MYKEY 자기 주권 신원 시스템 백서 1.0

개요

MYKEY (mykey.org)는 다양한 퍼블릭 블록체인(public blockchain)에서 사용되는 자기 주권 신원 시스템 (self-sovereign identity system)이다. 그 근간이 되는 프로토콜은 KEY ID 라 불린다. 본 문서를 통해 이 자산 관리 기능의 특징들을 살펴보고자 하며, 사회 관계와 정보 보호라는 두가지 측면에서 MYKEY 의 미래 발전 방향에 대해 간략하게 설명하고자 한다. 자산 관리 측면에서 보면 MEYKEY 는 사용자가 자신의 모든 자산을 관리할 수 있도록 해주는 멀티체인 월렛(multi-chain wallet)이다. 개인키를 분실했을 경우 사용자 본인이 계정을 동결하고 복원할 수 있다. MYKEY 는 또한 신뢰망(Web of Trust)의 구성 요소 중 하나이다. 웹 3.0 의 맥락에서 보면 MYKEY 는 정보의 소유권을 사용자에게 되돌려주며 이로써 **개인 정보 보호를 실현한다.**

1. 소개

MYKEY 는 여러 퍼블릭 블록체인에서 사용 중인 자기 주권 신원 시스템이다. KEY ID 자기 주권 신원 프로토콜을 처음으로 도입한 시스템이기도 하다. MYKEY 는 IOS 와 안드로이드에서 오픈소스 형태로 제공될 예정이다. KEY 토큰의 기능 중 하나가 프로토콜 내의 ID 를 구입하는 것이다. MYKEY Lab 이 KEY ID 프로토콜의 개발을 담당하며, 비후 키 재단(Bihu Key Foundation)은 100 억 KEY 를 MYKEY Lab 에 기부할 것이다. MYKEY Lab 은 MYKEY 앱을 운영하는 영리기업이다.

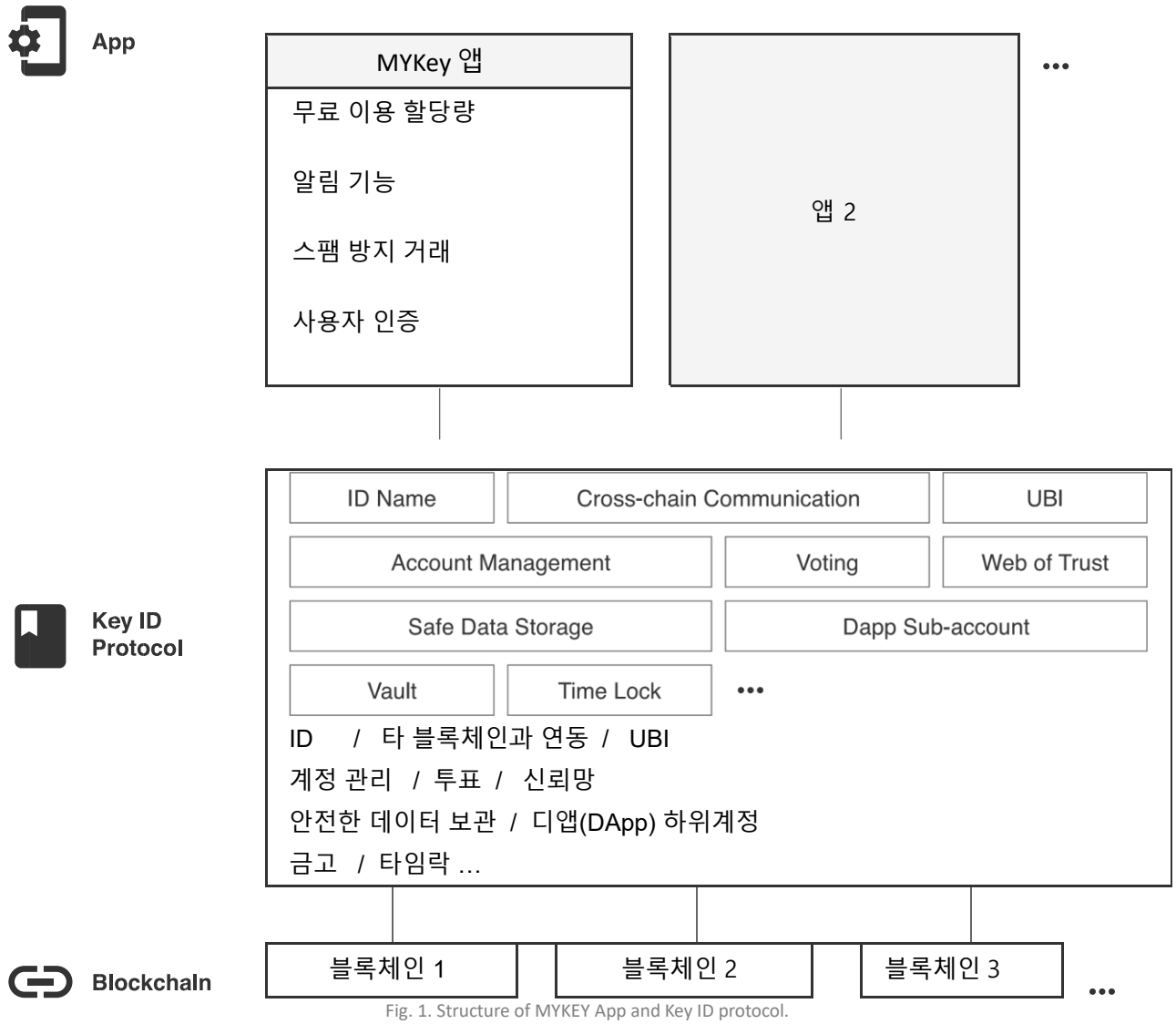

Fig. 1. Structure of MYKEY App and Key ID protocol.

최종 사용자의 입장에서 MYKEY 앱은 멀티체인 월렛, 신뢰망, 신뢰할 수 있는 데이터 보관이라는 세가지 특징으로 요약 설명할 수 있다.

