

Pomeranian Wallet 발표

2022. 08. 29.



01 프로젝트 개요

- Pomeranian
- 문제점
- 해결책

02 기획 & 설계

- 목표 서비스 구성도
- Business Process
- Flow chart

03 구현

- 개발일정 & 소스코드
- Client
- Smart Contract

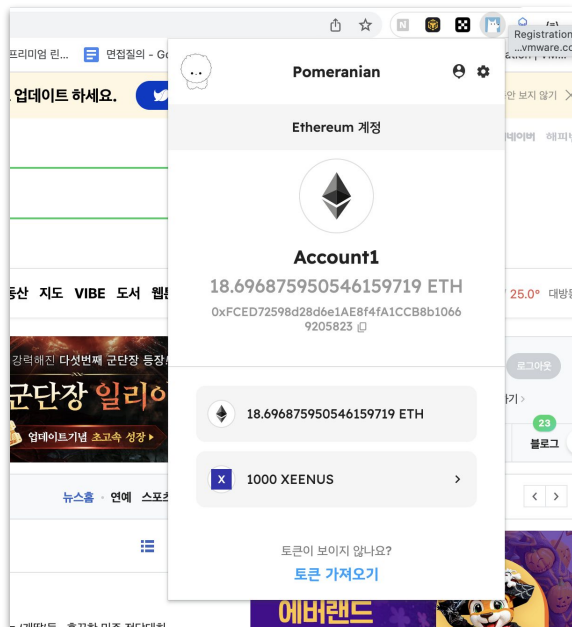
04 데모

- 시연
- 업데이트 계획

1. 프로젝트 개요

1-1

Pomeranian wallet



모아보자

여러 메인넷을 잘 모아놓은 누구나 쓰기 쉬운 지갑 서비스

심플한

직관적인

유연한

- 밝은 배경과 심플하고 직관적인 디자인
- 비트코인 이더리움 솔라나 등 체계가 다른 체인과의 연동성
- 데이터의 로컬화로 보안성 ↑
- 백업에 대한 문제를 기술적으로 해결

1. 프로젝트 개요

1-2

Problem?

메타마스크 등 지갑 플랫폼들은 Mnemonic을 통해 복원을 하더라도 Private key만 복원이 된다.
problem. 내가 지갑 플랫폼에 여러 메인넷의 지갑들과 토큰들을 등록하더라도 복원을 할 수 없다.

Mnemonic이 무엇인가요?

Mnemonic (니모닉)이란, 지갑을 복구하기 위한 12 단어입니다. 쉽게 설명하자면, Private Key가 너무 복잡한 단어들로 구성되어있기 때문에, 이를 쉽게 입력할 수 있도록 갖춰진 형식입니다.

METAMASK
< 뒤로

비밀 복구 구문으로 계정 가져오기

금고를 복구하려면 비밀 구문을 여기에 입력하세요.

비밀 복구 구문 제 구문은 12개의 단어로 이루어져 있습니다

비밀 복구 구문 전체를 아무 입력만으로도 불러낼 수 있습니다

1.	<input type="text"/>	2.	<input type="text"/>	3.	<input type="text"/>
4.	<input type="text"/>	5.	<input type="text"/>	6.	<input type="text"/>
7.	<input type="text"/>	8.	<input type="text"/>	9.	<input type="text"/>
10.	<input type="text"/>	11.	<input type="text"/>	12.	<input type="text"/>

1. 프로젝트 개요

1-3

Solution!

