노드 모델에서는, 검증자 노드는 전통적인 키 서버와 유사하지만, 단순히 [address -> public key] 매핑을 저장하는 것을 넘어 다음과 같이 이를 인증하는 기능도 수행합니다.

사용자가 해당 스키에 공개키를 등록하고자 할 때, 먼저 개인/공개키 쌍을 생성한 후, 자신의 [address -> public key] 매핑을 검증자 노드에 제출합니다. (우리의 사용 사례에서는 address가 사용자의 휴대전화 번호이지만, 일반적인 경우에는 비밀 메시지를 전송할 수 있는 어떤 주소라도 가능합니다.) 검증자 노드는 이 항목에 명시된 주소로 서명된 비밀 메시지를 전송합니다. 사용자는 그 메시지를 Attestations 스마트 계약으로 전송하며, 계약은 사용자와 검증자의 공개키를 이용해 각각의 서명을 복호화하여 검증합니다. 복호화된 메시지가 원래의 비밀 메시지와 일치하면, 스마트 계약은 데이터베이스에 다음 항목을 기록합니다: [address, user public key, secret message, user signed secret]

message, validator signature].

단점

이 단순화된 버전은 다음과 같은 단점을 가집니다:

주소 수집(address harvesting). 공개적으로 열람 가능한 데이터베이스에 암호화되지 않은 휴대전화 번호가 저장되어 있는 경우, 스파머가 모든 사용자의 휴대전화 번호를 수집할 수 있습니다. 이를 방지하기 위해, 주소 자체 대신 주소의 단방향 해시 값을 저장할 수 있습니다. 해시된 문자열의 엔트로피를 높여(즉, 해시 복원을 더 어렵게 만들어) 보안을 강화하기 위해, 해시 처리 전 문자열에 pepper를 추가할 수 있습니다².

² pepper를 추가하더라도 다음과 같은 시나리오는 여전히 가능합니다: 스파머가 가능한 모든 10자리 숫자와 가능한 모든 pepper 조합을 단방향 해싱한 뒤, 해당 해시 값이 데이터베이스에 존재하는지를 확인합니다. 그러나 오늘날에도 높은 비용을 감수하면, 가능한 모든 10자리 숫자에 대해 SMS를 보내고, 도달 여부를 확인함으로써 동일한 수집이 가능합니다. 따라서 우리의 목표는, 해시를 복호화하는 실제 비용이 대량 SMS 전송 비용보다 더 높아지도록 만드는 것입니다.

주소당 단일 키(single key per address).

실제로는 사용자들이 하나의 주소에 여러 개의 공개키를 연결해 저장하고자 할 수 있습니다. 그러나 단순화된 프로토콜에서는 이를 위한 메커니즘이 제공되지 않습니다. 이를 해결하기 위해, 키를 "주소 + 임의의 문자열"을 연결한 값의 해시로 정의할 수 있도록 허용할 수 있습니다. 예를 들어, Bob은 `hash("4155551212 || application_name")` 형식으로 애플리케이션 키를 저장하거나, `hash("4155551212 || application_name || 20171117")` 형식으로 일시적 애플리케이션 키를 저장할 수 있습니다.

노드 장애(node failure). 시스템 상태 유지를 단일 노드에 의존하는 모델은 해당 노드의 장애에 취약합니다. 이 문제를 해결하기 위해 여러 노드가 상태 유지에 참여하도록 할 수 있습니다. (이 경우, 인증 요청을 발한 사용자에게 비밀 메시지를 보내는 노드 수를 제한하여 사용자가 과부하되지 않도록 해야 합니다.) 이 모델에서는 비밀 메시지가 해당 메시지를 생성하지 않은 다른 검증자들에 의해서도 검증 가능해야 하며, 이를 위해 검증자가 해당 메시지를 자신의 개인키로 서명해야 합니다. 반복 공격을 방지하기 위해 동일한 검증자로부터 발송되는 각 메시지는 고유해야 합니다.

악의적인 검증자(malicious validator). 악의적인 검증자 노드는 메시지/응답 절차를 우회하여, 다른 사람의 주소를 임의로 선택하고 해당 주소에 대한 자신만의 키 쌍을 생성한 뒤, 그 개인키로 비밀 메시지에 서명하여 원장에 항목을 기록할 수 있습니다. 이를 통해 검증자는 해당 주소를 위조하여 다른 사람이 받을 지불을 자신이 수령하게 만들 수 있습니다. 이 문제는 서로 담합할 수 없는 다수의 검증자 간의 합의를 요구함으로써 해결할 수 있습니다.

거래 투명성(transaction transparency). 전화번호를 해시한 값을 공개키로 사용하는 경우, 기존의 비트코인 스타일 블록체인에서는 사용자가 자신의 주소록에 있는 연락처의 거래 내역을 볼 수 있게 됩니다. 이를 해결하기 위해 [12]에서 설명한 계산적으로 효율적인 zk-snarks 방식을 구현할 수 있습니다.

DDoS 공격. 마지막으로, 악의적인 사용자가 수천 건의 허위 요청을 검증자에게 제출하여 검증자의 자원을 소모시키고, 사실상 검증자를 스팸 공격 도구로 활용할 수 있습니다. 이 문제는 인증(attestation)에 일정 비용을 부과함으로써 완화할 수 있습니다.

