IDHub 백서
블록체인 기반 디지털 신원

개요

인터넷 상에는 신원 정보가 없습니다. IP 주소는 컴퓨터에 연결되어 있지 사람에게 연결되어 있지 않습니다. 거래를 할 때 상대방의 진짜 신원을 파악할 수 없습니다. 복제 계정이나 가짜 계정을 방지할 수 있는 효과적인 방법에 대한 필요성이 매우 큽니다. 여러 방법들 중에 사람과 식별자 간에 고유한 연결을 만들어 신원 검증(IDV , identity verification)을 하는 방법이 바람직합니다. 이 방법에서는 사용자의 신원을 쪼개어 서비스 공급자들 간에 배포합니다. 이 방법에 따르면 웹사이트 별로 로그인 암호를 따로 외워야하는 번거로움을 피할 수 있습니다. 우리는 신원 정보에 대한 주권을 사용자가 되찾을 수 있도록 도울 수 있습니다. 신원은 깨졌습니다. 이제 바로잡을 때입니다..

IDHub 는 블록체인 기반의 디지털 신원 플랫폼입니다. IDHub 는 블록체인의 탈중앙화 아키텍처와 스마트 계약을 통한 개인 정보 보호를 이용하여 사용자들이 자신의 신원 정보에 대해 자주권을 확보할 수 있도록 합니다(“나의 신원정보는 내가 소유하고 내가 완전히 통제합니다.”). IDHub 의 디자인 원칙은 자주권, 보안, 개인 정보 보호입니다. 보안은 블록체인 아키텍처의 불역성과 NaCl 등과 같은 암호화 라이브러리를 통해 확보됩니다. 개인 정보 보호는 Kademlia 등과 같은 정보 분산 저장에 의해 달성됩니다. 우리는 또한 연구 보고서인 “Engineer-ing Privacy”에 명시되어 있는 지침을 따릅니다. IDHub 의 신원은 트리 구조와 그래프로 표시됩니다. Merkle 트리는 신원 정보 요소들의 노출을 최소화시킵니다. 신원 그래프는 사용자들 간의 상호 작용을 도식적으로 나타내 보여줍니다. 신원의 핵심 속성은 평판입니다. 대출자의 평판에 대한 정확한 평가는 신용 대출에 필수적입니다.

경쟁사의 모델들은 토큰을 소비하는 문제점을 갖고있습니다. 토큰이 검증자에서 보유자로 그 다음 인증자에게로 흘러갑니다. 인증자들은 상당한 양의 토큰을 모으지만 “인증자들은 토큰을 어떻게 사용할것인가?”에 대한 질문에 답하지 않습니다. 이로 인해 인증자들은 적극적 참여를 망설이게 됩니다. 우리는 인증자들이 생태계와 토큰의 화폐 전환 메커니즘에 참여하도록 인센티브를 제공합니다. IDHub 는 광고를 통해 이 문제를 해결합니다. 광고주가 인증자들로 부터 토큰을 구매합니다.

IDHub 는 이주 노동자, 난민, 경제적 약자들이 어디에서나 자신들의 디지털 신원에 접속할 수 있도록 함으로써 도움을 줍니다. 여기에 당국과 제 3 자로부터 인증을 받을 수 있도록 함으로써 IDHub 는 소액대출, 디지털결제, 금융포용을 지원합니다. 투명하고 신회할 수 있는 "서비스로서의 신원(ID as a Service, IDaaS)" 생태계를 구축함으로써 IDHub 는 비전인 “하나의 신원, 하나의 세상”을 실현합니다.

목차

1. 가치제안

우리가 제안하는 IDH 는 자주성, 보안, 개인 정보 보호에 중점을 두는 블록체인 기반의 신원 시스템 상에서 이뤄지는 토큰의 교환입니다. IDHub 시스템이 제공하는 것은 다음과 같습니다.

- 사용자: 신원 정보 저장이나 인증 시 그리고 토큰 공유 시 강력한 개인정보 보호와 보안
- 인증자: 수익개선 및 화폐 전환 메커니즘 향상.
- 검증자: 검증 비용 절감, 사기 사건 발생 저하, 즉각적 대응.

2. 서론

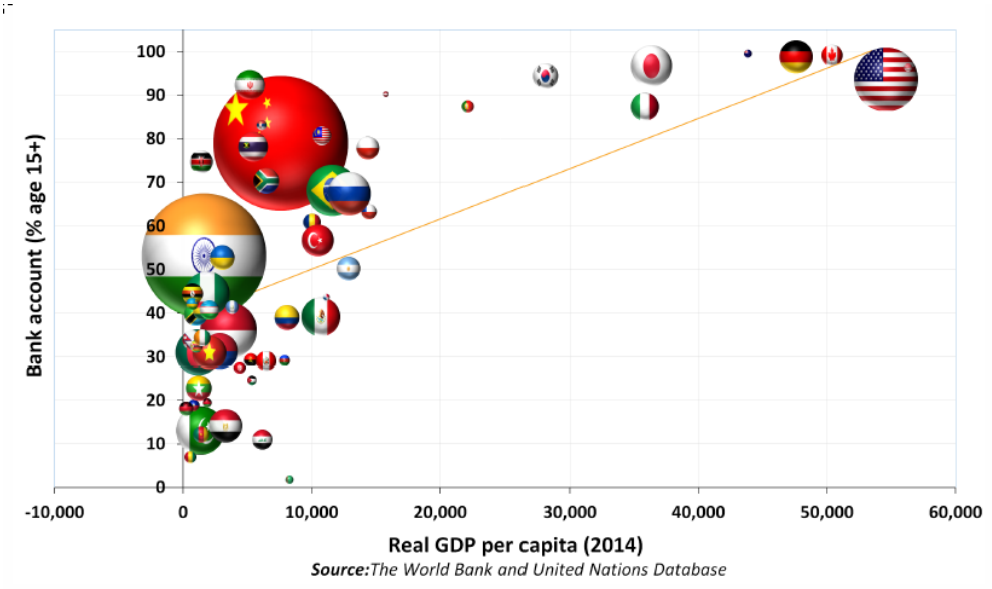
2.1 디지털 신원

디지털 신원이란 식별자와 상관 관계를 갖는 한덩어리의 속성들입니다. 신원이 없는 사람들은 금융제도와 사회보장 제도로부터 배제됩니다. 세계은행에 따르면 전세계 20 억명이 은행 계좌를 갖고 있지 않습니다 [1]. 신원이 없는 사람들이 겪고 있는 심각한 어려움은 전세계 차원에서 인식하고 있는 문제입니다. 유엔 지속개발 목표 16.9 에서는 2030 년까지 전세계 모든 사람들에게 출생 등록을 포함한 법적 신원을 제공하는 것을 목표로 명시되어 있습니다. IDHub 는 경제적 약자, 이주노동자, 난민, 은행 계좌가 없는 사람들에게 디지털 신원을 제공함으로써 이들을 돕고자 합니다.

법적 신원이 없는 사람들은 은행 계좌 개설 신청을 할 수 없습니다. 은행 계좌가 없는 사람들은 신용 대출을 신청할 수 없습니다. 이는 가난의 악순환을 가중시킵니다. 그림 1 은 전세계 60 개국의 은행 계좌 보유 비율을 나타낸 것입니다. 각 국가를 나타내는 원의 크기는 해당 국가의 인구수에 비례합니다. 은행 계좌 보유율이 20% 미만인 국가는 투루크매니스탄, 기니아, 아프카니스탄, 이라크, 카메룬, 파키스탄, 이집트, 말라위, 아이티, 니카라구아입니다. 이중 투르크매니스탄이 가장 낮은데 겨우 1.8%입니다. 이들은 주로 중앙아시아, 서아프리카, 중미 지역에 있는 국가들 입니다. 이 지역 사람들은 금융제도 참여 기회가 희박합니다. 우리는 이들에게 신원을 제공하여 은행계좌를 개설할 수 있도록 함으로써 이들의 삶은 개선하는 데 도움을 줄 수 있습니다. 따라서 우리의 구호는 “은행이 없는 이들에게 은행을”입니다.

신원 시스템들은 두가지로 나뉩니다[3]. 첫째는 기반 신원 시스템인데 이는 포괄적 다목적 시스템으로서 모든 응용 분야에 걸쳐 법적 신원에 대한 모든 니즈를 충족시킵니다. 두번째는 신원 기능 시스템으로서 이는 안전망, 금융, 보건의료, 교통,

출입국, 선거 등과 같은 구체적 응용 분야를 지원하기 위해 개발됩니다. 이중 안전망은 신원 시스템을 통해 고유성과 전자 현금 이체를 사용하여 금융 사기를 예방합니다. 금융의 경우 신원 시스템은 디지털 뱅킹과 디지털 결제를 이용하여 금융포용을 가속시킵니다. 또한 보건 영역에서는 아동 면역 현황을 추적하고 교통 영역에서는 운전면허증 발급을 처리합니다. 더불어 월경 내역 추적과 여권 발급을 지원함으로써 출입국관리 영역을 지원합니다. 또한 유권자 인증서를 발급함으로써 선거 부정을 방지할 수 있습니다. IDHub 는 신원 기능 시스템으로서 그림 2 에서 볼 수 있듯이 안전망과 금융 부문만을 지원합니다.



