Celo: A Multi-Asset Cryptographic Protocol for Decentralized Social Payments

Sep Kamvar, Marek Olszewski, Rene Reinsberg

DRAFT version 0.23

Translated by: jiyun.kim@dsrvlabs.com

Version: First release

Terminology

Reserve	리저브
Mapping	매핑
Scheme	설계
Identity	신원
Token	토큰
Protocol	프로토콜
governance	거버넌스
mechanism	메커니즘
coin	코인
stablecoin	스테이블 코인
incentive	인센티브
validator	검증인
Introduction	도입

Celo: 분산화된 사회적 결제를 위한 다중-자산 암호학 프로토콜

Abstraction (초록)

Two of the biggest barriers to the large-scale adoption of cryptocurrencies as a means of payment are ease-of-use and purchasing-power volatility. We introduce Celo, a protocol that addresses these issues with an address-based encryption scheme and a stable-value token. We show how these attributes together can be used to foster a monetary ecology that includes global reference currencies, local and regional stable-value currencies, and a social dividend. Our first application is a social-payments system centered around mobile phones.

지불 수단으로서 사용되는 암호 화폐의 대중적 확산에 대한 두가지 큰 장벽은 사용의 용의성과 구매력에 대한 변동성이다. 우리는 이러한 이슈들을 주소 기반 암호화 설계와 안정된 가치의 토큰으로 설명하는 celo 프로토콜을 소개한다. 우리는 이러한 요소들이 전체 참조용 통화와, 국소적이고 지역적인 안정된 가치의 통화 및 배당을 포함하여 어떻게 통화 생태계를 강화시키는데 사용될 수 있는지 보일 것이다. 우리의 첫번째 응용사례는 주변의 휴대폰을 중심으로 하는 사회적 결제 시스템이다.

Contents (목차)

1. Introduction (소개)
2. Ease of Use through Lightweight Identity (가벼운 신원을 통한 사용 편의)
  2.1 Address-Based Encryption (주소 기반의 암호화)
    2.1.1 Single-Node Address-Based Encryption (단일 노드의 주소 기반 암호화)
    2.1.2 Drawbacks (결점)
    2.1.3 Distributed Scheme (분산화된 설계)
    2.1.4 Summary of Operations (동작의 요약)
  2.2 Aggregating Reputation Signals through Encrypted EigenTrust (암호화된 고유 신뢰를 통한 평판 지표 수집)
    2.2.1 EigenTrust (고유신뢰)
    2.2.2 Privacy-Preserving EigenTrust through Zero-Knowledge Proofs (영지식 증명을 통해 개인정보를 보호하는 고유신뢰)
    2.2.3 Personalized Pre-Trusted Peers (개인화된 이미-신뢰된 피어들)
    2.2.4 Practical Implications (실제 의미)
3. Stabilizing Value (가치 안정화)
  3.1 Elastic Coin Supply and Shifting Volatility Risk (탄력적 코인 공급과 변동성 위험 이동)
  3.2 Protocol Summary (프로토콜 요약)
  3.3 Shared Reserves (공유된 리저브)
  3.4 Price Discovery and Mechanics of Reserve Asset Purchasing (리저브의 가격 전개 및 역학)
4. Governance and Incentives (거버넌스와 보상)
  4.1 Maintaining the System (시스템 유지)
  4.2 Bolstering Reserves and Contracting Stable-Value Currency Supply when Needed (필요에 의한 리저브 강화와 안정된 가치 통화의 공급 축소)
  4.3 Increasing User Base and Usage of the System (사용자 기반 및 시스템 사용량의 증가)
  4.4 Improving the Protocol (프로토콜 개선)
    4.4.1 Technical Improvements (기술적 개선)
    4.4.2 Introducing Regional Currencies and Broadening the Reserve Base (지역 통화 발행 와 리저브 기반 확장)
    4.4.3 Futarchical Governance (구조적 거버넌스)
    4.4.4 Partitioned Reserves (분할된 리저브)
5. Conclusion (결론)

1 Introduction (소개)

Cryptocurrencies have several advantages to fiat currencies as a means of payment. They enable transfer of value that is much faster than a bank wire, at lower cost (especially for international payments), in a publicly auditable and secure manner, using a technology that is globally accessible so long as you have a smartphone. Further, cryptocurrencies can be programmed; allowing financial contracts, escrow, and insurance, all without intermediaries.

결제 수단으로서 암호화폐는 기존 화폐 대비 몇가지의 장점을 가지고 있다. 암호화폐는 은행보다 송금이 빠르고, 저렴하며(특히 국가간 송금에서), 공개적으로 검증가능하고 안전하며 스마트폰을 통해 세계적으로 접근 가능한 기술을 가지고 있다. 게다가 암호화폐는 금융계약이나, 에스크로, 보험등을 중재자 없이 프로그램 가능하다

However, at the moment, there are several barriers to the mainstream adoption of cryptocurrencies as a means of payment. First, due to deterministic supply rules and unpredictable coin demand, successful coins 1 experience deflationary price instability. As a result, users rationally prefer to use them as a store of value rather than a medium of exchange. Second, even when people do wish to use price-volatile cryptocurrencies as a means of payment, they need to generate a private/public key pair to receive a payment, and enter in somebody's public key in order to send a payment. While these may seem small obstacles, experience has shown that small differences in user experience lead to large differences in usage outcomes.

그러나, 현재 암호 화폐는 주요 결제 수단으로 인정 받기에 몇가지 장애물을 가지고 있다. 첫째로 이미 정해진 공급량과 예측불가능한 수요때문에 성공적인 프로젝트의 코인들도 디플레이션적인 가격 불안정을 겪고있다. 그 결과 사용자들은 합리적으로 암호화폐를 일반적인 거래보다 가치를 저장하는 수단으로 사용하는것을 선호한다. 두번째로 가격 변동성에도 불구하고 결제수단으로 사용하기로 결심한 사람들은 결제를 받기 위해 개인/공개키 조합을 만들고, 돈을 보내기 위해 누군가의 공개키를 입력해야 한다. 이러한 문제는 작은 불편함으로 느껴질수 있지만, 경험상 사용자 경험 측면에서의 작은 차이가 큰 사용 차이를 유발시킨다.

For a cryptographic social payments system to prosper, sending a payment should be as easy as sending a text message, and the volatility of the currency should be minimal. We describe Celo, a protocol that addresses each of these issues. To address ease of sending payments, Celo introduces a cryptographic scheme that we call address-based encryption, in which participants verify a series of cell-phone number-to-public-key mappings, allowing users to then use their friends' cell phone numbers as public keys.

암호화 결제 시스템이 번영하기 위해서는, 결제가 문자 메시지를 보내는 것처럼 쉬워야 하고 화폐의 변동성이 작아야 한다. 우리는 이러한 문제를 관리하기 위해 celo프로토콜을 제안한다. 쉬운 결제를 위해 셀로는 "주소 기반 암호학"이라는 암호학적 기법을 사용해 참여자들이 전화번호와 공개키 쌍을 이용하여 검증하고, 친구의 전화번호를 공개키처럼 사용할 수 있게 한다.

To address stability of value, Celo introduces a token whose value is stabilized using a monetary policy with elastic supply rules, backed by a variable-value reserve. Further, it introduces a governance structure that allows the protocol to create a family of local, regional, and utility stable-value currencies, where the introduction of new successful stable-value coins to the family strengthens the stability characteristics of the existing coins.

가격의 안정성에 대해 다루기 위해, 셀로는 다양한 가치의 리저브에 의해 유지되는 탄력적인 공급 정책을 이용하여 가격을 안정 시킨 토큰을 소개한다. 또한 이미 존재하는 안정된 가치 특성을 가진 지역적인 화폐를 도입하기 위한 거버넌스 구조를 소개한다.

Finally, Celo introduces a mobile block reward mechanism in which all users involved in transactions are also able to participate in verifications, creating a broad participant base and making block rewards more accessible to day-to-day users. Together, these underpin a compelling social payments protocol.

마지막으로 모바일 기반의 블록 보상 메커니즘을 제공한다. 트렌젝션에 참여한 모든 사용자들은 검증에 참여할 수 있고, 광범위한 참여기반을 만들며, 매일 블록보상을 받을수 있다. 이것들은 강력한 사회적 결제 프로토콜을 뒷받침 한다.

2 Ease of Use through Lightweight Identity (가벼운 신원을 통한 사용 편의)

An important obstacle for the mainstream adoption of cryptocurrencies as a means of payment is the lack of intuitive, decentralized public key infrastructures. As a result, in order to send a payment in today's decentralized systems, users must know the public key of the intended recipient (unless they are operating through a centralized gateway). And in order to receive a payment, a user must first set up a private/public keypair and broadcast it. It would be far easier to send a payment directly to an email address or phone number, and to be able to receive a payment without having to first set up a wallet.

암호화폐의 결제로서의 광범위한 사회적 수용에 대한 중요한 장애물은 직관성의 결여와 분산화된 공개키 환경이다. 그 결과 요즘의 분산화된 결제 시스템에서 송금하기 위해서는 사용자는 수신자의 공개키를 반드시 알아야 한다(중앙화된 시스템을 통하거나). 또한 수신을 위해서는 사용자가 반드시 공개/개인키 쌍을 생성하여 공개해야 한다. 이메일이나 전화번호를 통해 송금하는것은 훨씬 쉬우며, 처음 설정없이 돈을 받을 수 있게 된다.

Identity-based encryption [18] holds promise towards this end. In this scheme, when Alice wants to send an encrypted message to Bob at bob@company.com, she can simply use the public key string bob@company.com, without needing to obtain Bob's public key certificate. While a cryptocurrency system based on identity-based encryption would lead to a much more seamless user experience, both the original proposal and subsequent implementations [4, 6] are hindered by the fact that they require a trusted third party, called a private-key generatorr, to generate private keys. As a result, these schemes are less useful in open, permissionless systems.

정체성 기반이 암호학은 이러한 일들을 종결시킨다. 이 구조에서는 엘리스가 밥(bob@company.com)에게 암호화된 메시지를 보내길 원할때, 밥의 공개키 확인 없이 bob@company.com을 공개키로 간단히 사용할 수 있다. 이러한 기반의 암호학을 사용한 암호화폐 시스템은 훨씬 더 원활한 사용자 경험을 제공하며, 기존의 제안과 그에 따른 구현들은 개인 키를 생성하기위해 개인키 생성자로 불리우는 신뢰된 제 3자를 요구한다는 사실에 의해 제한된다. 그 결과 이러한 설계는 공개된 비 허가형 시스템에서 활용도가 낮다.

