

블록체인 시스템 엔지니어 양성과정 최종프로젝트

WALLET & SCAN



CONTENTS

- 001 개발자 소개
- 002 프로젝트 소개
 - EtherWallet
 - EtherScan



Part 1.

Developer Introduction



개발자 소개



윤창흠

맡은 역할
Back End

사용 기술
JS / Node.js / EJS / Web3.js /
jQuery / MySQL



조현걸

맡은 역할
Back End

사용 기술
JS / Node.js / EJS / Web3.js /
jQuery / MySQL



남이은

맡은 역할
Front End

사용기술
HTML5/ CSS / JS / jQuery



이지영

맡은 역할
Front End

사용기술
HTML5/ CSS / JS / jQuery

Part 2.

EtherWallet



EtherWallet 이란?



- EtherWallet은 암호화폐 자산 중 이더리움을 보관하기 위한 소프트웨어 프로그램을 의미
- Web3라이브러리를 통해 이더리움을 주고 받거나 본인 지갑의 개인 키, 공개 키, 그리고 자산을 관리할 수 있음

EtherWallet 개발 목적



- 기본적인 dApp 개발에 대한 이해
- 기본 기능 구현을 통한 지갑 구조 이해
- 블록체인 기술에 있어 개인키 관리의 중요성 확인

EtherWallet 회원가입



Create Wallet



userID

Password

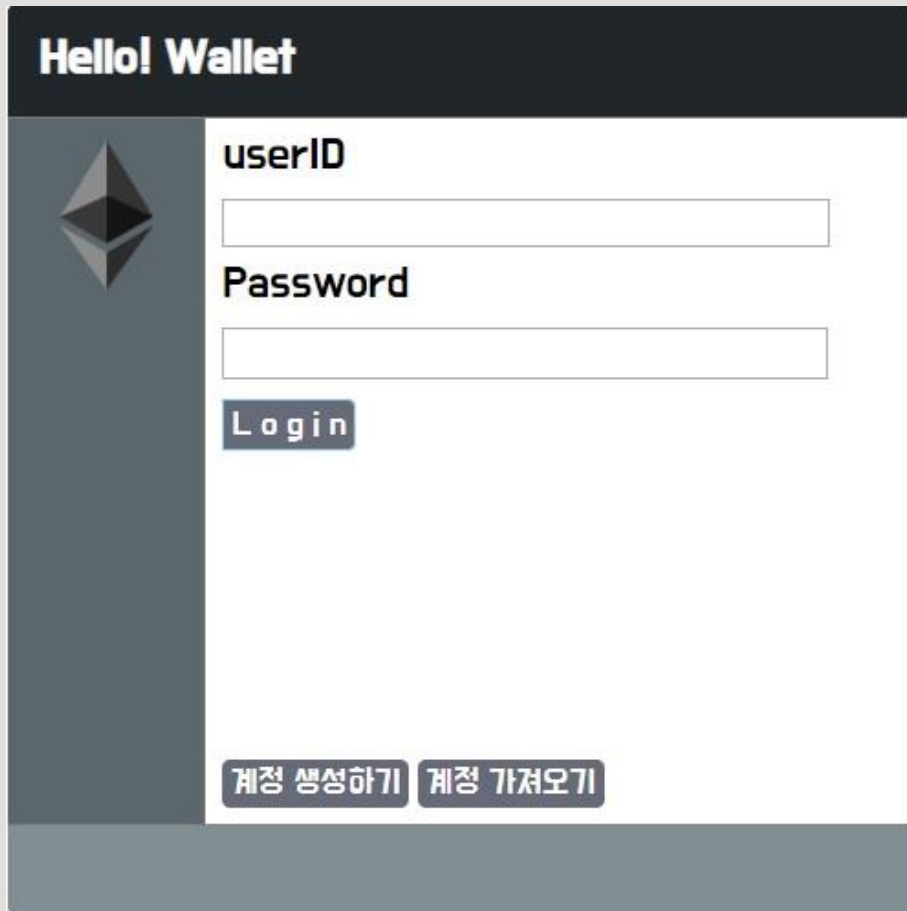
Password 확인

Create

뒤로가기

- 사용자 password와 생성된 privatekey는 암호화 후 database에 저장
- 계정 생성시 publickey와 privatekey 생성
- 중복된 ID, privatekey에 관한 error처리
- ID/ Password 정규식 적용

