SNU Wallet

목차

- 개요 (SNU 월렛 서비스)
- 프로젝트 목적 및 필요성
- SNS 및 SNU ID 를 이용한 간편로그인
- MPC + TSS 를 사용한 시드구문 관리
- 지원하는 네트워크
- 프로젝트 로드맵
- 팀 소개

SNU 월렛 서비스

사람과 사람 사이를 이어주는 **Social Infra 구축**

- 송금에 대한 진입장벽을 낮춤으로 **실생활 개인 간 교류 활성화**

- SNU Wallet 은 단순히 토큰의 관리 및 전송에 그치는 지갑 솔루션에 국한되지 않고, **모임통장과 같은 공동 지갑 서비스 등의 확장된 서비스 제공을 목표로 하고 있다.**

SNU 월렛 서비스

누구나 자유롭게 가상자산을 수탁 및 예치할 수 있는 비허가형 프로토콜

자체 DB 를 바탕으로 가상자산을 전송하는 내부 입출금 시스템 사용

- 송금이 오프체인(Off-Chain)으로 발생하기 때문에 이용 수수료를 부과하지 않을 수 있고,
  송금 시에 개인의 지갑주소가 노출되지 않는다.

OAuth 방식을 사용하여 간편한 지갑 생성 및 사용

- SNS 계정 연동을 통해 간편하게 지갑을 생성 및 이용할 수 있다.

프로젝트 목적 및 필요성

기존 블록체인 관련 프로젝트의 문제점

- 매우 높은 진입장벽
  - 지갑 생성 및 시드문구 관리
  - 트랜잭션별 수수료 발생
  - 중앙화거래소 사용

- **일상생활 속에서 발생한 문제를 해결하지 못함**

프로젝트 목적 및 필요성

기존 송금 시스템의 문제점

- 개인 간 송금을 위해서는 금결원의 승인을 받은 금융 기관의 인프라를 활용해야 함.
- 해외 송금 시에는 각 국가의 법정화폐를 고려해야하고, 송금 시 국가별 지급결제망을 거쳐야 하는 불편함이 존재.
- 해외에 체류 중인 사람들(ex. 교환학생)이 현지의 사람들과 자산을 주고 받기 위해 복잡한 절차를 거쳐야 함.

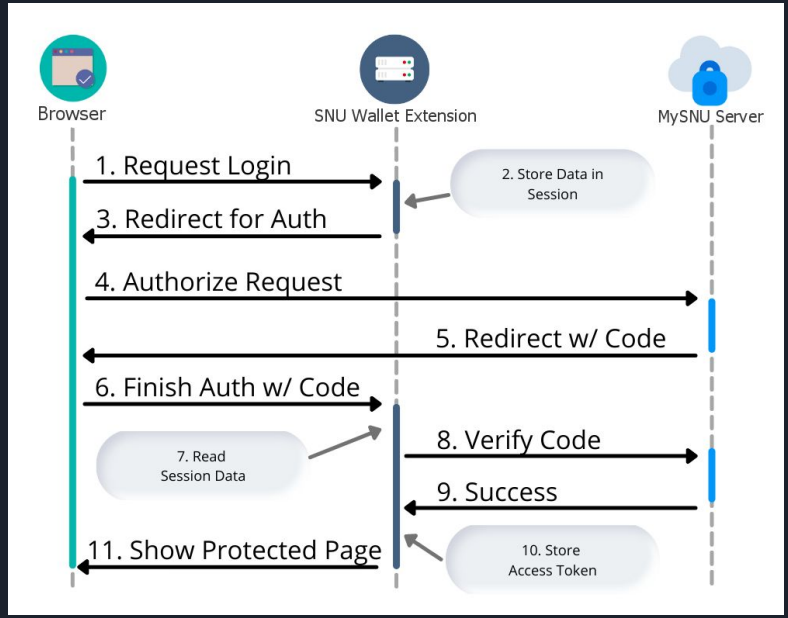
  ➡ **블록체인을 사용한 자체 지급결제망과, SNS 계정 및 SNU ID 를 사용한 간편 로그인 서비스를 제공**

- 가상자산 월렛의 시드구문을 개인이 관리하는 것에 어려움이 존재함.