MYKEY 앱은 다양한 퍼블릭 블록체인에서 월렛 서비스를 제공하며 다음과 같은 특징들이 있다.

1. 범용 ID
2. 제한적 무료 이용
3. 향상된 계정 보안을 위한 접근제어 방식의 종합 설계
4. 개인키 분실에 대비한 계정 복원 기능
5. 프로토콜 업그레이드 기능
6. 스팸 방지 기능

신뢰망 속에서 각 계정은 세가지 요소로 구성된다.

1. 영구적 소유권이 부여된 범용적 고유 ID
2. 신원 계정 파일
3. 스마트 계약 계정이 제어하는 분산식 시큐어 데이터 엔클레이브(decentralized secure data enclave).

'베리파이어블 클레임'(verifiable claim)은 신뢰망의 또다른 기본 구성 요소 중 하나이다. 신뢰망에서 각 ID 계정은 다른 계정과 수많은 베리파이어블 클레임을 주고받는다. 건실한 신뢰망은 상호연결 된 베리파이어블 클레임으로 구성된다. 베리파이어블 클레임은 각각 뒷받침하는 문서가 존재하며 이를 작성할 수도 있다. 또한 해당 문서는 분산식 데이터 엔클레이브에 보관된다. 타 계정은 소유자의 허가 없이 엔클레이브에 접속할 수 없다.

신뢰할 수 있는 데이터 보관: 엔클레이브에 보관 된 데이터가 반드시 베리파이어블 클레임과 연동 되는 것은 아니다. 독립적으로 보관할 수 있으며, 계정 소유자의 동의 하에 타 계정을 통해 접근할 수 있다. 계정 소유자는 또한 파일을 공개할 수 있다. 데이터 보관 서비스와 신뢰망은 분산 보관이라는 동일한 구조에 기반하고 있으며, 유사한 인증 메커니즘을 사용한다.

신뢰망과 데이터 보관 서비스 모두 분산 보관 기술의 발전을 전제조건으로 한다. 따라서 현 시점에서 두 기술을 발전시키는 것은 미래로 미룰 수밖에 없다.

2. 정체

'신원'(identity)이란 무엇인가? '신원'이란 '본인'을 수용하는 '틀'(shell)이다.

신원이란 사회 관계, 자산, 데이터라는 세가지 요소로 구성된다.

사회관계란 사회적인 맥락 속에서 본인이 누구인가를 나타낸다. 사회 속에서 한 개인이 어떤 위치에 있나? 아버지의 아들일 수도 있고 아내의 남편일 수도 있으며, 부하의 상관일 수도 있고 특정 단체에 소속된 운동가일 수도 있다. 사회 관계는 '내가 누구인가'를 정의한다. 따라서 사회관계가 없는 신원은 그 존재 자체가 무의미하다.

자산이란 한 '신원'이 소유한 자산을 의미한다. 예를 들어 부동산은 해당 '신원'의 이름으로 등록되어 있으며, 신용카드 또한 누군가가 소유하는 것이며, 한 개인이 컴퓨터를 대여하여 활용할 수 있는 것이다.
이 모든 것이 한 '신원'이 가진 자산적 특징이다.

데이터란 '신원'과 관련된 모든 정보를 의미한다. 예를 들어 한 개인이 특정일에 항공권을 구매하며, 한 개인이 사진 1000 장을 소유하고, 온라인 쇼핑몰의 거래내역도 한 개인의 거래 내역이고, SNS 사이트에서 사용자 활동 내역도 개인의 것이며, 웨어러블 기기도 개인 정보를 기록한다.

신뢰망 속에서는 블록체인 기술과 분산 보관 기술을 이용하여 본인의 정체를 앞서 언급한 세가지 측면에서 재구성할 수 있다. 신뢰망을 통해 온라인과 오프라인에 분산된 신상정보를 통합할 수 있다. 그런 면에서 종합적인 '틀'을 구축하여 '본인'을 재정의한다. 웹 2.0 기술과는 달리, 이런 중요한 정보는 신상정보 소유자가 전적으로 제어할 수 있으며 소유자의 허락을 통해서만이 접근 가능하다. 신뢰망 속에서 신상정보란 현실세계에 실존하는 사람을 전자 상에 나타내는 셈이다. 비록 '나'는 수명이 다하면 존재가 소멸하게 되지만, 해당 신상정보의 '틀'은 보관 비용을 충분히 지급했다는 가정 하에 수천년 간 존재할 수도 있는 것이다.

3. ID 월렛

3.1 멀티체인 월렛

MYKEY 멀티체인 월렛은 다양한 스마트 계약 플랫폼을 지원한다. MYKEY 계정은 각각 스마트 계약의 형태로 존재하기 때문에 MYKEY 월렛은 스마트 계약 기능이 없는 블록체인은 지원하지 않는다.

각 체인간 토큰 전송은 어떻게 하나? 쉽게 말하면 크로스체인 기술이 발달되기 전에는 불가능하다. KEY 는 이더리움 네트워크 상에 존재하는 ERC20 토큰이기 때문에 MYKEY 는 KEY 토큰이 부분적으로 기타 퍼블릭 블록체인으로 전송되는 문제를 해결해야만 한다. 가장 빠르고, 또 보기에 따라서는 가장 효율적일 수도 있는 방식은 MYKEY Lab 이 자사의 KEY 토큰 소유량을 이더리움 블록체인에 공개한 다음 다른 블록체인에 동일한 양의 매핑 된(mapped) 토큰을 제공하여 수수료를 제외한 1:1 토큰 전환 서비스를 제공하는 것이다. 크로스체인 기술이 이후에 발전되면 MYKEY Lab 은 다시 무 신뢰(trustless) 크로스체인 거래 방식을 활용할 것이다.