2.1 Address-Based Encryption (주소 기반의 암호화)

We propose a variant on identity-based encryption, called address-based encryption. Rather than directly using an e-mail address or phone number as a public key, and then relying on a trusted privatekey generator to generate a corresponding private key, we have users generate their own private/public key pair in the traditional manner. The user then registers their public key in a public, append-only database that stores [address -> public key] tuples. This database is functionally decentralized, so that no central owner is responsible for storing,

managing, or maintaining the database, but logically unified, so that everybody can at any time see all the entries in the database. Crucially, the [address -> public key] tuples are attested to by a peer-to-peer network. To perform attestation, randomly selected validators in the network send a signed and secure message to the registrant, who then signs the message with her private key and returns it to an Attestations smart contract. The Attestations contract checks that the validator did indeed send the message, and that the signature matches the public key of the recipient.

우리는 주소 기반 암호학이라는 신원 기반 암호학의 한 종류를 제안한다. 이메일이나 전화번호를 공개키로 직접 사용하는것 보다, 관련된 개인키를 신뢰된 개인키 생성자에 의존하는 것 보다, 우리는 전통적으로 유저들이 직접 공개/개인키를 생성한다. 사용자는 이후 그들의 공개키를 [주소 -> 공개키] 매핑 튜플을 저장하는 추가만 가능한 공개 DB에 등록한다. 이 데이터베이스는 기능적으로 분산화 되어 있으므로, 모든 사람이 언제든 전체 내역을 조회할 수 있다. 결정적으로 [주소 -> 공개키] 튜플은 peer-to-peer 네트워크에 의해 증명된다. 증명을 수행하기 위해 랜덤하게 선택된 네트워크 상의 검증자는 자신이 서명한 안전한 메시지를, 증명 스마트 계약으로 전송할 수신자를 위해 전송한다. 증명 계약은 검증자가 진짜로 메시지를 전송 하였는지, 서명이 수신자의 공개키와 맞는지를 체크한다.

This protocol works not just with email addresses, but with any channel to which a secure message can be sent, for example, a cell phone number, an IP address, or even a bank routing and account number. Further, arbitrary strings may be appended to the address in the database key, allowing multiple public keys to be stored for each address, each for a different application. As a consequence, the encryption scheme supports a large number of cryptographic applications, from two-factor authentication to decentralized social networks, without relying on trusted third-parties.

이 프로토콜은 이메일 주소뿐만 아니라, 예를 들어 전화번호, IP주소, 은행 경로 및 계좌 번호 등의
암호화 된 메시지가 전달될 수 있는 모든류의 채널에서 동작한다. 추가로 임의의 문자열이 데이터베이스 키의 주소에 붙게되면 각각의 다른 응용프로그램에 대한 각각의 어드레스를 저장하는 것을 허용한다. 결과적으로 이 암호학 구조는 신뢰된 제 3자에 대한 의존성 없이 분산화된 사회적 네트워크로부터의 2차 인증을 통해 다수의 암호학적 응용 프로그램을 지원한다.

For the social payments use case, it allows for two important features. First, a user can send Celo currencies to a friend by using her phone number as the public key, allowing easy payments to contacts. Second, a user can send Celo currency to a friend even if the friend has not yet downloaded a Celo wallet.

이 기법은 사회적 결제 수단의 사용을 위하여 2가지 중요한 기능을 제공한다. 첫번째 유저는 친구의 전화번호를 공개키로 이용하여 연락 대상자에 대한 쉬운 결제로서 셀로 화폐를 전달가능하며, 두번째 친구가 아직 셀로 지갑을 다운 받지 않았더라도 셀로 화폐를 전송할 수 있다.

2.1.1 Single-Node Address-Based Encryption (단일 노드의 주소 기반 암호화)

For the purposes of explanation, we begin by describing a simplified version of the address-based encryption scheme in which a single node, called a validator node, maintains the state of the system.

설명을 목적으로 우리는 단순한 버전의 주소 기반 암호화 설계를 검증자로 불리는 시스템의 상태를 유지하는 단일 노드에서 설명한다.

The key role of the validator node is to maintain a public, append-only database of [address -> public key] mappings. In the single node case, the validator node is similar to a traditional key server except that it not only stores the [address -> public key] mappings, but also attests to them as follows:

검증자 노드의 핵심 기능은 공개되고 추가만 가능한 [주소 -> 공개키] 튜플의 데이터 베이스를 유지하는 것이다. 단일 노드 사례에서, 검증자 노드는 [주소 -> 공개키] 매핑을 저장하고 다음의 내용을 증명하는것만 제외하고는 전통적인 키 서버와 유사하다:

When a user wishes to register a public key with the scheme, they generate a private/public key pair, and then submit their [address -> public key] mapping to the validator node. (In our use case, the address is the cell phone number of the user, but in the general case it could be any address to which a secret message can be sent.) The validator node sends a signed secret message to the address in the entry. The user then sends that message to an Attestations smart contract, which verifies both signatures by decrypting them with the public keys of the user and the validator. If the decrypted message matches the secret message, the smart contract writes the following entry to the database [address, user public key, secret message, user signed secret message, validator signature].

사용자가 구조적으로 공개키를 등록하고 싶을때, 그들은 개인키/공개키 쌍을 생성하고 [주소 -> 공개키] 매핑을 검증자 노드로 제출한다. (우리의 경우, 주소는 사용자의 전화번호이지만, 일반적인 사용예에서는 이주소는 전송 가능한 비밀 메시지에 대한 어떤 주소도 될수 있다). 검증자 노드는 서명된 비밀 메시지를 리스트 상의 주소로 전송한다. 사용자는 자신의 공개키와 검증자의 공개키로 두 서명을 검증할 증명 스마트 계약으로 메시지를 전송한다. 만약 해독된 메시지가 비밀 메시지와 부합할 경우 스마트계약은 다음 항목들을 데이터 베이스에 저장한다
[주소, 사용자 공개키, 비밀 메시지, 유저가 서명한 비밀 메시지, 검증자 서명]

2.1.2 Drawbacks (결점)

This simplified version has the following drawbacks:
이 단순화된 버전은 다음과 같은 결점을 갖는다:

Address harvesting. A publicly viewable database with unencrypted phone numbers allows spammers to harvest the cell phone numbers of all of the users. To address this, we can store a one-way hash of the address rather than the address itself. To increase the entropy of the underlying string (to make reversing the hash more difficult) we may append a pepper to the string to be hashed2 .

주소 수집. 암호화 되지 않은 휴대 전화 번호가 기록된 모두에게 공개된 데이터 베이스는 스팸 전송자들이 모든 사용자들의 전화번호를 수집하는 것을 허용한다. 이것을 해결하기 위해서는 우리는 주소 자체를 저장하기 보다, 주소의 단일 방향 해시를 저장할 수 있다. 원래 문자열의 엔트로피를 증가시키기 위해서(해싱의 역방향을 좀더 어렵게 만들기 위해) 우리는 해시될 문자열에 후춧가루를 추가할 것이다.

Single key per address. In practice, people may want to store multiple public keys associated with their address. The simplified protocol gives no mechanism to do so. As a solution to this, we can allow the key to be the hash of an address concatenated with an optional arbitrary string. This allows, for example, Bob to store an application

key at hash(“4155551212 || application_name”), or an ephemeral application key at hash(“4155551212 || application_name || 20171117”).

주소당 단일키. 실제로는 많은 사람들은 주소에 연관된 다양한 공개키를 저장하기 원할것이다. 이 단순화된 프로토콜은 이러한 메커니즘이 없다. 해결책으로서 우리는 추가적으로 임의의 스트링을 이어 붙여 해싱될 키를 허용할 수 있다. 예를 들어 밥은 hash(“4155551212 || application_name”)에 저장하는 것을 허용하거나, 짧은 응용키를 hash(“4155551212 || application_name || 20171117”) 에 저장하는 것을 허용한다.

Node failure. Any model that relies on a single node to maintain state is susceptible to that node failing. We can address this by having multiple nodes participate in maintaining the state. (In doing so, we must also ensure that only a small number of nodes send a secret message to a user issuing a attestation request, to avoid overloading the user.) In this model, the secret message must also be verifiable by other validators, even if they did not construct it. This is achieved by signing the message with the private key of the validator sending it. To avoid repeat-attacks, each message from the same validator must be unique.

노드 실패. 상태를 유지하는 싱글 노드 기반의 모든 모델은 노드 실패에 민감하다. 우리는 상태를 유지하는 다수의 노드를 가짐으로서 이 문제를 해결한다. (따라서, 우리는 유저 증명을 위해 유저에게 비밀 메시지를 전송하는 노드의 수를 유저의 과부하를 회피하기 위해 적은 수로 유지해야 한다) 이 모델에서, 비밀 메시지는 그 메시지를 생성하지 않은 다른 검증인에 의해서도 검증이 가능해야한다. 이것은 메시지를 전송한 검증인의 개인키로 메시지에 서명하는 것으로 가능하다. 반복 공격을 피하기 위해 동일한 검증인에 의해 전달된 모든 메시지는 유니크해야 한다.

Malicious Validator. A malicious validator node may choose to bypass the message/response step, and instead, write an entry to the ledger in which they choose somebody else’s address, generate their own key pair for that address, and then sign the secret message with the private key that they generated. Doing so allows the validator to spoof an address, claiming payments intended for somebody else. We can address this by requiring consensus between multiple validators who have no mechanism to collude.

악의적 검증자. 악의적 검증자는 다른 유저의 주소를 선택하고 해당주소에 대해 고유한 키쌍을 만든 다음 생성된 개인키로 비밀 메시지에 서명하는 형태로 메시지/응답을 우회할 수 있다. 이것을 통해, 검증인은 주소를 spoofing하여 의도된 다른 사람에게 지불을 요청할 수 있다. 우리는 충돌이 없는 구조를 가진 다양한 검증인 사이의 합의를 요청하여 이 문제를 풀 수 있다.

Transaction Transparency. If we are using hashed phone numbers as public keys, then a traditional bitcoin-style blockchain will allow a user to see the transactions of the contacts in their address book. We can address this by implementing the computationally efficient version of zk-snarks as described in [12].