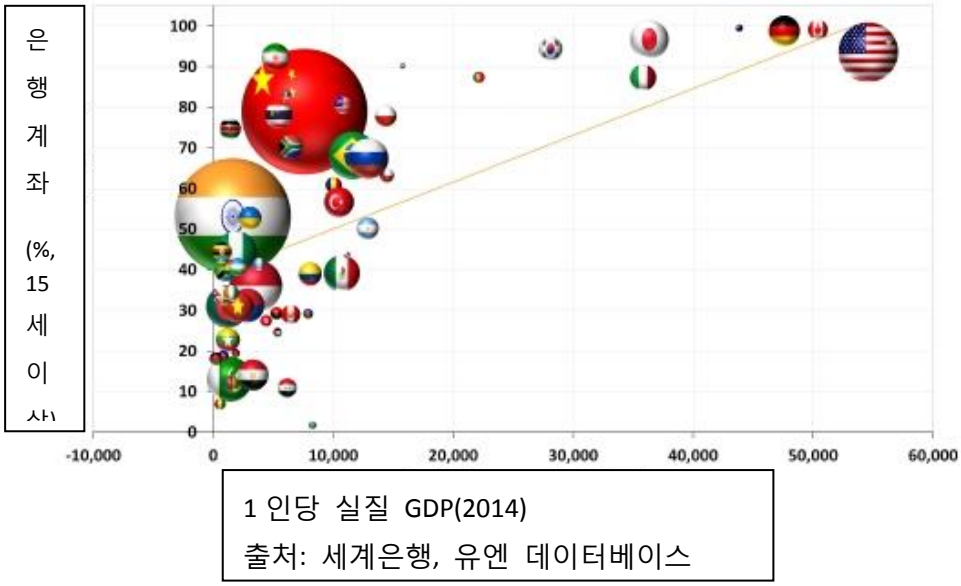


그림 1: 1 인당 GDP 대비 은행 계좌 보유 비율

2.2 관련국가

2.2.1 중국

중국, 광동 포샨시 창천 지방 정부는 2017 년 6 월 지능형 다기능 신원(IMI, Intelligent Multifunctional Identity)[4]시스템을 발표했습니다. IMI 는 블록체인과 실명 인증을 기반으로 온라인 상에서 거주자 신원을 파악하는 시스템입니다. IMI 시스템이 주장하는 세가지 특징은 검증된 정보, 신뢰할 수 있는 정보 출처, 정보 공개 최소화입니다. IMI 시스템 상의 모든 신원 속성들은 정부나 기타 신뢰할 수 있는 정보 출처가 보증하기 때문에 그 진위가 검증됩니다. 여러 다른 정보 출처들이 제공하는 인증들이 신원을 구성합니다. 사용자에 대해 신분 인증은 정부가 제공하고, 소득 인증은 회사가 제공하며, 진료기록에 대한 인증은 병원이 제공합니다. 정보 공개 최소화 원칙이란 공개할 정보의 범위를 최소화하고 정보를 그대로 공개하는 것이 아니라 대략적으로 공개하는 것입니다. 예를 들어 대출 신청 시 신청자가 자신의 소득 금액을 정확히 밝히는 대신 범위 형태로 공개합니다. 창천 지역 거주자 중 IMI 시스템 인증을 받은 사람들은 정부 서비스 접근 권한을 받게됩니다. 또한 IMI 시스템은 개인키와 공개키 쌍을 이용하기 때문에 사용자들이 서비스 센터까지 와서 직접 신원 정보를 제출할 필요 없이 사용자들의 신원을 자동으로 검증할 수 있습니다.

2.2.2 에스토니아

에스토니아는 2014 년 12 월 1 일 e-Residency 프로그램을 출범했습니다. 전세계 누구라도 e-Residency 를 신청하여 유럽연합에서 사업을 할 수 있고 공공 서비스를 이용할 수 있습니다. E-Residency 는 기업 등록, 문서결재, 암호화된 문서의 교환, 온라인뱅킹,

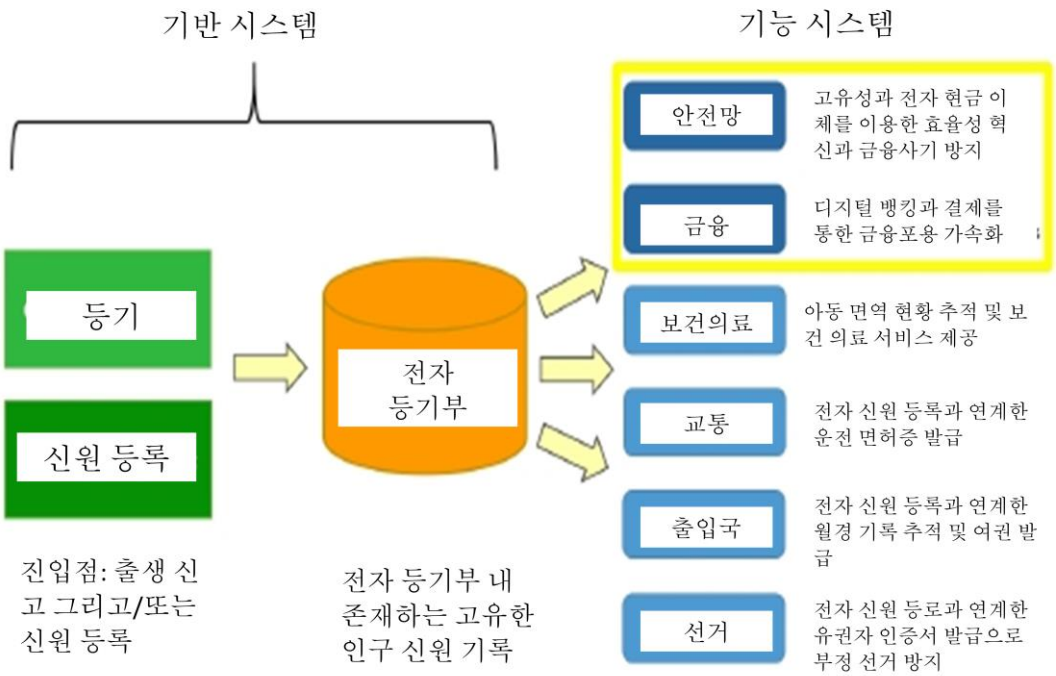


그림 2: 신원 기반 시스템과 신원 기능 시스템.

세금 신고, 처방전 처리를 지원합니다. E-Residency 등록자들은 에스토니아가 아니라 자신들의 본국에서 세금을 납부하고 해당 국가가 그들에게 공급 서비스를 제공합니다. 또한 E-Residency 등록자들의 금융 기록은 디지털 형태로 투명하게 모니터링 됩니다. E-Residency 시스템에 등록했다고 해서 에스토니아 거주권이 주어지는 것은 아닙니다. e-Residency 프로그램 이외에 에스토니아는 E-Residency 등록자들에게 통화를 제공하는 방안을 검토하고 있습니다.

2.2.3 말라위

아프리카 남동부에 위치한 말라위는 내전을 겪고있지 않은 몇 안되는 아프리카 국가들 중 하나입니다. 유엔 기준 최대 미개발국 중 하나인 말라위의 경우 국민들 중 55%가 빈곤층에 속합니다. 말라위는 농산물 수출에 크게 의존하고있기 때문에 말라위 경제는국제 농산물 가격의 불안정성에 매우 민감합니다. 2016 년까지 말라위에 국가 차원의 신원 관리 시스템이 없었기 때문에 디지털 신원을 도입하는 것이 적절합니다.

2.2.4 뉴질랜드

2013 년 출범한 RealMe [5] 시스템은 뉴질랜드가 추진하는 신원 확인 서비스입니다. RealMe 시스템을 통해 뉴질랜드 시민들은 하나의 계정으로 신원과 기타 다른 온라인 서비스 접근이 가능합니다. RealMe 는 두가지 주요한 기능을 갖고있는데 그 첫번째는 한번만 로그인하여 여러 온라인 서비스를 이용할 수 있도록 하는 싱글 로그인 기능입니다. RealMe 계정은 일단 확인이 되면 온라인 신원 기능도 함께합니다. 두번째 대표 기능은 개인정보 관리와 개인정보 도난 방지입니다. RealMe 는 문지기 역할을 하며 사용자들이 공유하는 정보를 저장하지 않습니다. 정보 공개는 최소화한 상태에서 제 3 자가 사용자의 신원을 파악한 후 서비스를 제공합니다. [6]

2.2.5 스위스

Crypto Valley 로 알려져있는 스위스의 도시 저그는 암호화폐 사업을 지원합니다. 저그는 이더리움 기반의 디지털 신원 서비스를 출범시켰는데 이 서비스를 통해 거주자들은 디지털 서명을 사용할 수 있습니다. 저그 시는 2018 년 봄 전자 투표 시스템 구현을 계획하고 있습니다.

2.3 관련기구

2.3.1 ID2020

ID2020 [7]은디지털 신원을 통해 삶을 개선하고자 결성된 연맹입니다. 이들이 제안하고 있는 네 가지 범주는 다음과 같습니다. 개별성, 영속성, 휴대성, 기밀성. “개별성”이란 특정 사용자에만 해당되는 고유한 것을 의미합니다. “영속성”은 태어나서 사망할 때까지 지속됨을 의미합니다. “휴대성”은 어디에서든 접근 가능함을 의미합니다. “기밀성”은 사용자만이 자신의 데이터를 사용하거나 볼 수 있도록 허용할 수 있음을 의미합니다.