  ➡ **MPC(Multi-Party Computation)을 활용한 TSS(Threshold Secret Sharing) 방식의 키 관리 기능을 통해 간편한 시드구문 관리 서비스를 제공**

SNS 및 SNU ID 를 이용한 간편로그인

- “SNS 로 로그인" 과 같은 버튼을 통해 로그인 요청 및 SNU wallet 에 로그인 하기 위한 정보를 저장
- 선택한 SNS 경로에서 사용자의 계정 정보를 바탕으로 인증 요청
- 인증 성공 시 access token 을 발급 받을 수 있는 code 를 발급해주고, 사전 합의된 SNU wallet 의 경로로 redirect
- SNU wallet 서버를 거쳐 위의 code 와 함께 사전 합의된 client ID, client secret 을 통해 access token 발급 요청
- 요청 성공 시 발급 받은 access token 을 SNU wallet 의 로그인 정보와 연결하여 저장
- SNS 에 필요한 데이터를 요청하는 경우 이 token 을 바탕으로 SNS 서버와 통신
- 토큰 만료 시 로그아웃 또는 리프레시 요청



MPC + TSS 를 사용한 시드구문 관리

MPC(Multi-Party Computation) 을 활용한 TSS(Threshold Secret Sharing) 방식

- 시드구문(mnenonic)을 서울대학교 정보화본부 내 서버와 DECIPHER 내 서버에 분산하여 관리한다.
- 유저들이 가진 분할된 키 조각들은 다른 유저들과의 상호 작용을 통해 중간 결과를 공유하지만 개인이 가진 별도의 키 조각은 비공개로 유지된다.

MPC + TSS 방식의 이점

- **직접 니모닉을 관리하지 않아도 되므로 불편함이 줄어든다.**
- 시드구문이 서버에 분산되어 관리되므로 특정 서버가 공격을 당하는 경우에도 개인의 지갑이 해킹당할 확률이 줄어든다.
- 부분 서명을 생성하는데 필요한 계산 비용이 감소하므로 자원을 효율적으로 사용할 수 있다.

지원하는 네트워크

SNU Wallet 은 다음과 같은 5가지 네트워크와 이 네트워크를 기반으로 하는 토큰 및 코인을 지원하고 있으며, 목록에 없는 신규 토큰의 경우 토큰의 컨트랙트를 직접 입력함으로써 서비스를 이용할 수 있다.

Bitcoin (BTC)

Ethereum (ETH)

Binance Smart Chain (BSC)

Polygon (MATIC)

Klaytn (KLAY)

프로젝트 로드맵

2023 상반기

- mySNU 계정 연동 월렛 서비스
- mySNU 계정 친구 불러오기 및 친구 간 무료송금 기능 출시
- 5개 네트워크 지원 (비트코인, 이더리움, 바이낸스 스마트 체인, 폴리곤, 클레이튼)

2023 하반기

- 4개 네트워크 추가 지원 (솔라나, 아발란체, 아비트럼, 옵티미즘)
- 친구 간 채팅기능 및 간편송금 기능 출시

2024 상반기

- 3개 메인넷 추가 지원 (라이트코인, 코스모스, 도지코인)
- 공용 지갑 서비스 출시
- 혁신금융서비스 신청 (금융 규제 샌드박스)

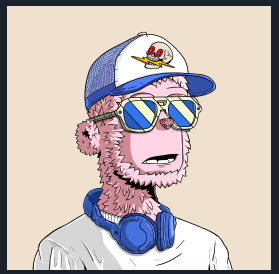
2024 하반기

- 글로벌 버전 월렛 서비스 출시 (한국어, 중국어, 일본어)

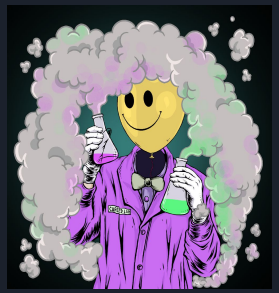
팀 소개

[팀원]