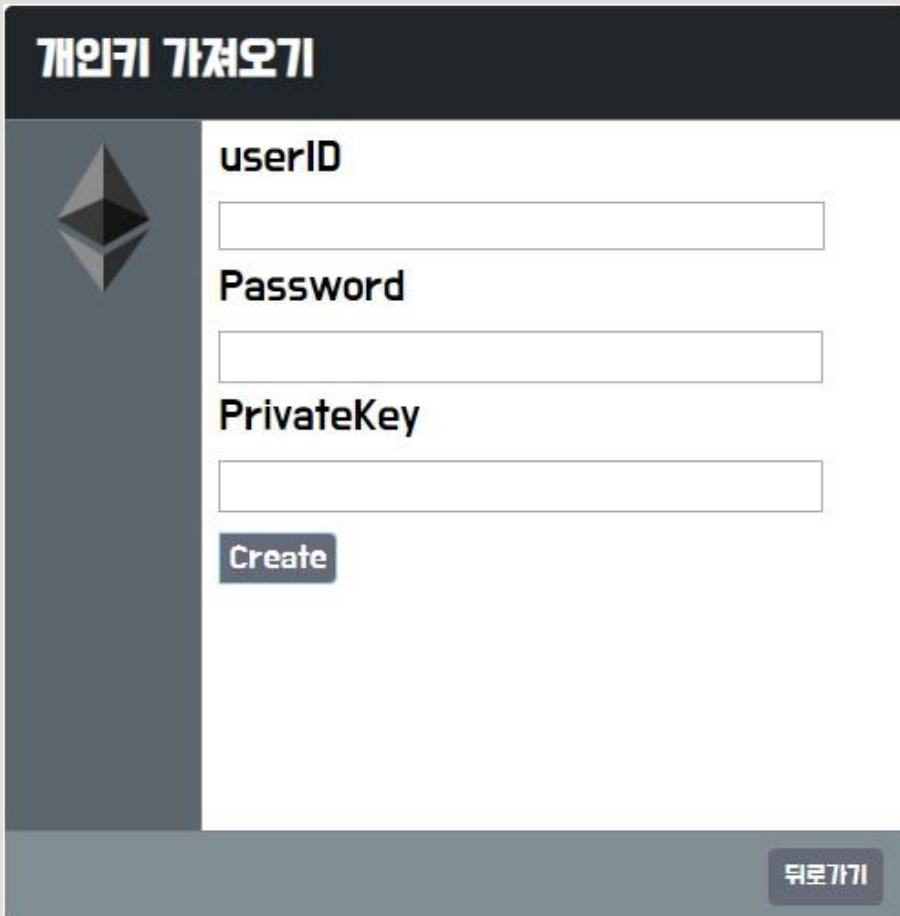
EtherWallet 로그인



The screenshot shows the EtherWallet login page. At the top, there's a dark header with the text "Hello! Wallet". Below this, on the left, is the Ethereum logo. To the right of the logo are two input fields: "userID" and "Password". Below the "Password" field is a "Login" button. At the bottom of the form area, there are two buttons: "계정 생성하기" (Create Account) and "계정 가져오기" (Import Account).


- ID / Password를 통한 로그인
- Database에 저장된 password를 복호화하여 사용자가 입력한 값과 비교
- ID, Password 잘못 입력 시 error처리

EtherWallet 개인키 가져오기



The image shows a web form titled '개인키 가져오기' (Import Private Key) with the EtherWallet logo on the left. The form contains three input fields: 'userID', 'Password', and 'PrivateKey'. Below the 'PrivateKey' field is a 'Create' button. At the bottom right of the form is a '뒤로가기' (Go Back) button.