3.2 신원

KEY ID 프로토콜은 이를 이용하는 모든 블록체인에 거쳐 범용적인 고유 ID 를 생성한다. 신상정보 계정은 계정에 귀속된 모든 ID 에 대한 영구적인 소유권과 사용권을 지닌다. 크로스체인 기술의 부재로 인하여 특정 블록체인이 ID 를 보관하기 위한 루트 체인(root chain)의 역할을 수행해야만 한다. KEY ID 프로토콜을 적용하는 첫 블롯체인이 루트 체인이 되며, 타 블록체인과 루트 체인과의 ID 매핑이 이루어지게 된다.

매핑을 도입할 수 있는 방법 중 하나가 '스테이킹+챌린지 기간(staking+challenge period)' 방식이다. KEY ID 프로토콜을 사용하는 모든 블록체인에 거쳐 사용자 별로 UUID(Universally Unique Identifier)를 부여하여 각 계정의 소유자가 동일하다는 것을 나타낸다. 또한 사용자가 각각 다른 블록체인에서 동일한 ID 를 사용한다. 하지만 누구든 새로 생성된 신원 계정과 UUID 를 연동할 수 있어 사용자를 식별하기 위한 목적으로 보면 UUID 는 결정적 증거가 될 수 없다. 신원은 ID 가 루트 체인 상에 존재하는 계정에 귀속될 때만 성립된다.

비루트체인(non-root chain)에서 신원 계정과 ID 간의 매핑을 처음으로 수행하기 위해서 사용자는 루트체인 상에서 동일한 UUID 와 해당 ID 가 이미 연동되어 있는지 확인할 필요가 있다. 그런 다음 비루트체인에서 신원 매핑을 실시하기 위하여 정해진 양의 KEY 토큰을 담보로 스테이킹(staking)해야 한다. 이후 이어지는 '챌린지 기간'(challenge period) 동안 누구든 동일한 양의 KEY 토큰을 스테이킹하여 계정에 대한 소유권을 주장할 수 있다. 챌린지 기간이 끝나기 전까지 다른 사용자가 계정 소유권을 주장하지 않을 경우, 비루트체인에서도 신원 매핑이 성공적으로 이루어진다. 하지만 챌린지 기간 동안 소유권을 주장하는 사용자가 나타날 경우, 소유권을 주장하는 사용자는 동일한 양의 KEY 토큰을 스테이킹해야 한다. 이 시점에서 중재자는 두가지 사항을 확인하게 된다. 첫째로 루트 체인 상의 UUID 와 이와 연동 된 ID 가 비루트체인에 등록된 것과 동일한지 확인하며 둘째로 비루트체인 계정에 귀속된 기본공개키(계정 생성시 기존 공개키 항목)와 계정 정보가 루트체인과 동일한지 확인한다. 중재자는 이 두가지를 통해 결정을 내리고, 패자는 스테이킹한 토큰을 전부 잃게 되며 스테이킹되었던 토큰은 승자, 중재자, MYKEY Lab 이 일정 비율로 나눠 갖는다. 정확한 비율은 후일 결정될 것이다. MYKEY Lab 이러한 '챌린지'의 수행을 위한 시스템을 구축할 예정이다.

그럼 중재자를 어떻게 선정하는가? 만약 비루트체인에서 이미 신뢰성이 높은 오라클 시스템을 갖췄을 경우, 이미 갖춰진 시스템을 활용한다. 그렇지 않은 경우에는 MYKEY 커뮤니티 내에 신뢰할 수 있는 오라클 단체가 구축 되어야할 것이다.

비루트체인에 이미 귀속된 신원 계정과 ID 의 경우, 사용자는 잘못된 정보를 수정하기 위해 마찬가지로 '스테이킹+챌린지 기간' 시스템을 활용할 수 있다. 하지만 기존 계정 생성에 비해 조건이 엄격할 것이며, 스테이킹해야 하는 KEY 토큰의 양도 상대적으로 높을 것이고, 챌린지 기간 동안 상당히 길어질 것이다. 마지막으로 사용자가 챌린지 기간을 요청할 수 있는 횟수에는 제한이 없을 것이다.

ID 생성 규칙:
1. ID 의 길이는 1-63 문자로 제한
2. 허용된 문자: a-z 까지 26 개 영문자를 대소문자 구분하여 사용 가능, 하이픈 '-'과 0-9 까지 숫자 사용 가능
3. ID 는 대소문자를 구분
4. ID 의 첫 문자와 마지막 문자로 하이픈 '-'을 사용 불가능

MYKEY 신원 계정은 여러 ID 를 소유할 수 있으나 MYKEY 신원 계정과 한번 연동된 ID 는 다른 계정과 연동이 불가능 해진다. MYKEY 계정은 한 ID 에만 귀속될 수 있으며, 귀속되지 않은 ID 는 타인에게 소유권을 이전할 수 있다.

ID 선점을 방지하기 위해 ID 는 경매를 통해 점진적으로 공개될 예정이다. KEY ID 프로토콜의 공개적인 특징 때문에 경매에는 MYKEY 계정이 아닌 모두가 참여 가능하다. 보다 구체적으로 말하자면 루트체인에 존재하는 모든 블록체인 계정이 동일하게 경매에 참여할 수 있다. 경매의 수익금은 MYKEY Lab 가 가지게 된다. 경매의 규칙은 다음과 같다.

1. ID 공개 개수와 일정
    *단일 문자 ID: 120 일 단위로 1 개 ID 공개
    *2 문자 ID: 7 일 단위로 1 개 ID 공개
    *3 문자 ID: 매일 5 개 ID 공개
    *4 문자 ID: 매일 125 개 ID 공개
    *5 문자 ID: 매일 3000 개 ID 공개
    *6 문자 ID: 매일 85000 개 ID 공개
    *7 문자 이상 ID: 제한 없음
2. 모든 ID 는 최소 0.1KEY 를 비용으로 지불해야함
3. 입찰 단위는 전 입찰 대비 금액이 10% 높아야 함
4. ID 경매는 24 시간 내 새로운 입찰이 없을 경우에만 낙찰
5. ID 분류별로 입찰이 높은 순으로 낙찰되며 일일 제한까지 낙찰이 된 경우 낙찰되지 않은 ID 는 익일로 넘어감. 익일로 연기된 입찰은 낙찰에 있어 우선순위가 가지지 않음
6. 낙찰되지 않은 ID 는 모두 입찰 가능

3.3 제한적 무료 이용

'무료이용'이란 KEY ID 프로토콜에 내장된 요소가 아닌 KEY ID 프로토콜을 사용하는 첫 시스템인 MYKEY 앱이 제공하는 특전이다.

