DID 기반의 디지털 헌혈증 발급 서비스

****변재영, *김주희, **성연주, *안현서, ***이은영, ***임지연
*서경대학교 컴퓨터과학과
**동덕여자대학교 컴퓨터학과
***성신여자대학교 컴퓨터공학과
****LG CNS
jaeyoung.byun@lgcns.com, yellowgreen423@gmail.com, yj.caplin.s@gmail.com, rlawn97@skuniv.ac.kr,
eun970923@naver.com, jiueon6@gmail.com

DID-based digital blood donation certification issuance service

*JooHee Kim, **YeonJu Seong, *HyunSeo Ahn, ***EunYoung Lee, ***JiYeon Lim
*Dept. of Computer Science, Seokyeong University
** Dept. of Computer Science, Dongduk-Women's University
**Dept. of Computer Engineering, Sungshin-Women's University

요 약

기존 종이 헌혈증의 단점을 보완하기 위해, 블록체인과 DID 를 활용하여 개발한 전자 헌혈증 서비스로 헌혈자에게 편리한 헌혈증 사용 및 기부 인터페이스를 제공한다.

1. 서론

대한민국은 현재 급격한 인구 감소를 격감하고 있다. 하지만 그에 반해, 혈액 수요 그래프는 상승세를 기록하고 있다. 특히나 2020 년 코로나의 여파로 꾸준한 수요량에 비해 기대치에 채 못 미친 공급량으로 혈액난을 겪기도 하였다. 혈액의 주요 공급원인 헌혈 활동은 정부의 갖은 노력에도 매년 헌혈자 수가 감소하는 추이다.

헌혈증과 관련된 설문조사를 통한 통계에 따르면 과반수의 사람이 헌혈증을 관리 또는 사용하는 데에 있어 불편함을 느끼고 있다고 응답했다. 이는 헌혈 횟수를 감소시키는 이유 중 큰 비중을 차지한다.

불편함을 느끼는 이유에 대해 물은 문답에서는 '관리하기 어려움'이 가장 큰 비율을 차지했고, 다음으로 '헌혈증을 사용할 일이 없을 것 같아서'가 다음으로 큰 비율을 차지했다. 이와 같은 이유들이 생겨난 공통적인 문제점은 현재 통용되고 있는 헌혈증이 '종이 헌혈증'이라는 것에 있다.

종이 헌혈증은 실물 헌혈증으로 디지털로 관리할 수 없다는 문제점이 있다. 따라서, 사용 및 관리에 어려움이 있다는 것이다. 또한, 종이 헌혈증서는 재발급이 허용되지 않으며, 분실하거나 훼손한 경우 수혈 비용 보상 혜택을 받을 수 없다.

본 논문에서는 이와 같은 문제를 해결하여 헌혈자의 편의 증진과 헌혈 활성화를 위해 블록체인 기반 DID(DID, Decentraized Identity)의 기술의 적용해 전자 헌혈증을 개발하였다.

