

사용자 주권을 보장하는 블록체인 기반 개인데이터 거래 플랫폼 구조 연구

윤대근, 노성기
한국전자통신연구원

dayoon@etri.re.kr, sknoh@etri.re.kr

Designing a blockchain-based data trading platform to ensure personal data sovereignty

Yoon Dae Geun, Noh Sung Kee

Electronics and Telecommunications Research Institute.

요 약

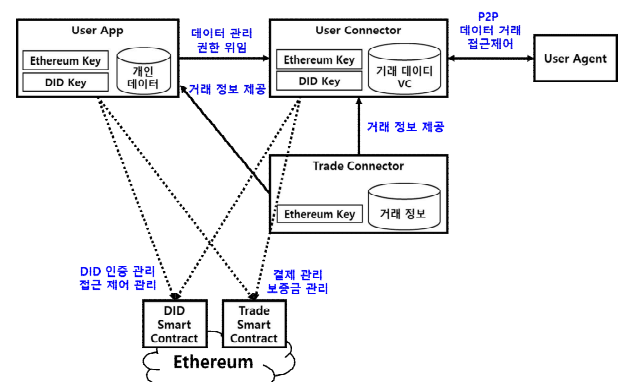
초연결 네트워크의 진화와 모바일 기기의 확산으로 인해 개인데이터 발생량은 시간이 지남에 따라 폭발적으로 증가하고 있다. 빅데이터 분석, AI 기술에서의 활용 등으로 오늘날의 개인 데이터는 21 세기 디지털 원유로 불릴 만큼 중요성이 점차 강조되고 있으나 개인이 생성하는 데이터를 통해 개개인이 적당한 혜택을 얻을 수 있는 환경이 갖춰져 있지 않다. 본 논문은 개인이 생성하는 데이터를 안전하게 관리할 수 있는 환경에서 개개인이 직접 데이터를 판매 및 구매할 수 있는 블록체인 기반 개인데이터 거래 플랫폼 (Trusted Data Connectome, TDC) 구조를 제안한다. TTP-free 구조인 TDC 플랫폼을 통해 사용자는 개인데이터 및 인증정보 관리와 자율적인 데이터 가치 결정이 가능한 환경에서 개인데이터 거래를 수행할 수 있다.

I. 서 론

오늘날 개인이 사용하는 스마트폰, 스마트워치 등의 모바일 기기는 실시간으로 개인 데이터를 생산하고 있다. 개인 데이터는 사업 혹은 정책의 방향을 분석하기 위한 빅데이터 분석, 금융이나 자율주행 등에 사용되는 AI 모델 개발을 위한 리소스 등 다양한 분야에 활용될 수 있으며, 이러한 이유로 오늘날의 개인 데이터는 21 세기의 디지털 원유로 불릴 만큼 중요성이 강조되고 있다. 하지만 개인이 생성하는 가치 있는 데이터를 통해 글로벌 플랫폼 사업자들은 많은 혜택을 보고 있는 반면 개개인이 얻을 수 있는 혜택은 거의 전무하다. 최근 ‘마이데이터 발전 종합정책[3]’ 등이 시행되었지만 개인의 동의 하에 정보 활용 기관이 데이터를 효율적으로 사용하는데 초점을 두고 있으며 개인이 직접 데이터에 접근하여 혜택을 얻는 내용은 포함하지 않고 있다. 데이터 공유경제의 활성화와 개인데이터 거래에 대한 필요성이 제시되고 있지만 관련 연구 개발은 미진한 상태이다.

본 논문에서는 글로벌 플랫폼과 같은 TTP 기반 환경에 의존하지 않고 개개인의 개인데이터 주권 보장 및 거래가 가능한 블록체인 기반 개인데이터 거래 플랫폼 (Trusted Data Connectome, TDC) 구조를 제안한다. TDC 플랫폼이 제공하는 사용자 앱(User App), 사용자 커넥터(User Connector), 거래 커넥터(Trade Connector), 스마트 컨트랙트 등을 통해 개인데이터 및 인증정보 관리와 자율적인 데이터 가치 결정이 가능한 환경에서 개인데이터 거래를 수행할 수 있다.