백업 데이터의 '암호화'와 고객의 '선택'으로 문제점의 해결



ethereum

- 보안 **上**
- 탈중앙화 **上**
- 수수료 **↑**
- 관리 **↓**



HYPERLEDGER
FABRIC

- 보안 **中**
- 탈중앙화 **中**
- 수수료 **中**
- 관리 **中**

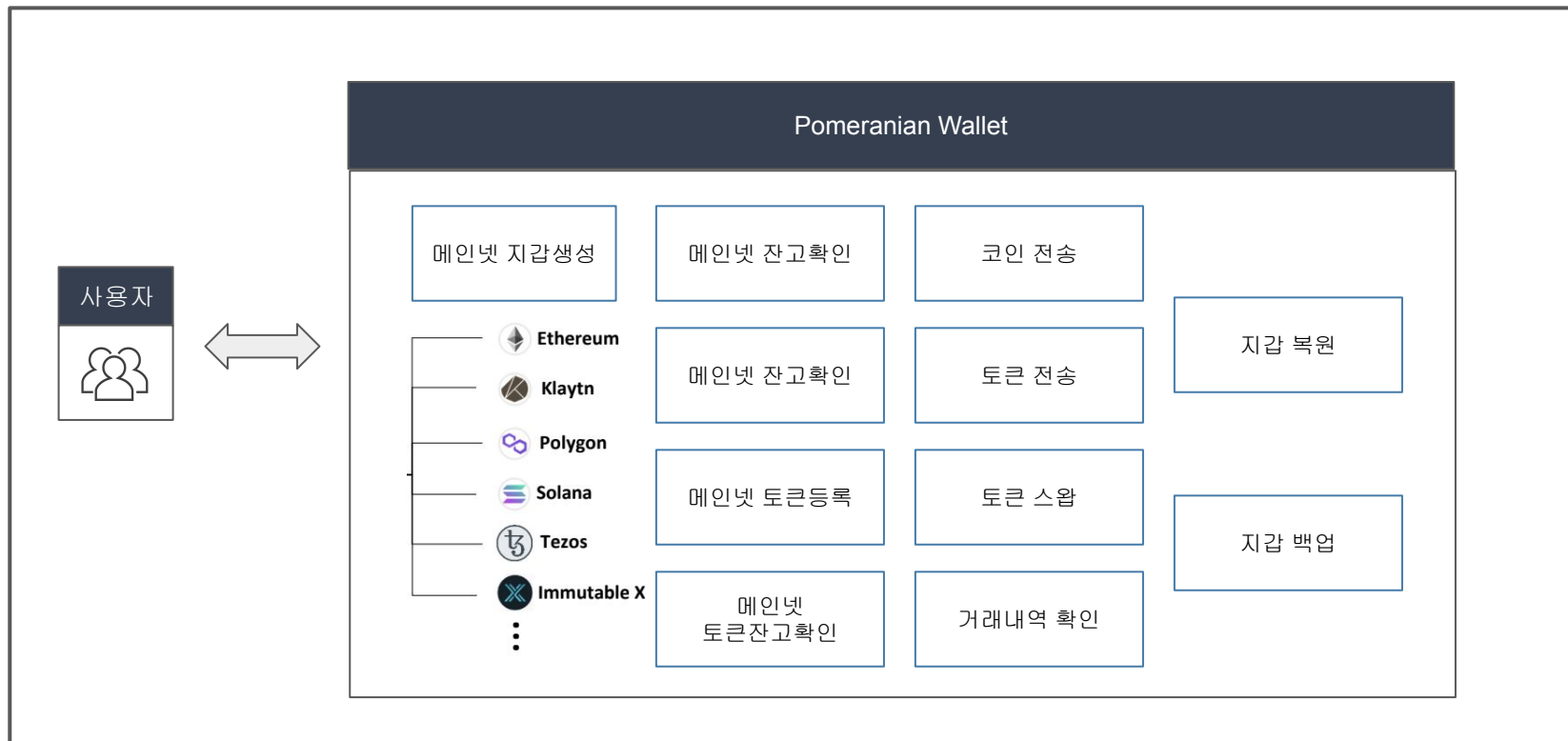


- 보안 **↓**
- 중앙화
- 수수료 **中**