분산형 스킴

여기서는 앞서 제안된 모든 기능들을 포함하는 분산형 스킴(distributed scheme)을 소개합니다. 이 스킴에서는 2.1.1절에서 설명한 단일 검증자 노드 대신, 다수의 검증자 노드로 구성된 P2P 네트워크가 데이터베이스를 유지합니다. 이 네트워크는 개방적이고 허가가 필요 없으며, 누구든 검증자로 참여할 수 있고 언제든지 떠나거나 다시 합류할 수 있습니다. 각 검증자는 인증 대기 큐와 인증된 사용자 데이터베이스의 전체 복사본을 유지합니다. 각 인증 요청에 대해, 검증자는 무작위로 선택되어 인증을 수행하게 됩니다.

인증 절차는 다음과 같은 흐름을 가집니다. 먼저, 사용자가 Attestations 스마트 계약에 인증 요청과 함께 인증 수수료를 전송합니다. Attestations 계약은 검증자 집합 중에서 무작위로 검증자를 선택하고 해당 검증자를 위한 메시지를 생성합니다. 선택된 검증자는 해당 메시지에 서명하여 등록자에게 전송하고, 등록자는 그 메시지에 다시 서명하여 Attestations 계약으로 돌려보냅니다. 이후 Attestations 계약은 등록자와 검증자의 서명을 확인하고, 일치할 경우 인증을 기록합니다. 대부분의 dApp은 다중 인증을 요구하기 때문에, 블록체인 상에 충분한 인증이 기록되지 않았다면 추가 인증을 요청하게 됩니다.

다수의 검증자를 운영함으로써 노드 장애 문제를 해결할 수 있습니다. 다중 인증 요구는 악의적인 검증자 문제를 해결합니다. 인증 수수료는 DDoS 공격 문제를 해결합니다. 또한 인증 요청은 (address | pepper | application string)의 해시 형태로 발행되어 주소 수집을 방지하고, 주소당 다수의 키를 허용할 수 있게 합니다.

운영 요약

이 프로토콜을 이해하는 또 다른 방법은 시스템 내 각 노드에 허용된 역할과 작업을 설명하는 것입니다.

운영 요약 (계속)

모든 사용자는 다음을 수행할 수 있습니다:

- [hash(address | optional appended string) -> public key] 튜플을 인증 대기 큐에 브로드캐스트하여, 자신의 주소와 연관된 공개키에 대한 인증을 요청할 수 있습니다.

인증된 사용자는 다음을 수행할 수 있습니다:

- [hash(address | optional appended string) -> public key] 매핑을 생성하여 새로운 공개키를 추가할 수 있습니다.
- 자신의 주소와 연결된 공개키를 철회할 수 있습니다.
- 자신의 주소와 연결된 공개키를 변경할 수 있습니다.

검증자는 다음을 수행할 수 있습니다:

- 블록 기록 권한을 얻기 위해 다른 검증자들과 경쟁하고, 인증 대기 큐에 있는 주소로 비밀 메시지를 전송하며, 이전 블록의 인증에 대한 서명 응답을 검증할 수 있습니다.

누구나 다음을 수행할 수 있습니다:

- 인증된 사용자 데이터베이스에서 주어진 주소 해시(또는 주소 해시 || 문자열 연결)의 공개키를 조회할 수 있습니다.

암호화된 EigenTrust를 통한 평판 신호 집계

전화번호와 공개키 간의 탈중앙화된 매핑이 존재하게 되면, 이는 사용자가 새로운 거래 상대방의 신뢰성을 판단하는 데 도움이 되는 평판 시스템의 기초로 활용될 수 있습니다.

한 사람의 휴대전화 연락처 목록은 그녀가 어느 정도 신뢰하고 있는 사람들의 리스트를 대략적으로 나타내는 1차 근사값이라 볼 수 있습니다. 이러한 신뢰 프록시(proxy)는 명시적 신호(예: 사용자가 특정 애플리케이션을 통해 연락처에 있는 사람을 평가하거나, 해당 연락처가 실제 사람인지 여부를 명시적으로 인증하는 방식)나 암묵적 신호(예: 사용자가 자신의 연락처 중 한 명에게 결제를 진행한 경우)를 통해 정교화할 수 있습니다. 이들 신호는 사용자의 휴대전화 내에서 로컬하게 유지되며, 제3자에게 공유되지 않아도 됩니다.

이와 같이 연락처 기반의 신뢰 신호들은 논리적·기능적으로 모두 탈중앙화된 신뢰 네트워크를 형성합니다. 전체 신뢰 네트워크를 저장하거나 그 내용을 전부 파악하는 단일 주체는 존재하지 않으며, 각 사용자는 자신이 신뢰하는 사람들과 그 신뢰 수준만 알고 있을 뿐입니다. 아래에서는 이러한 탈중앙화된 신뢰 네트워크를 기반으로 Sybil 공격에 강하고 프라이버시를 보장하는 평판 점수를 집계하는 방법을 설명합니다.

EigenTrust

EigenTrust [14]는 쌍별 로컬 신뢰 점수를 기반으로 글로벌 평판 점수를 계산하는 탈중앙화 알고리즘입니다. EigenTrust의 핵심 직관은, 한 사람의 평판 점수는 그 사람을 신뢰하는 사람들의 수에 따라 결정되며, 이들 각각의 평판 점수에 의해 가중된다는 것입니다. 이 재귀적 계산은 모든 노드에 대해 신뢰 행렬 T 의 주 고유벡터(principal eigenvector)인 $\vec{t}$ 로 수렴합니다. 여기서 T_{ij} 는 0과 1 사이의 숫자이며, 이는 노드 i 가 노드 j 를 신뢰하는 상대적 수준에 비례합니다³.