2.3.2 탈중앙화 신원 재단(Decentralized Identity Foundation)

5 월 22 일 개최된 Consensus 2017 에서 Microsoft, uPort, Gem, Evernym, Block-stack, Tierion 에서 참석한 패널들은 탈중앙화 신원 재단(DIF, Decentralized Identity Foundation)결성을 선언했습니다. DIF [8]의 미션은 사람, 기관, 어플리케이션, 장비들이 사용할 수 있는 오픈소스 탈중앙화 신원 생태계를 구축하는 것입니다. DIF 는 어디에서나 발견할 수 있는 제로 트러스트 데이터 저장소에 연결되어있는 블록체인 신원들에 의해 지탱되고 있는 분산된 신원들을 이와 같은 새로운 생태계를 떠받치는 기둥으로 보고 있습니다.

IDHub 는 ID2020 와 DIF 에 참여하여 이들 단체와 공조하여 신원 관련 문제 해결에

동참할 계획입니다. DIF 산하 네 개 실무 그룹들 중 우리가 가장 큰 관심을 두고있는 그룹은“Storage & Compute” and “Attestations & Reputation”입니다.

2.4 신원 시스템

신원 시스템의 디자인 원칙은 자주성, 보안, 개인 정보 보호입니다. 현행 신원 시스템들은 서로 분리되어 있는 형태로서 각 시스템들이 신원 속성들 중 일부를 보유하는 형태입니다. 사용자들의 신원 정보가 쪼개져 있는 것입니다. 웹사이트 별로 다른 아이디와 암호를 사용해야 하는 것은 성가시고 불필요한 과정입니다. 사용자들은 자신의 신원정보에 대한 통제권과 소유권을 상실하고 그들의 개인정보는 돈을 받고 팔립니다. 여기에서 신원 시스템의 첫번째 디자인 원칙인 자주성이 대두됩니다. 신원 시스템은 통제권을 사용자들에게 돌려주어 이들이 자신들의 신원 정보를 수정 및 갱신하고 말끔하게 종합할 수 있도록 해야합니다. 사용자들은 원할 경우 자신들의 계정을 삭제할 수 있어야 합니다. 즉 사용자들이 잊혀질 권리를 갖는다는 것입니다. 보안은 또 다른 중요한 원칙입니다. Aadhaar 와 같은 중앙 집중식 신원 시스템들에서 사용자 데이터가 유출됐다는 사실이 알려진 바 있습니다. 중앙 집중식 신원 시스템들은 저장되어 있는 데이터의 가치가 높고 서버의 수가 한정되어있기 때문에 해커가 아주 좋아하는 먹잇감입니다. 중앙 집중식 아키텍처는 또한 랜섬웨어 공격에 취약합니다. 블록체인 기반의 신원 시스템이 갖는 탈중앙화는 공격 비용을 높이고 시스템 보안성과 견고성을 제공합니다. 끝으로 개인정보 보호는 사용자들이 갖는 가장 핵심적인 관심 사항입니다. 블록체인 기술은 아직 유아기 단계에 머물러있고 개인정보 보호 등의 측면이 아직은 약한 것으로 알려져있습니다. 블록체인은 보안 제공에 필요한 기본 바탕입니다. 하지만 개인정보 보호를 위해서는 다른 모듈들도 필요합니다. IDHub 의 기본 개념은 블록체인, 암호화 라이브러리, 분산 저장을 활용하여 신원 시스템의 세가지 디자인 원칙을 구현하는 것입니다.

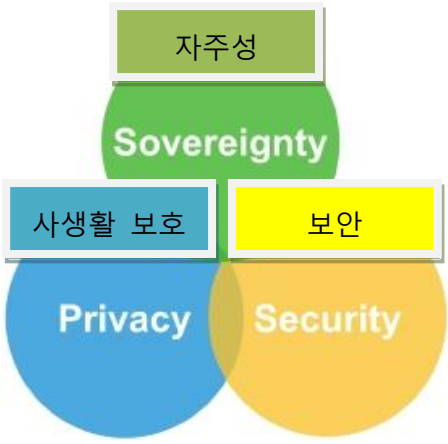


그림 3:신원 시스템의 디자인 원칙

3. 아키텍처

블록체인의 탈중앙화를 기반으로 하는 IDHub 는 디지털 신원 어플리케이션 플랫폼으로서 신원을 하나의 서비스로서(IDaaS) 제공하는 것을 목표로 합니다. 사용자 한 명 당 사용 계정 수는 증가하지만 개인 정보는 사용자 자신이 아닌 서비스 공급자가 통제하고 보유합니다. 신원과 어플리케이션을 분리하는 것이 디지털 사회에서 분명한 추세입니다. IDHub 는 휴대형 신원 관리 메커니즘을 구축함으로써 이와같은 분리를 구현하며 이와 같은 메커니즘은 서비스 공급자들 간 장벽을 낮추고 서비스 공급자들 간 전환 시 발생 비용을 낮춥니다. IDHub 는 신원을 디지털 자산으로 간주합니다. 신원 정보 제공 요청의 신뢰성을 높이기 위해 IDHub 는 외부 인증을 신원 보증 장치로서 포함시키고 검증 가능하며 신뢰할 수 있는 디지털 자산 생태계를 구축합니다. IDHub 는 서비스 공급자들 간 데이터 일치 작업이나 데이터 이전 작업 시 중추적 역할을 합니다. 특히 상호 신뢰가 존재하지 않을 경우 더욱 그러합니다. 또한 IDHub 는 자치 정부와 거주자들이 지속 가능하고 확장성을 갖춘 신원 시스템을 구축할 수 있도록 합니다.

IDHub 신원과 연계되어 있는 속성들을 신원주장(claim)이라 합니다. 이 용어는 신원 정보를 필요로 하는 모든 시스템으로 부터 독립적으로 사용자가 디지털 신원을 밝히는 방법인 '주장 기반 신원'에 그 연원을 두고있습니다. IDHub 신원 관리의 1 차 목표는 신원 보유자가 자신의 개인 정보, 인증 정보, 보상 정보, 등급 정보에 대한 자신의 신원 주장과 증명을 쉽게 할 수 있도록 하는 것입니다. 신원주장 관리가 IDHub 아키텍처의 중심을 차지하고 있습니다. 아키텍처가 검증 가능한 신원 주장을 지원하기 위해서는 반드시 핵심 행위 주체들의 필수 역할을 구분할 수 있어야 하고 이들 간의 관계, 즉 이들이 어떻게 상호 작용하는지를 구분할 수 있어야 합니다. 역할은 개념으로서 여러 다른 방법으로 구현될 수 있습니다. 역할을 분리한다는 것은 표준화를 위해 적절한 인터페이스나 프로토콜을 제안하는 것입니다. IDHub 아키텍처에 있는 역할들은 다음과 같습니다. 보유자는 인증자로부터 인증을 획득하고 이를 선택적으로 검사자에게 제공합니다. 인증자는 보유자에게 인증을 발급합니다. 검사자는 인증 정보에 대한 검증을 위해 보유자로부터 인증 정보 제공을 요청합니다. 식별자 등록소가 전세계적으로 고유한 식별자의 생성과 검증을 중재합니다. 식별자 등록소는 반드시 식별자들을 자주적인 방식으로 관리해야 합니다. 저장소가 보유자들을 대신하여 인증 정보를 저장하고 관리합니다. 검증자가 검사자를 대신해 인증 정보를 검증합니다. 예를들어 검사자는 특정 산업에 적용되는 비즈니스 규칙을 인증에 적용함으로써 보다 깊이있는 검증을 할 수 있도록 할 수 있습니다.

신원 관련 주요 행위로는 등록, 주장, 승인이있습니다. 사용자는 스마트 계약을 통해

신원을 등록하고 신원과 개인키를 연결합니다. 신원 복구가 필요할 경우 권한 위임을 설정합니다. 사용자 데이터의 값과 정합성은 신뢰할 수 있는 인증 발급자들이 제공하는 인증에 의해 보증됩니다. 신뢰할 수 있는 개인이나 기관이 자신들의 개인키로 신원 주장에 서명을 하고 검사자가 이들 서명자들의 공공키로 신원주장을 검증합니다. 제 3 자가 데이터를 요청할 경우 승인 모듈이 이를 사용자에게 통보합니다. 사용자가 승인하면 승인된 범위 내의 데이터가 제 3 자에게 전송됩니다.

IDHub 의 인프라는 블록체인 구성 노드들에 기반한 P2P 네트워크입니다. 유틸리티 레이어는 식별자 등록소, 신원 주장 정의, 증명 검증 등과 같은 공통 기능 콤포넌트들로 구성되어 있습니다. 이와 같은 인프라 위에 네가지 모듈이 구축되어 있는데 그것은 신원관리, 신원검증, dApp 인터페이스, 디지털 자산입니다. 사용자들은 등록, 속성 수정, 다른 사용자들과 연결, 복구를 통해 자신의 신원을 관리합니다.