- 관리 **上**

2. 기획 & 설계

2-1

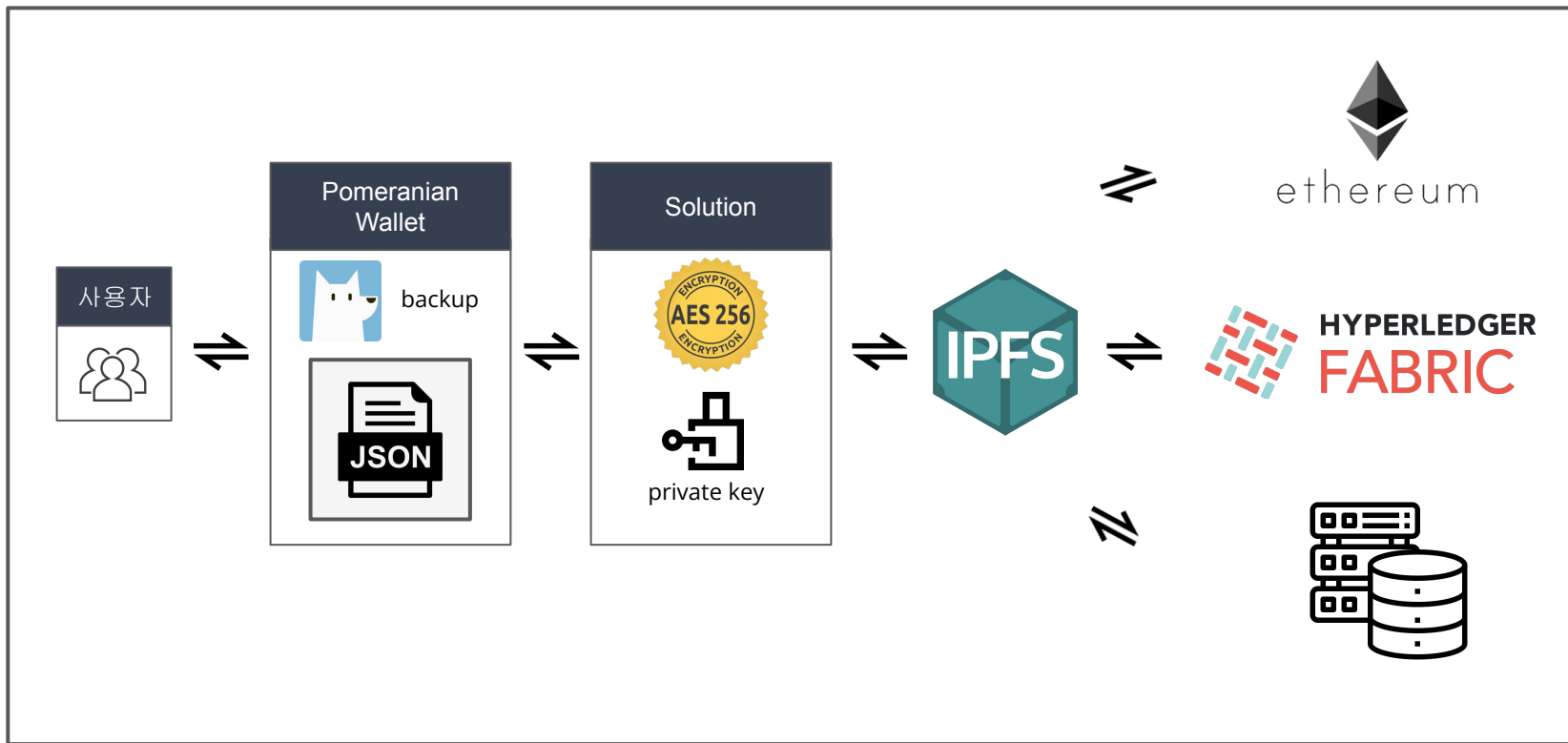
목표 서비스 구성도



2. 기획 & 설계

2-2

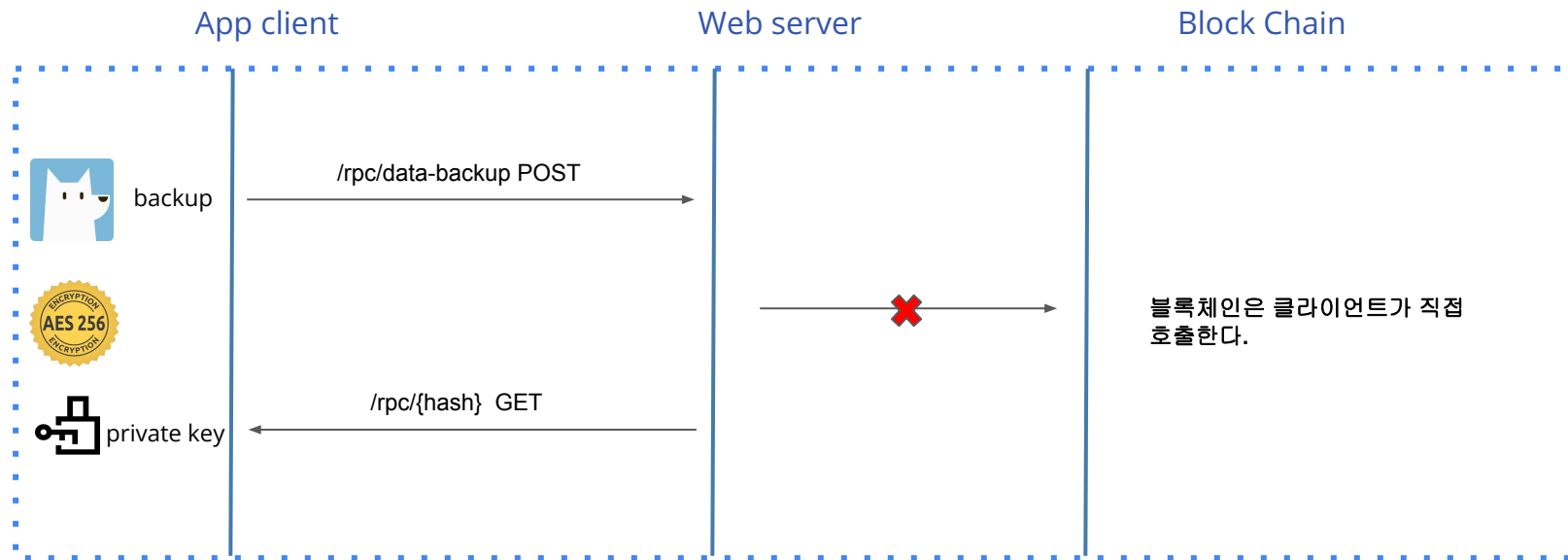
Business Process



2. 기획 & 설계

2-3

Flow chart



3. 구현

3-1

개발일정 & 소스코드

