

업비트 API 기반
디지털 가상자산 거래소(CEX)
개발 및 자체적 코인 발행



팀명 언체인(un-chain)

조원1 201624526 유상욱

조원2 201624521 용태완

1. 과제의 배경 및 목표	3
1-1. 과제 배경	3
1-2. 과제 목적	4
1-3. 기대 효과	4
2. 세부 구현 목표	5
2-1. 코인 발행	5
2-2. 거래소 구현	5
2-3. 로그인기능 및 인증기능	6
3. 제약사항	7
3-1. 제약사항 분석	7
3-2. 해결 방안	8
4. 개발 환경	9
4-1. vue.js	9
4-2. solidity	9
5. 개발 일정 및 역할 분담	9
5-1. 개발 일정	9
5-2. 역할 분담	10
6. 참고 자료	10

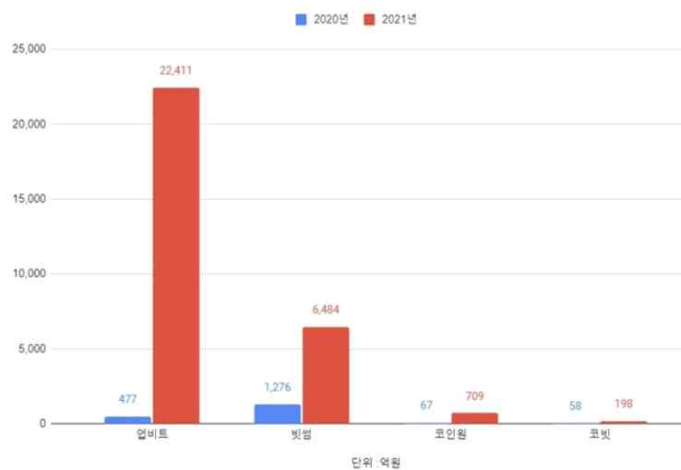
1. 과제의 배경 및 목표

1-1. 과제의 배경

최근 몇 년간 비트코인 및 여러 종류의 알트코인이 등장하였고 언론에서도 많은 주목을 받고 있다. 이에 따라 암호화폐 투자에 관심을 가진 사람들이 계속해서 늘어나고 있으며, 가상화폐의 실용화를 논하게 된 2016년 이래로 코인의 사용처는 계속 늘어나고 있다. 비트코인을 법정화폐로 쓰는 나라도 생겼고, 기부금 납부, 음식점, 영화관, 교육기관 등록금 등 다양한 실생활에 사용되고 있다.

새로운 가상화폐의 종류가 늘어나고 사용처도 늘어나는 만큼, 가상화폐 거래소 또한 늘어나는 추세이다. 실제로 국내 주요 암호화폐 거래소중 하나인 '업비트'는 2022년 현재 수수료 수익이 일일 약 100억원에 달할 만큼 큰 규모가 되었다.

가상화폐 거래소 순익 추이



국내 4대 가상자산 거래소 연간 순이익 추이 / 자료=각사 사업보고서 등

그림 1. 최근 2년 가상화폐 거래소 순익 추이

가상화폐가 상용화 되고있는 만큼, 이에 관련된 지식이나 기술이 다수 필요하게 될 것으로 보인다. 따라서 암호화폐를 직접 만들거나, 거래소를 만들 수 있는 능력은 훌륭한 경쟁력이 될 것이다.

1-2. 과제 목적

본 과제는 거래중개 사이트(업비트)에서 제공하는 API를 받아 코인의 시세 동향 파악 및 매도,매수 기능을 거래소 웹사이트에 구현하고 웹사이트를 운영하는 방식으로 거래소를 만든다.

추가적으로 코인 지갑 보안 시스템, 코인 전송 수수료 실시간 조회/적용, 매수/매도 알림 서비스, 통계 시스템 등을 구현해 실제로 사용되고 있는 코인 거래소와 유사한 역할을 수행할 수 있게 만든다.

거래소 구현 후 이더리움을 기반으로 하여 자체적으로 코인을 발행하고 역할 부여 후 거래소에 등록한다.

1-3. 기대 효과

최근 일어난 스테이블 코인(기존 화폐에 고정적인 가치로 발행되는 암호화폐)인 '루나'관련 사태를 보면, 많은 화폐들이 발행됨에 따라 소위 '사기행위'로 느껴 질 만큼 불합리한 구조를 띤 화폐들도 많이 발행되고 있고 관련한 지식을 충분히 갖고있지 못한다면 이에 충분히 현혹될 수 있을 것이다.

즉, 가상화폐 및 거래소의 이용률에 비하면 제작 및 전문지식을 갖고 있는 사람은 상대적으로 매우 적다는 것이다. 암호화폐의 발행 구조 및 기능을 제대로 알지 못하면 언제든지 이런 위험에 노출 될 수 있다.

또한 화폐 자체의 위험 외에도 거래소에도 위험이 존재 할 수 있다. 암호화폐 자체의 거래 내역은 위조나 해킹이 어렵지만, 거래 및 결제 서비스를 담당하는 거래소는 구현 방식에서의 보안 취약점이 발생할 수 있다.