사용자들은 인터넷 상에서 무료 이용이라는 개념과 친숙하나 블록체인 사용 비용을 지불하는 것은 꽤나 귀찮은 일이다. 스팸 공격을 예방하기 위해 퍼블릭 블록체인에는 수수료가 기본적으로 동반되기 때문이다. '무료'라고 선전하는 일부 블록체인은 토큰의 시간가치를 통해 수수료를 받으며, 결국 '무료'가 아니게 된다.

수수료는 블록체인 사용에 있어 차질을 빚으며 사용자 참여를 제한한다. 원활한 대중화를 위하여 MYKEY 는 프로토콜을 사용하는 모든 퍼블릭 블록체인을 무료로 이용할 수 있도록 할당량을 제공한다. MYKEY 계정을 생성할 시 사용자는 인증을 통해 무료 계정과 무료 이용 할당량 제공 받을 수 있다. MYKEY Lab 은 인증이 완료된 후 사용자를 식별할 수 있는 정보를 보관하지 않는다. 개인정보를 보호하는 동시에 무료 계정을 반복적으로 생성하는 것을 방지하기 위해 이름, 문서 종류, 문서 부호, 무작위 부호가 기록된 해시(hash)만 보관한다.

무료 이용 할당향은 KeyPoint(KP)에 기록되며 이는 이전할 수 없다. 초기에는 1KP 당 1USD 의 비율로 정해지며 인증한 모든 사용자는 일정량의 KP 를 할당 받는다. 추가 KP 는 사용자의 활동 내역에 따라 더 지급될 수 있다.

인증을 거치지 않은 사용자는 블록체인 비용을 개인적으로 부담해야한다. KP 를 구매하여 사용할 수는 있다.

3.4 계정 보호

MYKEY 계정의 보안은 몇 가지 시스템을 통해 이루어진다. 먼저 MYKEY 앱은 오픈소스 프로젝트로서 커뮤니티가 전체적으로 검토하게 될 것이다. 코드상 취약점을 발견하는 사용자에게 보상이 지급 될 것이다.

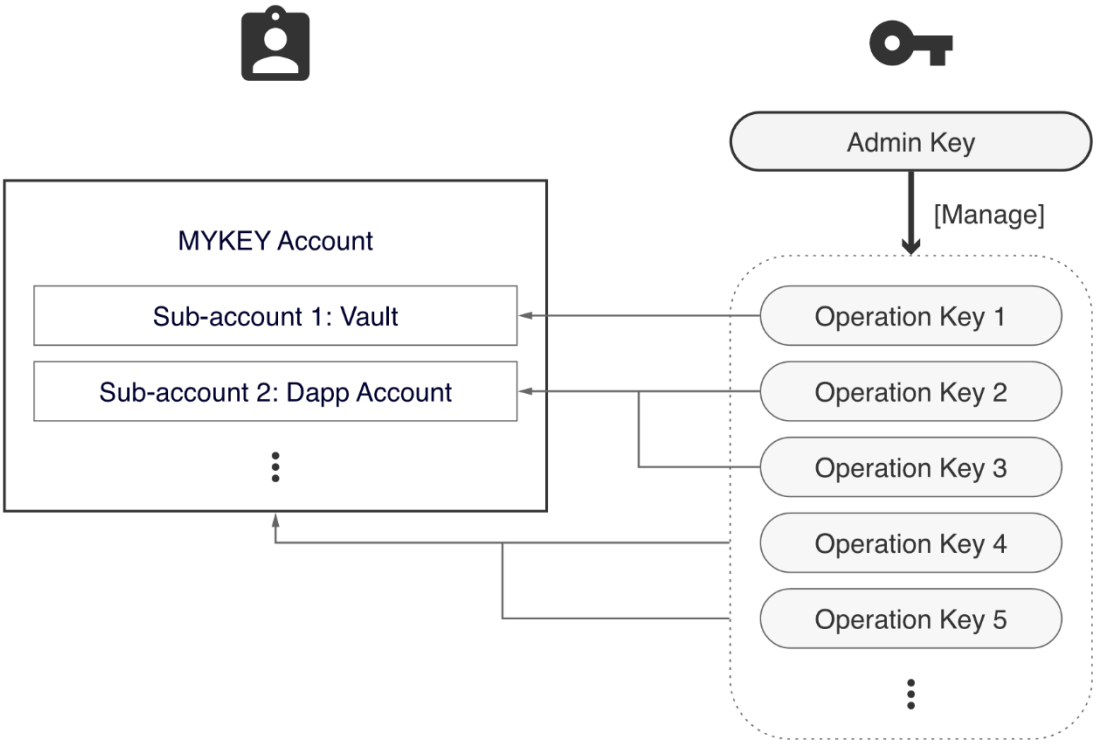

표 2. MYKEY 계정 시스템 및 개인키 인증 구조

표 2 에서 볼 수 있듯이 MYKEY 는 보안을 강화하기 위해 접근 제어 시스템 간의 균형을 맞추는 동시 시간차(time-delay) 시스템을 적용하여 설계했다. 덕분에 단일 장애점(one-point-failure)으로 인한 취약점을

예방할 수 있다. 접근 인증은 관리자 개인키(Admin Private Key)와 운영 개인키(Operation Private Key)를 통해 다음과 같이 이루어진다.