트랜젝션 투명성. 만약 우리가 해싱된 전화번호를 공개키로서 사용한다면 전통적인 비트코인 스타일의 블록체인은 유저가 그들의 주소록의 연락처의 트랜젝션을 볼 수 있다. 우리는 이 문제를 참고문헌 12에 표현된 zk-snarks의 연산 효율이 개선된 버전을 사용해 해결한다[12].

DDoS. Finally, a malicious user may submit thousands of bogus requests to the validator, both tying up the validator and effectively using the validator as a spam agent. We can mitigate this by introducing a cost to attestation.

DDoS. 마지막으로 악의적 사용자는 수천개의 보거스 요청을 검증자에게 전송하거나, 검증자를 묶거나 검증자를 스팸 유발자로서 효율적으로 활용할 수있다. 우리는 증명에 대한 비용을 소개하여 이 문제를 완화 시킨다.

2.1.3 Distributed Scheme (분산화된 설계)

We introduce here a distributed scheme that introduces each of the features suggested above. In this scheme, rather than the single validator node we describe in Section 2.1.1, a peer-to-peer network of multiple validator nodes maintains the database. The network is open and permissionless; anybody may join as a validator, and validators may leave and rejoin the network at will. Each validator maintains a full copy of the attestation pending queue and attested user database. For each attestation request, validators are chosen at random to handle the attestation.

우리는 위에서 소개된 각 항목을 분산화된 구조에서 다룬다. 이러한 구조에서는 우리가 섹션 2.1.1에서 소개한 단일 검증자 노드와 달리 다중 노드가 데이터 베이스를 관리한다. 네트워크는 공개되고 비허가이기 때문에 누구나 검증인으로 참여할 수 있고, 검증인은 원할때마다 네트워크를 떠나거나 참여할 수 있다. 각 검증인은 증명 대기 큐와 증명된 사용자 데이터 베이스의 전체에 대한 복사본을 유지한다. 각 증명 요청에 대해 검증인들은 증명을 처리하기 위해 랜덤하게 선택된다.

An attestation workflow would then look like this. First, a user will issue an attestation request by sending the request to the Attestations smart contract, along with an attestation fee. The Attestations contract then selects a validator at random from the validator set and generates a message for the validator; the validator then signs that message, sends it to the registrant, who also signs it and sends it back to the Attestations contract. The Attestations contract then verifies the signatures of the registrant and the validator, and if they match, then records the attestation. Most dapps will require multiple attestations (for example, the Celo Wallet requires three attestations), in which case, if there are not enough attestations recorded on the chain, they will simply request more

증명의 작업흐름은 이렇다. 첫번째 사용자는 증명 수수료와 함께 증명 요청을 증명 스마트 계약에 대해 요청을 보냄으로서 시작한다. 증명 스마트 계약은 증명자 세트로 부터 랜덤하게 증명자를 선택하고, 검증인을 위한 메시지를 생성한다; 검증자는 메시지에 서명하고, 이 것에 대해 서명하고 증명 계약으로 재 전송할 요청자에게 전달한다. 증명 스마트 계약은 등록자와 검증자에 대한 서명을 확인하고 일치할 경우 증명을 저장한다. 대부분의 Dapp은 여러번의 증명이 필요할 것이다. (예를 들어 셀로 지갑은 세번의 증명이 필요하다). 체인상의 증명이 충분하지 않을 경우 단순히 여러번 추가 요청할 것이다.

Having multiple validators addresses the node failure issue. Requiring multiple attestations addresses the malicious validator issue. The attestation fee addresses the DDos issue. And the attestation requests are issued as a hash of the (address | pepper | application string), so as to avoid address harvesting, and to allow for multiple keys per address.

여러 검증인을 갖는 것은 노드 실패 문제를 해결한다. 다중 인증은 악의적 검증자 문제를 해결한다.
검증 수수료는 DDos문제를 해결한다. 그리고 증명 요청들은 (address | pepper | application string)의 해시로서 발생하기 때문에 주소 수집을 회피할 수 있으며 주소별 다중키를 허용한다.

2.1.4 Summary of Operations (동작의 요약)

An alternative way of framing the protocol is in describing the roles and operations allowed to each node in the system.

시스템의 각 노드에게 허용된 역할과 동작들에 대한 표현으로 프로토콜을 다른 시각에서 설명한다.

Any user may:
• request verification of a public key associated with her address, by broadcasting her [hash(address | optional appended string) -> public key] tuple to the verification pending queue

A verified user may:
• add a new public key by creating a [hash(address | optional appended string) -> public key] mapping
• revoke any public key associated with their address
• change any public key associated with their address

A validator may:
• compete with other validators for the right to write a block and send a secret message to the addresses on the verification pending queue, and validate the signed responses of the previous block's verifications.

Anybody may:
• look up the public key for a given address hash (or address hash || string concatenation) in the verified user database.

유저들은:

- 자신의 주소와 관련된 공개키에 대한 검증 요청을 [hash(address | optional appended string) -> public key] 형태로 검증 대기 큐로 브로드캐스팅한다.

검증된 유저들은:

- [hash(address | optional appended string) -> public key] 를 사용하여 새로운 공개키를 추가한다.
- 자신의 주소와 관련된 공개키를 취소한다
- 자신의 주소와 관련된 공개키를 변경한다

검증자는:

- 블록에 쓰는 권한과 검증 대기 큐상의 주소들에게 비밀 메시지를 전달하는 권한, 그리고 이전 블록의 검증에 대한 서명 응답에 대한 권리를 얻기위해 다른 검증자들과 경쟁한다.

모두는:

- 검증된 사용자 데이터베이스에서 주어진 주소 해시에 대한 검색을 한다.

2.2 Aggregating Reputation Signals through Encrypted EigenTrust (암호화된 고유 신뢰를 통한 평판 지표 수집)

Once there exists a decentralized mapping of phone numbers to public keys, it brings about interesting potentialities for trust computations in the payment network. For example, it can be used to bootstrap a reputation system that helps users determine the trustworthiness of any new users they may transact with.

전화번호와 공개키의 분산화된 맵핑이 존재한다면, 결제 네트워크에서 신뢰를 계산하기 위한 재미있는 가능성을 가져온다. 예를들어 사용자가 거래가능한 새로운 사용자의 신뢰도를 판단할 수 있는 초기의 평판 시스템으로서 사용가능하다.

A person's cell phone contact list is a rough first-order proxy for a list of people that in whom she has a certain level of trust. One can imagine refining this trust proxy through explicit signals (for example, a user may rate people in her contact list in an application-specific manner, or attest to whether a contact in their address book is a person or not), and implicit signals (for example, if a user makes a payment to somebody in her contact list). These signals can be maintained locally, on the user's cell phone, without sharing them with anybody else.

개인의 전화번호부는 해당 리스트상의 사람들에 대한 대략적 신뢰에 대한 첫번째 진입지점으로 사용될 수 있다. 한가지 상상할수 있는 부분은, 명백한 지표나 (예를 들어 사용자는 응용 프로그램에 따라 연락처의 사람들을 수치화하거나 연락처가 사람인지 아닌지 증명하거나), 절대적 지표(예를들어 사용자가 누군가의 연락처로 돈을 보냈을때) 를 통해 신뢰 정제를 대체하는 것이다. 이러한 지표들은 누구와도 공유되지 않도록 사용자의 휴대폰 속에 국소적으로 유지될수 있다.

Such address-book based trust signals define a trust network that is both logically decentralized and functionally decentralized. No single entity stores or has visibility into the entire trust network; each user simply knows the people whom they trust, and the level to which they trust them. We describe below how to compute sybil-resistant, privacy-preserving aggregate reputation scores given this decentralized trust network.

이러한 주소록 기반의 신뢰 지표는 이론적으로, 또 기능적으로 분산화 된 신뢰가능한 네트워크를 정의한다. 어떤 단일 개체도 전체 네트워크를 저장하거나 가시화 할수 없다. 개개인의 사용자들은 단순히 그들이 믿는 사람과 그들이 믿는 레벨만을 알수있다. 우리는 아래에 주어진 분산화된 신뢰 네트워크에서 어떻게 시빌에 대응하고 프라이버시를 지키면서 평판 점수를 수집하는지 보인다.

2.2.1 EigenTrust (고유신뢰)

EigenTrust [14] is a decentralized algorithm for computing global reputation scores, given pairwise local trust scores. The key intuition behind EigenTrust is that a person's reputation score can be defined as the number of people who trust that person, weighted by their reputation scores. This recursive computation converges for all nodes to the principal eigenvector ~t of the trust matrix T, where Tij is number between 0 and 1, and whose magnitude is proportional to the relative level that node i trusts node j 3 .

고유신뢰는 주어진 지역적 신뢰 쌍들 점수에서 전체적인 평판 점수를 연산하는 분산화된 알고리즘이다. 고유신뢰의 배경이되는 직관적 핵심은 개인의 평판 점수가 그들이 신뢰하는 사람과 그들의 평판 점수를 가정하여 정의할수 있다는 것이다. 이러한 반복적인 연산은 Tij가 숫자 0과 1 사이이고, 크기가 node i가 node j를 신뢰하는 상대적 래벨에 비례할때 모든 노드에 대한 주요 고유벡터 t의 신뢰 매트릭스 T로 수렴한다.

In EigenTrust, the principal eigenvector of T is computed using a distributed variant of the Power Method [20]. In the context of a social payments network, it would proceed as follows: The trust network Tij would be some variant of the payment network, where Tij would be nonzero if node i has paid node j, and node j is in the address

book of node i. Each node stores their own current ti , and has access to the values of Tij in row i and column j (the people with whom the node has interacted). The principle eigenvector ~t would then be computed in an iterative fashion as follows. At each iteration, each node send across their ti · Tij scores to each node j that they've paid in the past. The nodes j wait to receive all of the scores from the nodes that have paid them in the past, and then compute their own tj , and then pass their tj · Tjk along to the nodes k that they have paid.