EigenTrust에서는 T 의 주 고유벡터를 분산형 파워 메소드(Power Method) [20]의 변형을 통해 계산합니다. 소셜 결제 네트워크 문맥에서 이를 적용하면 다음과 같은 방식으로 진행됩니다: 신뢰 네트워크 T_{ij} 는 결제 네트워크의 변형이며, 노드 i 가 노드 j 에게 결제를 수행했고, j 가 i 의 주소록에 있을 경우 T_{ij} 는 0이 아닌 값을 가집니다. 각 노드는 자신의 현재 t_i 를 저장하고 있으며, 행 i 와 열 j 의 T_{ij} 값(즉, 자신과 상호작용한 사람들에 대한 정보)에 접근할 수 있습니다. 주 고유벡터 $\vec{t}$ 는 아래와 같은 반복 과정을 통해 계산됩니다.

³ 이 문제를 다른 방식으로 표현하면, 신뢰 네트워크에 의해 정의된 에르고딕 마코프 체인의 정상 분포(stationary distribution)를 계산하는 것이라 할 수 있습니다.

제로 지식 증명을 통한 프라이버시 보존형 EigenTrust

우리가 제안하는 알고리즘과 기존 EigenTrust 알고리즘 간에는 두 가지 주요 차이점이 존재합니다.

첫째, 앞서 설명한 단순화된 방식에서는 노드가 자신의 t_i 값을 거짓으로 보고할 수 있습니다. 기존 EigenTrust 알고리즘은 각 노드의 t_i 계산을 위임받은 score manager들을 통해 이 문제를 해결합니다. 이 구조에서 각 노드는 분산 해시 테이블을 통해 무작위로 할당된 세 개의 score manager를 가지며, 이들은 각 노드의 T_{ij} 값을 저장하고 t_i 를 계산 및 보관합니다. 이 방식은 부정직한 노드의 공격을 완화할 수 있지만, 트랜잭션 정보를 네트워크 내 다른 피어들과 공유해야 하므로 소셜 결제 시나리오에는 적합하지 않습니다. 우리는 각 피어가 단순화된 방식에 따라 자신의 t_i 를 직접 계산하도록 하되, 인접 노드들에게 해당 계산이 정확히 수행되었음을 높은 확률로 입증하도록 요구합니다. 이를 위해서는 [10, 3, 5]에 언급된 다양한 암호학적 방법을 활용한 제로 지식 증명(zero-knowledge proof)을 구성할 수 있습니다.

개인화된 사전 신뢰 피어

둘째, 악의적인 클릭(clique)을 방지하고 파워 메소드의 수렴성과 주 고유벡터의 유일성을 확보하기 위해, EigenTrust는 사전 신뢰 피어(pre-trusted peers)라는 개념을 도입합니다. 이는 활동적이며 전역적으로 신뢰받는 것으로 간주되는 피어 집합을 의미합니다. 이러한 존재는 그래프가 비순환이며 강하게 연결되어 있도록 보장하며(행렬이 환원 불가능하고 문제가 잘 조건화되어 있도록), EigenTrust의 계산 수렴성과 정확도를 유지하는 데 기여합니다. 그러나 이 방식은 시스템이 전역적으로 신뢰받는 피어 집합을 미리 정의해야 하며, 이들에게 평판 부여에 과도한 권한이 집중된다는 단점이 있습니다.

이 문제는 개인화(personalization)를 통해 해결할 수 있습니다. 단일 글로벌 평판 벡터를 계산하는 대신, 시스템은 각 피어마다 개인화된 글로벌 평판 벡터를 계산할 수 있습니다. 이 벡터는 네트워크 내 각 피어 j 에 대한 평판 점수를, 단일 피어 i 의 관점에서 나타냅니다. 피어 i 에 대한 개인화된 EigenTrust를 계산하기 위해, 전통적인 EigenTrust 계산을 수행하되, 피어 i 의 연락처 목록을 사전 신뢰 피어 집합으로 사용하면 됩니다.

이 방식은 단일 EigenTrust 계산에 비해 훨씬 계산 비용이 크지만, 우리는 개인화된 PageRank [13] 계산에서 사용된 다양한 계산 최적화 기법들을 개인화된 EigenTrust에도 적용합니다.

실용적 함의

친구에게 돈을 문자로 보내는 소셜 결제의 경우, 주소 기반 암호화 방식은 경량 신원 프록시로 충분히 가능하며, 지갑을 등록하지 않은 사용자에게도 직접 휴대폰 번호를 이용해 송금할 수 있게 해줍니다.

사용자들이 자신의 직접적인 연락처 범위를 넘어서 대상에게도 결제를 하고자 하는 경우, 네트워크 내에서 신뢰 신호를 집계하여 구매, 결제, 신용 결정 등에 활용하고 악의적 행위를 줄이는 것이 유용합니다.

나아가, 우리가 설명한 평판 스킴은 보다 견고한 신원 시스템을 가능하게 합니다. 대부분의 신원 시스템은 타인으로부터의 인증에 기반하며, 해당 인증에 인증자(attestor)의 평판 점수를 가중치로 반영할 수 있다면 보다 신뢰성 높은 시스템이 구현될 수 있습니다.

