S N U W A L L E T

블록체인의 실무응용 1

김경은, 김무진, 송효진, 신성헌, 홍준일

SNU WALLET: Social based Blockchain Wallet Service

초록. SNU 월렛은 가상자산을 자유롭게 수탁 및 예치할 수 있는 월렛으로, 이용자는 누구나 자유롭게 월렛을 생성 및 사용할 수 있는 비허가형 프로토콜이다. SNU 월렛을 사용함으로써 사람들은 **연락처 목록에만 있다면 지인, 친구 그리고 가족에게 간단한 방법으로 가상자산을 전송**할 수 있으며 여타의 가상자산 월렛과는 다르게 전송 시에도 **수수료는 부과되지 않는다.** 또한 송금을 하면서 지갑주소가 노출될 걱정을 하지 않아도 된다. 이를 위해 자체 DB 를 바탕으로 가상자산을 전송하는 **내부 입출금 시스템을 구축**하였으며, SSO(Single Sign On) 방식으로 지갑서비스에 접근할 수 있도록 Web3Auth 의 솔루션을 차용하였다. 또한 본 프로젝트는 단순 토큰의 전송만 제공하는 지갑 솔루션에 국한되지 않고 나아가 계모임, 모임통장과 같이 공동 지갑 등의 서비스 제공을 계획하고 있으며 사람과 사람 사이를 이어주는 Social Infra 구축을 목표로 하고 있다.

1. 소개

블록체인의 미래는 밝을까. 최근 2023 년 3 월 Pew Research Center 는 미국인들을 대상으로 암호화폐(Cryptocurrency)에 관한 설문조사를 진행하였는데, 암호화폐를 알고 있다고 응답한 88%의 응답자 중, 4 분의 3 이 현재 암호화폐 투자, 거래, 사용 방식을 신뢰할 수 없으며 그것이 안전하다고 확신하지 못한다 답했다.[1] 또한 2022 년 온라인 웹 플랫폼인 CouponFollow 에서 수행한 설문조사에 따르면 응답자 중 42%는 디지털자산의 가치에 대해 이해할 수 없다고 밝혔고, 35%는 디지털자산이 마치 사기와 같다고 응답했다.[2] 가상자산과 관련한 돈세탁, 해킹, 범죄행위 등이 연일 미디어를 통해 다뤄지면서 국내에서의 가상자산에 대한 인식이 크게 다르지 않을 것이라고 조심스레 짐작해볼 수 있다.

하지만 블록체인과 가상자산에 대해 부정적인 인식만 존재하는 것은 아니다. 마찬가지로 2022 년 4 월 StarkWare 에서 수행한 설문조사에 따르면 응답자의 53%는 암호화폐를 "금융의 미래"로 생각하며, 심지어 젊은 연령대(25 세 - 34 세 사이)에서는

[1] https://www.pewresearch.org/short-reads/2023/04/10/majority-of-americans-arent-confident-in-the-safety-and-reliability-of-cryptocurrency/

[2] https://cryptopotato.com/the-reasons-why-some-crypto-skeptics-have-not-entered-the-market-survey/

이러한 인식이 68%에 달하며[3] 청년층의 가상자산 및 블록체인에 대한 기대감을 확인할 수 있었다. 결국 상기 3 개의 설문조사를 종합해보면 블록체인의 장점을 십분 활용하여 대중의 니즈를 충족시켜줄 서비스가 필요함을 추론해볼 수 있다. 하지만 현재의 블록체인 기반 서비스는 대체로 현실세계에서 발생한 어려움을 해결하는 것보다는 자체적인 생태계를 구축함으로써 현실세계와는 다소 동떨어진 행보를 보이고 있다. 따라서 본 프로젝트는 블록체인과 현실세계를 이어줌으로 현실세계에서 발생한 니즈를 포착하고 이를 충족하기 위해 탄생했다.