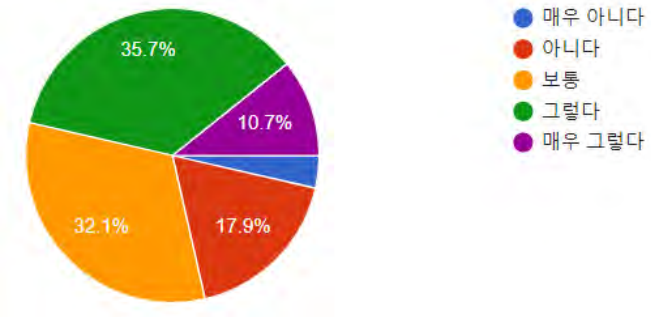
2.1 헌혈증 사업 현황

[1]병원에서 실제로 사용된 헌혈증서는 970 만 장으로, 제도가 시행된 1981 년부터 지금까지 발급된 헌혈증서 총 7 천 680 만 장 대비 사용률이 12.7%에 불과한 것으로 확인됐다. 국회 보건복지위원회 김순례 의원(자유한국당, 비례대표)이 10 월 15 일 대한적십자사부터 제출 받은 '헌혈 환급적립금제도 통계' 자료에 따르면 헌혈증서 사용률이 매우 저조한 것으로 나타났다. 김 의원은 그 배경으로 헌혈증서가 종이로 발급되는 데 원인이 있다고 지적했다. 수년 전에 받은 종이 헌혈증은 찾기도 어려울 뿐만 아니라 헌혈증을 잃어버렸을 경우 재발급이 불가능하기 때문이다.

152 명이 참여한 대한민국 전 국민을 대상으로 한 설문조사에서도 '종이 헌혈증 사용에 불편함을 느꼈는가' 란 질문에 '아니다' 와 '매우 아니다' 에 21.5%가 응답 것과 비교하면 '그렇다' 또는 '매우 그렇다' 에 대한 응답은 46.4%로 2 배 가까이 높은

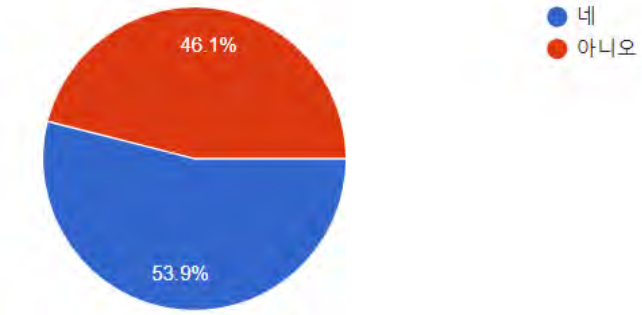
[1] 최관식, 실제 사용된 헌혈증서 12.7% 불과, 병원신문

것으로 밝혀졌다.



(그림 1) '종이 헌혈증 사용에 불편함을 느꼈는가' 에 대한 설문조사 응답

대한적십자사의 통계 자료에 따르면, 2019 년 모금기간 내의 헌혈자 중 기부권을 선택한 헌혈자는 182,437 명으로 [2]6.9%에 그쳤다고 한다. '헌혈증 기증 및 사용 방법에 대해 알고 있는가'란 질문에 46.1% 가 '모른다'라고 응답하였다.

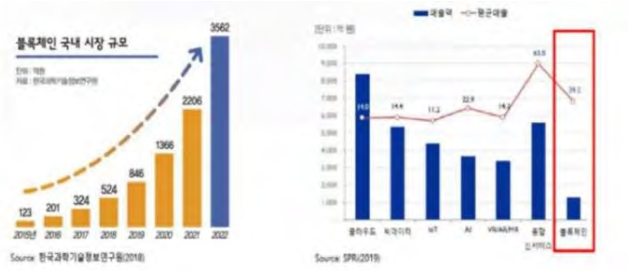


(그림 2) ' 헌혈증 기증 및 사용 방법에 대해 알고 있는가' 에 대한 설문조사 응답

헌혈증은 방문 또는 우편을 통해서만 기증할 수 있다. 현재는 코로나 19 로 인해 센터 내 외부인 출입을 차단하고 있어 그마저도 방문 기증은 불가하고 우편으로만 가능한 상태이다.

2.2 블록체인 사업 현황

[3]국내 블록체인 시장이 2022 년까지 연평균 약 61.5% 성장해 3,500 억 원 규모를 형성할 것이라는 전망이 나왔다. 정보통신산업진흥원(NIPA)은 최근 발간한 '블록체인 산업 현황 및 국외 정책 동향' 보고서에서 이같이 전망했다. 보고서가 인용한 한국과학기술정보연구원 자료에 따르면 2019 년 현재 우리나라 블록체인 시장 규모는 약 846 억원이다. 국내 시장 규모는 2020 년 1,366 억 원, 2021 년 2,206 억 원으로 증가해 2022 년에는 약 3,562 억 수준에 도달할 것이라고 보고서는 전망했다.