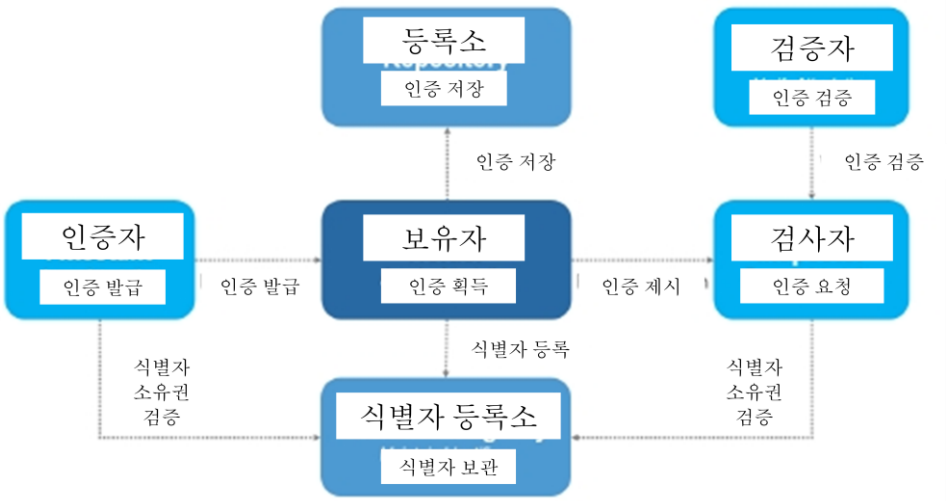


그림 4:역할: 보유자, 인증자, 검사자, 검증자

신원 검증 서비스에는 OAuth 와 디지털 서명이 포함되어 있습니다. 계약 서버가 블록체인 상에서 공공 데이터와 활동 로그를 가져옵니다. DApp 인터페이스 서비스는 dApp 과 블록체인 간 상호 작용을 지원합니다. 디지털 자산 서비스가 사용자 신원의 현재값을 검증하고 거래 역량을 제공합니다. 이들 서비스들을 이용하여 금융, 교육, 보건, 상거래, 여행 부분을 지원하는 솔루션들이 개발되고 있습니다.

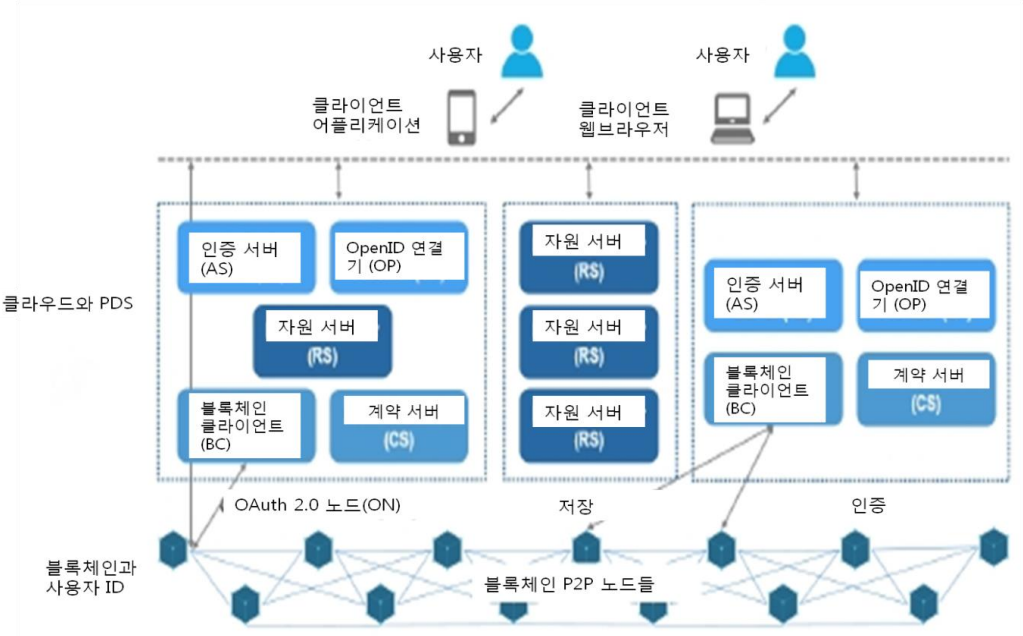


그림 5: IDHub 아키텍처

3.1 신원주장

신원주장이란 사용자가 직접 할당한 한 덩어리의 속성들입니다. 신원 속성들은 가능한 schema.org 의 포맷을 따라야 합니다. 이 포맷에 열거되어 있는 속성들로는 식별자, 사진, 성, 이름, 이메일, 주소, 전화번호, 생일, 출생지, 순자산, 직책, 신장, 체중 등이 있습니다[9]. 스스로 선언한 신원주장의 정확성에 대해서는 이의 제기가 있을 수 있습니다. 신원주장은 인증 기관이 그 정확성을 보증할 때, 즉 인증서가 발급되고 이것이 신원주장에 첨부될 때 가치를 갖게 됩니다.

3.2 인증

신원주장의 유효성은 인증에 의해 보증되는데 이 인증은 JSONWeb Token (JWT)의 포맷으로 되어 있습니다 [10]. JWT 는 공개 표준(RFC 7519)으로서 거래 당사자들 간에 정보를 JSON 객체 형태로 안전하게 전송하는 소형의 독립된 방식을 정의한 것입니다. 이와 같은 정보는 전자서명이 이뤄지기 때문에 검증할 수 있고 신뢰할 수 있습니다. JWT 의 구조는 헤더, 페이로드, 서명의 세부분으로 되어 있고 이들은 점으로 분리됩니다. 헤더는 토큰 형태인 JWT 로 이뤄져 있으며 ES256k 나 RSA 등과 같은 해시 알고리듬이 사용됩니다. 페이로드에 신원주장이 들어있습니다. 신원주장은 객체에 대한 설명 정보와 추가 메타 데이터로 이뤄져있습니다. 독점적으로 사용되는 신원주장 정보로는 발행자, 만기 시점, 대상자, 청중 등이 있습니다. 암호화된 헤더와 암호화된 페이로드를 개인키로 서명하고 헤더에 있는 특정한 알고리듬을 통해서 서명이 생성됩니다. 서명은 JWT 발행자를 검증하고 메세지가 전송되는 동안 변질되지 않도록 하는데 사용됩니다.

3.3 인증 관리

신원 속성들에 대한 인증은 매우 가치가 크고 민감합니다. 만족스러운 인증 관리 시스템이라면 정보 공개 최소화 원칙을 충족시킬 수 있어야 합니다. 이 원칙에 따르면 신원 시스템은 거래를 위해 거래 주체가 공개해야 하는 정보를 최소화할 수 있도록 해야 하며 그 이상의 정보 공개는 이뤄지지 않도록 해야합니다. 이 원칙을 따라야하는 이유는 개인의 사생활 정보를 보호해야 하고 정보 공개에 따른 발생 가능한 부작용을 경감시킬 수 있어야 하기 때문입니다. Merkle 트리도 본질적으로 정보 공개 최소화 원칙을 충족합니다. Merkle 트리의 모든 잎노드에는 데이터 블록이 붙어있고 잎노드가 아닌 모든 노드에는 자식 노드 라벨의 암호화된 해시값이 붙어있습니다. Merkle 트리는 커다란 데이터 구조를 가진 내용을 안전하고 효과적으로 검증할 수 있도록 합니다. 특정한 해시값을 제공함으로써, 즉 필요한 정보만 공개되도록함으로써 정보 최소 공개 원칙이 지켜집니다.

3.4 승인

승인은 제 3 자가 사용자 데이터를 요청할 경우 등장하는 개념입니다. 사용자가 승인하면 사용자가 지정한 범위 내의 데이터가 제공됩니다. IDHub 의 승인 과정에 OAuth 2.0 가 실행됩니다. OAuth 2.0 승인 프레임 워크[11]는 리소스 소유자와 HTTP

서비스간에 이뤄지는 승인을 위한 상호작용을 조율함으로써 제 3 자가 리로스 소유자를 대신하여 HTTP 서비스에 제한적으로 접근할 수 있도록 합니다. OAuth 2.0 는 리소스 소유자가 제 3 자에게 암호를 알려주지않은 상태에서 제 3 자가 리소스 소유자를 대신하여 서버 리소스에 접근할 수 있도록 합니다.

3.5 신원 그래프

신원 그래프란 신원들 간에 발생하는 활동들을 표시한 것입니다. 신원 그래프 상에서는 노드가 신원을 나타내고 에지가 활동을 나타냅니다. 활동에는 친구추가, 보증, 코멘트가 포함됩니다. 블록 체인 상에서 활동을 거래로 전환시킴으로써 거래 기록에 따라 신원의 평판이 계산됩니다. 신원 그래프 상에서 데이터 흐름을 처리하는 데는 플로우 기반 프로그램[12]이 적합합니다. 왜냐하면 플로우 기반 프로그램은 어플리케이션을 데이터 덩어리의 흐름을 통해 정보를 주고받는 비동기식 프로세스로 이뤄진 네트워크로 보기 때문입니다. 이 네트워크의 핵심 목표는 어플리케이션 데이터를 변경시켜 원하는 결과를 만 들어내는 데 있습니다. 네트워크는 프로세스에 대해 외부적으로 정의됩니다.

IDHub 시스템에서 신원은 트리와 그래프로 표시됩니다. 신원주장과 신원 인증은 Merkle 트리에 저장되고 다른 신원들과의 상호 작용 정보는 신원 그래프로 저장됩니다.