블록체인의 장점 중 하나는 바로 그 자체로 지급결제망을 제공해준다는 것이다. 통상적으로 한 사람이 다른 사람에게 돈을 전송하기 위해서는 그것을 처리해주는 지급결제망을 필요로한다. 가령 모바일송금 어플리케이션을 통해 송금을 하기 위해서는 이를 처리해주는 은행의 지급결제시스템과 은행간 자금 이동을 처리해줄 금융결제원의 인프라가 뒷받침되어야 한다. 또한 지급결제시스템은 한 국가의 법정화폐를 단위로 존재하며 이에 따라 한국에서 미국에 있는 사람에게 현금을 지급하기 위해서는 한국의 지급결제망을 거쳐 미국의 지급결제망까지 도달해야 한다. 하지만 블록체인은 다르다. 블록체인을 통해 희망하는 거래를 제출하고 해당 거래가 처리된 다음 수많은 개인에 의해 거래가 확정 및 저장되어 그 자체로 지급결제 업무가 완결된다. 따라서 블록체인을 활용한다면 서로 다른 나라에 사는 사람들이 보다 자유롭고 편리하게 자금을 전송하고 받을 수 있다. 본 SNU 월렛은 이러한 블록체인의 이점을 바탕으로 서울대학교 구성원들끼리 가상자산을 간단하고 편리하게 송금할 수 있는 서비스를 제공하고자 한다. 특히, 서울대학교 구성원 중에서도 서로 다른 지급결제망을 사용하는 서울대학교 재학생들과 외국인 교환학생들이 서비스 주 대상자이다.

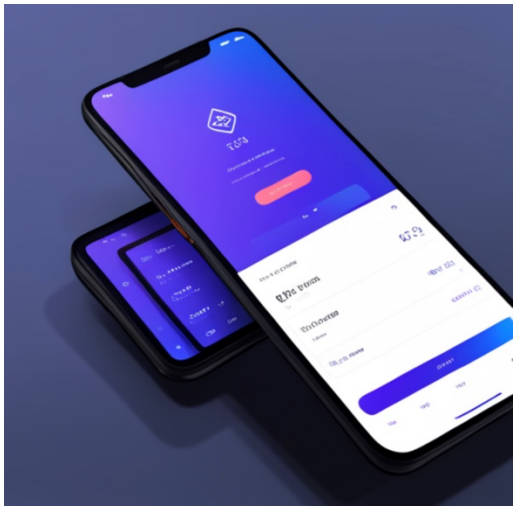
가상자산 월렛을 사용하기 위해서는 몇 가지 난관이 존재한다. 그 중 가장 큰 난관은 바로 '시드구문' 관리이다. 체이널리시스의 2017 년 리포트에 따르면 최소 2.78M 최대 3.79M 비트코인이 잃어버린 상태[4]라고 한다. 즉, 지갑 키관리를 제대로 하지 못하여 사용할 수 없는 비트코인만 원화 기준 100 조원에 달하고, 2,100 만개인 비트코인의 최대 공급 대비 15% 수준이다. 이처럼 과거부터 지갑의 시드문구를 개인이 관리하는 것에는 어려움이 있었고, 대중의 블록체인에 대한 거대한 난관으로 작용하게 되었다. 본 SNU 월렛에서는 Web3Auth 의 솔루션을 활용하여 MPC(Multi-Party Computation)을 활용한 TSS(Threshold Secret Sharing)방식의 키 관리를 제공하며, 해당 내용에 대한 상세한 설명은 다음 장에서 다룰 예정이다. 해당 방식을 차용함으로써 사람들은 누구나 자신의 SNS 계정을 통해 지갑을 손쉽게 만들 수 있으며 시드문구 역시 간편하게 관리할 수 있다.

