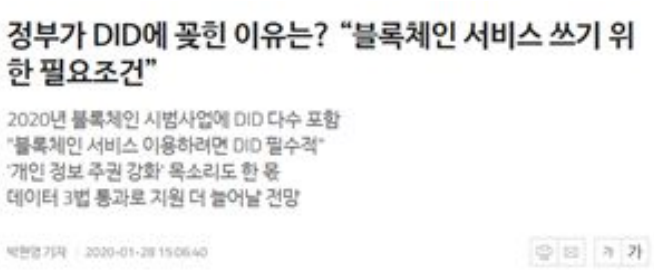
문제정의서(연구계획서)

과제명	블록체인 기반 자기주권형 분산 신원 증명 연구

조	9 조
지도교수	류재철 교수님 (서명)
조원	201502015 권재승 201502122 조성락 201601155 오하늘

1. 연구의 필요성


정부가 DID에 꽂힌 이유는? "블록체인 서비스 쓰기 위한 필요조건"

2020년 블록체인 시범사업에 DID 다수 포함
"블록체인 서비스 이용하려면 DID 필수적"
'개인 정보 주권 강화' 목소리도 한 몫
데이터 3법 통과로 지원 더 늘어날 전망

대한민국 정부의 데이터3법통과로 인해, DID의 사용량이 늘어날 전망이고, 삼성 SDS 블록체인 연구소는 이미 블록체인 DID에 대해 프로젝트가 진행 중에 있다. 뿐만 아니라, 비트코인 이후 잠시 주춤하는 듯 했으나, DID로 인해, 다시 떠오르고 있는 분야 중 하나이다.

요즘 아파트내에서, 스토커, 성폭행 등의 범죄사건이 간간히 일어나고 있는 가운데, 아파트의 출입 시스템은 매우 취약함. 비밀번호를 알아내면, 누구나 다른 인증없이 자유롭게 출입이 가능하고, CCTV에 의지하기에는 역부족이다. 이에, 몇몇 업체는 카드형 신분증이라는 아이템을 내놓았지만, 보관이 다소 어렵고, 분실하거나 유실될 가능성이 있다는 단점이 있다. 따라서 아파트에는 보다 보안성이 높은 안전한 출입시스템이 필요하다. 이에 대한 해결책으로 블록체인 DID시스템을 제시할 수 있다.

블록체인을 이용한 DID 출입시스템의 장점은 다음과 같다.

1. 도민증을 보유한 지역주민 혜택을 통한 지역 경제 활성화 및 인구 유입 효과
2. 모바일 신분증을 통해 카드형 신분증 발행 비용과 유지비를 절감하여 지자체 예산 절감 효과
3. 모바일 신분증을 이용한 주거 공간 외부인 출입 통제를 통해 거주민 안전 확보

2. 연구의 목표 및 내용

본 연구는 블록체인을 활용한 자기주권형 분산 신원 증명 구현을 통해 아파트와 같은 공용 주거 공간에서의 자기 주권형 신원 인증을 통한 출입, 범죄 예방, 외부인 출입 문제 등의 문제를 해결하려고 한다.

2-1. 목표

- 아파트 출입 로그의 무결성 보장(변조 불가능)
- 중앙기관에 의지하는 않는 탈중앙화된 자기 주권형 신원증명
- 블록체인 기반의 분산 신원 증명 출입증 및 전자 지갑 앱 개발을 통한 공용 주택 출입서비스 시스템 운영 기반 조성
- 라즈베리파이, 아두이노를 활용한 아파트 출입 시스템 구현 및 테스트

2-2. 연구범위

□ 블록체인 분산 신원 증명(DID) 플랫폼

◦ DID 생성 및 관리

◦ DID 인증 및 권한 관리

◦ 내역 관리(발급 및 인증)