3.6 사생활 정보 보호

우리는 사생활 정보 보호를 IDHub 디자인의 중심에 두고있습니다. 신원 시스템은 사생활 정보 보호를 최우선 순위로 삼아야 사용자들의 신뢰를 얻을 수 있습니다. 8 가지 사생활 정보 보호를 위한 설계 전략들은 크게 다음 두 가지로 묶을 수 있습니다: 데이터 중심 전략, 프로세스 중심전략 [13]. 데이터 중심 전략에는 MINIMISE, HIDE, SEPARATE, AGGREGATE 가 포함됩니다. 처리 대상 개인 데이터의 양은 가능한 최소로 제한해야 합니다. 모든 개인 데이터와 이 데이터들 간 관계는 그냥 봐서는 보이지 않게 숨겨지도록 해야 합니다. 개인 데이터는 가능한 분산해서 처리해야 합니다. 개인 데이터는 데이터 종합도는 최대 수준으로 하면서 상세화 정도는 효용성을 해치지 않는 수준에서 최대한 낮게 해야합니다. 프로세스

중심 전략에는 INFORM, CONTROL, ENFORCE, DEMONSTRATE 이 포함됩니다. 개인 데이터를 처리할 때는 항상 데이터 소유 주체들에게 적절한 통보가 이뤄지도록 해야합니다. 데이터 주체들의 개인 데이터가 처리될 때는 데이터 주체들이 위임권을 주도록해야 합니다. 법적 요건을 충족하는 사생활 정보 보호 정책이 마련되고 시행되어야 합니다. 사생활 정보 보호 방침 및 기타 모든 관련 법적 요건들을 충족한다는 점을 입증할 수 있어야 합니다. 그림 6 은 8 가지 사생활 정보 보호 디자인 전략을 나타낸 것입니다.

이들 전략이 실행되기 위해서는 데이터 수집을 최소화 해야합니다. 모든 데이터 요청에 대해 사용자가 승인을 하도록 해야합니다. 제공되는 데이터는 정확한 데이터 형태가 아닌 범위 형태로 대략적으로 제공되도록 해야합니다. 사용자들의 경우 자신들의 데이터를 클라우드에 저장할 것을 권장합니다.

3.7 보안

IDHub 는 데이터 색인을 블록체인에 저장하고 데이터값은 Kademlia 등과 같은 분산 저장 시스템에 저장합니다[14]. 블록체인은 투명성과 불역성으로 잘 알려져있습니다. 블록체인 상의 데이터는 이들 데이터를 변경하려는 자들이 해당 블록체인 상의 컴퓨팅 파워의 대다수를 지배하지 않는 한 절대 변경할 수 없고, 특정인이 블록체인 상의 컴퓨팅 파워의 대다수를 지배하는 것은 불가능합니다. Kademlia 는 P2P 분산 해시 테이블로서 이 테이블에서는 해쉬키들 간의 거리를 비트간 배타적 논리합(XOR)으로 정의합니다.

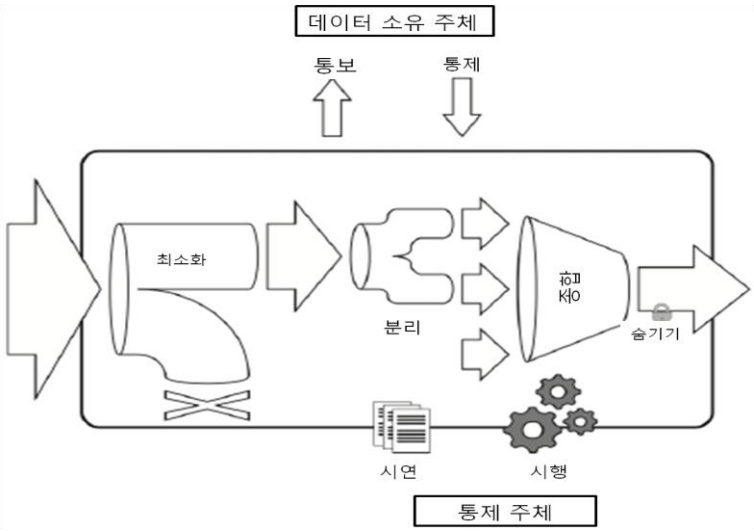


그림 6:사생활 정보 보호를 위한 8 가지 디자인 전략.

Kademlia 는 비트 간 배타적 논리합 기반의 거리 위상이라는 새로운 기법을 사용하기 때문에 증명 가능한 일관성, 성능, 지연 최소화 라우팅, 무지연 장애복구, 대칭 단방향 거리 위상 등과 같은 뛰어난 기능을 갖추고있습니다. Kademlia 는 병렬 비동기 쿼리를 사용하여 장애발생 노드로 인한 타임아웃 지연을 피할 수 있습니다. 노드들이 서로 서로의 존재를 기록하는 알고리즘이 특정한 기초적인 디도스 공격에 저항할 수 있도록 설계되어 있습니다. IDHub 는 분산 저장 시스템을 사용하기 때문에 중앙 집중식 신원 시스템보다 더 안전하고 견고합니다. 여기에 더해 저장 전에 암호화를 하기 때문에 보안은 더욱 강화됩니다. 가장 이상적인 암호화 툴로는 NaCl 을 꼽을 수 있습니다 [15] [16]. NaCl ("설트"라읽음)은 네트워크 통신, 암호화, 복호화, 서명을 지원하는 고속 라이브러리입니다.

3.8 고유성

고유성은 복지 수당 지급을 위한 신원 확인과 허위 직원을 제거하는 데 있어서 핵심적인 역할을 합니다. 신원이 고유하면 사회 복지 수당의 중복 수급을 방지할 수 있습니다. 나이지리아는 공무원을 위한 디지털 신원 시스템을 구축하여 허위 근로자를 제거함으로써 연간 7,760 만 달러를 절약했습니다 [17]. 생체 인식이란 신체 특징이나 행동 특징을 기반으로 개인의 신원을 파악하는 것을 말합니다. 즉 안면, 안면열상, 지문, 장문, 홍채, 망막패턴, 서명, 음성 등과 같은 생체 정보를 검증하고 비교합니다[18]. 사용에 가장 바람직한 생체 정보는 지문과 홍채로서 Aadhaar 시스템은

이들 정보를 통해 사용자를 판별합니다. 이외에 안면열상도 유망해 보입니다. 열이 안면 피부를 통과하고 얼굴 피부에서 발산될 때 얼굴 피부 아래에 있는 혈관들이 사람마다 고유한 모양을 만들어냅니다 [19]. 이러한 고유한 패턴을 적외선 카메라로 촬영한 것이 안면열상입니다. 안면열상은 사람마다 고유하기 때문에 위변조에 취약하지않다. 성형수술을 했더라도 정맥내 혈액의 흐름이 바뀌지는 않기 때문에 안면열상에는 영향을 미치지 않습니다. 지문을 QR 코드로 전환시키는 데는 다음 두 단계를 걸칩니다[20]: 지문의 중심점 추출, 지문의 특징 추출, 이러한 특징들을 수치값으로 전환, 이렇게 전환된 수치로 QR 코드 생성. 지문 중심점을 찾는 가장 일반적인 방법은 Poincar´e 색인 방법입니다. 지문의 융선 문양에서 발견되는 불연속점이 지문들을 서로 비교하는 데 주로 사용됩니다. 불연속점에는 두 종류가 있는데 하나는 융선 말단이고 다른 하나는 분기점입니다. 이들을 선택하여 특징을 추출합니다

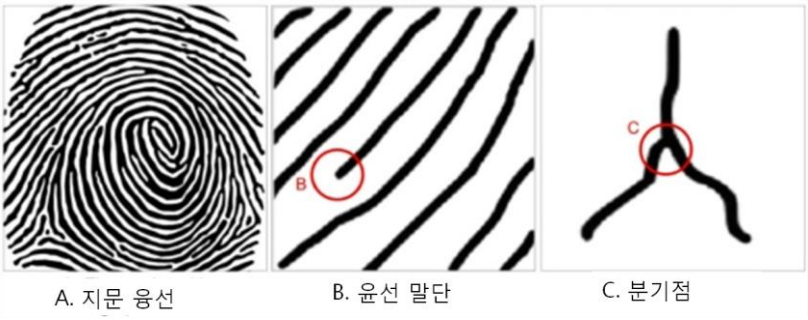


그림 7:지문 융선과 불연속점.

IDHub 는 두 가지 생체 정보, 즉 지문과 홍채를 이용하여 신원의 고유성을 구현합니다. 안면열상의 경우 비용이 감당할 수 있는 수준이 된다고 판단될 때 사용을 고려할 예정입니다.

3.9 휴대성

사용자의 신원 정보가 여러 웹사이트에 흩어져 있다는 점이 큰 불편을 유발합니다. 매일 웹사이트에 접속할 때마다 로그인을 반복해서 해야하는 것은 불편하고 불필요한 작업니다. 더 심각한 것은 웹사이트마다 사용하는 신원 속성의 포맷이 서로 호완되지 않아서 공유해서 사용할 수가 없다는 것입니다. 신원 자주성이란 사용자가 자신들의 신원정보를 완전히 통제함을 뜻합니다. 자주성을 나타내는 한가지 척도로 사용자가

여러 웹사이트들 간의 전환을 얼마나 매끄럽게 할 수 있는가를 평가할 수 있습니다. IDHub 는 소셜 네트워크들로부터 신원 속성들을 가져온 다음 이것을 디아스포라(Diaspora)와 동기화시킴으로써 신원정보를 사용자가 휴대할 수 있도록, 즉 어떤 웹사이트로 가든 함께 가져갈 수 있도록 합니다[21]. 디아스포라(Diaspora)란 사생활 정보를 인식하고, 사용자가 소유하고 있는 분산형 오픈 소셜 네트워크입니다. 소셜 네트워크들은 사용자들 간의 상호작용들을 분석하여 그 결과를 광고에 사용함으로써 수익을 얻습니다. 디아스포라는 사용자가 다른 사용자와 연결하고 다른 사용자와 공유하도록 하는 것 이외에는 다른 어떤 용도로도 사용자 데이터를 사용하지 않습니다.