가치 안정화

암호화폐가 지불 수단으로 활용되는 데 있어 가장 큰 장애물 중 하나는 바로 그 변동성입니다. 소비자들은 통상적으로 변동성이 큰 암호화폐를 구매하여 지출하려 하지 않는데, 이는 해당 암호화폐의 수요 변동에 따라 계좌의 구매력이 크게 출렁이기 때문입니다. 암호화폐를 수용하는 상인들도 지불을 받은 후 즉시 법정화폐로 환전할 가능성이 높는데, 이는 그들의 비즈니스 모델이 암호화폐 투기에 기반하지 않기 때문입니다. 더욱이, 현재 가장 성공적인 암호화폐들은 단지 변동성이 클 뿐만 아니라 디플레이션적 속성도 가지고 있어, 그 성공 자체가 가격 상승으로 이어지며, 그 결과 해당 통화로 표시된 가격은 하락하게 됩니다. 합리적인 행동은 이러한 통화를 교환 수단이 아니라 가치 저장 수단으로 사용하는 것이며, 실제로도 그렇게 사용되고 있습니다.

안정가치 암호화폐는 암호화폐 생태계에 여러 가지 이점을 제공합니다. 첫째, 가격이 안정되면 암호화폐를 교환 수단으로 사용하는 데 있어 큰 장벽이 제거됩니다. 급여, 상품 가격, 고정 계약 의무 등은 모두 해당 통화의 미래 가치에 대한 투기 없이 안정가치 암호화폐로 설정될 수 있습니다. 나아가, 안정가치 코인을 활용하면 금융 계약을 보다 쉽게 구성할 수 있는데, 이는 발행자가 계약의 기능과 통화의 가격 위험을 분리할 수 있기 때문입니다.

하나의 안정가치 통화만으로도 도움이 되겠지만, 건강한 암호화폐 생태계는 현재 존재하는 다양한 변동성 자산들처럼, 다수의 안정가치 통화군으로 구성될 때 더욱 효과적입니다. 예를 들어, 미 달러에 연동된 암호화폐는 미국 내 소셜 결제부터 초인플레이션 국가에서의 자발적 달러화, 고빈도 암호자산 거래의 효율적인 결제 수단까지 다양한 용도로 활용될 수 있습니다. 동시에, 유로에 연동된 암호화폐, 그리스의 상품 바스켓 가격에 연동된 통화, 원유 배럴 가격이나 샌프란시스코의 주택 가격에 연동된 통화 역시 다양한 목적에 유용할 수 있습니다. 이처럼 지역별, 광역적, 기능적 안정가치 통화들은 사람들이 자산 중 일부를 자신이 자주 사용하는 상품 가격과 안정적인 관계를 가지는 통화로 표시함으로써 가격 위험을 헤지할 수 있게 해줍니다.

탄력적 코인 공급 및 변동성 위험의 전이

분산형 안정가치 암호화폐에 대해서는 이미 여러 프로토콜이 제안된 바 있습니다(예: [17, 2, 1, 19]). 이들에 대한 전체적인 검토는 본 문서의 범위를 벗어나지만, 이들 모두는 공통적으로 두 가지 특징을 공유합니다. 첫째, 기존의 결정론적 코인 공급 규칙(즉, 외생 정보와 무관하게 사전에 정해진 공급량 및 증가율)을 대신하여, 수요에 따라 공급량을 조절함으로써 통화 가치를 안정화시키는 탄력적 공급 규칙(elastic coin supply rule)을 도입합니다. 둘째, 이들 모두는 하나의 통화를 안정적으로 유지하면서, 수요 감소 시 리스크를 부담하고 수요 증가 시 보상을 받는 하나 이상의 보완적 암호화 자산을 도입한 다중 자산 생태계(multi-asset ecology)를 구성합니다. 본질적으로, 이들 시스템은 통화 보유자로부터 보완 자산 보유자로 변동성 위험을 이전시키는 구조입니다.

Celo 프로토콜은 이 두 가지 핵심 개념을 동일하게 활용하면서도 다음의 다섯 가지 새로운 특징을 도입합니다: (a) 여러 지역 및 로컬 안정가치 통화를 지원하는 다중 자산 계층형 준비금 구조(tiered reserve)를 도입하며, (b) 준비금 비율에 따라 조정되는 공급 확장/축소 파라미터를 설정하고, (c) 중앙 기관 없이 다양한 지역 통화와 준비 통화 간 상호 교환이 가능한 분산형 거래소를 도입하여 이를 통해 통화의 공급 확장과 축소를 실행하며, (d) 블록 보상과 기타 인센티브를 준비 통화로 지급하며, (e) 장기 보유자가 준비 자산과 신규 통화 발행에 대한 거버넌스를 담당하는 메커니즘을 구성합니다.

프로토콜 요약

높은 수준에서 본 프로토콜의 작동 방식은 다음과 같습니다:

1. 프로토콜은 Celo(또는 Celo 기본 자산이라 불리는)라는 고정 공급량의 자산을 설정하며, 그 일부는 시간이 지나며 분배됩니다. 초기 자산 분배 시 일부는 준비금으로 할당되어 다양하게 구성됩니다.
2. 프로토콜은 지불 수단 통화로서 Celo Dollar를 설정하며, 이는 미국 달러에 대략적으로 연동되도록 설계되었고 다음과 같은 탄력적 코인 공급 규칙을 따릅니다:
통화 공급이 확장되어야 할 때(즉, Celo Dollar의 가격이 기준보다 높을 경우), 프로토콜은 [17, 1, 2]에서와 같이 새로운 코인을 생성합니다. 그러나 이를 기존처럼 토큰 보유자에게 분배하는 대신, 스마트 계약을 통해 시장 가격으로 암호화폐 바스켓⁴을 구매하는 데 사용합니다. 이 구매한 자산들은 준비금에 추가됩니다. 이는 중앙은행이 금융 자산을 공개 시장에서 매입하여 준비금에 예치함으로써 통화 공급을 확장하는 방식과 유사합니다.
반대로 통화 공급이 축소되어야 할 때, 프로토콜은 준비 자산을 사용하여 공개 시장에서 Celo Dollar를 매입합니다. 이는 중앙은행이 통화 공급을 축소하기 위해 공개 시장에서 금융 자산을 매도하는 방식과 유사합니다.
3. 프로토콜은 Celo 기본 자산에 대해 가변 전송 수수료(variable rate transfer fee)를 설정하여, 준비 통화의 장기 보유를 장려합니다. 이 수수료는 준비금을 강화하는 데 사용되며, 수수료율은 준비금 비율에 따라 조정됩니다 — 준비금 비율이 낮을수록 수수료는 더 높아집니다.
4. 프로토콜은 거버넌스에 지분 증명(PoS, proof-of-stake) 모델을 사용합니다. 거버넌스 결정에서 각 노드의 영향력은 그들이 스테이킹한 Celo의 양⁵에 따라 결정됩니다.
5. 블록 보상이 배포될 때마다 동일한 양의 Celo가 새롭게 발행됩니다. 준비금 비율이 목표 비율보다 충분히 높을 경우, 새롭게 발행된 자산은 대부분 인센티브(예: 개발자 및 사용자 보상)로 할당됩니다. 반면, 준비금 비율이 목표보다 낮을 경우, 대부분의 자산은 준비금 강화에 사용됩니다.

이 프로토콜의 안정성 특성에 대한 분석은 [7]에 제시되어 있습니다.

공유 준비금

단일 안정가치 코인(stable coin)은 암호자산 거래나 인터넷 상거래 등 여러 목적에서 유용할 수 있지만, 보다 견고한 생태계는 지역(local), 광역(regional), 기능별(utility) 안정가치 코인들로 구성된 통화 군을 필요로 합니다. 이러한 통화 생태계(monetary ecology)의 이점에 대해서는 [9, 16, 15] 등에서 폭넓게 논의된 바 있으며, 여기서는 그 중 하나에 집중합니다: 어떤 안정화된 통화가 실제로 의미를 가지려면, 해당 통화를 사용하여 구매되는 재화와 서비스의 가격에 대해 안정적이어야 한다는 점입니다. 글로벌 통화를 로컬 거래에 사용할 경우, 지역 소비자 물가 변동이 글로벌 물가 동향과 다를 경우에는 가격 변동성이 도입될 수 있습니다⁶.

프로토콜 관점에서 우리는 다음 두 가지 메커니즘에 주목합니다: (a) 새로운 지역 안정가치 코인을 도입할지 여부를 결정하는 거버넌스 체계, (b) 새로운 안정가치 코인의 성공적인 도입이 기존 통화 군의 안정성 특성을 높이는 구조입니다.

시작점으로, 우리는 각 새로운 안정가치 코인이 독립적으로 운영되는 프로토콜을 상상할 수 있습니다 — 각 통화마다 블록체인과 준비금이 별도로 존재하는 방식입니다. 이 구조에서는 거버넌스 문제는 단순합니다 — 각 팀은 프로토콜 외부에서 독립적으로 새로운 안정가치 코인을 도입하고, 사람들은 시장에서 해당 코인과 그 보완 자산을 선택적으로 구매할 수 있습니다. 이 경우, 거버넌스는 프로토콜 외부의 시장에 의해 결정됩니다.

그러나 이 단순성에는 대가가 따릅니다: 새로운 안정가치 코인의 성공적 도입은 기존 통화의 안정화 효과를 주지 못하고, 오히려 경계 상황에서는 소폭의 불안정성⁷을 유발할 수 있습니다.

이 문제를 해결하기 위해 우리는 공유 준비금(shared reserves) 개념을 도입합니다. 예를 들어, 프로토콜이 유로에 연동된 새로운 안정가치 코인(Celo Euro)을 도입할 경우, 해당 통화의 준비금은 기존 Celo Dollar의 준비금과 동일하게 공유됩니다. Celo Euro의 공급이 확장되어야 할 경우, 기존과 동일한 방식으로 — 새로운 Celo Euro를 발행하고, 이를 사용하여 암호자산 바스켓을 시장 가격으로 매입하여 준비금에 추가합니다. Celo Euro의 공급을 축소해야 할 경우에도 동일한 방식이 적용됩니다: 준비 자산을 매도하여 Celo Euro를 확보하고, 이를 폐기(retire)합니다.

⁴ 초기에는 Celo 기본 자산으로, 이후에는 크로스체인 분산형 거래소를 통해 암호자산 바스켓으로 전환될 예정입니다.

⁵ 향후 버전에서는 스테이킹 금액과 잔여 기간에 기반한 거버넌스 구조로 진화할 수 있습니다.

⁶ 예: 유로를 사용하는 그리스의 사례 또는 우루과이의 달러화 사례.

⁷ 새로운 안정가치 코인에 대한 수요가 충분히 높을 경우, 기존 안정가치 코인에 대한 수요가 축소되어 그 보완 자산의 가치가 하락하고, 기존 코인에 대한 장기 수요의 불확실성이 증가할 수 있습니다.

프로토콜은 다음과 같은 방식으로 이 과정을 보다 효율적으로 수행할 수 있습니다: 준비금을 매도하기 전에, 먼저 Celo Dollar의 공급을 확장할 필요가 있는지를 확인합니다. 만약 확장할 필요가 있다면, Celo Dollar를 발행한 뒤, 이를 현재 환율에 따라 Celo Euro로 직접 교환하고, 교환된 Celo Euro를 폐기(retire)합니다. 이는 본질적으로 준비금을 Celo Dollar로 교환하고, Celo Euro를 폐기한 후, 다시 준비금을 Celo Dollar로 재매수하는 것과 기능적으로 동일하지만, 준비금 거래 과정을 간접화(disintermediate)한 것입니다. 준비금을 직접 사용하는 것은 Celo Euro의 축소 필요성이 프로토콜이 지원하는 다른 모든 스테이블코인의 확장 필요성보다 클 경우에만 해당됩니다.