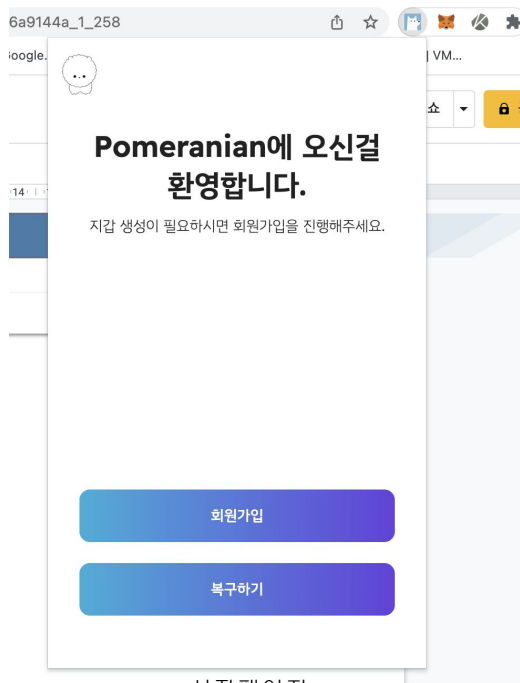


Github 주소 : <https://github.com/tyrannojung/Pomeranian>

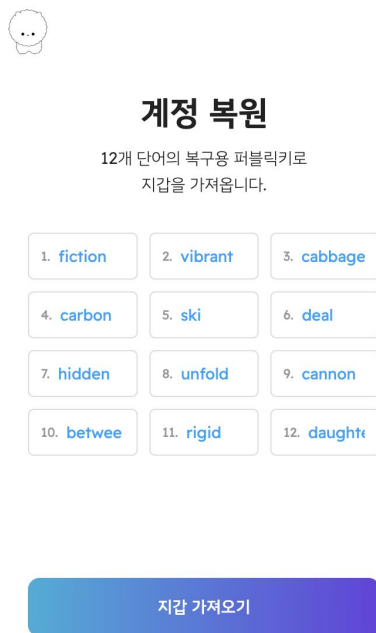
[illegible]

3-2

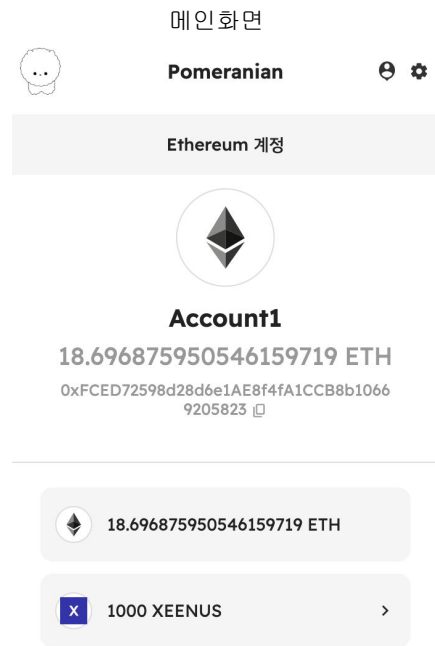
Client



시작페이지



복원



토큰이 보이지 않나요?