4. 경쟁 환경

4.1 Aadhaar

인도에는 정부가 빈곤층에 지급하는 생활 보조금을 부패 공무원들이 빼돌리는 문제가 있습니다. 이 문제를 해결하기 위해 보조금 지급 시 수급자의 신원을 먼저 확인하여 보조금을 이들에게 직접 송금할 수 있도록 합니다. Aadhaar[22] 번호는 인도 거주민들에게 발급되는 12 자리의 고유한 신원 확인 번호입니다. Aadhaar 번호는 고유하기 때문에 수취인의 계좌로 송금 시 사용할 수 있는 금융 주소 역할을 합니다. Aadhaar 번호를 금융 주소로 사용하기 때문에 개인에 대한 재정 지원 혜택을 빠짐없이 추적할 수 있습니다. 정부가 특정 Aadhaar 번호로 보조금을 송금하고 해당 Aadhaar 번호를 가진 수급자가 해당 보조금을 소형 현금 인출기에서 인출합니다. Aadhaar 는 경제적으로 취약하고 주변부에 있는 사람들이 이와같이 중개 기관을 거치지 않고 공공 서비스와 재정 지원 혜택을 누릴 수 있도록 합니다. 지금까지 발급된 Aadhaar 번호는 11 억 7 천개에 이른다. Aadhaar 는 데이터 중복 제거에 전력하고 있습니다. Aadhaar 는 사진, 열손가락 지문, 양안 망막 스캔 등과 같은 생체정보를 수집하여 거주자들을 분별하는 데 사용합니다. Aadhaar 는 거주자 정보를 MySQL 데이터베이스에 저장합니다.

4.2 Civic

Civic [23]은 신원 검증 업계의 비용을 낮출 수 있는 방법을 제시하고 있습니다. 신원 검증 서비스를 연구해온 기관들은 자신들이 소유하고 있는 프로세스들을 화폐로 정할

수 있습니다. 분산 데이터 모델과 인증 모델 그리고 토큰을 기반으로 구축된 Civic 은 참가자들에게 보상을 제공하고 사용자들이 자신들의 데이터를 완전히 통제할 수 있도록 신원 검증 서비스 공급자들이 인증 정보를 공유하도록 하는 플랫폼을 제공할 것입니다. Civic 은 암호와와 생체 정보를 통한 잠금 방식을 사용하여 사용자의 전화에 사용자의 데이터를 저장합니다. 사용자 데이터에 대한 검증 절차는 Civic 이 수행합니다. Civic 은 검증이 완료된 데이터 인증 정보를 블록체인에 기록합니다. Civic 의 신원 파트너들은 맞춤 QR 코드를 통해 사용자의 데이터를 요청할 수 있고, 해당 QR 코드를 사용자가 스캔합니다. 사용자가 이러한 코드들을 스캔하고 요청받은 데이터를 검토한 후 해당 데이터 요청을 승인할지 거부할지를 결정합니다.

4.3 GSMA Mobile Connect

Mobile Connect [24]은 이동통신 사업자들로 구성된 협회인 GSMA 가 제안하는 보안 범용 로그인 솔루션입니다. Mobile Connect 은 사용자와 이들의 이동전화를 비교 검증하여 해당 사용자들이 웹사이트에 로그인할 수 있도록 합니다. Mobile Connece 의 로그인 메커니즘은 OpenID Connect 를 기반으로 합니다. Mobile Connect 은 완전한 신원 시스템이라기 보다는 주로 써드파티 로그인 모듈입니다.

4.4 Sovrin

Sovrin [25]은 분산 신원 네트워크입니다. 이 네트워크에서는 사람들과 기관들이 휴대 가능하고 자주성을 갖춘 디지털 신원들을 생성할 수 있도록 하며 이렇게 생성된 디지털 신원은 그 소유자들이 통제합니다. Sovrin 신원 네트워크(SIDN)는 전세계에 퍼져있는 다중 분산 노드들로 구성되어 있습니다. 각 노드들이 원장의 사본을 갖고있는 상태에서 노드들에 대한 호스팅과 관리는 스튜어드가 수행합니다. 신원 속성들에 대한 요청이 이뤄지고 해당 요청에 승인이 이뤄지면 요청자가 인증자의 디지털 서명으로 요청된 정보의 정확성을 검증할 수 있습니다. 분산 관리를 통해 Sovrin 은 신원 속성들의 정확성과 보안을 보장하고 신원 위조를 방지할 수 있습니다. Sovrin 은 시스템 장애에 대해 견고하고, 해킹 공격에 대해 회복력이 높으며, 공격자들의 파괴 시도에 면역력을 갖춘 신뢰할 수 있는 네트워크로 자기 자신을

만들어가고 있습니다. Sovrin 의 단점은 무엇인가를 신뢰할 것인지 아닌지를 결정하는 책임을 맡고있는 사람들에 의존하고 있다는 것입니다. Sovrin 은 오픈 소스 공개 신원 네트워크이기 때문에 네트워크 상의 신원 정보가 권위있는 신뢰성을 갖추고 있지 못합니다. Sovrin 네트워크가 얼마나 잘 작동하는지는 사용자 경험과 사람들이 본인들이 받은 요청 사항을 이해할 수 있는지 여부에 따라 달라집니다. [26] IDHub 가 제안하는 솔루션은 정부와 은행 등과 같이 권위있는 실제 세계의 인증 제공자들과 협업하자는 것입니다. 이러한 권위있는 기관들로 인해 시스템의 신뢰성을 상당히 신장시킬 수 있을 것입니다.

4.5 uPort

uPort [27]는 이더리움 기반의 스마트 계약 시스템입니다. uPort 기술은 다음 세가지 주요 부분으로 구성되어 있습니다; 스마트 계약, 개발자 라이브러리, 모바일 앱. 모바일 앱에 사용자 키가 저장됩니다. 스마트 계약들이 신원의 핵심을 이루고 있으며 여기에 모바일 장비를 분실했을 때 신원 정보를 복구할 수 있도록 하는 로직이 담겨있습니다. 개발자 라이브러리는 개발자들이 uPort 를 앱과 통합시키는 데 필요합니다. uPort 신원의 핵심 기능은 신원 주장이나 활동 또는 거래에 대해 디지털로 서명하고 검증하는 것입니다. 신원들은 사진이나 친구 추가 등과 같이 파일을 직접 업데이트할 수 있고 다른 사람들에게 특정 파일을 쓰거나 읽을 수 있는 임시 허가를 부여할 수 있습니다. uPort 신원은 블록체인과 상호 작용이 가능하기 때문에 암호화폐나 기타 토큰화 자산 등과 같은 디지털 무기명 자산들도 통제할 수 있습니다.

5. 생태계

5.1 IDH 토큰

IDHub 토큰 (IDH)의 주된 사용처는 사용자의 신원을 입증하고, 인증자들이 인증을 제공하도록 인센티브를 제공하며, 신원 속성 저장소를 할당하는 것입니다. IDH 의 최대 공급량은 5 억개로서 이들 중 44%는 퍼블릭 세일 참가자들에게 제공되고 16%는 프리 세일 참가자들에게 제공됩니다. 창업팀이 20%를 받게 되고 4 년간 소유권을 유지하게 됩니다. 10%는 IDHub 재단 펀드에 제공되어 연구개발, 행정, 커뮤니티 운영, 시장진출, 법률자문 용으로 사용됩니다. 초창기 후원자들은 10%의 지분을 갖습니다.

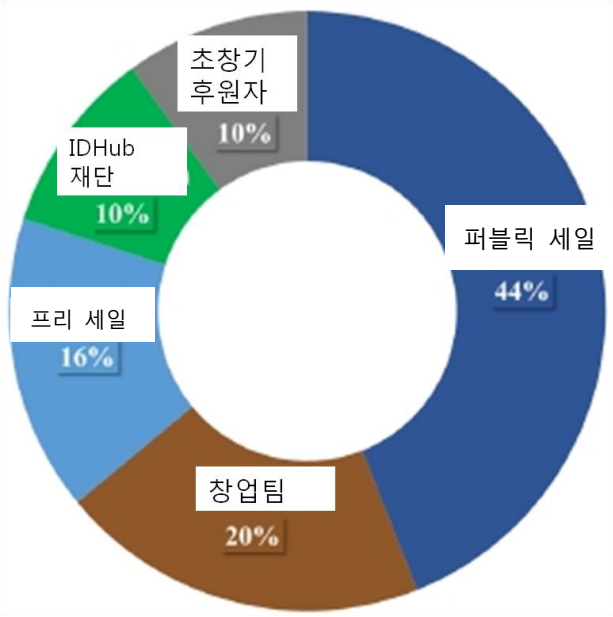


그림 8: IDH 토큰 배분

5.2 인증

IDH 토큰은 가치 공급자들에게 흘러갑니다. 보유자란 자신들이 보유한 속성들에 대해 신원 주장을 하는 자들을 말합니다. 신원주장은 제 3 자가 보증할 때 신뢰성과 가치를 갖습니다. 인증자가 신원주장을 검증하고 인증을 발급하고 이에 대해 보유자가 인증자에게 IDH 로 보상합니다. 검사자는 보유자에게 보증을 받은 신원 주장을 제공해줄 것을 요청하고 그 댓가로 IDH 를 지급합니다. 검사자는 본인이 직접 인증을 검증하거나 검증자에게 대가를 지불하고 인증의 유효성을 검증해줄 것을 요청합니다. IDH 토큰은

검사자로부터 보유자로 그리고 인증자로 흘러갑니다. IDHub 는 인증자들에게 인센티브를 제공하는데 왜냐하면 인증자들이 IDHub 생태계의 신뢰도와 가치를 높이기 때문입니다.