---

[3] https://cryptopotato.com/over-50-of-americans-believe-crypto-will-be-the-future-of-finance-survey/

[4] https://www.bankrate.com/investing/how-to-recover-lost-bitcoins-and-other-crypto/

2. 기술적 개요

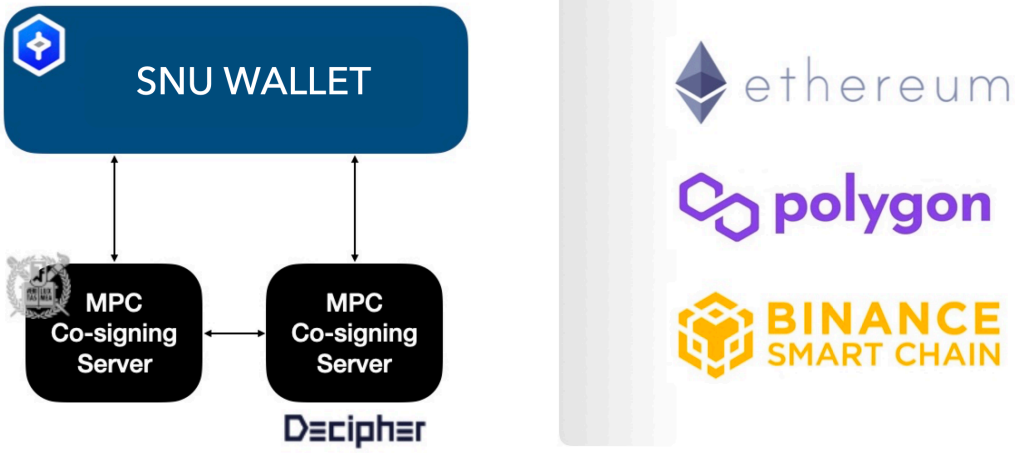


Wallets with a better user experience
니모닉 없는 복구, 쉬운 설치

Wallets with Social Networking
mySNU, 카카오톡 계정으로 친구찾기/추가

Wallet to Transfer asset with Global Friends
친구간 간편 무료송금 서비스

MPC(Multi-Party Computation) 기술은 시드문구를 여러 개로 쪼개어 관리하는 방법을 말한다. MPC 는 암호화폐 월렛에 보안과 효율성을 제공하기 위해 사용되며, 지갑의 키 관리 및 트랜잭션 승인과 관련된 작업을 수행하는 데 사용된다.



키가 분할되고 조합되는 과정은 아래와 같다.키가 분할되고 조합되는 과정은 아래와 같다.

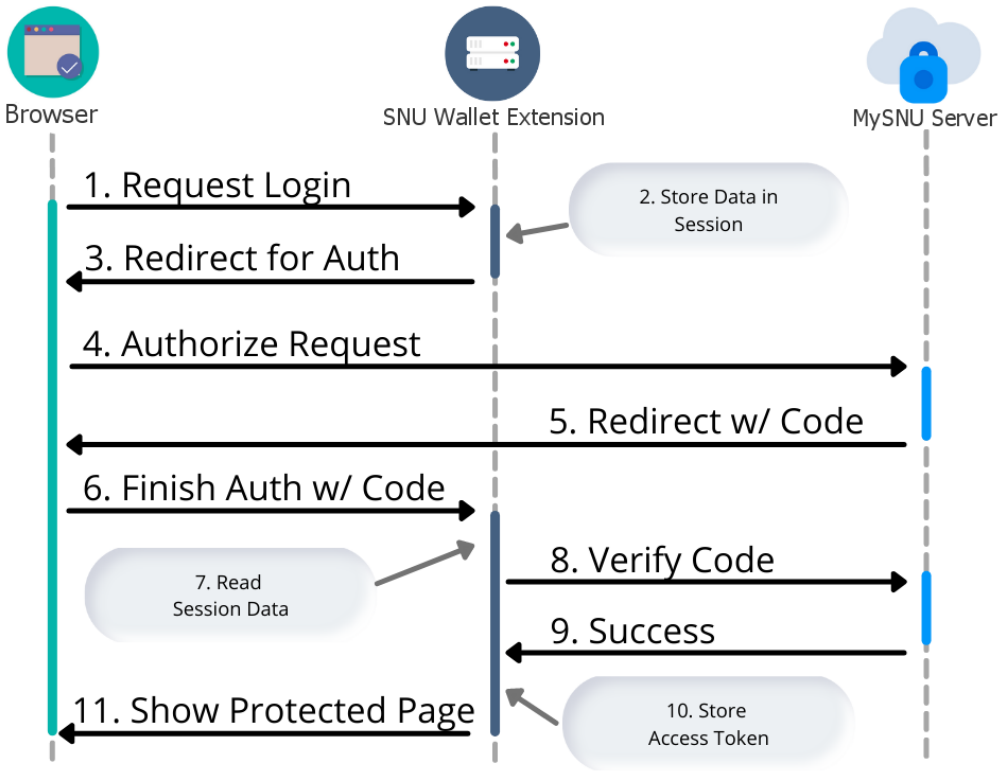
1. 키분할: 개인 키는 여러 참가자들이 별도로 계산할 수 있도록 여러 개의 비밀 조각으로 분할됩니다. 각 참가자는 자신의 키 분할을 저장하고 보호합니다. SNU 월렛은 서울대학교 정보화본부 와 서울대 블록체인 학회 'DECIPHER'에 각각 서버를 두어 키를 분할하여 관리합니다.