◦ 연동 API 및 어플리케이션 개발

- 디지털증명서 발급기관(Issuer)용 : 아파트관리사무소 또는 보안관리회사
- 디지털증명서 제출기관(Verifier)용 : 아파트출입시스템

◦ 블록체인 기능

- 분산 신원 증명(DID), 스마트 컨트랙트(Smart Contract), 분산원장(Ledger)
- 발급기관(CA) 등록, 인증서 발급 정보 저장 등

□ 블록체인 기반 자기주권형 분산 신원 증명(DID) 시스템 개발

◦아파트 출입증 발급관리 시스템

- 출입증 발급 : 사용자 회원가입 및 본인인증 후 발급
- 출입증 관리(갱신, 폐기) 및 발급 내역 관리
- 검증 기관(Verifier) 등록 및 관리
- 전자증명서를 발행 기관(Issuer) 등록 및 관리

□ 블록체인 기반 자기주권형 분산 신원 증명(DID) 사용자 어플리케이션 개발

◦ 회원가입 및 본인확인

- 서비스 사용을 위한 회원가입
- 본인 인증을 위한 증명서 제출

◦ 블록체인 플랫폼으로부터 발급받은 출입증(출입자격) 저장

◦ 출입증 및 출입자격을 제출

◦ 전자 자격증명서 관리

- 발급받은 자격증명의 갱신 및 폐기

3. 연구의 추진전략 및 방법

❍ 온라인 협업도구(Notion, github 등)를 활용한 프로젝트 진행상황 공유 및 업무 task 분할

❍ 프로젝트 진행에 있어 필요한 지식 학습

- 블록체인, 이더리움, DAPP, 솔리디티

❍ 온라인 회의 및 대면을 통한 프로젝트 진행방향 결정

- 개발 전략 및 방법

- **Gradle 적용**
  - ◇ Java dependency 관리 용도로 사용
  - ◇ 팀원들간의 공통된 라이브러리(Library)를 공유하고 세팅하는 불편함을 덜기 위해 사용
  - ◇ 협업 시 서로가 개발한 영역에 필요한 dependency를 별도의 설치나 설정 과정없이 곧 바로 빌드할 수 있게 하기 위함
- **Web3j 사용**
  - ◇ 자바와 안드로이드에서 사용할 수 있는 이더리움(Ethereum)과 스마트 컨트랙트(smart contract)를 쉽게 활용할 수 있게 해주는 라이브러리
  - ◇ 이더리움(Ethereum)의 JSON-RPC client API의 완벽한 구현이 되어있어 이를 활용하여 자바로 개발된 앱과 이더리움 네트워크와 통신하기 위해 사용
- 브라우니(Browine) 사용한 테스팅
  - ◇ 스마트 컨트랙트(Smart contract)의 Deploy와 Testing을 도와주는 Python 기반 테스트 프레임워크인 브라우니를 사용하여 테스팅

4. 연구 팀의 구성 및 과제 추진 일정

1) 연구진 구성 및 역할

참여자격	성 명	역할
팀장	권재승	· 전체적인 진행을 이끌어나감 · 전체적인 프로토콜 제시 · 스마트컨트랙트 기술을 중심으로 기능 구현
팀원	조성락	· 사설 네트워크 구축 및 환경설정 · 기술을 중심으로 기능 구현
팀원	오하늘	· UI 설계 및 구현 · DID 등록 및 검증 기능 구현

2) 추진 일정

연구 활동	1 학기							
	4/27	5/4	5/11	5/18	5/25	6/1	6/8	6/18
문제 정의서 작성								
Application 요구사항 명세서 작성								
Application use-case 명세서 작성								
UI 프로토타입 제작								
class diagram 작성								
SW 테스팅								
sequence diagram 작성								
1차 프로토타입 Demo								
Survey 및 Monitring								
1차 프로토타입 Demo								
Survey 및 Monitring								
Final 프로토타입 Demo								

- 참고문헌(Reference)

- https://www.youtube.com/watch?v=bleTPilDpb4
- https://decenter.kr/NewsView/1YXTM47UEF/GZ01