5.3 대출

평판은 신원을 구성하는 속성들 중 결정적인 속성입니다. 평판이 좋거나 신용 점수가 높은 사람은 대출 신청 시 낮은 금리를 적용받습니다. 신용도를 정확히 판단하기 위해서는 훈련 모델에 상당량의 데이터가 제공되어야 합니다. 경쟁사들에 비해 IDHub 가 갖는 강점은 사용자 데이터의 양과 질에 있습니다. 경쟁사들은 사용자 거래 정보만을 기준으로 신용도를 평가하지만 IDHub 는 거래 정보 외에 인증서, 고객행위정보, 신원들 간의 상호작용 등으로부터 추가 정보를 파악하여 신용도 평가에 사용합니다. 이에 따라 IDHub 는 하나의 신원에 대한 평판을 총체적으로 파악할 수 있습니다. 이렇게 이뤄지는 신용평가를 근거로 IDHub 는 사용자의 대출 신청을 검토하고 적절한 금리 범위를 제시합니다. 여신 업체의 가장 큰 문제는 채무 불이행입니다. IDHub 는 채무 불이행 위험을 경감시키기 위한 집단 대출이나 대출채권의 유동화를 지원합니다. 향후 여신 업체가 채무 불이행으로부터 더 높은 안전을 원할 경우 대부 보험 메커니즘 도입도 고려할 것입니다. 대출자 편의를 위해 IDHub 는 IDH 와 통화 간 자동 환전을 제공합니다. 대출자는 원할 경우 화폐로 대출 상환을 할 수 있습니다.

5.4 게임화

게임화를 통해 사용자 경험을 향상시킬 수 있습니다. 사용자가 맡은 역할이 사용자 자신이 되는것 입니다. 레벨을 올리기 위해 사용자들은 새로운 기술을 익히고, 새로운 친구를 사귀고, 새로운 장소를 방문하고, 훈련을 함으로써 자신의 역할을 강화시킵니다. 일상 임무는 청구서 제출 등과 같은 쉬운 임무로서 해당 임무를 수행함으로써 사용자는 경험치를 쌓게됩니다. 경험치가 특정 수준에 도달하면 사용자들은 이에 대한 보상으로 배지를 받습니다. IDH 를 지급하고 평가나 장비를 구매할 수 있습니다. 사용자 프로파일 정보는 레이더 차트 형태로 시각화됩니다. 각각의 축이 하나의 속성을 나타냅니다. 건강축에는 달린 거리, 소모 칼로리, 체중, 혈압, 의료 기록이 포함됩니다. 관계축에는 동료, 급우, 가족관계도, 페이스북이나 링트인 또는 트위터 친구들이 포함됩니다. 자산축에는 예금증서, 증권, 부동산 소유권, 암호화폐 지갑 주소 등이 포함됩니다.

신용축에는 거래, 신용카드, 세금, 범죄기록, 대출기록 등이 포함됩니다. 기술축에는 Cousera 인증서와 GitHub 약속 등이 포함됩니다. 가치축에는 사용자가 제공하는 재화나 용역 그리고 IDHub 포럼에 사용자가 올린 글들이 포함됩니다. 여행축에는 방문했던 도시와 숙박시설 기록이 포함됩니다. 사생활 정보 보호 측면에서 이들 여러 가지 축들 중 어떤 축을 공개할 것인지 사용자가 결정합니다.

5.5 광고

광고주는 사기 행위로 손해를보고 소비자들은 사생활 침해로 감정이 상하는 일이 발생합니다. IDHub 는 이들 두 집단 모두에 도움을 줄 수 있고 광고 산업을 재편할 수 있습니다. 사기꾼들은 봇을 이용해서 광고에 허위로 반응하고 클릭함으로써 광고 캠페인에서 부당 이익을 얻습니다. 광고주들은 가짜 클릭에 돈을 지불하면서 광고 효과는 전혀 거둘 수 없게 됩니다. 소비자들의 개인 정보가 동의 없이 돈을 받고 팔리는 일이 벌어지고 있습니다. 이 문제에 대해 IDHub 이 제안하는 솔루션은 광고 수익을 소비자들과 나누는 것입니다. 소비자들은 광고를 볼지 여부를 결정하고, 광고를 보면 이에 IDH 로 보상을 받습니다. 소비자 중에 광고를 본 후 구매를 하는 소비자는 더 많은 IDH 를 보상으로 받게 됩니다. 이로써 광고주에게 비효과적인 광고비 지출이라는 끔찍한 문제가 해결되는 것입니다. IDHub 사용자는 검증 가능한 사람이지 봇이 아닙니다. 광고주들은 인증을 받은 사용자들이 자신들의 광고를 보거나 클릭할 때만 비용을 내게 됩니다. 소비자들은 광고 수익을 나눠가질 수 있기 때문에 자발적으로 그리고 적극적으로 광고를 둘러보게 됩니다. 더불어 광고주들은 정확한 마케팅을 할 수 있다는 장점을 누릴 수 있게됩니다. IDHub 사용자들의 신원 속성들은 인증 과정을 거치고 데이터가 정확하기 때문에 사용자들의 선호도를 파악하는 데 탄탄한 기초 역할을 합니다. 사용자와 광고주 모두 IDHub 생태계가 창조하는 윈윈 환경에서 혜택을 누릴 수 있습니다.

5.6 비지니스 모델

IDHub 비지니스의 핵심을 차지하고 있는 것은 신원 검증입니다. 이 핵심 비즈니스를 확장하여 추가된 것이 대출(신용도 기반 대출)과 광고(검증된 신원 기반 광고)입니다. 우리가 제안하는 가치는 신원 검증 비용을 낮춰준다는 것입니다. 검사자는 원하는 인증을 구매함으로써 시간을 절약할 수 있습니다. 인증자는 신뢰할 수 있는 데이터를

제공하고 시스템의 가치를 향상시키기 때문에 IDH 토큰으로 보상을 받습니다. 사용자가 자신들의 신원에 대해 완전한 통제권을 갖고 그들의 사생활 정보는 보호받습니다. 우리의 핵심 파트너는 인증자, 커뮤니티, 여신업체, 광고주입니다. 커뮤니티 구성원들은 IDHub 얼리 어답터들을 말하는데 이들은 GitHub 데이터 저장소를 발전시키는 데 기여합니다. 신원 검증 이외에 거래도 IDHub 의 또 다른 주요 활동입니다. 사용자의 거래 기록이 해당 사용자의 신용 평가의 기초가 됩니다. 신용 평가에 사용되는 주된 자원은 인증입니다. 인증자들과의 연계 또한 매우 중요한데 그 이유는 인증자를 더 많이 확보하면 할수록 생태계가 더 강력해지기 때문입니다. 우리가 목표로 하는 대상 고객은 인증 보유자, 검사자, 광고주입니다. 우리는 고객 관계 유지를 위해 충성 고객 프로그램을 통해 보너스나 할인을 제공합니다. 게임화를 통해 사용자 경험과 고객 참여를 촉진시킵니다. 잠재 사용자에 접근하기 위해 사용하는 채널로는 동호회, 제품소개, 언론, 소개 프로그램이 있습니다. 주요 비용 항목은 마케팅 비용, 제품 개발 비용, 행정 비용입니다. 우리의 수익원은 인증 수수료, 여신 수수료, 광고 수수료입니다.

그림 9 는 IDHub 의 비지니스 모델을 간략히 도식화한 것입니다.