2. 분산 계산: SNU 월렛유저들은 분할된 키를 사용하여 트랜잭션 서명과 같은 암호 연산에 참여합니다. 유저들은 서로 상호 작용하여 결과를 얻는 중간 결과를 공유하지만, 각자 별도의 키 조각은 비공개로 유지됩니다.
3. 복구 및 조합: 각 유저들이 제공한 중간 연산 결과들을 조합하여 최종 결과를 얻습니다. 이 과정에서 유저들의 개인 키 조각이 노출되지 않으면서도 정확한 결과를 계산할 수 있습니다.

MPC 기술을 활용하여 우리는 다음과 같은 장점을 가질 수 있다.

- 보안성: MPC 를 사용하면 개인 키를 분할하여 다양한 거래소 또는 배포된 서버에 저장할 수 있으므로 특정 장소가 공격당할 경우에도 도난이 막아집니다.
- 비용 절감 및 효율성: 부분 서명을 생성하는데 필요한 계산 비용이 감소하며, 사용자들이 각자 보관하는 키 조각에 여러 참가자 간의 협력을 요구하는 연산을 수행할 수 있습니다.
- 사용 편의성: MPC 로 생성된 트랜잭션 서명을 이용하면 사용자는 개인 키를 직접 관리하지 않고도 자산을 안전하게 이용할 수 있습니다.
- SNS, mySNU 를 통한 가입/로그인

SNU_ID 계정 로그인 프로세스



3. 사용자 경험

- SNU WALLET 사용 방법
- 사용자 인터페이스 설명
- 편의성 및 기능성 평가
- 사용자 문제 해결 방법

상기 항목들은 SNU WALLET 기획안 및 화면설계서를 통해 확인이 가능하다.

SNU WALLET 에서 지원되는 네트워크

Bitcoin BTC	
Ethereum ETH	
Binance Smart Chain BNB	
Polygon MATIC	
Klaytn KLAY	

SNU 월렛은 상기 네트워크를 기반으로 하는 토큰의 입출금 및 거래를 지원하고 있으며, 월렛의 토큰목록에 없는 신규 토큰의 경우 토큰의 컨트랙트를 입력함으로써 자산의 확인 및 모든 서비스를 이용할 수 있다.

가상자산의 입출금 확인

블록체인 메인넷을 기반으로 한 토큰의 전송 등은 아래의 네트워크별 블록탐색기를 통해 확인할 수 있다. 단, SNU 월렛을 활용하여 수수료가 발생하지 않은 전송 건은 블록탐색기를 통해 확인이 불가능하다.