개인키 가져오기

 userID

Password

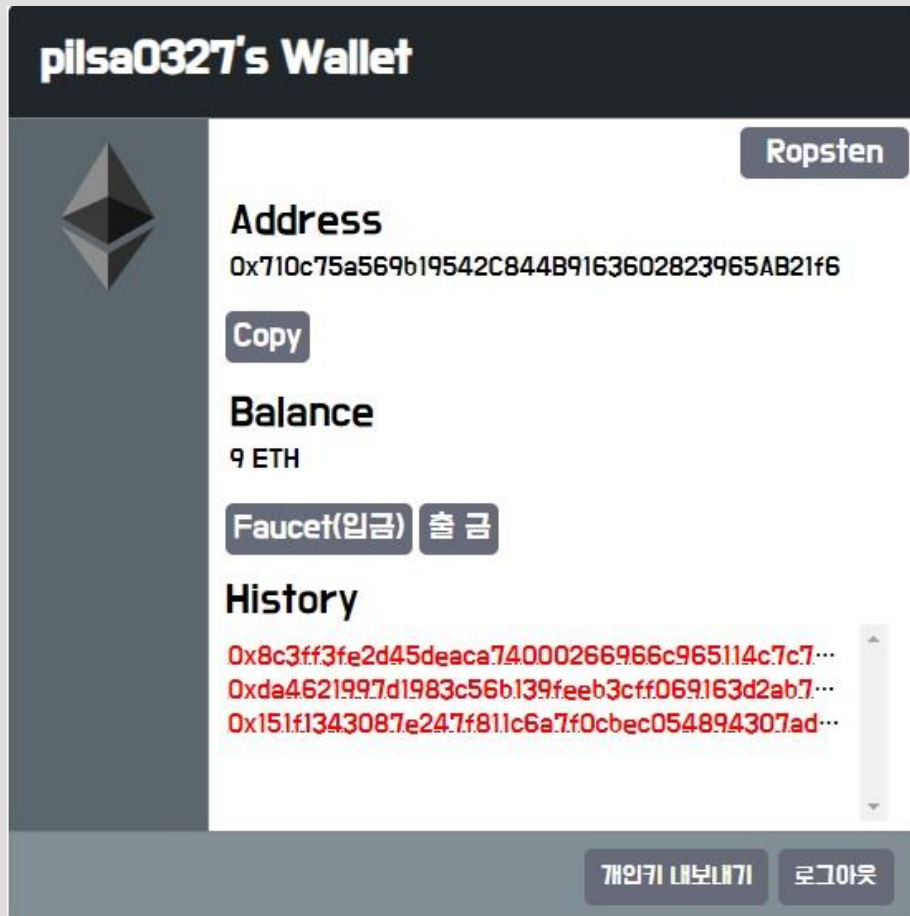
PrivateKey

Create

뒤로가기

- 기존 privatekey로 계정 생성
- 사용자 password와 privatekey는 암호화 후 database에 저장
- Privatekey 유무 체크


EtherWallet 메인



- 계정의 Address, Balance, txHash 값 출력
- (Ropsten 서버) Faucet 버튼 클릭시
faucet.metamask 사이트로 address 값 요청 후
txHash 값 변환(DB에 저장) / 테스트 이더 입금
- Server 변경 기능

EtherWallet 이더 전송

Send coin



Check password

To

Gas price

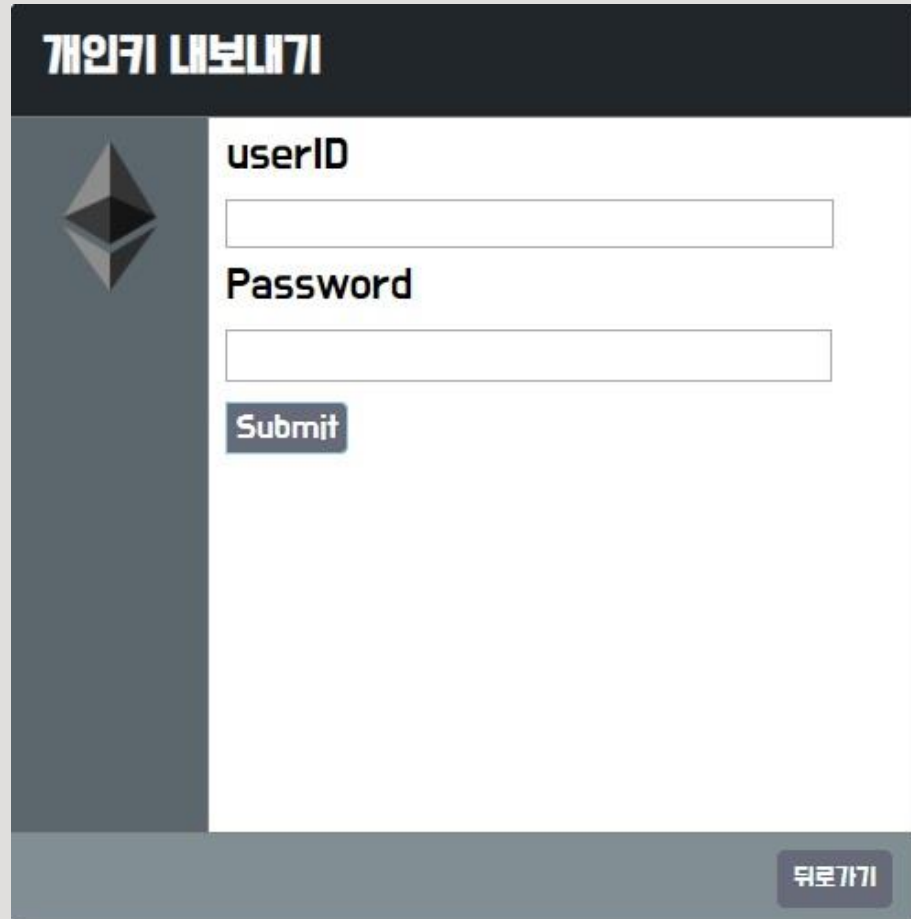
Value

Send


뒤로가기

- 사용자의 privatekey로 서명하여 이더 전송4
- 암호화, 복호화 하는데 salt 값을 client가 입력한 password로 사용함으로써 보안강화