김경은



김무진



송효진

신성헌

홍준일

프로젝트 문의처

E-mail: ocl0601@snu.ac.kr

 @snuwallet

 @snuwallet

 @snuwallet

닉네임

메인 지갑 200,000 KRW

이더리움 메인넷

Tether (USDT) 40 USDT

NEAR Protocol (NEAR) 100 NEAR

동아리 회식비 지갑 500,000 KRW

투자 지갑 2,000,000 KRW

메인 지갑

Main Viewport

Tether (USDT) = 1.00024 USD

테더에 관한 간단한 설명

설명1
설명2

사용가능 50 USDT

총 보유량 50 USDT

스테이킹 0 USDT

락업 0 USDT

SNU 구성원 송금

외부 입출금

입금

출금

내 지갑으로 보내기

내 계좌에서 채우기

닉네임

메인 지갑 3,200,000 KRW

이더리움 메인넷

Tether (USDT) 40 USDT

NEAR Protocol (NEAR) 100k NEAR

동아리 회식비 지갑 500,000 KRW

투자 지갑 2,000,000 KRW

메인 지갑

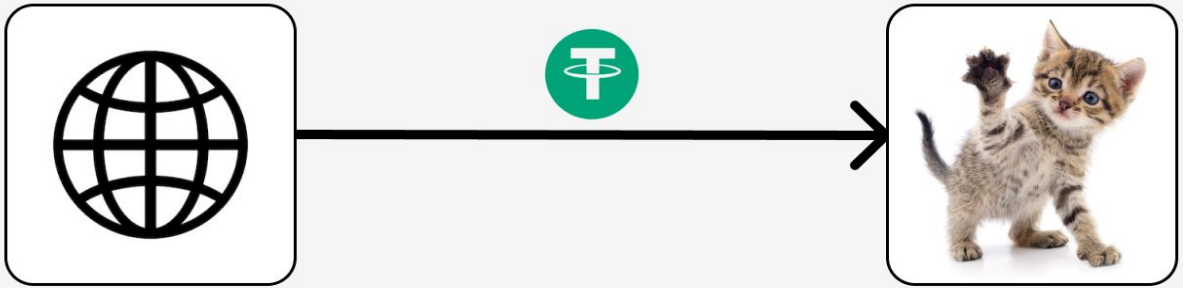
Main Viewport

진행 중

문제 발생 (원인 제공)

입금 대기중

외부로부터 Tether (USDT) 입금



메인넷	ERC20
지갑 주소	0×4a4...

입금 상태

완료 !

닉네임

메인 지갑 200,000 KRW

이더리움 메인넷

Tether (USDT) 40 USDT

NEAR Protocol (NEAR) 100 NEAR

동아리 회식비 지갑 500,000 KRW

투자 지갑 2,000,000 KRW

메인 지갑

Main Viewport

Tether (USDT) 외부로 출금

메인넷 ERC20

지갑 주소 0×41a...

출금 토큰 수 1000 USDT

출금하기

닉네임

메인 지갑 200,000 KRW

이더리움 메인넷

Tether (USDT) 40 USDT

NEAR Protocol (NEAR) 100 NEAR

동아리 회식비 지갑 500,000 KRW

투자 지갑 2,000,000 KRW

메인 지갑

Main Viewport

Tether (USDT) 외부로 출금

메인넷 ERC20

지갑 주소 0×41a...

출금 토큰 수 1000 USDT

출금까지 10초

출금 취소

닉네임

메인 지갑 200,000 KRW

이더리움 메인넷

Tether (USDT) 40 USDT

NEAR Protocol (NEAR) 100 NEAR

동아리 회식비 지갑 500,000 KRW

투자 지갑 2,000,000 KRW

메인 지갑

Main Viewport

진행 중

문제 발생
(원인 제공)

출금 대기중

Tether (USDT) 외부로 출금

메인넷 ERC20

지갑 주소 0×41a...

출금 토큰 수 1000 USDT

출금 상태

완료 !

닉네임

메인 지갑 200,000 KRW

이더리움 메인넷

Tether (USDT) 40 USDT

NEAR Protocol (NEAR) 100 NEAR

동아리 회식비 지갑 500,000 KRW

투자 지갑 2,000,000 KRW

메인 지갑

Main Viewport

Tether(USDT) 구성원 간 송금

구성원 syuka@snu.ac.kr

이름 전석재

송금 토큰 수 1 USDT

송금하기

닉네임

메인 지갑 200,000 KRW

이더리움 메인넷

Tether (USDT) 40 USDT

NEAR Protocol (NEAR) 100 NEAR

동아리 회식비 지갑 500,000 KRW

투자 지갑 2,000,000 KRW

메인 지갑

Main Viewport

Tether(USDT) 구성원 간 송금

구성원 syuka@snu.ac.kr

이름 전석재

송금 토큰 수 1 USDT

송금 상태

완료 !