(그림 3) [4]블록체인 국내 시장 규모

IT 시장분석 및 컨설팅 기관 IDC 도 지난 3 월 발간한 '전 세계 블록체인 반기(Semiannual) 투자 보고서' 에서 2018 년부터 2022 년까지 전 세계 블록체인 시장의 연평균성장률(CAGR)이 약 76%일 것으로 예측했다. 전 세계 시장과 비교해서도 우리나라 블록체인 시장의 성장률이 비슷한 수준을 보일 것이라는 분석이다. 또 블록체인 기술이 기존에는 암호화폐 송금, 거래와 같은 금융 분야에서만 한정적으로 활용됐지만, 에너지, 공공서비스, 의료 및 헬스케어, 물류 및 유통, 부동산 등 다양한 분야에 확대 적용될 것이라고 분석했다.

2-3. DID 기술(탈중앙화 신원증명 기술)

[5]DID 란 개인정보를 사용자의 단말기에 저장한 다음에, 개인정보 인증 시 필요한 정보만 골라서 사용하도록 하는 탈중앙화 전자신원증명 기술이다. 기존의 중앙화 된 인증방식의 반대된 개념이다. 자신의 유일한 식별자인 키를 통해 자신을 증명하고 서버에 접속할 수 있도록 한다. 이를 통해 다른 누군가에게 자신의 신원 증명을 맡기는 것이 아니고 자기 자신의 신원 증명에 대한 권한을 갖도록 하는 것이다 [6](SSI-Self-Sovereign Identity, 자기 주권 신원). 전자 헌혈증의 경우에는 보안상의 문제가 생겨서 해커가 개인정보를 조작하고 개인정보가 유출될 수 있다는 문제가 발생한다. 본 작품은 DID 기술을 이용해서 이런 문제점을 해결하도록 한다. 사용자의 개인정보를 보호하고 개인정보의 투명성, 안정성을 보장해 주기 때문에 사용자가 이 프로그램을 신뢰하면서 사용할 수 있다.

[7]DID 기술의 구현 방식은 다음과 같다. 한 개인의 신원 정보 및 인증과 관련된 메타 데이터를 DID Document 라는 형식으로 정의하고 이를 가리키는 일

[2] 대한적십자사, 2019 년 모금집행내역
[3] 정유림, 국내 블록체인 시장, 연평균 61.5%↑…2022 년 3500 억 원 규모
[4] 정보통신산업진흥원, 블록체인 국내 시장 규모
[5] 김기영, 탈중앙화 신원증명(DID),데이터의 주권은 개인에게 있다
[6] 유수웅, DID 가 극복해야 할 문제
[7] W3C, 분산 식별자(DID)v1.0

종의 주소인 Decentralized Identifiers 를 블록체인 상에 정의하면 인증 요청 주체가 이 Document 를 통해 사실 여부를 확인하게 된다.

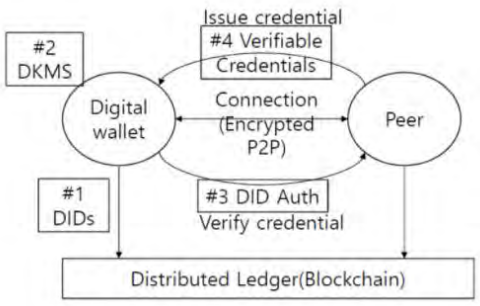
[8]DID 의 기술요소로는 Verifiable Credentials, DID Auth, DKMS(Decentralized Key Management System),DIDs(Decentrailzed Identifiers)가 있다.