1. **관리자 개인키:** 관리자 개인키는 계정에 대한 권한이 가장 높다. 계정 소유자 본인이 **단독**으로 **독립적**으로 소유해야 하며 그 어떤 상황에서도 타인과 공유해서는 안된다. 관리자 개인키는 MYKEY 앱이 설치되어있는 장치에 보관되지 않는다. MYKEY 앱은 대신 사용자로 하여금 12 자리의 비밀번호를 오프라인의 문서상으로 기억하도록 메시지를 띄운다. 12 자리의 비밀번호 시스템은 이후에 하드웨어로 대체될 수도 있다. 관리자 개인키는 운영 개인키를 동결하거나 교체할 수 있으며 스스로도 교체할 수 있다. 하지만 자산 이전과 같은 직접 계정 인증은 불가능하다.

   관리자 개인키의 권한은 다음과 같다.

   A. 계정의 운영 개인키를 독자적으로 즉시 동결

   B. 계정의 운영 개인키를 독자적으로 7 일 지연 기간 후 동결 해제, 혹은 비상연락 대상자가 동시 승인할 경우 즉시 동결 해제

   C. 계정의 운영 개인키를 독자적으로 7 일 지연 기간 후 교체, 혹은 비상연락 대상자가 동시 승인할 경우 즉시 교체

   D. 관리자 개인키를 21 일 지연 기간 후 교체, 혹은 비상연락 대상자가 승인할 경우 즉시 교체

   E. 관리자 개인키 교체, 운영 개인키 교체, 운영 개인키 교체를 비롯한 지연된 모든 활동을 독자적으로 즉시 취소 가능

   F. 비상연락 대상자를 독자적으로 21 일 지연 기간 후 추가/삭제 가능

   G. 운영 개인키 분류를 즉시 생성 가능

2. **운영 개인키:** 운영 개인키의 각 분류는 특정 기능에 대한 승인권을 가진다. 각각 기능은 오직 정해진 분류를 통해서만 승인될 수 있다.

   2-1. 비상 연락 대상자의 **회신 개인키:** MYKEY 계정은 각각 다른 MYKEY 계정의 비상연락 대상자가 될 수 있는데, 이를 통해 모든 사용자는 신뢰할 수 있는 개인이나 단체를 비상연락 대상자로 설정할 수 있다. 계정의 기본 비상연락 대상자는 MYKEY Lab 으로 설정된다. 사용자는 비상연락대상자를 추가/삭제 할 수 있으며, 비상연락처는 최소 하나에서 최대 여섯 개까지 저장 할 수 있다. 비상연락처 갯수 제한은 KEY ID 프로토콜이 아닌 MYKEY 앱이 설정한다. 비상연락 대상자는 비상시 계정 소유자에게 도움을 줄 수 있다. 계정 활동은 비상연락 대상자의 60% 이상이 승인할 때 실행된다. 회신 개인키의 권한은 다음과 같다.

      A. 운영 개인키 동결 해제를 위해 관리자 개인키 소유자를 지원

      B. 관리자 개인키 교체를 위해 관리자 개인키 소유자를 지원

      C. 운영 개인키 교체를 위해 관리자 개인키 소유자를 지원

      D. 계정 소유자의 관리자 개인키를 독자적으로 30 일 지연 기간 후 교체

   2-2. **자산 관리 개인키:** 자산 관리 개인키는 MYKEY 주 계정이 소유한 모든 자산을 이전하거나 담보화하는 등 관리할 수 있다. 자산 관리 개인키는 MYKEY 에 특수목적으로 생성된 하위계정에 대한 권한을 갖지 않는다.

   2-3. **특수목적 하위계정(special-purpose-sub-accounts)을 위한 운영 개인키**는 예금 계좌나 외부 이용을 위한 하위계정 등을 관리한다.

   2-4. **로그인 개인키:** MYKEY 계정을 이용해 외부 앱에 로그인하는 것을 승인하기 위해 사용.

2-5. **투표를 위한 개인키:** MYKEY 계정내 제안 사항에 대해 투표하기 위해 사용.

2-6. **베리파이어블 클레임을 위한 운영 개인키:** MYKEY 계정은 KEY ID 프로토콜을 활용한다. 자기 주권 신원 프로토콜의 기초 구성요소 중 하나로서 KEY ID 는 다른 KEY ID 와 베리파이어블 클레임을 주고받는다.

이상 인증 권한 설정을 통해 다음과 같은 상황에서 비상연락처가 유효할 경우 계정을 복구할 수 있다.

1. MYKEY 앱 비밀 번호 분실
2. 스마트폰과 같은 기기 분실
3. 운영 개인키 유출
4. 관리자 개인키 분실
5. 운영 개인키 유출
6. 기기와 관리자 개인키 동시 분실
7. 사용자가 심각한 사고로 인해 장기적으로 실종되거나 사망

사용자가 계정을 복구할 수 없는 경우는 관리자 개인키가 유출되고 동시에 분실된 경우에 한한다. 이런 경우 시스템 상에서 개인키를 현재 보유한 사용자가 정당한 계정 소유자인지 구분할 방법이 전혀 없기 때문이다. 바꿔 말하면 사용자가 관리자 개인키를 단독으로 소유하고 있는지 여부가 정당한 계정 소유자를 판단하는 가장 중요한 조건이다. 그렇기 때문에 MYKEY App 은 초기 설정 시 비밀번호 사본을 적어도 2 부 이상 작성하여 각각 타인이 모르는 장소에 따로 보관하도록 권고할 것이다. 이렇게 함으로써 비밀번호가 기록된 사본을 타인이 취득할 경우 사용자는 다른 사본을 참고할 수 있게 된다.
이후 MYKEY 는 기관을 위한 맞춤형 서비스를 개발할 수도 있으며 이러한 기관을 위해 인증 방식을 다양화할 계획이다.

3.5 프로토콜 업그레이드 기능

프로토콜의 장기적 성공을 위해 업그레이드 가능성은 매우 중요한 요소이다. KEY ID 자기 주권 신원 프로토콜은 사용자 니즈에 맞춰 분산 보관이나 크로스체인 기술과 같이 그 기반이 되는 기술의 발전과 함께 진화할 것이다.