II. 본론

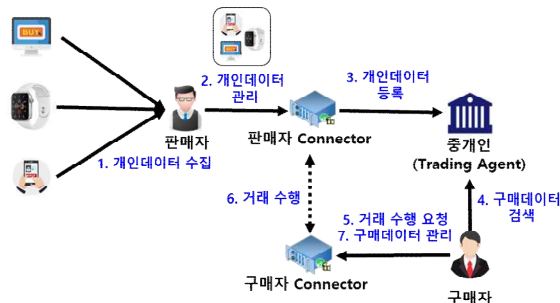


<그림 1. TDC 플랫폼 구조>

TDC 플랫폼 구조는 그림 1 과 같다. TDC 플랫폼은 개인이 생성한 데이터를 제 3 자에 의존하지 않고 관리하며 개인 간 거래가 가능하도록 설계되었다. TDC 플랫폼의 구성 모듈은 크게 사용자 앱(User App), 사용자 커넥터(User Connector(Agent)), 거래 커넥터(Trade Connector), 스마트 컨트랙트 4 가지로 구성된다. 사용자는 User App 을 통해 개인데이터를 생성하고 개인 간 데이터 거래를 수행할 수 있다. 개인 간 거래에 필요한 신원인증은 User App 에서 생성하는 Decentralized Identifiers (DID)[1]를 통해 수행할 수 있다. 모바일 단말의 특성상 충분한 기능을 가지지 못하는 User App 의 한계를 극복하기 위해 User App 에서 생성한 개인데이터를 User Connector를 통해 관리할 수 있다. 사용자는 DID document 항목을 통해 제 3 자의 개입 없이 직접 User Connector 에 권한을

부여할 수 있다. User Connector 는 사용자가 부여한 권한 범위 내에서 개인데이터를 관리하고 거래를 수행할 수 있다. 데이터 거래에 참여하는 사용자 간 인증정보 및 User Connector 권한에 대한 인증 정보는 모두 Ethereum 상에 저장되어, 제 3 자가 제공하는 서버 없이 필요할 때마다 인증 정보를 생성/수정/호출할 수 있다. Trade Connector 는 사용자가 판매를 위해 등록된 개인데이터 목록을 사용자에게 제공해주며 거래에 필요한 알람 등의 메타데이터 또한 User App 과 User Connector 에 제공해준다. 데이터거래 관련 스마트 컨트랙트는 Trade Connector 가 Ethereum 상에 설치하고 관리하며 해당 기능 사용에 대한 수수료를 통해 이익을 얻을 수 있다.

TDC 플랫폼을 통해 판매자가 판매데이터를 Trade Connector 에 등록하고, 구매자가 Trading Connector 에서 데이터를 검색하여 구매하는 개인데이터 일괄 거래 모델과, 구매자가 원하는 데이터 요구사항을 Trade Connector 에 등록하고, 판매자가 구매자의 요구사항에 맞는 데이터를 일정 기간 제공하는 데이터 구독 거래 모델이 있다.