Verifiable Credentials: 물리적인 증명서와 같은 역할로, 사진, 이름 ,식별번호 등 증명 주제 관련 정보와 발행기관, 증명 도출 증거, 만료일 정보 등 포함 - 표준화 단체 : W3C

DID Auth: DID 소유자가 사설 키 제어를 증명으로 인증 - 표준화 단체: DIF

DKMS: DIDs 에서 필요한 사설 키를 관리하기 위해 제안된 공개 표준 - 표준화 단체 : OASIS

DIDs: RFC 2141 URN 기반 Scheme: method: method-specific identifier 로 구성- 표준화 단체: W3C



(그림 4) DID 기술 구성도

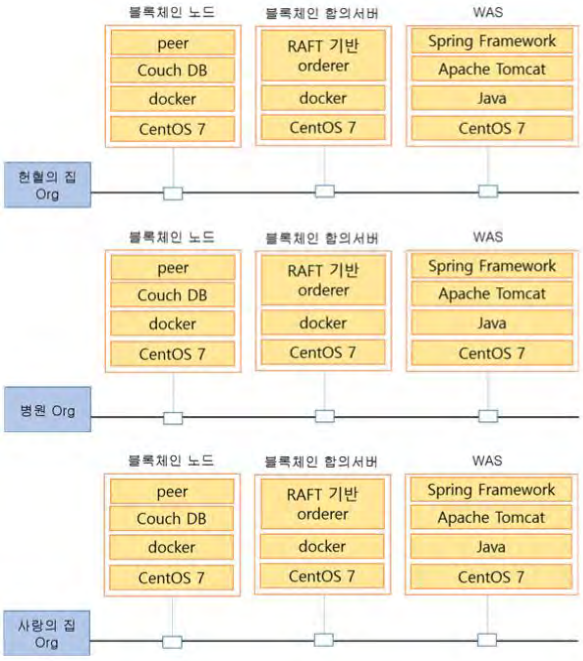
2.4 시스템 아키텍처

시스템은 centOS 7 환경에서 구축하며 apache tomcat 기반 spring framework 로 웹을 구성하고 node.js 로 SDK 를 구성한다. 구성된 SDK 를 이용하여 리눅스 재단의 오픈소스 프라이빗 블록체인인 하이퍼레저 패브릭에 연동한다. 웹으로부터 받아온 클라이언트 정보는 RAFT 기반의 합의 알고리즘을 이용하여 블록체인과 maria DB 에 저장한다.

블록체인은 하나의 ch(channel id) 채널과 헌혈자인 Donor 와 혈액원인 Blood, 헌혈증을 요청하는 병원인 Hospital 세 개 조직으로 구성되어 있다. 세 개의 조직이 헌혈증에 대한 정보를 공유하기 때문에 서로 비밀을 유지할 필요가 없어 한 개의 채널로 구성할 수 있고 조직은 각각 하나의 peer 로 구성되어 있으므로 각 peer 들은 anchor peer 지정을 할 필요가 없다. 각 조직은 peer 를 통해 ch 채널에 가입한다. 체인코드는 Java, go 등의 다양한 언어로 작성할 수 있지만 본 서비스에서는 Java 로 작성했다. 작성된 체인코드를 설치하고 인스턴스 화 하여 헌혈증을 발급, 기부하는 기능을 처리한다.

기존의 헌혈증을 전자 헌혈증으로 재발급하거나 헌혈증을 새로 발급받는 경우는 블록체인과 DB 를 이용하여 처리하지만 기부명세 혹은 요청명세를 조회, 검색 등의 기능을 처리할 때는 DB 만 사용하여 처리한다.

본 서비스는 DID(탈중앙화 신원증명) 기술을 이용하여 위변조 불가, 분실까지 방지하는 블록체인 기반의 헌혈증을 구현한다. 또한, 사용자 인터페이스로 헌혈증을 블록체인에 저장한다. 블록체인은 읽고 추가하는 기능만 가능하므로 헌혈증의 발급 및 기부 관련 정보가 블록체인에 영구적으로 남아있게 되고 권한이 있는 사람은 누구나 볼 수 있게 된다. 이 때문에 헌혈증의 기부명세와 기부 과정 등의 투명성을 보장한다.