고유신뢰의 경우 T의 주요 고유벡터는 분산된 Power method의 변종[20]에 의해 연산된다. 사회적 지불 네트워크 측면에서, 다음과 같이 진행된다: 만약 node i가 지불했던 노드 j를 가질때 Tij가 0이 아니고, 노드 j가 node i의 주소록에 존재한다면, 신뢰 네트워크 Tij는 결제 네트워크의 변종이다. 각 노드는 그들의 현재 ti를 저장하고 i열과 j행의 Tij값에 접근한다.(node가 상호통신했던 사람). 주요 고유벡터 t는 다음에 따르는 반복적 형태에 의해 연산될수 있다. 각 반복에서 각 노드는 자신의 ti*Tij 점수를 이전에 지불한적이 있던 각 노드 j에게 전송한다. 노드 j는 과거에 거래한적이 있던 모든 노드들로부터 점수를 수신하기를 기다리고, 자신의 tj를 연산하고 자신의 tj*Tjk를 거래한적있던 K에게 전달한다.

2.2.2 Privacy-Preserving EigenTrust through Zero-Knowledge Proofs (영지식 증명을 통해 개인정보를 보호하는 고유신뢰)

There are two differences between the algorithm we propose and the original EigenTrust algorithm

우리가 제시한 고유 신뢰 알고리즘과 일반적인의 고유 신뢰 알고리즘은 크게 2가지 차이가 있다.

here are two differences between the algorithm we propose and the original EigenTrust algorithm. First, the simplified description above allows nodes to lie about their own ti . The original EigenTrust algorithm addresses this by relying on score managers to steward the computation of ti for each node. In the original scheme, each node has three score managers, assigned at random through a distributed hash table, who store the Tij values for each node and compute and store ti for each node. While this addresses the dishonest node attack, it is not ideal in the social payments scenario, as it requires sharing transaction information with other peers in the network. We address this by having each peer perform the computation themselves, as per the simplified version, but also prove, to a high probability, to all adjacent nodes that they have performed the computation correctly. One can do so by constructing a zero-knowledge proof using a variety of cryptographic means, including [10, 3, 5].

첫번째, 상술했던 단순화된 표현에서는 노드가 자신의 ti에대해 거짓말을 할 수 있다. 본래의 고유신뢰 알고리즘은 이것을 각 노드에 대한 ti 계산을 관리하는 점수 관리자에 의존하여 해결한다. 본래 구조에서 각 노드는 각노드의 Tij값을 저장하고 각 노드에 대한 ti를 계산하고 저장하는 분산화된 해시테이블을 통해 지정된 랜덤한 3개의 점수 관리자를 가진다. 이 것은 불성실한 노드 공격을 해결하는 반면 네트워크 상의 다른 피어에게 트렌젝션 정보를 공유하는것을 요구하는 이상적인 사회적 결제 시나리오는 아니다. 우리는 단순화된 버전에 따라 각 피어가 스스로 연산을 수행할 뿐만아니라 높은 확률로 인접한 노드들에 대한 연산을 올바르게 했는지를 증명해야 한다.
[10, 3, 5]를 포함한 같은 다양한 암호학적 의미를 사용하여 영지식 증명을 생성함으로서 그렇게 할 수 있다.

2.2.3 Personalized Pre-Trusted Peers (개인화된 이미-신뢰된 피어들)

Second, in order to break malicious cliques, and to ensure convergence of the power method and uniqueness of the principal eigenvector, EigenTrust introduces the notion of pre-trusted peers, a group of peers that are active and assumed to be universally trusted. This ensures that the graph is acyclic and strongly connected (and that the matrix is irreducible and that the problem is well-conditioned). However, it requires the system to define a set of universally trusted peers, and concentrates outsized power to confer reputation in those pre-trusted peers.

두번째, 악의적 파벌을 깨뜨리기 위해서, 또 power method의 수렴과 주요 고유벡터의 고유성을 보증하기 위해서, 고유신뢰는 활성화되고 보편적으로 신뢰 가능한 피어그룹인 이미 신뢰된 피어의 개념을 소개한다. 이것은 그래프가 순환하지 않고 강력하게 연결되어 있음을 보증한다.(그리고 행렬이 축소될수 없으며, 문제가 잘 정의되었음을). 그러나 이것은 전체적으로 신뢰할수 있는 피어들의 모임을 정의하는 시스템이 필요하다. 이러한 미리 신뢰된 피어들의 평판을 참조하는데 과한 힘을 집중해야 한다.

We can address this through personalization. Rather than computing a single global reputation vector, the system can compute a personalized global reputation vector for each peer, that gives the reputation score of each peer j in the network from the point of view of a single peer i. To compute personalized EigenTrust for peer i, one can simply perform a traditional EigenTrust computation, but use the contact list of peer i as the set of pre-trusted peers.

우리는 이 문제를 개인화를 통해 해결한다. 단일의 전체 평판 벡터를 연산하기 보다, 시스템은 단일 노드 i의 시점으로부터 네트워크 상의 각 피어 j의 평판 점수를 나타내는 각 피어의 개인화된 전체 평판 벡터를 연산할 수 있다. 피어 i에 대한 개인화된 고유벡터 i를 연산하기 위해 단순히 전통적인 고유평판 연산을 하지만, 이미 신뢰된 피어의 모임으로 피어 i의 연락처 리스트를 사용한다.

This is far more computationally expensive than a single EigenTrust computation; however, we apply many of the computation-saving techniques that enabled personalized PageRank [13] to a personalized EigenTrust computation.

이것은 단일의 고유신뢰를 연산하는것보다 상당히 비싼 연산이다: 그러나, 우리는 개인화된 고유신뢰 연산을 위한 개인화된 페이지 랭크[13]를 가능케 하는 다양한 연산 절감 기법을 적용할 것이다.

2.2.4 Practical Implications (실제 의미)

For the social payments case, in which people text money to friends, the address-based encryption scheme suffices as a lightweight identity proxy, allowing people to send money directly to people’s cell phone numbers, even if they have not signed up for a wallet.

사람들이 친구들에게 돈을 문자처럼 전송하는 사회적 지불 케이스에서, 주소 기반의 암호학 구조는 가벼운 아이디에 대한 대리로 충분하며, 친구가 지갑이 없는 상태이더라도 사람들이 친구의 전화번호로 직접 돈을 보내는 것을 허용한다.

As people are interested in using the protocol to pay people outside of their direct circle of contacts, it is useful for a user to be able to aggregate the trust signals of those in their network to make purchase, payment, and credit decisions, and to mitigate bad actors

사람들은 이 프로토콜을 사용하여 직접적으로 연락을 하지 않는 사람들에게도 돈을 지불하는것 관심이 있으므로, 사용자가 구매나 지불, 신용적 판단, 불순 행위자에 대한 완화를 하기 위해 네트워크에 있는 사람들의 신뢰지표를 수집할수 있는것은 매우 유용하다.

Further, a reputation scheme as we described enables a more robust identity scheme. Most identity schemes are based on attestations from others, and it would be useful to be able to weight those attestations by the reputation score of the attestor.

게다가 우리가 제시한 평판 구조는 좀더 견고한 신원 구조를 가능케 한다. 대부분의 신원 구조는 다른 사람으로부터 증명 되는 것을 기초로 하며, 입증자의 평판 점수를 사용해 증명에 대한 가중치를 사용할 수 있는것은 매우 유용하다.

3 Stabilizing Value (가치 안정화)

Perhaps the biggest hurdle to the use of cryptocurrencies as a means of payment is their volatility. Consumers are unlikely to want to buy a volatile cryptocurrency to spend it, since the purchasing power of their accounts would fluctuate widely with market demand for the currency. Merchants who accept cryptocurrencies are likely to convert to fiat upon payment, because their business model does not involve speculating on cryptocurrencies. And the most successful cryptocurrencies today are not 7 just volatile but deflationary – their success leads to their price rising; as a result, prices denominated in the currency fall. Rational behavior would be to use such currencies as a store of value rather than a medium of exchange, and in practice that is what has happened.

사회적 결제수단으로서 가장 큰 허들은 변동성 일것이다. 소비자들은 구매 이후 시장의 화폐 수요에 따라 크게 변동하는 계좌의 구매력 때문에 변동성 높은 화폐를 사거나 소비하기 원하지 않는다. 암호화폐를 수용하는 상인들은 지불시 현금으로 전환할 것이다. 왜냐하면 그들의 비즈니스 모델이
암호 화폐에 대한 투기성을 포함하지 않기 때문이다. 또한 요즘의 성공적인 암호 화폐는 대부분 변동성뿐만 아니라 디플레이션적이다. - 그들의 성공은 가치를 상승시키고, 그 결과 시장의 가격이 통화 하락으로 표시된다. 합리적인 행동은 이러한 화폐들을 교환의 매개체 보다는 가치를 저장하는 것에 사용하는 것이며, 실제로 이러한 일들이 일어나고 있다.

Stable-value cryptocurrencies would bring a number of benefits to the cryptocurrency ecosystem. For one, stable prices remove a considerable barrier for using cryptocurrencies as a medium-of-exchange; salaries, prices of goods, fixed obligations, can all be set in a stable value cryptocurrency without requiring either party to speculate on the future value of the currency. Further, financial contracts are more easily built with a stable value coin, because the issuer can separate the function of the contract from the price risk of the currency in which it’s denominated.

안정된 가치의 화폐는 암호화폐 생태계에 몇가지의 이득을 가져온다. 하나는 안정된 가격이 거래의 매개체로서 암호화폐를 사용하는 것에 대한 많은 장벽을 제거한다는 것이다; 임금이나 물건의 가격, 고정된 채무는 모두 어느쪽이든 통화의 미래 가치에 대한 추측 없이 안정적인 가치의 암호화폐로 설정이 가능하다. 추가로 금융계약은 안정된 가치의 코인으로 쉽게 만들어질 수 있다. 왜냐하면 발행자가 계약의 기능을 액면가에 대한 가격의 위험성으로부터 분리할 수 있기 때문이다.

While a single stable-value currency would be helpful, a thriving cryptoeconomy is best-served by a family of stable-value currencies, much as it is well-served by the family of variable-value cryptoassets that we have today. Certainly a cryptocurrency pegged to the US Dollar has several uses, from social payments in the US, to

user-initiated dollarization in hyper-inflationary markets, to the efficient settlement of high-frequency crypto-asset trades. At the same time, a cryptocurrency pegged to the Euro would also be useful for many purposes, as would a cryptocurrency pegged to the price of a basket of goods in Greece, as would a cryptocurrency pegged to the price of a barrel of oil, or housing in San Francisco. Stable-value local, regional, and utility currencies allow people to hedge price risk in their lives by denominating a portion of their personal economy in currencies that are stable vis-a-vis the price of the goods they regularly use.