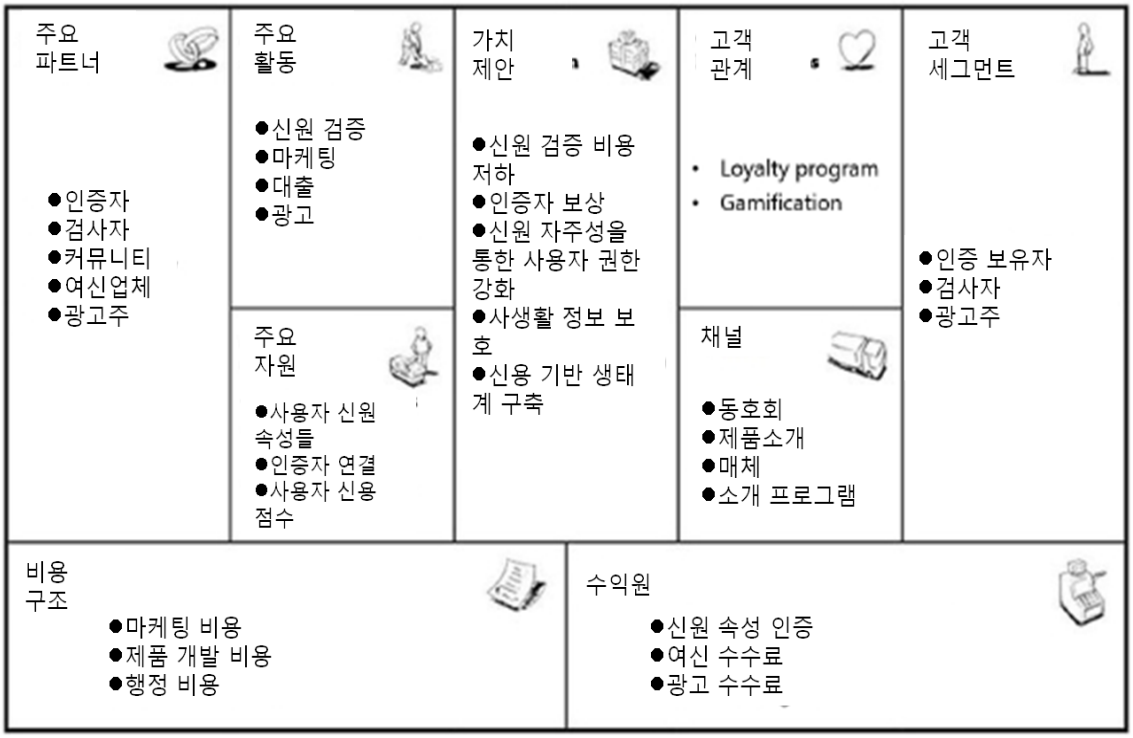


그림 9: 비지니스 모델 다이어그램

6. 준법

6.1 1995 년 유럽 연합 데이터 보호 지침

지침 95/46/EC 라고 알려져 있는 유럽 연합 데이터 보호 지침은 유럽 연합 시민들의 개인 정보와 사생활을 보호하기 위한 규정입니다. 지침 95/46/EC 의 근간은 다음 7 가지 원칙입니다: 1) 개인의 데이터를 수집할 때는 해당 데이터의 소유 주체에게 필히 해당 사실을 통보해야 합니다. 2) 개인의 데이터를 수집할 때는 해당 데이터를 수집하는 당사자가 누구인지를 해당 데이터의 소유 주체에게 통보해야 합니다. 3) 수집한 개인 데이터는 오용, 도난, 분실로부터 안전하게 보관해야 합니다. 4) 개인 데이터는 해당 데이터 소유 주체(들)의 동의 없이 제 3 자에게 공개하거나 제 3 자와 공유할 수 없다. 5) 데이터의 소유 주체들은 자신들의 개인 데이터에 접속이 허용되어야 하고 부정확한 사항은 수정할 수 있도록 해야 합니다. 6) 수집된 데이터는 명시된 목적(들)으로만 사용되어야 하고 그외 다른 어떤 목적으로도 사용될 수 없다. 7) 데이터를 수집하는 당사자들은 데이터 소유 주체들에 대해 이 7 가지 원칙들 모두 지킬 책임을 갖습니다.

6.2 1996 년 건강 보험 휴대성 및 책임성에 관한 법(HIPAA)

HIPAA 는 미국의 보건 의료 산업에 적용되는 규제입니다. HIPAA 의 주요 구성 부분은 환자의 사생활, 전자의료기록(EMR)의 교환, EMR 의 불역성, EMR 저장입니다. IDHub 는 OpenPDS 를 통해 환자의 사생활을 보호하고 블록체인을 통해 EMR 저장과 불역성을 지원합니다. EMR 교환에 사용되는 용어들은 Health Level 7 (HL7) 표준을 따라야 합니다. 전통적 형태의 보험금 지금 신청은 피호험자의 의료 기록 전체를 요구합니다. IDHub 는 의료 기록을 공개하지 않고 보험금 청구서 요건을 충족시킬 수 있습니다. 따라서 IDHub 는 HIPAA 가 요구하는 것보다 더욱 엄격한 접근 방법을 적용하고 있습니

7. 팀

Doer Qu
Founder
Council member of Connected City Advisory Board (CCAB)

Kenneth Chen
Technical Director
Former CTO of APTG
Co-Founder & CTO of Genie Networks Ltd.

Xiaoyu Li
Core Developer

Don Hsieh
Core Developer

Jamie Lin
Core Developer

Zeqian Yao
Developer

Jiaqi Li
Developer

Michael Wang
Business Development

Cecilia Wu
Marketing Director

Leo Cao
Marketing Manager

Derek Xue
Marketing & PR Manager

Lekch Tasya
Community

8. 결론

IDHub 는 이주 노동자들이나 난민들 또는 사회 내 경제적 약자들이 어디에서든 자신들의 디지털 신원 데이터에 접속할 수 있도록 함으로써 이들에게 도움을 주는 역할을 합니다. 이렇게 디지털 서명을 갖춘 경제적 약자들은 중계 기관으로부터 소외되지 않고 직접 사회 복지 제도를 이용할 수 있게 됩니다. 투명하고, 불역적이며 견고한 블록체인 아키텍처를 통해 사용자 데이터가 보호됩니다. 정보 공개 최소화 원칙을 구현하고 있는 Merkle 트리를 통해 사생활 보호를 보장합니다.

참고 자료

[1] Asli Demirg¨u¸c-Kunt et al. “The global findex database 2014: Measuring financial inclusion around the world”. In: (2015).

[2] Division for Sustainable Development. Sustainable Development Goal 16. https://sustainabledevelopment.un.org/sdg16. Accessed at 2017-12-22.

[3] Joseph Atick. “Digital identity: the essential guide”. In: ID4Africa Identity Forum. 2016.

[4] Coindesk. Local Government in China Trials Blockchain for Public Services. https://www.coindesk.com/local-government-china-trials-blockchain-public-services. Accessed at 2018-02-01.

[5] New Zealand Post. RealMe. https://www.nzpost.co.nz/personal/realme-id-apply/realme. Access at 2017-12-29.

[6] New Zealand Government ICT. RealMe Verified Account Service. https://www.ict.govt.nz/services/show/RealMe-Verified-Account-Service. Access at 2017-12-29.

[7] Inc Identity2020 Systems. ID2020. https://id2020.org. Accessed at 2018-02-06.

[8] Decentralized Identity Foundation. DIF. http://identity.foundation. Accessed at 2018-02-06.

[9] Schema.org. Person. http://schema.org/Person. Accessed at 2017-10-03.

[10] Michael Jones, John Bradley, and Nat Sakimura. Json web token (jwt). Tech. rep. 2015.

[11] Dick Hardt. “The OAuth 2.0 authorization framework”. In: (2012).

[12] J Paul Morrison. Flow-Based Programming: A new approach to application development. CreateSpace, 2010.

[13] Jaap-Henk Hoepman. “Privacy design strategies”. In: IFIP International Information Security Conference. Springer. 2014, pp. 446–459.

[14] Petar Maymounkov and David Mazieres. “Kademlia: A peer-to-peer information system based on the xor metric”. In: International Workshop on Peer-to-Peer Systems. Springer. 2002, pp. 53–65.

[15] Daniel Bernstein, Tanja Lange, and Peter Schwabe. “The security impact of a new cryptographic library”. In: Progress in Cryptology–LATINCRYPT 2012 (2012), pp. 159–176.

[16] Daniel J Bernstein, Tanja Lange, and Peter Schwabe. “NaCl: Networking and cryptography library”. In: http://nacl.cr.yp.to (2011).

[17] Reuters. Tanzania orders probe into “ghost workers” on government payroll. https://goo.gl/5qFpBB. Accessed at 2017-10-17.

[18] Anil Jain, Ruud Bolle, and Sharath Pankanti. Biometrics: personal identification in networked society. Vol. 479. Springer Science & Business Media, 2006.

[19] Francine J Prokoski. “Disguise detection and identification using infrared imagery”. In: Optics and Images in Law Enforcement II. Vol. 339. International Society for Optics and Photonics. 1983, pp. 27–32.

[20] Sajan Ambadiyil, KS Soorej, and VP Mahadevan Pillai. “Biometric Based Unique ID Generation and One to One Verification for Security Documents”. In: Procedia Computer Science 46 (2015), pp. 507–516.

[21] Diaspora Foundation. The Diaspora Project. https://diasporafoundation.org. Accessed at 2017-10-03.

[22] Unique Identification Authority of India (UIDAI). Aadhaar. https://uidai.gov.in/your-aadhaar/about-aadhaar.html. Accessed at 2017-10-03.

[23] Civic Technologies. Civic Whitepaper. https://goo.gl/xzKvN7. Accessed at 2017-11-01. 2017.

[24] GSMA. Introducing Mobile Connect the new standard in digital authentication.

https://www.gsma.com/identity/mobile-connect. Accessed at 2017-10-19.

[25] Sovrin Foundation. Sovrin. https://sovrin.org. Accessed at 2018-02-06.

[26] Phil Windley. Sovrin Web of Trust. http://www.windley.com/archives/2017/05/sovrin_web_of_trust.shtml. Accessed at 2018-01-08.

[27] Christian Lundkvist et al. Uport: A Platform for Self-Sovereign Identity. https://whitepaper.uport.me/uPort_whitepaper_DRAFT20170221.pdf. Accessed at 2017-11-01. 2017.

— END —