[토큰 가져오기](#)

3-2

Client



Pomeranian



토큰 가져오기

사용자 정의 토큰



기존 토큰의 가짜 버전 생성을 포함하여 누구나 토큰을 생성할 수 있습니다.
사기 및 보안 위험에 주의하세요.

0xc6fDe3FD2Cc2b173aEC24cc

조회

YEENUS

8

맞춤형 토큰 추가

토큰조회



Pomeranian



보안 및 개인정보 보호

시드 구문 보기



지갑 데이터 백업 (Public)



지갑 데이터 백업 (Private) - 준비중

백업 유형



백업

Ethereum Network Backup

본인의 데이터와 대칭키로 암호화 하여 이더리움 네트워크에 저장합니다.

주의: 체인에 데이터를 저장하므로 약간의 수수료가 발생합니다.



예상가스요금 :
0.000059094018082764 ETH

완료

3-3

Smart Contract

Contract 주소 : 0x51a652a26B2BA5276321565B2ca4860184634940

```
contract > backup.sol X
contract > backup.sol
1 // SPDX-License-Identifier: MIT
2 pragma solidity ^0.8.12;
3
4 contract backup {
5
6     mapping(address => string) private userBackupMap;
7
8     function setBackupData(address key, string memory backup) public {
9         userBackupMap[key]=backup;
10
11     }
12
13     function getBackupData(address key) public view returns (string memory){
14         return userBackupMap[key];
15     }
16 }
17
18 }
```

체인코드



Rinkeby Testnet Network

All Filters

Search by Address / Txn Hash / Block / Token / Ens



Home

Blockchain

Tokens

Misc

Rinkeby

Contract 0x51a652a26B2BA5276321565B2ca4860184634940

Contract Overview

Balance: 0 Ether

More Info

My Name Tag: Not Available

Contract Creator: 0xfced72598d28d9e1ae... at txn 0x4ccf9247ca1578944ae...

Transactions

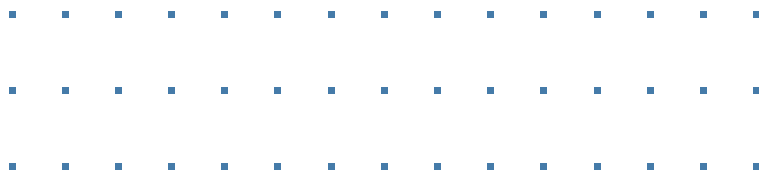
Latest 9 from a total of 9 transactions

Txn Hash	Method	Block	Age	From	To	Value	Txn Fee
0x81687ad2b9c5cc1f63e...	0x8116880	11268960	2 days 5 hrs ago	0xb62f69c4ed0cda4a...	0x51a652a26b2ba52763...	0 Ether	0.00003657
0xd238adecbda8950924...	0x8116880	11268933	2 days 5 hrs ago	0xb62f69c4ed0cda4a...	0x51a652a26b2ba52763...	0 Ether	0.00003657
0x12aa1a3d0966767927...	0x8116880	11268915	2 days 5 hrs ago	0xb62f69c4ed0cda4a...	0x51a652a26b2ba52763...	0 Ether	0.00003657

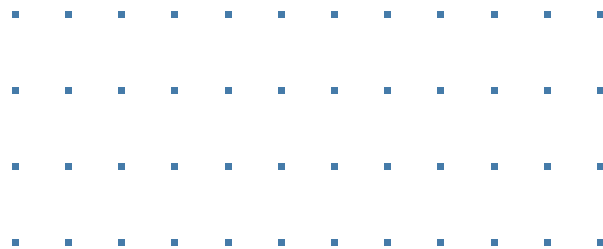
Rinkeby

4-1

시연



프로젝트 시연



4-2

업데이트 계획

.....
.....
.....

업데이트 계획

.....
.....
.....
.....

Pomeranian

X

Dawoon Jung



감사합니다