단일 안정된 가치 화폐도 유용하지만, 암호 경제의 번영은 우리가 오늘날 가진 다양한 가치의 암호자산의 군에 의해 제공되는 것보다 안정적인 가치 통화의 군에 의해 가장 잘 서비스된다. 특히 미국 달러가치에 고정된 된 암호 화폐는 미국에서 사회적 결제 부터 초 인플레이션 시장에서 자발적인 사용자의 화폐 달러화, 고빈도 암화자산의 거래에 대한 효율적인 정착 등 여러용도를 가진다. 동시에 유로에 고정된 암호화폐 역시 다양한 목적에 유용하다. 그리스의 바구니속 물건값에 패깅된 암호화폐처럼, 배럴당 오일의 가격에 페깅된 암호화폐처럼, 샌프란시스코의 집값처럼.
안정된 가치의 국소적, 지역적 활용 통화는 사람들이 삶속에서 일상적으로 사용하는 물건의 가격을 개인 경제의 일부를 안정된 통화로 표기하는 것의 가격 위험에 대한 회피를 허용한다.

3.1 Elastic Coin Supply and Shifting Volatility Risk (탄력적 코인 공급과 변동성 위험 이동)

Several protocols have been proposed for a stabilized value cryptocurrency (for example [17, 2, 1, 19]). While a full review of these proposals is outside of the scope of this paper, they generally share two properties. First, rather than a deterministic coin supply rule (in which the coin supply and growth rate are determined in advance, independent of exogenous information), they each introduce an elastic coin supply rule, that stabilizes the value of the coin by adjusting the supply of the coin to match the demand. Second, they each introduce a multi-asset ecology, in which one coin is intended to be stable, while one or more complementary crypto-assets bear the risk of a decrease in stablecoin demand (and receives a reward in the case of an increase in stablecoin demand). In essence, they each shift volatility risk from the coin holders to the complementary asset holders.

안정된 가치의 암호화폐를 위한 몇가지 프로토콜들이 있다(예를들어 [17, 2, 1, 19]). 이 제안들에 대해 모든 검토를 하는것은 이 문서의 영역을 벗어나지만, 그들은 일반적으로 두 가지의 속성을 가진다. 첫번째, 결정론적인 코인 공급 정책(코인의 공급과 증가 비율이 이미 결정되어 외부 정보에 무관한)보다는 수요에 대응해 동전의 공급을 조정하여 가치를 안정시키는 각자의 코인 공급 정책을 소개한다. 두번째, 그들은 하나의 코인의 가치는 안정을 지향하며, 반면에 하나 이상의 보완적인 암호화 자산이 스테이블 코인의 수요가 감소하는 위험을 감당하는 각각의 다중 자산 생태계를 소개한다. (그리고 스테이블 코인의 수요가 증가하는 경우 보상을 받는다). 본질적으로, 그들은 각각 코인 보유자로부터 보완적 자산 소유자로 변동성 위협을 이전시킨다.

Our protocol utilizes the same two key intuitions, with five novel features: (a) it introduces a multi-asset tiered reserve that supports several local and regional stable value currencies, (b) it sets expansion and contraction parameters that are tuned to the reserve ratio defined by the tiered reserve, (c) it introduces a decentralized exchange in which the different local and regional currencies and the reserve currency can be traded amongst one another without a central party, and that the protocol can use to perform expansions and contractions, (d) it releases block rewards and other incentives in the reserve currency, and (e) it has a governance mechanism in which long-term stakeholders in the reserve currency are responsible for governing the assets held in reserve and the new local currencies that are introduced.

우리의 프로토콜은 5개의 새로운 기능과 함께 동일한 2개의 핵심 직관을 활용한다: (a) 여러 국소적, 지역적으로 안정된 가치의 통화를 지원하는 다중자산 기반의 리저브, (b) 계층적 리저브에 의해 정의된 준비 비율로 조정되는 확장과 수축 변수 설정, (c) 서로 다른 국소적, 지역적 통화와 리저브 통화가 중앙화된 조직 없이 서로 거래될 수 있는 탈중앙화된 거래소, (d) 블록보상과 리저브상의 다른 인센티브, 그리고 (e) 리저브 통화를 장기간 보유한 홀더들은 리저브에 보유된 자산과 도입된 새로운 지역 통화들에 대한 관리 책임을 가진다.

3.2 Protocol Summary (프로토콜 요약)

At a high level, the protocol proceeds as follows:

높은 수준에서, 프로토콜은 다음과 같이 진행한다:

1. The protocol establishes a fixed supply of reserve tokens, called Celo Gold, a portion of which is distributed over time. From the initial token distribution, a portion is placed in reserve and diversified.

1. 프로토콜은 고정된 발행량의, 일부가 시간이 지나며 분배되는 셀로 골드라 불리우는 예비 토큰을 발행한다. 첫 토큰 분배로 부터 일부는 리저브로 할당되고 분산 된다.

2. The protocol also establishes a means-of-payment currency, called the Celo Dollar, that is intended to be pegged roughly to the US Dollar, that adheres to the following elastic coin supply rule: When coin supply needs to expand (when the price of Celo Dollar is above the peg), the protocol creates new coins, as in [17, 1, 2]. But rather than distributing them to token holders, it uses 8 them to purchase a basket of cryptocurrencies4 at market rates through a smart contract. These purchases get added to the reserves. This is analogous to a central bank expanding the money supply by buying financial assets on the open market and depositing them in the reserves. When the coin supply needs to contract, the protocol uses reserve assets to buy Celo Dollars on the open market. This is analogous to a central bank selling financial assets on the open market in order to contract the money supply.

2. 또한 프로토콜은 지불 수단 화폐인 셀로 달러를 발행한다. 이 것은 US달러에 대략적으로 고정될 예정이며 다음의 탄력적인 코인 공급 규칙을 준수한다: 코인의 공급이 증가될 필요가 있다면(셀로 달러의 가격이 고정 가격보다 높은경우), 프로토콜은 [17, 1, 2]과 같이 새로운 코인을 발행한다. 그러나 이것을 토큰 홀더들에게 분배하지 않고, 마켓 비율에 대한 일정량의 암호 화폐를 스마트 계약을 통해 구매한다. 이러한 구매자산은 리저브에 더해진다. 이것은 중앙은행이 돈의 공급을 위해 오픈마켓에서 금융자산을 구매하여 자산을 리저브에 예치하는 것과 유사하다. 코인의 공급을 줄여야 할 경우 프로토콜은 리저브 자산으로 오픈마켓에서 셀로 달러를 구매한다. 이것은 중앙은행이 돈의 공급을 줄이기 위해 금융 자산을 오픈 마켓에 판매하는 것과 유사하다.

3. The protocol has a variable rate transfer fee on Celo Gold, to encourage long-term holding of the reserve currency. The proceeds from the fee goes to bolster the reserves, and

3. 프로토콜은 리저브 통화를 장기간 보유하는 것을 격려하기 위해 셀로 골드에 대해 다양한 전송 수수료 비율을 가질 수 있다. 수수료로 부터 오는 수익금은 리저브 보강에 사용되며 비율은 리저브의 비율에 따라 결정된다 - 최저 리저브 비율, 최고 전송 수수료

4. The protocol uses a proof-of-stake model for governance. The weight of a node in governance decisions is dependent on the amount of Celo Gold they stake and the length of time remaining in their stake5 . This further encourages the long-term holding of the reserve currency, and aligns the interests of those making governance decisions around long-term stability of Celo Dollars.

4. 프로토콜은 관리를 위해 지분 증명 모델을 사용한다. 운영 결정에서 노드의 비중은 그들이 스테이킹한 셀로 골드의 양과 남은 스테이킹 기간에 의해 결정된다. 이것은 리저브 통화 에대한 장기간 보유를 장려할뿐 아니라, 셀로 달러의 장기간 안정성에 관련한 결정을 하는 사람들의 이익을 정렬한다.

5. Every time a block reward is distributed, an equivalent portion of Celo Gold is released. If the reserve ratio is substantially higher than the target reserve ratio, then the released amount is largely allocated for incentives (e.g. to developers and users). If the reserve ratio is substantially lower than the target reserve ratio, the released amount goes mostly to towards bolstering the reserves

5. 매시간 블록 보상은 분배 되며 동등한 량의 셀로 골드가 풀린다. 만약 리저브 비율이 대체로 목적된 비율보다 높다면 배포된 수량은 인센티브로 크게 할당된다(개발자나, 사용자). 만약 준비율이 대체로 목적한 준비율보다 낮다면 배포된 수량은 대부분 리저브을 강화하는데 사용된다.

We give a detailed analysis of the stability characteristics of this protocol in [7].
우리는 이 프로토콜에 대한 안정된 특징에 대한 자세한 분석을 [7]에서 제공할 것이다.

3.3 Shared Reserves (공유된 리저브)

While a single stable coin would be useful for several purposes (for example in cryptoasset trading and internet commerce), a more robust ecosystem would involve a family of local, regional, and utility stable value coins. The benefits of such a monetary ecology has been discussed broadly, for example in [9, 16, 15], but here we focus on one: a stable currency is only meaningful if it is stable vis-a-vis the price of goods and services that are purchased using that currency. Using a global currency for local transactions would introduce price volatility in regions where regional consumer price dynamics vary from the global consumer price dynamics6 .

단일의 스테이블 코인은 몇가지 목적에서 사용될 수 있지만(예를 들어 암호화 자산의 거래나 인터넷 상거래), 좀 더 건강한 생태계는 국소적, 지역적, 활용성있는 가격이 안정된 코인을 포함할 것이다. [9, 16, 15] 의 예처럼, 이러한 금융 생태계의 이점은 폭넓게 논의되어 왔다. 그러나 여기서 우리가 집중하는 한가지는: 안정된 화폐는 물건의 가격과 화폐를 사용해서 구매한 서비스의 가격에 대해 안정 되어야만 의미가 있다는 것이다. 지역 거래에 대해 세계 통화를 사용하면 지역 소비자 가격 구조가 세계 소비자 가격구조와 다른 지역에서는 가격 변동성이 발생할 수 있다.