EtherWallet 개인키 내보내기



개인키 내보내기



userID

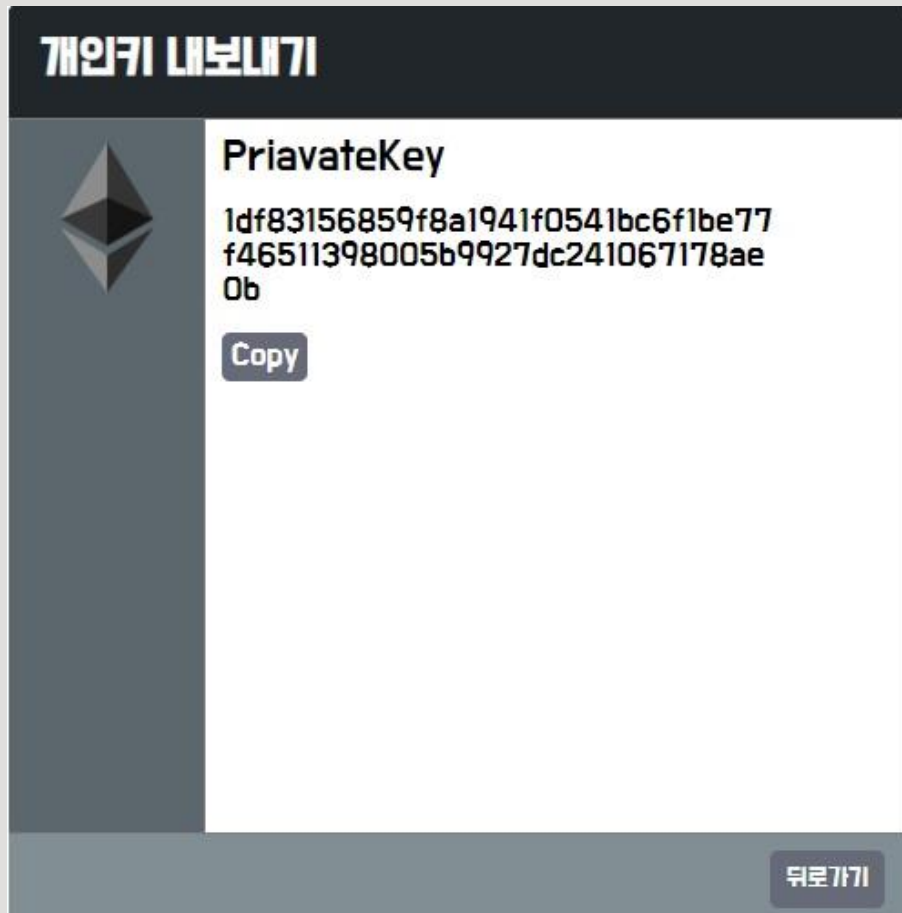
Password

Submit

뒤로가기

- ID / Password 입력시 DB에 저장되어 있는 암호화 된 privatekey를 복호화하여 출력

EtherWallet 개인키 내보내기



- 개인키를 복호화 해서 제공

EtherWallet

문제점

- 데이터 전송이 평문으로 진행되기 때문에 스니핑에 대한 위협
- output data 에 관한 transaction hash 값은 조회 가능
하나 input data 에 관한 transaction hash 값은 조회 불가함
- 서버마다 DB가 분리 되어있지 않음

해결방안

- 클라이언트에서 서버로 데이터 전송 전에 암호화 처리 또는 SSL 적용
- web3 라이브러리를 이용해서 address 에 저장된 transaction hash 값을 조회하여 database 에 저장 해서 호출해야함

<http://175.125.21.32:3001>

Part 2.

EtherScan



EtherScan 이란?



- 이더리움 서버 내에서 생성된 Block, Address, TransactionHash 값에 대한 정보를 조회하는 사이트
- Web3라이브러리를 통해 이더리움 플랫폼에서 해당 값을 받아와 사용자에게 그 정보를 출력해줌