공유 준비금 시스템은 어떤 새로운 스테이블코인을 언제 도입할지에 대한 결정을 내리는 데 있어 신중한 거버넌스 방식과 함께 도입되어야 합니다. 만약 생태계에 부정적인 효용을 가지는 새로운 스테이블코인이 도입된다면, 해당 코인에 대한 수요가 충분히 높고 변동성이 클 경우 다른 통화들의 안정성에 경미한 부정적 영향을 미칠 수 있습니다(예: 유명인사 이름을 붙인 초기 스테이블코인). 또는, 프로토콜이 지원하는 다른 통화에 대한 총 수요를 감소시키는 경우에도 영향을 줄 수 있습니다(예: 특정 지역에 차별점 없는 복수의 중복된 통화가 도입되어 혼란을 야기하는 경우). 이러한 이유로, 장기적으로 해당 코인의 도입이 전체 통화군의 총 수요를 증가시킬 것이라는 폭넓은 기대가 있는 경우에만 스테이블코인을 도입하도록 하는 거버넌스 모델이 바람직합니다.

이러한 거버넌스 모델에 대해서는 4.4.2절에서 설명합니다.

공유 준비금 시스템이 모든 새로운 통화의 공유 준비금을 요구하는 것은 아니라는 점도 중요합니다. 실제로, 지역 통화나 기능적 통화의 경우 공유 준비금 모델에 참여하지 않는 것이 더 유익한 여러 이유가 존재합니다. 이에 대해서는 4.4.4절에서 논의합니다. 이러한 통화를 지원하기 위해, 우리는 고유의 준비금을 가진 새로운 안정화 자산(stabilized asset)의 생성을 허용하며, 이를 분할 준비금(partitioned reserves)이라 부릅니다. 상위 수준에서, 이 메커니즘은 단일 안정화 자산 케이스와 동일하게 작동하지만, 제3자가 해당 자산을 생성하고 준비금을 개시할 수 있다는 점에서 차이가 있습니다. 분할 준비금의 경우, 각 준비금 배분은 초기화 시 25% Celo, 25% 로컬 준비 통화, 그리고 나머지 50%는 공유 준비금과 동일한 구성으로 설정됩니다.

가격 발견 및 준비 자산 구매 메커니즘

Celo 프로토콜은 Ethereum의 포크(fork)로 구현되어 있습니다. Ethereum 네트워크에서 연산 비용이 Ether로 지불되는 것처럼, Celo 네트워크에서는 Celo로 연산 비용이 지불됩니다. Celo의 안정 자산들은 ERC20 토큰과 동등한 방식으로 구현되어 있습니다. Celo 프로토콜과 Ethereum 간의 차이점 중 하나는, Ether 자체는 ERC20 표준을 따르지 않지만 Celo는 완전히 호환된다는 점입니다. 이로 인해, 스마트 계약을 통해 Celo 기본 자산과 다양한 Celo 안정가치 자산 간에 탈중앙화 거래소가 가능해지며, 이는 0x [21]와 유사합니다. 이러한 메커니즘은 크로스체인 분산형 거래소 없이도 자동으로 준비금을 구매하고 통화를 배분할 수 있게 합니다.

Celo 안정가치 통화의 가격을 결정하기 위해, 프로토콜은 이해관계자 간의 셸링 포인트(Schelling-point) 방식의 메커니즘을 사용합니다. 이때 각 이해관계자의 투표 가중치는 스테이킹한 Celo의 양에 따라 결정됩니다. 이 셸링 포인트 방식은 거버넌스 구조를 통해, 거래소의 가격 피드(price feeds)를 추가로 활용하여 보완될 수 있습니다.

거버넌스와 인센티브

Celo 프로토콜의 주요 인센티브 메커니즘은 블록 보상의 분배입니다. 이는 시스템에 기여하는 다양한 참여자들에게 배분됩니다 — 프로토콜을 유지하는 자들(검증자 선택, 트랜잭션 검증, 사용자 인증, 셸링 포인트 기반 가격 발견 메커니즘 참여 등), 준비금의 견고함에 기여하는 자들, 공급 축소 상황에서 리스크를 감수하는 자들, 프로토콜을 지불 수단으로 사용하는 자들, 다른 사용자의 참여를 유도하는 자들, 그리고 프로토콜 개선(거버넌스 참여 및 기술적 기여 등)을 수행하는 자들이 포함됩니다. 이들 각각에 대한 내용은 아래에 설명됩니다.

시스템 유지

시스템은 검증자 집합을 선택하고 거버넌스 결정을 내리는 데 있어 지분 증명(proof-of-stake) 메커니즘을 사용합니다. 검증자 선출과 거버넌스 결정은 모두 담보 스테이킹(bonded-stake)에 기반한 가중 투표 방식으로 수행됩니다. 모든 Celo 보유자는 스마트 계약에 Celo를 예치하여 담보 스테이킹을 설정할 수 있습니다. 투표(검증자 및 거버넌스 모두)는 담보로 예치된 Celo의 양에 비례하여 가중됩니다. 투표 후에도 일정

기간 동안 예치된 Celo는 계속 락업되어 있어야 하며, 향후에는 이 락업의 잔여 기간에 따라 투표 가중치를 부여하는 것이 바람직할 수 있습니다. 이는 준비 통화의 장기 보유를 장려하며, 거버넌스 결정을 장기적 관점에 맞게 정렬시켜 줍니다. 블록 보상은 검증자 선출 및 거버넌스 결정에 참여한 이들에게 분배됩니다.