From a protocol perspective, we are interested in two mechanisms here: (a) a governance scheme that determines how the protocol makes decisions on introducing new regional stable coins, and (b) a structure in which the introduction of a new successful stable coin increases the stability characteristics of the coins in the family.

프로토콜 관점에서, 우리는 두가지 메커니즘에 흥미를 가질 것이다: (a) 새로운 지역적 스테이블 코인들을 도입할 때 프로토콜이 어떻게 결정을 내리는 지에 대한 거버넌스, 그리고 (b) 새로운 성공적인 스테이블 코인의 도입으로 화폐군의 안정성 특성이 향상되는 지 여부.

As a starting point, we can imagine a protocol where each new stable coin is independent – there is a blockchain and reserve for each new currency introduced. In this scheme, the governance question is straightforward – teams will independently choose to introduce new stable value coins outside of the protocol, and people can choose independently to purchase the new coins and their complementary reserve assets. Governance on this issue is determined outside of the protocol, by the market.

시작점으로서, 우리는 새로운 스테이블 코인의 독립적인 상황에 대해 상상할 수 있다 - 각각의 블록체인과 새롭게 도입된 화폐에 대한 리저브가 있다 - 팀은 독립적으로 새로운 스테이블 코인을 프로토콜의 외부에서 선택하고, 사람들은 각각 새로운 코인이나 보완적인 예비 자산을 구매하는것을 선택한다. 이 문제에 대한 거버넌스는 시장에 의해 프로토콜의 바깥에서 결정된다.

However, this simplicity comes at a cost: the introduction of a new successful stable coin has no stabilizing effect on existing stable currencies, and on the margins it has a small destabilizing effect 7 . To address this issue, we introduce the idea of shared reserves. When the protocol introduces a new stable value coin – for example, a stablecoin pegged to the Euro – the reserves for that coin are the same reserves for Celo Dollars. When the supply of Celo Euros needs to expand, it expands using the same mechanism as with Celo Dollars – the protocol creates new Celo Euros, and uses those to purchase a basket of crypto assets for its reserves. When the supply of Celo Euros needs to contract, the protocol uses the same mechanism as before: it sells reserve assets in exchange for Celo Euros and retires the Celo Euros.

그러나, 이러한 단순성은 비용이든다: 새로운 성공적인 스테이블 코인의 도입은 이미 존재하는 스테이블 코인에 대한 안정성 효과가 없고, 마진에 작은 불안정된 효과를 가진다. 이 문제에 대해 언급하기 위해서, 우리는 공유된 리저브에 대한 아이디어를 소개한다. 프로토콜이 새로운 안정된 가치의 코인(예를 들어 유로에 맞춰지는 안정된 코인)을 도입했을 때, 이 코인에 대한 리저브는 셀로 달러에 대한 리저브와 같다. 만약 셀로 유로의 공급에 대한 요구가 커지면, 셀로 달러와 동일한 구조로 증가시킨다. - 프로토콜은 새로운 셀로 유로를 만들고 리저브를 위한 어느정도의 암호 자산을 구매한다. 만약 셀로 유로의 공급감소가 필요하다면 프로토콜은 이전과 동일한 매커니즘을 사용한다: 준비된 자산을 셀로 유로로 팔고 셀로 유로는 사라진다.

The protocol can make this process more efficient in the following manner: before selling the reserves, it first looks to see if the supply of Celo Dollars needs to expand. If so, it creates Celo Dollars, exchanges them directly for Celo Euros at the prevailing exchange rate, and retires the Celo Euros. This is functionally equivalent to selling reserves in exchange for Celo Euros, retiring the Celo Euros, and then buying reserves in exchange for Celo Dollars; it just disintermediates the reserves. It only uses the reserves directly if the need for contraction of the Celo Euros is greater than the need for expansion of all the other stablecoins supported by the protocol.

프로토콜은 이 과정을 주어진 방식에 따라 보다 효율적으로 처리한다: 리저브을 팔기 전, 셀로 달러의 공급이 확장되어야 하는지를 먼저 검색한다. 만약 그렇다면 셀로달러를 만들고 알려진 교환 비율에 따라 이를 직접적으로 셀로 유로로 바꾼후, 셀로 유로를 회수한다. 이것은 기능적으로 리저브을 거래소에서 셀로 유로로 바꾸고 유로를 회수한 뒤 셀로 달러로 리저브을 산것과 기능적으로 동일하다; 단지 리저브의 중간체 일뿐이다. 직접적으로 리저브을 사용하는 경우는 오직 셀로 유로의 감소에 대한 요구가 프로토콜에 의해 제공되는 다른 모든 안정된 토큰의 확장 요구보다 큰 경우이다.

A shared reserve system must come together with a thoughtful method of governing decisions on what new stable coins to introduce, and when to introduce them. If a new stablecoin is introduced that has negative utility to the ecosystem, it can have a marginal negative impact on the stability of the other currencies if the demand for that currency is high enough and volatile enough (for example, a celebrity vanity stablecoin early on), or if the coin decreases aggregate demand for other coins supported by the protocol (for example, the introduction of several duplicative regional currencies in the same region with no differentiating features, causing confusion). For this reason, it is useful to have a governance model that introduces a new stablecoin only if there is a widespread expectation that its introduction would increase the aggregate demand for the family of coins over the long run. We describe this governance model in Section 4.4.2.

리저브 공유 시스템은 어떤 새로운 스테이블 코인들을 도입하고 언제 제공할지에 대한 결정을 내리는 신중한 방법과 함께 제공되어야 한다. 만약 에코시스템에 부정적인 용도를 가진 새로운 스테이블 코인이 발행될 경우 해당 통화에 대한 수요가 충분히 높고 변동이 큰 경우나 (예를 들어 유명하지만 허상인 스테이블 코인 초기), 프로토콜에 의해 제공되는 다른 코인에 대한 총 수요를 감소시키는 경우에 다른 통화의 안정성에 미미하게 부정적인 영향을 줄 수 있다. (예를 들어, 특징이 없는 동일한 지역에 대한 여러 중복된 지역화폐가 도입 될 경우 혼란을 유발시킨다). 이러한 이유로 새로운 스테이블 코인의 발행이 통화군에 대한 총 수요가 증가할 것이라는 폭넓은 기대감이 있는 경우에만
새로운 스테이블 코인을 도입하는 거버넌스 모델을 갖는 것은 유용하다.
우리는 이 거버넌스 모델을 4.2.2 장에 설명한다.

It is useful to note that the shared reserve system does not require all new currencies to use the shared reserve. In fact, for local or functional currencies, there are several reasons why it would be useful to not engage in the shared-reserve model; we discuss these in Section 4.4.4. To support these currencies, we also allow for new tokens to be created with their own reserve; we call this partitioned reserves. At a high level, the mechanism works in the same manner as the single stable-value coin case, except that a third party can create the token and initiate the reserve for that token. For the partitioned-reserve case, each reserve allocations are initialized at 25% Celo Gold, 25% a local reserve currency, and the remainder the same allocations as the shared reserve

참고로 공유된 리저브를 모든 통화가 사용하도록 요구하지 않는다는 것은 유용하다. 실제로 지역적 기능의 화폐에 대해 공유된 리저브 모델에 관련되지 않는것이 유용한 몇가지 이유가 있다. 우리는 이것을 4.4.4장에서 소개한다. 이러한 통화를 지원하기 위해서, 우리는 새로운 토큰에 대해 그들만의 리저브를 생성하는 것을 허용한다; 우리는 이것을 분할된 리저브라 호칭한다. 높은 수준에서, 메커니즘은 단일 스테이블 코인의 경우와 동일한 형태로 활용된다. 분할된 리저브의 경우, 각 리저브는 25%의 셀로 골드와 25%의 지역적 리저브 통화, 그리고 나머지는 공유된 리저브와 동일한 비율의 할당량으로 초기화 된다.

3.4 Price Discovery and Mechanics of Reserve Asset Purchasing (리저브의 가격 전개 및 역학)

The Celo protocol is implemented as a fork of Ethereum. The cost of computation in the Celo network is paid in Celo Gold, just as Ether is used to pay for gas on the Ethereum network. Celo stable tokens are implemented as the equivalent of ERC20 tokens. One difference between Celo and Ethereum is that while Ether itself is not compliant with the ERC20 token standard, Celo Gold is. This allows a decentralized exchange, through smart contracts, between Celo stable value tokens as well as Celo Gold, much like 0x [21]. This allows the automatic purchasing of reserves and distribution of coins without cross-chain decentralized exchanges.

셀로 프로토콜은 이더리움의 포크로 개발되었다. 셀로 네트워크의 연산비용은 이더리움이 이더리움 네트워크에 대해 가스를 지불하는 것처럼 셀로 골드로 지불된다. 셀로 스테이블 토큰은 ERC20 토큰과 동일하게 구현되었다. 셀로와 이더리움의 한가지 다른 점은 이더리움은 ERC20 토큰 기준과 호환되지 않지만, 셀로골드는 호환이된다. 이것은 스마트 컨트렉트를 통해 0x와 같이 셀로의 스테이블 토큰과 셀로 골드 간의 분산화된 거래소를 허용한다. 이것은 리저브와 분산된 코인들을 체인간 분산거래소 없이 자동으로 구매할수 있게 해준다.

To determine the price of Celo stable currencies, the protocol will use a Schelling-point scheme amongst stakeholders, with the weight of the a stakeholder's vote dependent on the amount of Celo Gold at stake and the time remaining in the stake. One can imagine further augmenting the Schelling point scheme with price feeds from exchanges, as determined through a governance scheme.

셀로 스테이블 통화의 가격을 결정하기 위해, 프로토콜은 이해 당사자의 셀로골드 스테이크량과 스테이킹의 남은 기간에 기반하는 투표의 가중치를 사용하여 이해당사자들 간의 Schelling-point 설계를 사용할 것이다.

4 Governance and Incentives (거버넌스와 보상)

A primary incentive mechanism in Celo is the distribution of block rewards, which are allocated to the various contributors to the system – those who maintain the protocol (by selecting validators, validating transactions, verifying users, and participating in the Schelling-point price discovery mechanism), those who contribute to the robustness of the reserves, those who take on risk in the case that there is a contraction, those who use the protocol as their means of payment, those who invite others to use the protocol, and those who improve the protocol (by participating in governance, and by making technical contributions to the protocol). We describe these below.