EtherScan 개발 목적



- Web3.js 라이브러리를 사용하여 이더리움에 대한 이해도 향상
- 데이터 관리 방법과 중요성 이해

EtherScan Info

Escan

Search by Address/ Txn Hash / Block

Search

Ropsten

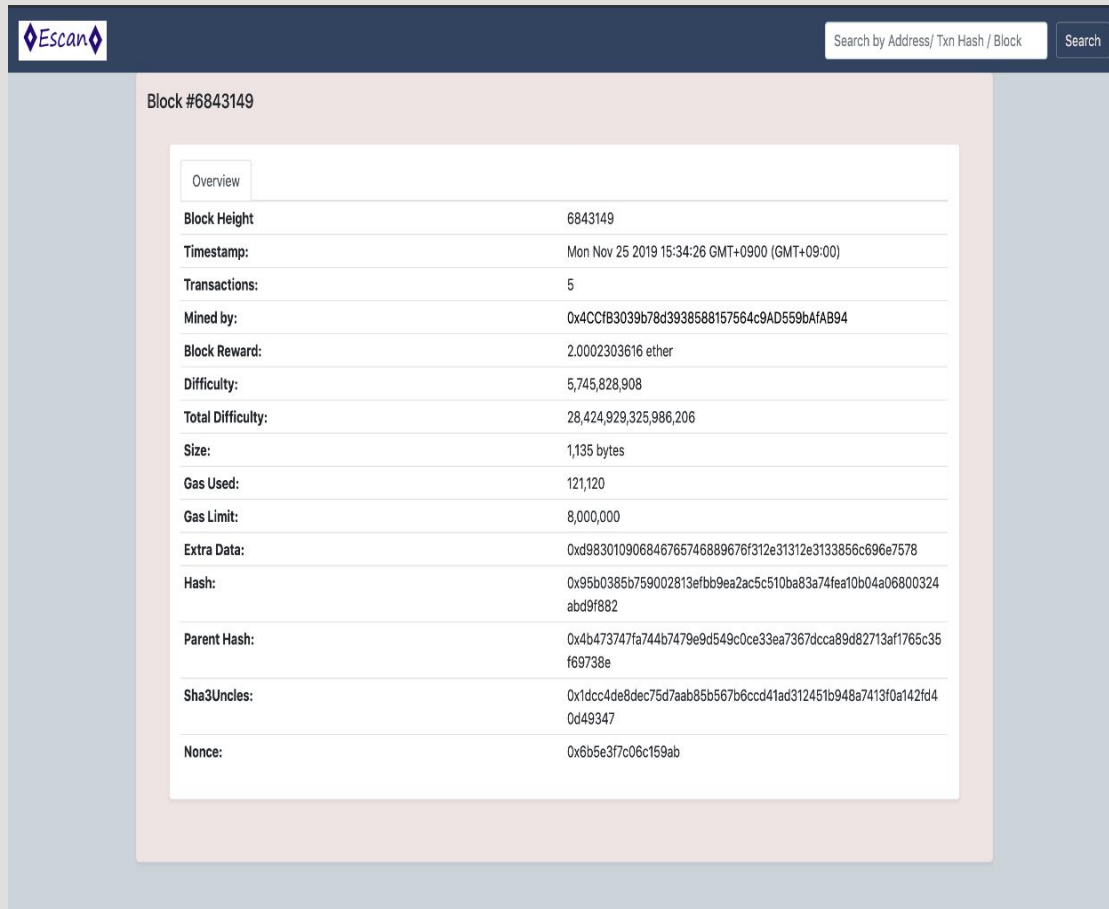
Latest Blocks		
Blocks Number	Miner	txns
6843149	0x4CCfB3039b78d3938588157564c9AD559bAf...	5
6843148	0xD7a15BAEB7EA05C9660CBe03fB7999c2C2e...	14
6843147	0xD7a15BAEB7EA05C9660CBe03fB7999c2C2e...	31
6843146	0x4CCfB3039b78d3938588157564c9AD559bAf...	5
6843145	0x4CCfB3039b78d3938588157564c9AD559bAf...	2

Latest Transactions		
Tx	From	To
0xd7e10c530617dcd58ff00105be4f6247a85f05...	0x18ad77CE213bf5C50Dbc9C1B92820b5957b7...	0xe8aa37Aa2D94C712333F935CafeE7c007150d...
0x68a97e72e99131ff196af268ba0bd0ecf8dd9...	0x18ad77CE213bf5C50Dbc9C1B92820b5957b7...	0x32636de4979Bb6753b8F338892C85a392D1...
0x4a215e586e2713d09b2b1753af2b80a8a1a6ee...	0x32636de4979Bb6753b8F338892C85a392D1...	0x18ad77CE213bf5C50Dbc9C1B92820b5957b7...
0x1f6eb137538d7d3a03e445c4636f952454ea3...	0xa1D084B802799f64DA0745FdDfcc488a9A4...	0x32636de4979Bb6753b8F338892C85a392D1...
0xb902dbf472c4e189a6d962d67c601236ae9f6...	0x6484f99d1e81F575B69f776568C620B35E16...	0x1d7cF6aD190772cC6177bEeA2E3ae24cC89b2...