사용자들은 개별 검증자에게 직접 투표하지 않습니다. 대신, 검증자들은 그룹을 형성하고, 계정 보유자들은 이러한 검증자 그룹에 대해 투표합니다. 민주주의에서 누구나 자신의 정당을 만들거나 선거에서 정당의 대표로 출마할 수 있듯이, 어떤 Celo 사용자든 검증자 그룹을 생성하거나 기존 검증자 그룹에 본인을 포함시켜달라고 요청할 수 있습니다. 검증자 선거는 매 에포크(epoch)마다 진행되며, 이는 대략 하루에 한 번 발생합니다.

선출된 검증자들은 슬래시(slash) 가능한 담보를 예치하고, 합의 프로토콜에 참여하며, 검증 메시지를 전송하고, 가격 발견을 위한 셀링 포인트 방식에 참여하게 됩니다. 이들은 시스템 유지 활동에 대한 비용 보전 및 인센티브로서 블록 보상을 수령합니다.

준비금 강화 및 필요 시 안정가치 통화 공급 축소

Celo 보유자는 Celo 기본 자산에 초기 가치를 부여하고, 준비금 내에 기타 암호화 자산을 도입하는 역할을 수행합니다. 또한, 공급 축소나 준비금 감소가 발생할 경우, 일정한 리스크를 감수합니다: 준비금 비율이 목표보다 낮아지면 전송 수수료가 부과되며, Celo 안정가치 통화에 대한 수요가 감소하면 Celo 자체의 가치도 하락할 수 있습니다. 이러한 역할을 수행하는 Celo 보유자는 두 가지 방식으로 보상을 받을 수 있습니다. 첫째, Celo 안정가치 통화에 대한 수요가 증가하면, 프로토콜은 더 많은 Celo를 매입하게 되므로 고정된 공급에 대한 수요가 증가합니다. 둘째, 준비금 비율이 목표보다 높을 경우, Celo 보유자는 블록 보상의 일부를 보상으로 받게 됩니다(단, 이들은 트랜잭션 검증에 대한 합의, 검증 메시지 전송, 가격 발견을 위한 셀링 포인트 투표에 참여해야 합니다). 이러한 보상은 스테이킹된 Celo의 양에 비례하여 지급됩니다⁸.

사용자 기반 확대 및 시스템 사용 증가

지불 프로토콜을 실제로 사용하고, 모바일 지갑을 통한 전화번호 인증에 참여하며, 소량의 Celo를 스테이킹하는 활동적인 사용자들은 블록 보상을 통해 인센티브를 받습니다. 실질적으로 이는 활동 사용자들의 거래 수수료를 감소시키는 효과를 가집니다. (예를 들어, 일정 시간 단위 내 안정가치 통화로 수행되는 일정 횟수의 거래에 대해 거래 수수료를 면제하고, 해당 수수료는 블록 보상의 일부로 총당하는 구조를 상상해볼 수 있습니다. 이때 수수료 면제 우선순위는 거래 속도를 확보할 수 있도록 설정된 비율에 따라, 사용자의 스테이킹 규모에 따라 결정됩니다.)

프로토콜 개선

지속적으로 진화하는 프로토콜에는 이를 개선하기 위한 인센티브와 거버넌스 체계가 필요합니다.

기술적 개선

프로토콜에 대한 기술적 개선을 위해, 누구든지 일정 주기마다 구현 비용에 대한 제안을 포함하여 기술 제안서를 제출할 수 있으며, 이를 위해 Celo를 담보로 예치해야 합니다⁹. 이러한 제안은 Dash의 마스터노드 방식 [8]과 유사하게, 장기 보유자들에 의해 투표로 결정되며, 투표는 스테이킹 금액과 공지 기간에 따라 가중됩니다. 특정 주기 내에 사용되지 않은 자금은 준비금에 추가됩니다.

⁸ 향후 프로토콜 버전에서는 스테이킹 기간의 잔여 시간도 가중치 산정에 포함될 수 있습니다.

⁹ 이 메커니즘은 마케팅 제안 등 다른 유형의 제안에도 적용될 수 있습니다

지역 통화 도입 및 준비금 기초 확대

시간이 흐름에 따라 더 많은 안정가치 통화를 도입하고, 준비금 보유 자산을 다양화하는 것은 프로토콜을 개선하는 데 도움이 됩니다. 새로운 안정가치 통화를 적절히 도입하면, 프로토콜의 효용성이 증가하고, 장기적인 코인 수요 성장률이 향상되며, 총 수요의 변동성도 감소시킬 수 있습니다. 또한, 새로운 암호 자산을 신중하게 선택하면 준비금의 변동성을 낮출 수 있습니다. 이 두 요소 모두 프로토콜이 지원하는 통화들의 안정성을 더욱 높이는 효과를 가집니다. 이러한 제안을 도입하기 위한 거버넌스 절차는 기술적 개선 제안과 유사한 구조를 가집니다.

정기적으로, 모든 Celo 보유자는 일정량의 Celo를 스테이킹하여 새로운 안정가치 통화를 도입하는 제안을 할 수 있으며(페그 대상 지정 포함), 장기 보유자들은 자신이 보유한 Celo의 양에 비례하여 투표하게 됩니다¹⁰. 일정 기준 이상의 투표 수가 충족되면, 해당 스테이블코인이 공유 준비금 체계에 도입됩니다.