(그림 1) DID 기반 시스템 아키텍처

Ⅲ. 결론

헌혈증의 사용방법을 모르거나 복잡해서 이용하기 어려워하는 사람들이 많다. 활발한 헌혈 활동을 위해서 혈액원의 기존 헌혈자 관리, 헌혈증의 사용방법 등에 대한 중요성이 커지고 있다.

따라서 본 서비스는 헌혈자의 적극적인 헌혈 활동과 헌혈증의 활용을 증진하기 위해 블록체인 기반의 DID(DID, Decentraized Identity) 기술을 적용하여 디지털 헌혈증 서비스를 만들었다.

전자 헌혈증의 이점은 분실과 훼손을 방지한다는 것이다. 기존의 헌혈증은 종이로 이루어져 있어 분실

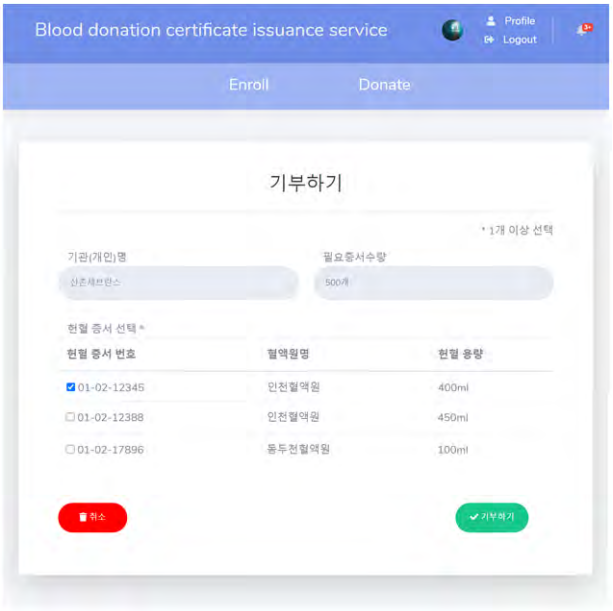
[8] 도리의디지털라이프

되거나 훼손될 경우 재발급이 가능하지 않아 사용하기 어렵다.

또한, 발급이나 기부 방법이 간단해진다. 기존의 우편을 통해서 기부하는 방법을 어려워하는 사람들을 위해 디지털 헌혈증 서비스에 접속해 편리하게 기부할 수 있도록 만들었다. 그뿐만 아니라 DID 를 사용하여 서비스를 구현하기 때문에 기존의 폐쇄적이었던 헌혈증의 사용과정을 투명하게 관리할 수 있으며 개인정보를 보호하여 안정성을 보장한다.

블록체인 기반의 DID 기술을 적용함으로써 개인정보의 보관과 유출에 대한 부담이 줄어들며, 중앙화된 기관도 요구되지 않아 비용을 절약할 수 있다.

디지털 헌혈증 서비스를 통해 헌혈이 모든 사람에게 보편적인 문화로 자리매김하길 바란다.



(그림 5) 실제 기부 페이지

본 논문은 과학기술정보통신부 정보통신창의인재양성사업의 지원을 통해 수행한 ICT 멘토링 프로젝트의 결과물입니다.

참고문헌

[1] 최관식, 실제 사용된 헌혈증서 12.7% 불과, 병원신문, 2019.10.15
[2] 대한적십자사, 2019 년 모금집행내역
[3] 정유림, 국내 블록체인 시장, 연평균 61.5%↑…2022 년 3500 억원 규모
[4] 정보통신산업진흥원, 국내 시장 규모
[5] 김기영, 탈중앙화 신원증명(DID),데이터의 주권은 개인에게 있다
[6] 유수웅, DID 가 극복해야 할 문제, 2019.9.9
[7] W3C, 분산 식별자(DID)v1.0, 2020.9.7
[8] 도리의디지털라이프, 2020.7.3