- Web3 라이브러리를 사용하여 이더리움 Server
에서 정보를 받아와 출력
- 최근 Block정보와 txHash값 제공
- Address/ txHash / Blcok 값 검색 가능

http://175.125.21.32:3000

EtherScan Block_Info

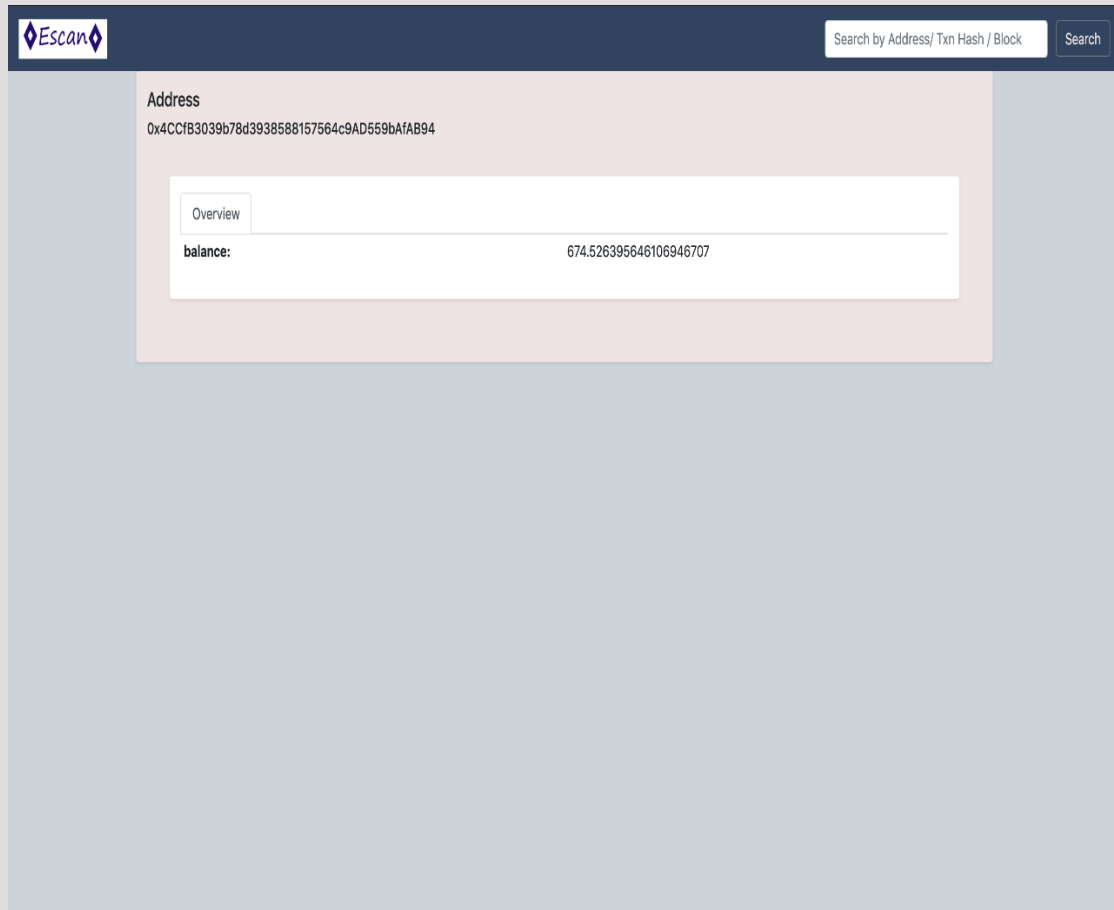


The screenshot shows the EtherScan website interface. At the top, there is a search bar with the text "Search by Address / Txn Hash / Block" and a "Search" button. Below the search bar, the page title "Block #6843149" is displayed. The main content area shows a table with various block details. The table has two columns: the property name and its corresponding value. The properties include Block Height, Timestamp, Transactions, Mined by, Block Reward, Difficulty, Total Difficulty, Size, Gas Used, Gas Limit, Extra Data, Hash, Parent Hash, Sha3Uncles, and Nonce.

Overview	
Block Height	6843149
Timestamp:	Mon Nov 25 2019 15:34:26 GMT+0900 (GMT+09:00)
Transactions:	5
Mined by:	0x4CCfB3039b78d3938588157564c9AD559bAfAB94
Block Reward:	2.0002303616 ether
Difficulty:	5,745,828,908
Total Difficulty:	28,424,929,325,986,206
Size:	1,135 bytes
Gas Used:	121,120
Gas Limit:	8,000,000
Extra Data:	0xd983010906846765746889676f312e31312e3133856c696e7578
Hash:	0x95b0385b759002813efbb9ea2ac5c510ba83a74fea10b04a06800324abd9f882
Parent Hash:	0x4b473747fa744b7479e9d549c0ce33ea7367dcca89d82713af1765c35f69738e
Sha3Uncles:	0x1dcc4de8dec75d7aab85b567b6ccd41ad312451b948a7413f0e142fd40d49347
Nonce:	0x6b5e3f7c06c159ab