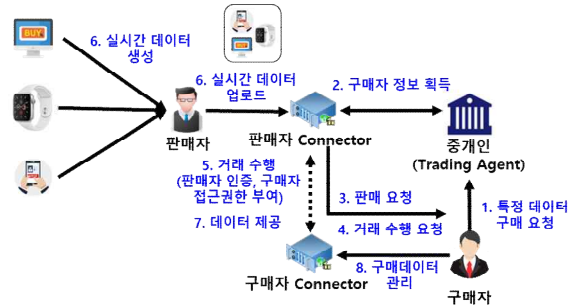


<그림 2. 개인데이터 일괄 거래 모델>

그림 2 는 개인데이터 일괄 거래 모델을 나타낸다. 개인데이터 일괄 거래 모델에서는 판매자가 수집한 개인데이터를 자신의 전용 에이전트를 통해 관리하고 수집하며, 수집한 데이터 중 판매를 원하는 데이터를 Trading Connector 에 등록한다. 이후 구매자가 구매를 원하는 데이터를 Trade Connector 를 통해 검색하여 판매자의 접근 정보 등의 메타데이터를 획득하고, 획득한 정보를 토대로 구매자 Connector 에 판매데이터 구매를 요청한다. 이후 구매자 Connector 와 판매자 Connector 간의 통신을 통해 데이터 거래가 수행되고, 거래가 종료되면 에이전트는 각각의 소유자에게 거래가 종료됐음을 알린다. 판매자는 블록체인을 통해 판매금액이 입금 됐음을 확인할 수 있고, 구매자는 Connector 를 통해 구매한 데이터를 관리할 수 있다.

그림 3 은 개인데이터 구독 거래 모델을 나타낸다. 개인데이터 구독 거래 모델에서는 구매자가 원하는 특정 데이터에 대한 구매 요청을 Trade Connector 에 등록한다. 이후 판매자가 Trade Connector 에 등록된 구매요청을 검색하여 자신이 가진 데이터와 일치할 시 등록된 구매요청에 대한 구매자 접속정보 등의 메타데이터를 Trade Connector 로부터 획득하여 구매자에게 데이터 거래 요청을 전송한다. 이후 구매자 Connector 와 판매자 Connector 간 DID, Verifiable Credential (VC)[2], 블록체인 기반 거래가 수행되고, 거래가 종료되면 각각의 소유자에게 거래가 종료됐음을 알린다. 거래가 정상적으로 완료되면 판매자는 판매한 데이터에 접근할 수 있는 접근 권한을 구매자에게 부여하고, 구매자는 판매자 Connector 로부터 접근 허가된 데이터를 가져올 수 있다. 데이터 일괄 거래

모델과는 달리 판매자와 구매자는 블록체인에 보증금을 입금하고, 구매자가 접근하여 데이터를 가져올 때마다 계약된 데이터의 가격만큼 보증금을 조정하고, 거래가 완료된 후에 남은 보증금을 정산하는 구조로 거래된다.



<그림 3. 개인데이터 구독 거래 모델>

III. 결론

본 논문에서는 글로벌 플랫폼과 같은 TTP 에 의존하지 않고 개인데이터 주권 보장과 거래가 가능한 블록체인 기반 개인데이터 거래 플랫폼인 TDC 플랫폼을 제안했다. TDC 플랫폼은 사용자가 개인데이터를 수집한 뒤 일괄 거래 가능한 개인데이터 일괄 거래 모델과 사용자가 주기적으로 수집한 데이터를 일정 기간 제공하는 개인데이터 구독 거래 모델을 통한 개인데이터 거래 기능을 제공할 수 있었다. TDC 플랫폼의 두 가지 개인데이터 거래 모델을 구현하여 개인이 생성한 데이터에 대한 합당한 이익을 개개인이 얻을 수 있는 환경을 구축할 수 있는 점을 확인하였다.

ACKNOWLEDGMENT

본 연구는 한국전자통신연구원 연구운영비지원사업의 일환으로 수행되었음. [22ZR1300, 지능형 사이버 보안 및 신뢰 인프라 기술 연구].

참 고 문 헌

- [1] W3C. Decentralized identifiers (DIDs) v1.0:Core architecture, data model, and representations. <https://www.w3.org/TR/did-core/>, 2022. W3C Recommendation.
- [2]. World Wide Web Consortium (W3C). Verifiable Credentials Data Model v1.1. <https://www.w3.org/TR/vc-data-model/>, 19 Mar. 2022. W3C Recommendation.
- [3] 대통령직속 4 차산업혁명위원회, 관계부처 합동."마이데이터 발전 종합정책," 2021.