- **Bitcoin** : https://blockchair.com/bitcoin
- **Ethereum** : https://etherscan.io
- **Binance Smart Chain** : https://bscscan.com
- **Polygon** : https://polygonscan.com
- **Klaytn** : https://scope.klaytn.com

4. SNU WALLET 입출금 비용

SNU 월렛에서 발생하는 비용은 오로지 SNU 월렛에서 지인이 아닌 대상에게 가상자산을 전송할 때이다. 각 메인넷별 수수료는 상이하며, 블록체인 네트워크의 혼잡도에 따라서 수수료는 변동할 수 있다. 2023 년 상반기 기준 기본 수수료는 다음과 같다.

- **Bitcoin :** 0.0018 BTC
- **Ethereum :** 0.0014 ETH
- **Binance Smart Chain :** 0.0002 BNB
- **Polygon :** 0.05 MATIC
- **Klaytn :** 0.5 KLAY

네트워크가 과도하게 혼잡할 경우 별도의 공지를 통해 안내 후 수수료가 인상될 수 있다. 또한 네트워크의 업그레이드, 하드포크 등이 발생할 경우 SNU 월렛과 외부 월렛 사이 입출금에 제한이 생길 수 있다. 해당 경우에도 별도의 공지를 통해 사전 안내가 제공되며 입출금이 제한되는 시기에 발생한 입출금 건에 오류가 발생할 수

있으며 본 **SNU WALLET 에서 해당 오류에 대처할 수 있는 부분은 제한적이므로 이용자들은 공지사항을 준수하여야 한다**.

비즈니스 파트너쉽 및 전략

- SNU-ID 통합인증
- 서울대학교 정보화본부 서버 사용 파트너십 체결
- 디사이퍼 서버 사용 파트너십 체결

최초 서비스는 서울대학교 외국인 교환학생들을 대상으로 진행할 예정이며, 이에 따라 서울대학교 정보화본부 및 MPC 활성화를 위한 디사이퍼 등과 파트너십을 체결할 예정이다.

5. 기타

프로젝트 로드맵

- 2023 년 상반기
  - mySNU 계정 연동 월렛 서비스
  - mySNU 계정 친구 불러오기 및 친구 간 무료송금 기능 출시
  - 5 개 네트워크(비트코인, 이더리움, 바이낸스 스마트 체인, 폴리곤, 클레이튼) 지원

- 2023 년 하반기
  - 친구 간 채팅기능 및 간편송금 기능 출시
  - 4개 메인넷 추가 지원 : 솔라나, 아발란체, 아비트럼, 옵티미즘

- 2024 년 상반기
  - 3 개 메인넷 추가 지원 : 니어, 코스모스, 도지코인
  - 공용 지갑 서비스 출시
  - 대한민국 혁신금융서비스 신청 (금융 규제 샌드박스)

- 2024 년 하반기
    - 글로벌 버전 월렛 서비스 출시
        - 지원 언어 : 한국어, 중국어, 일본어
- 2025 년
    - ISMS 인증 및 VASP 인가 도입 준비

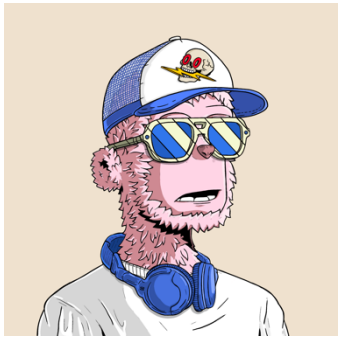
프로젝트 문의처

- 이메일 : ocl0601@snu.ac.kr
- SNS
    - Twitter : @snuwallet
    - Telegram : @snuwallet
    - Instagram : @snuwallet

6. Back Cover

팀원 소개


<김 경 은>


<김 무 진>


<송 효 진>


<신 성 헌>


<홍 준 일>