- 해당 블록에 대해 상세 정보 조회
- 채굴되지 않은 블록에 대해 조회 불가

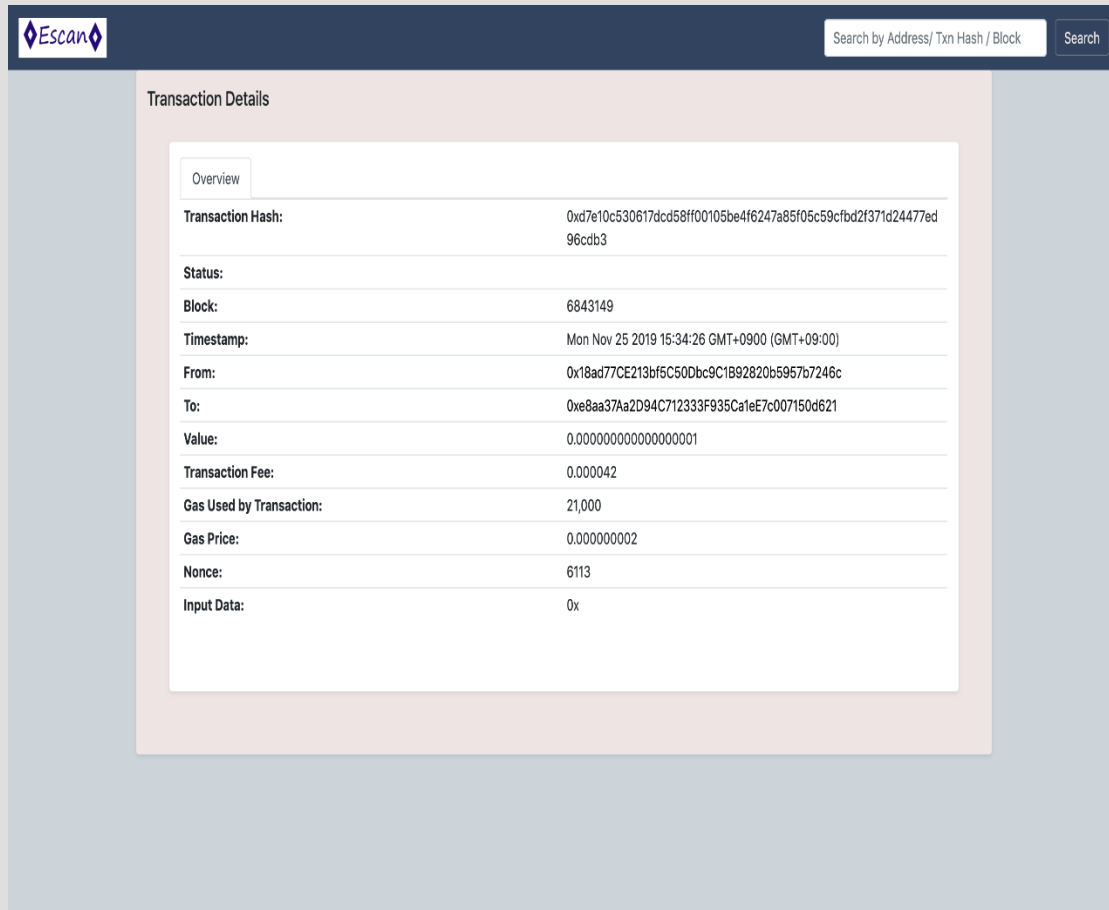
EtherScan Address



- Address 잔액 조회
- 각 정보를 Database에 저장하여 불러오는게 아니라 Web 라이브러리를 통해 정보를 조회하기 때문에 Address가 참여한 txHash에 대한 list-up이 불가능함