이와 유사하게, 모든 Celo 보유자는 특정 암호 자산을 준비금에 추가할 것을 제안할 수 있으며, 이때 해당 자산에 대한 향후 준비금 구매에서의 할당 비율도 함께 제안합니다. 장기 보유자들은 자신이 스테이킹한 Celo의 양에 비례하여 투표에 참여하게 되며¹¹, 기준 이상의 투표가 통과될 경우, 해당 자산은 향후 준비금 매입 시에 투표된 중간값 비율로 포함되며, 기존 자산들의 비율은 비례적으로 희석됩니다.

이러한 제안이 평가되어야 할 기준은 해당 제안이 장기적으로 통화의 안정성을 얼마나 향상시킬 수 있는지에 있습니다. 준비금에 도입되는 암호 자산이 기대 수익률을 증가시키고 변동성을 감소시킨다면, 이는 장기적 코인 안정성에 긍정적 효과를 줄 것입니다. 또한, 새로운 안정가치 통화의 도입이 장기적인 총 수요를 증가시키고, 총 수요 붕괴의 가능성을 줄인다면, 이는 해당 통화의 안정성을 강화하는 데 기여합니다.

¹⁰ 향후 버전에서는 보유량뿐 아니라 스테이킹 기간도 가중치로 반영될 수 있음

¹¹ 향후 버전에서는 스테이킹 중인 Celo뿐 아니라 락업 기간의 잔여 시간도 가중치에 포함될 수 있음

퓨타키 관점의 거버넌스 (Futarchical Governance)

향후에는 예측 시장(prediction markets)을 거버넌스의 보조 수단으로 도입할 수도 있습니다. 예측 시장을 통해 준비금 구성이나 스테이블코인 포트폴리오의 변화가 장기적인 코인 안정성에 긍정적인 영향을 줄 것인지 여부를 평가하게 할 수 있습니다. 더 나아가, 퓨타키 거버넌스 패러다임(futarchical governance paradigm) [11] 하에서는 예측 시장이 투표 메커니즘 자체로 작동하는 방식도 상상해볼 수 있습니다. 이는 향후 연구 주제로 남겨두는 방향입니다.

분할 준비금 (Partitioned Reserves)

공유 준비금에 의해 지원되지 않는 새로운 로컬 통화는 거버넌스 과정을 거치지 않고도 도입될 수 있습니다. 새로운 로컬 통화는 자체 준비금과 연계된 로컬 준비 통화를 기반으로 도입될 수 있습니다. 이러한 경우, 해당 준비금은 기본적으로 Celo, 로컬 준비 통화, Celo Dollar 등을 포함하는 다양한 암호 자산 바스켓으로 구성됩니다.

이러한 구조는 다양한 가능성을 열어줍니다. 첫째, 이러한 로컬 프로토콜들은 로컬 준비 통화의 일부를 모든 지역 주민에게 배포함으로써, 로컬 통화 채택 증가에 따른 혜택을 지역 주민들에게 제공하는 사회배당 (social dividend)을 실현할 수 있습니다.

둘째, 이러한 로컬 프로토콜들은 전송 수수료의 구현 방식을 다르게 설계할 수 있습니다. 예를 들어, 준비금 비율이 낮을 때 로컬 준비 통화로 전송 수수료를 부과하는 대신, 로컬 스테이블코인 자체에 주기적인 수수료를 부과하여 준비금을 보강할 수 있습니다. 이는 목표 준비금 비율보다 낮을 때에만 작동하는 것이 아니라, 일정 간격으로 항상 작동하는 감가(demurrage) 메커니즘을 통해 구현됩니다. 이러한 방식은 준비금을 강화하고, 로컬 지급 수단 통화의 유통을 장려하는 한편, 사용자가 가능할 경우 해당 통화를 벗어나려는 유인을 일부 제공하게 됩니다. 이와 같은 단점에도 불구하고, 감가 메커니즘에 대한 문헌([9, 15] 참고)은 해당 모델에 대한 더 많은 실험이 유익하다고 제시합니다.

마지막으로, 향후 더 많은 자산들이 토큰화됨에 따라, 분할 준비금 메커니즘은 준비금이 실물 자산(real assets)을 포함할 수 있도록 해줍니다. 이는 통화 안정성 관점에서도 유익하며, 다음과 같은 구조도 가능하게 만듭니다:

자연 자본(natural capital)을 담보로 한 지급 수단 통화(예: 산림 지대를 담보로 하는 통화)처럼, 해당 통화에 대한 수요가 증가할수록 그 통화를 담보하는 자연 자본의 규모도 함께 증가하는 구조입니다. 자연 자본 기반 통화에 대한 상세한 논의는 [9]를 참고하십시오.

결론

우리는 Celo 프로토콜이라 불리는 소셜 결제용 프로토콜을 소개하였습니다. Celo 프로토콜은 사용자가 전화번호 또는 이메일 주소를 공개키로 직접 사용할 수 있도록 해주는 주소 기반 암호화 방식과, 탄력적 공급 규칙을 통해 변동성을 최소화하는 준비금 기반 안정화 메커니즘을 결합합니다. 이 두 요소는 암호화폐를 지급 수단으로 사용할 때 보다 매끄러운 사용자 경험을 가능하게 합니다. 더 나아가, 이 프로토콜은 로컬 및 광역 통화, 사회배당, 감가 통화, 그리고 향후에는 자연 자본 기반 통화를 포함하는 통화 생태계를 실현할 수 있도록 설계되어 있습니다.