따라서 해당 과제에서 이더리움 기반으로 가상화폐를 직접 제작해보며 이에 관한 기초적인 지식을 익히고 블록체인의 핵심 기술 중 하나인 스마트 컨트랙트에 대해서도 이해할 수 있을 것이다. 더 나아가서 쉽게 테스트 용 코인을 발행하는 방법에 대한 가이드라인을 만들어 본다면 교육적인 목적으로도 사용할 수 있을 것이다. 추가적으로 거래소에 다양한 인증 시스템(비밀번호 인증 , 카카오 기반 인증 등)을 이용하여 보안 취약점을 극복하는 다양한 방법에 대해서도 학습하는 계기가 될 것이다.

2. 세부 구현 목표

2-1. 코인 발행

이더리움에서 제공한 코드 및 solidity를 통해서 오리지널 코인을 발행한다.

해당 프로젝트에서는 이더리움 기반의 ERC20 토큰을 Open Zeppelin 또는 Token Factory 등의 오픈소스 프로젝트를 기반으로 발행 할 것이며 대략적인 과정은 아래와 같다.

1. metamask(<https://faucet.metamask.io/>) 사이트에서 테스트용 블록체인에 접속하여 테스트용 이더를 수령한다.
2. 이더리움 토큰 사이트(<https://ethereum.org/token>)에서 코드를 받은 뒤 내용을 수정하여 코드를 Remix IDE 사이트(<https://remix.ethereum.org>)에 등록하고 업로드한다.
3. metamask를 이용하여 토큰을 추가하고 발행된 것을 확인한다.
4. 이후 기능을 추가하여 ICO(Initial Coin Offering)을 진행한다.

2-2. 거래소 구현

업비트 api를 활용하여 매도, 매수 기능을 구현하고 간략화된 시세 동향을 제공한다. 또한, 코인마다의 시세 동향을 차트로 시각화하여 제공한다.



그림 2. 업비트 api를 통한 코인 시세 동향 및 차트 구현 예상도

추가적으로 api를 연동한 후 거래소에 추가할 기본 기능들은 아래와 같다.

- 연동 후 업비트의 잔액 조회
- 코인 전송 수수료 실시간 조회/적용
- 매수/매도 알림 서비스
- 입/출금 내역
- 트레이딩 내역
- 회원 통계
- 수수료 수익 통계

2-3. 카카오 api를 통한 간편 로그인기능 및 인증기능 제공

kakao developers에서 제공하는 간편 로그인 api를 활용하여 안전하게 로그인을 진행할 수 있게 한다. 해당 과정은 아래의 순서와 같이 진행된다.

1. 거래소 서버에서 카카오 인증 서버로 인가 코드 받기를 요청하면 카카오 인증 서버에서는 사용자에게 카카오계정 로그인을 통한 인증을 요청한다.
2. 사용자가 카카오계정으로 로그인을 진행하면, 카카오 인증 서버가 사용자에게 '동의' 화면을 출력하여 사용자 동의를 요청한다.
3. 사용자가 원하는 동의 항목에 동의하면, 카카오 인증서버에서 거래소 서버로 Redirect URI로 인가 코드를 전달한다.
4. 거래소 서버가 전달받은 인가 코드로 토큰 받기를 요청하면, 카카오 인증서버가 토큰을 발급하여 전달한다.
5. 발급받은 액세스 토큰으로 사용자 정보 가져오기를 요청하여 로그인 또는 회원가입 과정을 진행한다.

인가 코드 발급 과정

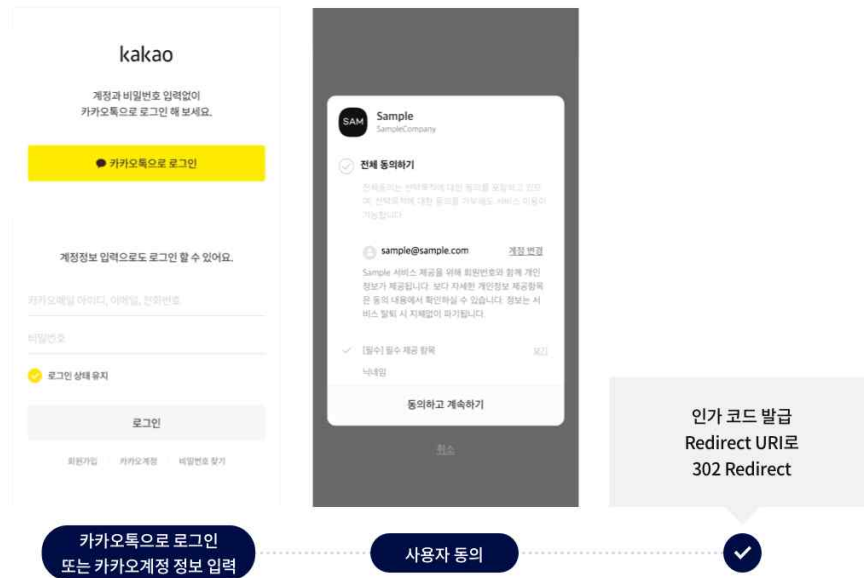


그림 3. 카카오 api를 통한 간편 로그인 과정

추가로이메일/휴대폰 인증 및 거래 비밀번호 인증을 구현한다.