<http://175.125.21.32:3000>

EtherScan TxHash_Info



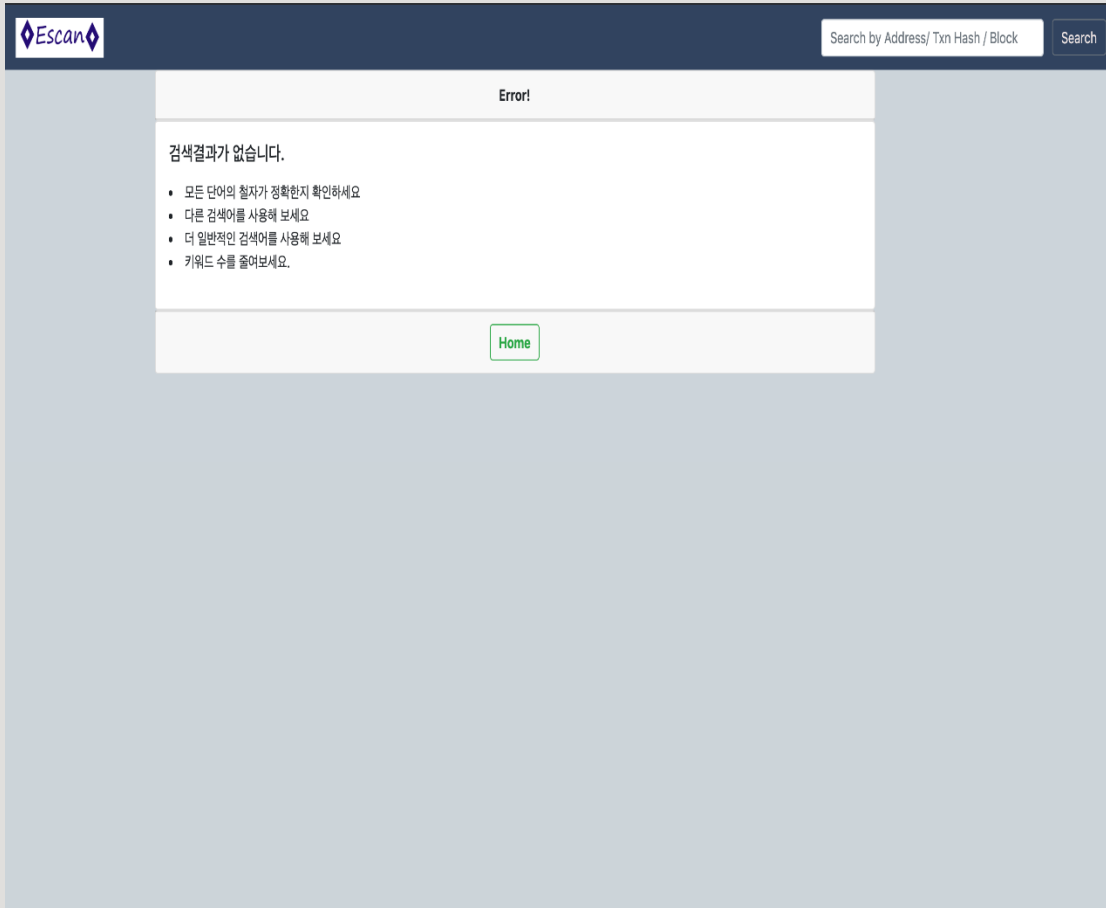
The screenshot shows the EtherScan website interface. At the top, there is a dark blue header with the 'Escan' logo on the left and a search bar on the right containing the text 'Search by Address/ Txn Hash / Block' and a 'Search' button. Below the header, the main content area is titled 'Transaction Details'. Inside this area, there is a white box with a tab labeled 'Overview'. Below the tab, a table displays transaction information. The table has two columns: a label column and a value column. The values are displayed in a light blue background. The transaction hash is a long hexadecimal string. The status is 'Success'. The block number is 6843149. The timestamp is 'Mon Nov 25 2019 15:34:26 GMT+0900 (GMT+09:00)'. The 'From' and 'To' fields contain hexadecimal addresses. The 'Value' field shows '0.000000000000000001'. The 'Transaction Fee' is '0.000042'. The 'Gas Used by Transaction' is '21,000'. The 'Gas Price' is '0.000000002'. The 'Nonce' is '6113'. The 'Input Data' is '0x'.

Transaction Details	
Overview	
Transaction Hash:	0xd7e10c530617dcd58ff00105be4f6247a85f05c59cfbd2f371d24477ed96cdb3
Status:	Success
Block:	6843149
Timestamp:	Mon Nov 25 2019 15:34:26 GMT+0900 (GMT+09:00)
From:	0x18ad77CE213bf5C50Dbc9C1B92820b5957b7246c
To:	0xe8aa37Aa2D94C712333F935Ca1e7c007150d621
Value:	0.000000000000000001
Transaction Fee:	0.000042
Gas Used by Transaction:	21,000
Gas Price:	0.000000002
Nonce:	6113
Input Data:	0x

➤ Transaction Hash에 대한 상세 정보 조회

<http://175.125.21.32:3000>

EtherScan Error



➤ 입력 값이 올바르지 않을 경우 err 페이지

I. 채굴되지 않은 Block number

II. 잘못된 Transaction Hash/ address 값

EtherScan

문제점 및 해결방안

- 기존에 있는 EtherScan과는 달리 DB에 정보를 저장하는 형태가 아닌 Web3.js 라이브러리에서 바로 정보를 조회하여 가져오기 때문에 속도가 느리고 얻을 수 없는 정보가 있음
- EtherScan에서 지원하는 API를 이용하면 그 정보를 받아와서 그 정보를 DB에 저장해서 이용 가능

활용 방안

- 서비스 제공 시 클라이언트에게 서비스에 관련된 정보들을 쉽게 조회하거나 Status Monitoring 시스템을 구축하여 서비스에 대한 신뢰성을 높일 수 있음

<http://175.125.21.32:3000>

ThankU.