프로토콜의 업그레이드 가능성과 무 신뢰의 개념은 근본적으로 대립된다. 이러한 대립을 적절하게 해소하기 위해서 대규모 MYKEY 커뮤니티와 소통하여 업그레이드에 대한 의견일치를 이루는 동시에 동의하지 않는 이들에게 새로운 기능을 사용하지 않을 권리를 부여해야 할 것이다. 새로운 코드는 반드시 충분한 시간이 주어진 상태에서 커뮤니티 감사를 거쳐야 하며 코드 취약점을 발견하기 위한 보상 시스템이 뒷받침되어야 한다. 프로토콜 업그레이드를 규정하는 스마트 계약에 대기 기간이 미리 명시된다. 이 대기 기간은 건너뛸 수 없기 때문에 사용자들은 탈퇴할 시간이 주어진다. 초기에 대기기간은 4 일로 설정되며 KEY ID 프로토콜이 성숙함에 따라 점차 길어질 예정이다.

프로토콜 업그레이드는 MYKEY Lab 이 관리하는 멀티시그너처(multisig) 계정이 개시한다. 6 번째 항목에 설명된 MYKEY Lab 의 분권화를 통해 프로토콜 업그레이드가 이루어지기 전 커뮤니티가 의견 일치를 이룰 수 있을 것이다.

3.6 스팸 방지

스팸 거래 필터링은 프로토콜 차원에서 제공되지 않는 MYKEY 의 강력한 기능 중 하나이다. MYKEY 앱은 스팸 거래를 방지하기 위한 적응적 스마트 시스템을 활용하여 쾌적한 사용 경험을 선사한다.

4. 신뢰망

본 문서가 이후 수정됨에 따라 신뢰망에 대한 추가 정보가 기재될 것이다. 현재는 기본 지침만 기술한다.

신뢰망은 신원 계정과 베리파이어블 클레임의 두가지 요소로 구성된다. 신원 계정은 KEY ID 자기 주권 프로토콜을 따르며, MYKEY 는 KEY ID 를 사용하는 시스템 중 하나이다. 베리파이어블 클레임은 신원 계정이 서로 활동 내역을 주장하는 행위이다. 예를 들어 신원계정 A 가 신원계정 B 의 연령이 21 세 혹은 그 이상이라 주장할 수 있다. 다양한 분산원장(distributed ledger) 기술을 기반으로 하여 아무도 눈치채지 못하도록 비밀리에 주체, 대상, 시간, 내용을 조작할 수 없게 되어있기 때문에 신뢰성이 확보 된다.

신원계정은 신뢰망의 교점이며 베리파이어블 클레임은 각 교점 간의 연결고리의 역할을 한다. 이를 통해 여러 독립적 신원 계정이 각각 사실확인 과정에 동원될 수 있으며 이로써 거대한 신뢰망이 구축되는 것이다. 신뢰망의 상호연결 구조가 신원확인의 효율과 신뢰성을 향상시켜 결과적으로 허위 클레임과 허위 신원의 종지부를 찍을 것이다. 계층적 구조(표 3 의 파란색 화살표)와 자유식 구조(녹색 화살표)를 통해 신뢰를 구축하고 향상시킬 수 있을 것이다.

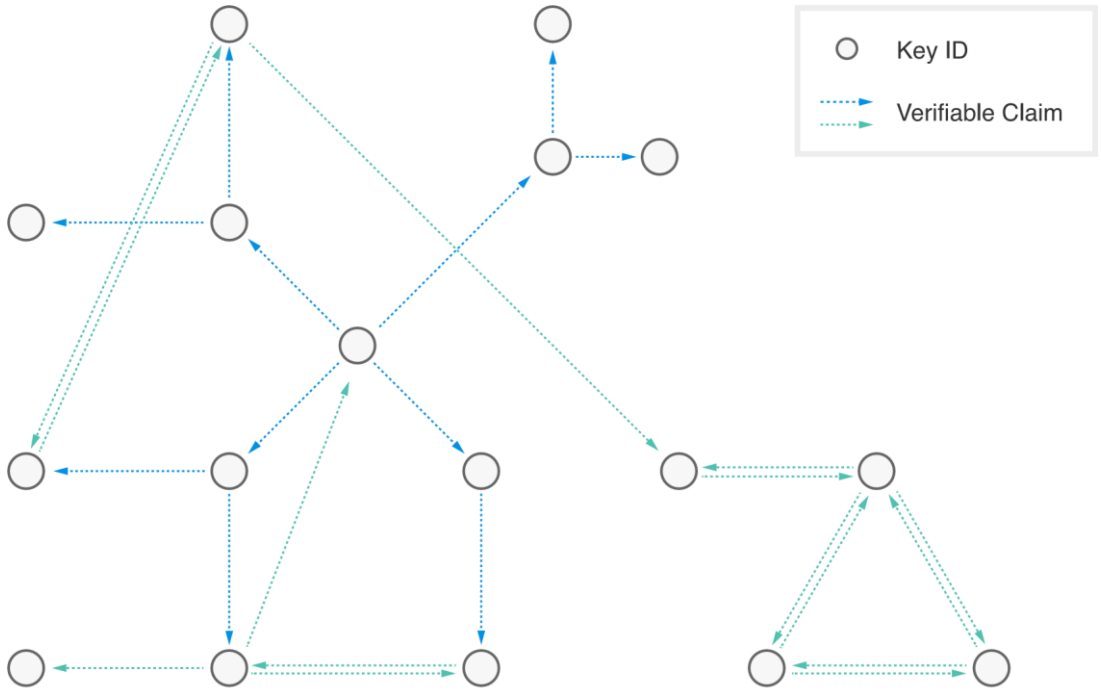

Fig. 3. An schematics of Web of Trust.