3. 제약사항

3-1. 중앙화 거래소의 문제점

3-1-1. 정보 유출 위험

cex(Centralized Exchange, 중앙화 거래소)는 이름 그대로 운영 방식이 중앙 집중화 되어있다. 따라서, 중앙 거래소가 해킹을 당할 경우, 정보 및 자산의 유출이 dex(Decentralized Exchange, 탈중앙화 거래소)에 비해 쉽다.

3-1-2. KYC(Know Your Cumstomer, 고객 확인 제도)의 번거로움

개인 정보 및 자산의 유출이 dex보다 상대적으로 쉬운 cex에서는
사용자에게 KYC를 요구하는 경우가 많으며, 해당 과정이 이용자에게
번거로울 수 있다.

3-2. 해결 방안

거래소 사이트를 개발할 때, 카카오 api를 통한 로그인 연동 기능을 제
공 할 계획인데, 거래 진행 시 카카오페이 인증을 통해 간단하게 KYC를 진
행하고 카카오페이에서 기존에 계좌 및 본인확인이 된 상태기 때문에 사
이트에 접근할 때 해킹 및 위변조의 위험또한 줄일 수 있을 것이다.

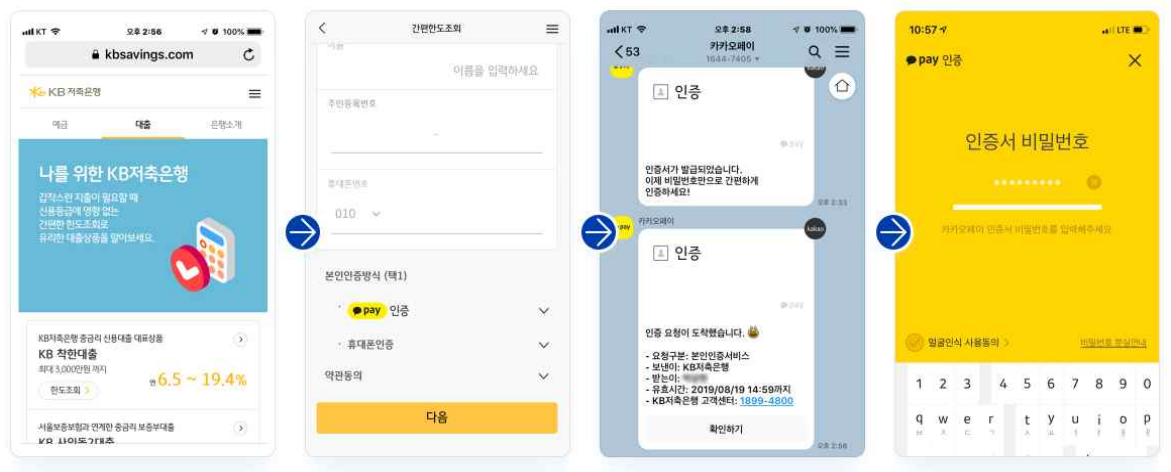


그림 4. 카카오 페이 api를 통한 인증 예시

4. 개발 환경

4-1. vue.js

upbit의 api를 받아와서 이를 이용해 트레이딩 시스템, 코인 시세 차트, 거래 등을 구현하는 코드를 작성한다. 또한 거래소를 만드는 전반적인 과정에서 vue.js를 사용할 계획이다.

4-2. solidity

해당 프로젝트에서는 Remix IDE를 활용하여 이더리움 코인을 발행하고 스마트 컨트랙트를 작성 할 예정이다.

5. 개발 일정 및 역할 분담

5-1. 개발 일정

5월		6월				7월				8월				9월			
3주	4주	1주	2주	3주	4주	1주	2주	3주	4주	1주	2주	3주	4주	1주	2주	3주	4주
거래소, 암호화폐 스터디																	
				거래소 기능 구현 및 UI 제작													
								중간 보고서 작성									
							보안설계 및 UI 디자인 보강										
										코인 개발 및 발행							
														오류 수 정			
														최종 발표/보고서 준비			

5-2. 역할 분담

유상욱	<ul style="list-style-type: none">● 거래소 UI 디자인 설계 및 개발● 업비트 및 카카오(페이,로그인) API 연동● 거래소 시스템 구현
용태완	<ul style="list-style-type: none">● 코인 개발 및 발행● 보안 시스템 구현● 코인 월렛 구현
공동	<ul style="list-style-type: none">● 테스트 및 디버깅● 오류 수정● 보고서, 문서 작성● 발표 심사 및 시연 준비

6. 참고 자료

[1] 이더리움 공식 웹페이지 - 이더리움 토큰 발행 가이드

<https://ethereum.org/en/developers/>

[2] 거래소 영업이익 차트

<https://www.4th.kr/news/articleView.html?idxno=2016424>

[3] kakao developers - API 제공 및 기능 설명

<https://developers.kakao.com/docs/latest/ko/kakaologin/rest-api>