셀로의 주 인센티브 매커니즘은 프로토콜을 유지 (검증인을 선택하고, 트렌젝션을 검증하고, 사용자를 검증하고, Schelling-point 가격 결정 매커니즘에 참여한)하고, 리저브의 건전성에 공헌하고, 통화 수축의 경우 리스크를 감내하고, 프로토콜을 지불 수단으로 사용하고, 다른 친구들을 프로토콜을 사용하도록 초대하고, 프로토콜을 개선(거버넌스나 프로토콜에 기술적으로 공헌한)한 시스템의 다양한 공헌자들에게 할당된 블록 보상 분배이다

4.1 Maintaining the System (시스템 유지)

The system uses a proof-of-stake mechanism for selecting the validator set and participating in governance decisions. Both validator election and governance decisions are made through a bonded-stake weighted voting scheme. Any Celo Gold holder may put up a bonded deposit, which involves sending Celo Gold to a smart contract and specifying a notice period to wait once the withdrawal is requested8 . Votes (for both validators and in governance) are weighted by the amount of Celo Gold in the bonded, and the time of the notice period. This incentivizes long-term holding of the reserve currency and aligns governance decisions with long-term perspectives. Block rewards are distributed amongst those who participate in validator elections and governance decisions

프로토콜은 검증자를 선택하고 거버넌스 결정에 참여하기 위해 proof-of-stake 매커니즘을 사용한다. 이러한 검증자 선택과 거버넌스 결정은 묶인 스테이킹 량에 가중치를 둔 투표 설계를 통해 결정된다. 셀로 골드 홀더라면 누구든 셀로 골드를 스마트 계약으로 보내고 출금

기간을 설정하여 자산을 맡길수 있다. 투표들(검증인들과 거버넌스의)은 맡겨진 셀로골드의 수량과 출금 기간에 의해 가중치가 계산된다. 이 방식은 리저브 통화를 장기간 보유한 홀더를 장려하고 장기적 견해를 가진 거버넌스 결정을 하게 만든다. 블록 보상은 검증인 선정과 거버넌스 결정에 참여한 사람들에게 분배된다.

Users don't vote for validators directly. Instead, validators are expected to organize themselves into groups and account holders vote for these validator groups. Just as anybody in a democracy can create their own political party, or seek to get selected to represent a party in an election, any Celo user can create a validator group and add themselves to it, or ask an existing validator group to include them. Validator elections are held once every epoch, which corresponds to approximately once per day

사용자들은 검증자에게 직접 투표하지 않는다. 대신 검증자들은 스스로 그룹화 하고 계정 소유자들은 그룹에 투표한다. 민주주의의 누구나 그들의 정당을 만들수 있는 것 처럼, 선거에서 정당을 대표하는 누군가를 찾는 것 처럼, 셀로 유저는 검증인 그룹을 생성하고 자신을 등록하거나, 이미 존재하는 검증인 그룹에 그들을 포함시킬 수 있다. 검증자 선정은 대략 하루 정도의 매 기회마다 진행된다.

Validators, once elected, put up a slashable bonded deposit, participate in the consensus scheme, send verification messages, participate in the Schelling-point scheme for price discovery, and receive block rewards to cover their costs and as an incentive for their work to maintain the system.

한번 선정되었던 검증인은, 삭감이 가능한 예치금을 넣고, 합의 설계에 참여하며 검증 메시지를 전송하고 가격 전개에 대한 Schelling-point 설계에 참여하며 그들의 비용과 시스템을 유지하는 그들의 업무에 대한 보상으로 블록 보상을 받는다.

4.2 Bolstering Reserves and Contracting Stable-Value Currency Supply when Needed (필요에 의한 리저브 강화와 안정된 가치 통화의 공급 축소)

Celo Gold holders, through their purchase of Celo Gold, give the initial value to Celo Gold and introduce other crypto assets into the reserves. Further, Celo Gold holders bear some risk in the case of contracting supply or a dip in the reserves: transfer fees are imposed if the reserve ratio goes below the target reserve ratio, and the value of Celo Gold may go down if there is a contraction in demand for Celo stable currencies. Celo Gold holders may be rewarded for playing these roles in two ways: first, as there is greater demand for Celo stable currencies, there will be more protocol-directed purchases of Celo Gold, increasing the demand for fixed supply. Second, if the reserve ratio is greater than the target reserve ratio, Celo Gold holders who have a long-term stake in Celo Gold are rewarded with a portion of the block rewards (provided that they are participating in consensus on transaction validation, sending verification messages when selected, and participating in Schelling-point voting for price discovery). These rewards are paid in proportion to the amount of Celo Gold at stake, and the time remaining in the stake.

셀로 골드를 구매한 홀더들을 통해 셀로 골드는 초기 가치를 가지며 리저브로 다른 크립토 자산을 도입한다. 또한 셀로 골드 홀더들은 공급 수축에 대한 위험을 감내하며, 리저브를 확보한다: 전송 수수료는 리저브 비율이 목표된 리저브 비율보다 낮을 경우나 셀로의 스테이블 통화에 대한 요구가 수축하여 셀로 골드의 가치가 낮아질 경우 부과된다. 셀로 골드 홀더들은 두가지의 역할을 수행함으로서 보상을 받는다. 첫번째 셀로의 스테이블 통화에 대한 요구가 클때, 셀로골드를 프로토콜이 직접 구매하는 일이 많아질 것이고, 고정된 공급량에 대한 요구가 증가한다. 두번째 만약 리저브 비율이 목표 리저브 비율보다 클때, 셀로 골드를 장기간 보유한 홀더들은 블록 보상의 일부를 보상으로 받는다. (트렌젝션 검증과

선정되었을때 검증메시지를 전송하는 것과, 가격 전개를 위한 Schelling-point 투표에 참여에 대한 분배). 이러한 보상은 셀로 골드의 스테이킹 량과 스테이킹의 잔여기간에 비율로 지불된다.

4.3 Increasing User Base and Usage of the System (사용자 기반 및 시스템 사용량의 증가)

Active users (people who use the payments protocol, participate in phone number validation through the mobile wallet, and maintain a nominal stake in Celo Gold) are rewarded through block rewards. In effect, this reduces transaction fees for active users. (One can even imagine a scenario in which these block rewards are issued by waiving transaction fees for a certain number of transactions in the stable currency per unit time, implemented through part of the block reward going to paying transaction fees of users, set at a rate to ensure a certain transaction speed, and prioritized based on the amount of their stake.)

지불 프로토콜을 사용하고, 모바일 지갑을 통해 전화번호 검증에 참여하고 작은 량의 셀로 골드를 스테이킹한 활성 사용자들은 블록보상을 받는다. 사실상 이것은 활성 사용자들의 트렌젝션 수수료를 감소시킨다.(한가지 상상 가능한 시나리오는 단위 시간에 대해 안정된 가치인 몇개의 트렌젝션에 대한 수수료 면제에 대한 블록 보상이며, 트렌젝션 수수료를 블록 보상의 일부로 처리해주는 것을 통해 구현되고, 특정 거래 속도를 보장하기 위한 비율을 설정하고, 스테이킹량에 기반하여 우선순위를 정한다.)

4.4 Improving the Protocol (프로토콜 개선)

And finally a continuously evolving protocol requires incentives, and a governance scheme, for improving the protocol.

마지막으로 지속적인 프로토콜의 개선은 보상과 프로토콜 개선을 위한 거버넌스 설계가 필요하다.

4.4.1 Technical Improvements (기술적 개선)

For technical improvements to the protocol, anybody may put up a bonded deposit to make a technical proposal, with a proposed fee-for-implementation, on a regular cycle9 . Proposals will be voted on by long-term stakeholders, similar to the voting scheme with Dash’s masternodes [8], with their votes weighted by the amount of their stake and notice period. Funds that are not allocated in a particular cycle are added to the reserves.

프로토콜의 기술적 개선을 위해, 자산을 예치한 누구나 구현에 대한 제안 수수료와 함께 정기적으로 기술 제안을 제출할 수 있다. 제안들은 Dash의 마스터노드 투표 설계와 유사하게 스테이킹량과 출금 기간에 가중된 투표로 장기 보유자들에 의해 투표된다. 특정 기간에 할당되지 않은 기금은 리저브에 추가된다.

4.4.2 Introducing Regional Currencies and Broadening the Reserve Base (지역 통화 도입과 리저브 기반 확장)

Over time, it would also improve the protocol to introduce more stable value currencies, and to broaden the reserve holdings. If new stable value currencies are introduced appropriately, they can increase the usefulness of the protocol, increase long-term growth in coin demand, and reduce aggregate demand volatility. And if new crypto-assets are chosen appropriately, they can decrease reserve volatility. Both of these have the effect of further stabilizing the coins supported by the protocol. The governance procedure for introducing these is similar to the governance around technical improvement.

시간이 지남에 따라 좀더 많은 안정된 가치의 통화들이 도입되도록 프로토콜이 개선될 것이고, 리저브의 량이 많아질 것이다. 만약 새로운 안정화된 가치의 통화가 적당하게 발행될 경우 그들은 프로토콜의 유용성을 증가시키고, 코인 수요를 장기적으로 증가시킬 것이며, 총 수요에 대한 변동성을 감소시킬 것이다. 이러한 것들은 프로토콜에 의해 지원되는 코인들의 가격을 안정화시키는 효과가 있다. 이를 도입하기 위한 거버넌스 과정은 기술 개선 거버넌스와 유사하다.

At regular intervals, any Celo Gold holder may stake a certain amount of Celo Gold to make a proposal on introducing a new stable value currency (by specifying a peg). Long-term Celo Gold holders vote in proportion to the amount of Celo Gold they own and the amount of time remaining in their stake. If a certain vote threshold is passed, a new stablecoin is introduced on the shared reserve.

일정한 간격으로 셀로 골드 소유자는 새로운 안정된 가치의 통화를 도입하기 위한 제안을 만들기 위해 특정 수량의 셀로골드를 스테이킹 할 것이다(페깅을 지정하여). 장기간의 셀로 골드 홀더는 그들이 소유한 셀로 골드의 수량과 남은 시간에 비례하여 투표한다. 만약 특정 투표 한도가 넘어갈 경우 새로운 스테이블 코인이 공유 리저브에 도입된다.