표 3. 신뢰망 구조

기술적인 측면에서 신원 계정은 1) ID, 2) 신원 파일, 3)분산 보관 기술에 기반하고 신원 스마트 계약이 규정한 시큐어 데이터 엔클레이브로 구성된다. ID 에 관한 내용은 3.2 에 기술되어 있다. 신원파일은 신원계정의 특성들에 대해 기록한다. 보다 자세한 사항은 여기서 확인 가능하다. 시큐어 데이터 엔클레이브란 신원계정 스마트 계약이 규정한 특수한 분산형 데이터 보관소이다. 시큐어 데이터 엔클레이브의 구조와 그 개발 속도는 분산형 보관 기술의 발달에 달려있다. 그전까지는 절충안을 활용할 필요성이 보인다.

신뢰망은 다음과 같은 사항을 포함한다.

1. 딥페이크(DeepFake)와 같은 영상/음성 합성 기술을 활용한 가짜 뉴스, 허위 정보, 사기로 인해 발생하는 문제를 해결

2. 신뢰 부족으로 인한 마찰(본인의 모친이 실제로 모친임을 증명하라는 등의 상황)을 완화하기 위해 보다 종합적이고 효율적인 개인 신용평점 시스템 구축
3. 신뢰망에 기반한 혁신적 공조 기회 창출

5. 신뢰할 수 있는 데이터 보관

해당 항목은 본 문서가 이후 수정됨에 따라 더 상세하게 기술될 것이다. 현 시점에서는 기본적인 사항만 기술한다.

앞서 언급되었던 시큐어 데이터 엔클레이브는 신뢰망의 핵심적인 요소일 뿐만 아니라 신원확인과 관련된 다른 분야에서도 중요하다. 따라서 개별 항목을 통해 다룰 필요가 있다.

5.1 신뢰망에서 개인정보 보호

퍼블릭 블록체인 상의 정보는 모두에게 공개되어 있는 만큼 블록체인 상에 개인 정보를 보관하는 것은 적절치 못하다. 베리파이어블 클레임의 모든 내용을 블록체인 상에 저장하는 것은 바람직하지 않다. 대신 신원계정이 제어하는 시큐어 데이터 엔클레이브에 보관한다. 사실확인을 위해 암호화된 정보만이 퍼블릭 블록체인에 공개될 뿐이다. 해당 정보는 머클 트리(Merkle Tree)와 같은 해시 트리(hash tree)의 루트 해시 값의 형태로 공개 될 수도 있다.

5.2 개인 정보 전체 내역

분산형 보관 기술에 기반하여 시큐어 데이터 엔클레이브는 계정 스마트 계약이 전적으로 통제권을 가지게 된다. 다시 말하면 신원계정의 소유자가 엔클레이브 상의 데이터를 전적으로 통제할 수 있다는 뜻이며 사용자의 허가 없이는 아무도 데이터에 접근할 수 없다. 따라서 사용자가 매우 민감한 정보를 엔클레이브에 보관해도 안전하다. 다음과 같은 정보가 그 예가 될 수 있다.

1. 개인 건강 정보
2. 온라인 활동 전체 내역
3. 유서
4. 웨어러블 기기가 기록한 정보

데이터는 사용자의 동의 하에 다른 신원계정과 공유할 수 있으며 공개할 수도 있다. 스마트 계약의 프로그램 가능성 덕분에 데이터를 공유하는 방식을 여러가지 미리 프로그래밍해둘 수가 있다. 예를 들어 엔클레이브 상의 유서는 사용자의 신원계정이 장기간 활동이 없을 경우 특정 계정과 공유되도록 설정할 수 있다. 혹은 신원 소유자가 사망한 후 50 년이 지난 시점에서 엔클레이브 상 모든 정보가 공개되도록 할 수도 있다. 분산형 보관 기술의 뛰어난 신뢰성 덕분에 충분한 비용이 지급 될 경우 수천년 간 데이터를 보관 할 수도 있다.

5.3 디앱

디앱(DApp)상의 정보는 부분적으로, 또는 전체를 분산 보관할 수 있다. 따라서 해당 데이터에 접근하기 위해서 사용자 계정의 인증이 필요하다. 디앱의 데이터 일부가 사용자 엔클레이브에 저장될 수도 있다. 디앱과 신원계정은 각자 고유의 시큐어 데이터 엔클레이브가 존재한다. 이러한 이중 데이터 보관 구조는 디앱 개발에 있어 높은 수준의 유연성을 제공한다. 예를 들어 선거 디앱은 영지식 증명(zero-knowledge proof)를 통해 선거 내역을 공개하지 않으면서도 개인 정보를 보호할 수 있다. 전체 내용은 사용자 엔클레이브에 비밀 보관된다.

6. MYKEY Lab 의 토큰화

고지사항: 해당 항목의 본사의 의무 사항이나 공약을 기술한 것이 아니며, MYKEY Lab 의 토큰화 여부, 시기, 방식에 관해 MYKEY Lab 의 주주와 경영진이 독자적인 결정권한을 가진다.

중앙화(centralization)가 분권화(decentralization)에 비해 확실하게 효율성에 있어 우월하다. 급속한 발전의 초기 단계에서 중앙화 된 팀의 강력한 추진력이 프로젝트에 도움이 되는 경우가 많다. MYKEY 는 비록 중앙화 된 개발 방식에 시작하였으나, 인류 사회구조의 핵심적인 기반이 되고자 하는 원대한 포부에 따라 커뮤니티가 주권을 이어받아 모두가 소유하고 관리하는 공공 앱을 추구한다.

토큰화가 이루어진 이후 MYKEY Lab 은 MYKEY 의 관리 기구로서의 역할을 더 이상 수행하지 않으며 독립적인 집단으로서 존재하게 될 것이다. 대신 거버넌스 토큰(Governance Token)이라 불리는 토큰이 MYKEY 앱과 KEY ID 프로토콜에 관한 결정 권한을 가지게 된다. MYKEY Lab 의 수익의 대부분은 토큰화 후 GT 의 형태로 유지 될 것이며 토큰 투표를 통해 분배 될 것이다.