Similarly, any Celo Gold holder may stake a certain amount of Celo Gold to make a proposal on introducing a new crypto asset to the reserves (by specifying a suggested percentage of future reserve purchases to be allocated to that asset). Long-term Celo Gold holders vote in proportion to the amount of Celo Gold they have at stake and the amount of time in their notice period. If a certain vote threshold is passed, then future purchases for the reserves will include the new crypto-asset with an allocation given by the median percentage of all votes (with the allocation of all other assets being diluted pro-rata).

유사하게, 어떤 셀로 골드 홀더는 새로운 자산을 리저브로서 소개하는 제안서를 만들기 위해 특정 수량의 셀로골드를 스테이킹 할 것이다(자산에 할당될 미래의 리저브 구매 제안율을 정의하여). 장기간의 셀로 골드 홀더들은 그들의 스테이킹 소유량과 남은 기간의 셀로 골드 비율에 따라 투표할 것이다. 만약 어떤 투표가 통과될 경우 새로운 암호화폐 자산을 포함하여 투표의 중간 비율로 할당된 미래를 위한 리저브가 구매될 것이다. (다른 자산의 할당은 비례로 희석된다)

The criteria by which these proposals should be evaluated is the extent to which they would increase in the long-term stability of the stable currencies. Introductions of crypto-assets to the reserves that increase the expected appreciation of reserves and decrease the volatility of the reserves would have positive benefits to the long-term coin stability. Introductions of new stable-value coins that increase long-term aggregate coin demand and decrease the possibility of an aggregate crash in coin demand also increase the stability characteristics of the coin.

이러한 제안을 평가하는 기준은 안정적 통화의 장기적 안정성을 증가시키는 방향으로 평가되어야 한다. 리저브에 대한 암호자산의 도입은 리저브에 대한 기대 가치를 높이고, 리저브의 변동성을 감소 시키며, 장기적 코인의 안정성에 대한 긍정적 가능성을 가져야 한다. 새로운 안정된 가치의 코인의 도입은 장기적으로 모든 코인의 수요를 증가시키고, 코인 수요에 대한 통합적인 충돌에 가능성을 감소시키며, 코인의 안정화된 특성을 증가시켜야한다.

4.4.3 Futarchical Governance (구조적 거버넌스)

It is possible that in the future, we introduce prediction markets as a supplemental form of governance – where prediction markets will also weigh in on whether a change in the composition of the reserves or the composition of stablecoin portfolio would increase or decrease long-term coin stability. It is even possible to have the prediction markets serve directly as the voting mechanism, in a futarchical governance paradigm [11]. While this is an interesting direction, we would be unlikely to do this in the near term, to avoid unintended side effects.

우리는 미래에 예측 마켓을 거버넌스의 보완적인 형태로 소개할 수 있다.
- 리저브 구성의 변화나 스테이블 코인의 포트폴리오 구성이 장기적 코인의 안정성을 증가/감소시키는 것에 예측마켓의 무게를 둘 것이다.
심지어 예측마켓이 기발한 거버넌스 패러다임에서 투표 메커니즘의 역할을하는 것도 가능하다 [11]. 이것이 흥미로운 방향이지만, 의도하지 않은 부작용을 피하기 위해 단기적으로는 도입하지 않는다.

4.4.4 Partitioned Reserves (분할된 리저브)

The introduction of a new local currency does not need to go through the governance process if it is not backed by the shared reserve. One can introduce a new local currency backed by its own reserve, with its own affiliated local reserve currency, similar to the single Celo Dollar and Celo Gold case. In these cases, the default reserve would include in its reserve a basket of diversified crypto assets that includes Celo Gold, the local reserve currency, Celo Dollars, and others.

새로운 지역 통화의 도입은 이 통화가 공유된 리저브에 의해 지원되지 않을때는, 거버넌스 프로세스를 필요로 하지 않는다. 누구나 셀로 달러와 셀로 골드처럼, 연관된 지역 리저브 통화와 함께, 자신만의 리저브에 의해 지원되는 지역화폐를 도입할 수 있다. 이러한 경우 기본 리저브에는 셀로 골드, 지역 리저브 통화, 셀로 달러등을 포함하는 다양한 암호 자산이 포함된다.

Doing so opens many possibilities. First, these local protocols may choose to distribute some of the local reserve currency to all local inhabitants, effectively creating a social dividend that allows local residents to benefit from the increased adoption of a local currency.

이럴 경우 많은 가능성이 열린다. 첫번째로, 이러한 지역적 프로토콜은 약간의 지역 리저브 통화를 지역 주민들에게 분배하는 것을 선택할 수 있고, 지역 통화에 대한 수용으로부터 지역의 거주자들의 이익을 허용하는 효과적 사회적 배당을 만들수 있다

These local protocols may also choose to implement the transfer fee in a different way; rather than having the transfer fee payable in the local reserve currency when the reserve ratio is low, they may choose to bolster the reserves by issuing the fee directly on the local stable currency, at regular intervals rather than just when the reserve ratio is lower than the target reserve ratio. This implementation of demurrage has the effect of bolstering the reserves and encouraging circulation of the local means-of-payment currency, at the expense of giving

people a moderate incentive to switch out of the currency when possible. Despite this drawback, the literature on demurrage (see, for example, [9, 15]) suggests that more experiments with demurrage are useful.

이러한 지역적 프로토콜은 전송 수수료를 다른 방식으로도 선택할 수 있다; 리저브 비율이 낮을때 지역 리저브로 이체 수수료를 지불 하는 대신, 리저브 비율이 낮을 때보다 주기적 간격으로 지역 안정 통화로 직접 수수료를 발행하여 리저브를 강화하도록 선택할 것이다. 이러한 초과수수료 구현은 리저브를 강화하고 지역의 사회적 지불 통화의 순환을 촉진하며, 사람들에게 가능할 경우 통화를 교환하는 적당한 보상을 제공한다. 결점에도 불구하고, 초과수수료에 대한 문헌은(예를들어 [9,15]) 더 많은 중도 실험이 유용하다는 것을 보인다.

And finally, as more assets get tokenized in the future, the partitioned reserve mechanism allows for the reserves to include real assets. This is helpful from a stability perspective, and also allows for natural-capital-backed means-of-payment currencies (for example, currencies backed by forestland), where the growth in demand for those currencies will increase the amount of natural capital backing them. For a detailed discussion of natural-capital-backed currencies, see [9].

최종적으로, 미래에 더 많은 자산이 토큰화 되었을때, 분할된 리저브 매커니즘은 현실의 자산을 위한 리저브를 허용한다. 이것은 안정적인 측면에서 유용하며, 이러한 화폐들에 대한 성장 요구가 증가하였을때 자연 자본을 기반으로 한 지불 수단 통화를 허용한다.

좀더 자세하게 자연 자본에 의해 유지되는 통화를 알고 싶다면 [9]에 설명되어 있다.

5 Conclusion (결론)

We have introduced a protocol for social payments, called Celo. Celo combines an address-based encryption protocol that allows a sender to use a phone number or email address directly as a public key, with a reserve-backed protocol to minimize volatility through an elastic supply rule. Together, these allow for a more seamless experience using cryptocurrencies as a means of payment. Further, they enable a monetary ecology that includes local and regional currencies, social dividends, demurragecharged currencies, and in the future, natural-capital-backed currencies.

우리는 셀로라 명칭한 사회적 결제 프로토콜을 소개 했다. 셀로는 전송자가 전화번호나 이메일 주소를 공개키로 직접 사용하는 주소 기반의 암호화와, 탄력적인 공급 규칙을 통해 변동성을 최소화시킨 리저브 기반 프로토콜을 조합한다. 또 이것들은 암호 화폐를 결제수단으로 사용하는데 있어서 좀더 경계없는 경험을 제공한다. 추가로 지역통화나, 사회적 배당금, 통화 탈퇴, 미래에는 자연자본에 의해 지원되는 화폐에 대한 생태계를 가능케 한다.

References (참고문헌)

[1] Nader Al-Naji, Josh Chen, and Lawrence Diao. Basis: A price-stable cryptocurrency with an algorithmic central bank. 2017.
[2] Ferdinando M Ametrano. Hayek money: The cryptocurrency price stability solution. 2016.
[3] Eli Ben Sasson et al. Scalable, transparent, and post-quantum secure computational integrity. 2017.
[4] Dan Boneh and Matt Franklin. Identity-based encryption from the weil pairing. In Advances in Cryptology—CRYPTO 2001, pages 213–229. Springer, 2001.
[5] Benedikt Bunz et al. Bulletproofs: Efficient range proofs for confidential transactions. 2017.
[6] Sanjit Chaterjee and Palash Sarkar. Identity-Based Encryption. Springer, 2011.
[7] Roman Croessman et al. An analysis of the stability characteristics of Celo. 2018.

[8] Evan Duffield and Daniel Diaz. Dash: A privacy-centric crypto-currency, 2014.
[9] Charles Eisenstein. Sacred economics: Money, gift, and society in the age of transition. North Atlantic Books, 2011.
[10] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack. 18:186–208, 1989.
[11] Robin Hanson. Futarchy: Vote values, but bet beliefs. 2000.
[12] Daira Hopwood, Sean Bowe, Taylor Hornby, and Nathan Wilcox. Zcash protocol specification, version 2018.0-beta-20. 2018.
[13] Sepandar Kamvar. Numerical Algorithms for Personalized Search in Self-Organizing Information Networks. Princeton University Press, 2009. 13
[14] Sepandar Kamvar, Mario Schlosser, and Hector Garcia-Molina. The eigentrust algorithm for reputation management in peer-to-peer network. In Proceedings of the 12th international conference on World Wide Web. ACM. ACM, 2003.
[15] Bernard A Lietaer. Mysterium Geld: Emotionale Bedeutung und Wirkungsweise eines Tabus. Riemann, 2000.
[16] Bernard A Lietaer. The future of money: A new way to create wealth, work and a wiser world. Century, 2001.
[17] Robert Sams. A note on cryptocurrency stabilisation: Seigniorage shares. Technical report, Working paper, 2015.
[18] Adi Shamir et al. Identity-based cryptosystems and signature schemes. In Crypto, volume 84, pages 47–53. Springer, 1984.
[19] Maker Team. The dai stablecoin system. 2017.
[20] Lloyd Trefethen and David Bau. Numerical Linear Algebra. SIAM, 1997.
[21] Will Warren and Amir Bandeali. 0x: An open protocol for decentralized exchange on the ethereum blockchain, 2017.