거버넌스 토큰의 분배. 거버넌스 토큰의 총량은 1000 억으로 40%가 사용자에게, 20%가 운영 및 홍보진에게, 25%가 MYKEY Lab 의 주주에게, 15%가 이후 설립될 KEY ID 재단에 분배될 것이다. 25%와 15% 분배될 토큰은 4 년에 거쳐 일정량 씩 공개될 것이다.
이 과정은 토큰화 과정에서 성립될 스마트 계약으로 규정될 것이다.

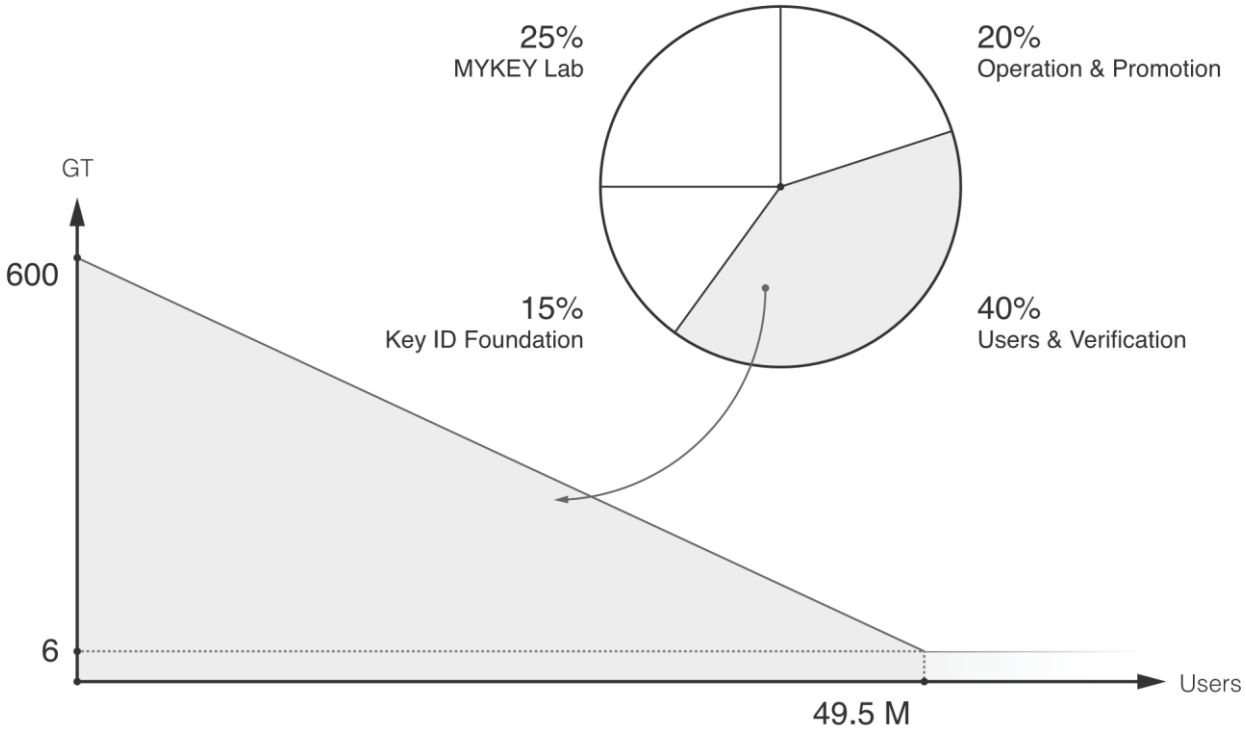

Fig 4. Distribution of GT

표 4. 거버넌스 토큰 분배

400 억개 거버넌스 토큰의 분배 계획

1. 신원 확인이 된 첫번째부터 10000 번째 사용자까지 각자 600 거버넌스 토큰 분배
2. 신원 확인이 된 10001 번째부터 20000 번째 사용자까지 각자 (600-1*0.12) 거버넌스 토큰 분배
3. 신원 확인이 된 20001 번째부터 30000 번째 사용자까지 각자 (600-2*0.12) 거버넌스 토큰 분배

4. 이하 동일한 기준을 적용하여 6 거버넌스 토큰으로 보상이 줄어들 때까지 분배. 이후 신원 확인 되는 모든 사용자에게 사용자용 거버넌스 토큰이 고갈될 때까지 6 거버넌스 토큰을 지급
5. 이상 설명된 계획은 각 사용자에게 지급될 평균 양을 나타내며 시장내 피드백에 따라 수정될 수 있음. 예를 들어 토큰의 20%를 추천 보상으로 지급 가능
6. 신원 확인 비용은 전부 사용자용 거버넌스 토큰으로 부담

토큰화 이후 MYKEY 커뮤니티는 대의민주주의 형태로 운영되며 필요에 따라 직접민주주의와 유동민주주의로 보완한다. 더 자세하게 설명하면 거버넌스 토큰 보유자들이 4 년마다 선출하는 위원회가 MYKEY Lab 과 새로 설립될 KEY ID 재단을 운영한다. MYKEY Lab 은 토큰화 이후 첫 임시 위원회를 구성하여 2 년 간 운영권을 이양할 것이다. 임시 위원회는 'MYKEY 커뮤니티 합의에 관한 협정'(MYKEY Community Consensus Convention)을 작성할 것이다. MYKEY 커뮤니티 합의에 관한 협정은 위원회의 권한, 의무, 이해관계, 규정을 바꾸는 것에 관한 규정을 명시할 것이다. 원칙적으로 커뮤니티는 참여도가 일정 비율을 넘고 찬성율이 2/3 을 넘는다는 가정 하에 거버넌스 토큰 총투표를 통해 규정을 수정할 수 있다. (투표 알고리즘이 토큰 투표에 국한된 것은 아니기 때문에 해당 비율은 반드시 투표 비율과 동일할 필요는 없음) 이러한 방식을 통해 유연하고 발전적인 운영을 실현할 수 있다. 참고 사항으로 귀속된 거버넌스 토큰만이 정당한 투표권을 가지게 된다.