



---

# Web2를 넘어 Web3 보안을 탐험하는 이유

고려대학교 조원민

---

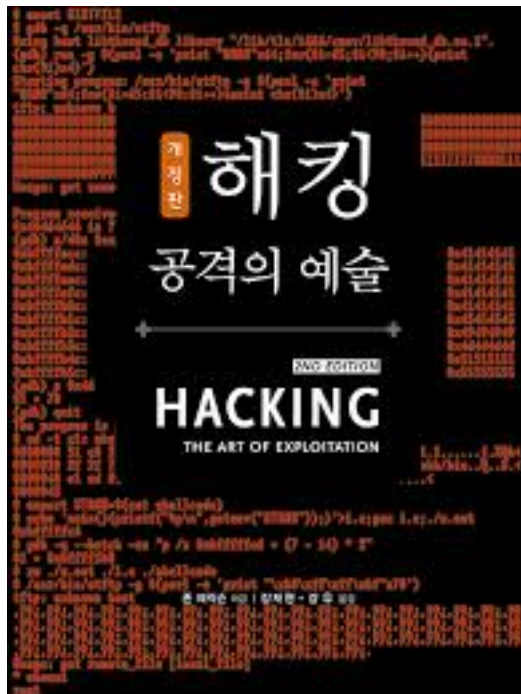
## ■ 발표자 소개

- 고려대학교 스마트보안학과
- CyKor 동아리
- Upside Academy 2기

자세한 내용... [wiimdy.kr/about](http://wiimdy.kr/about)



## ■ 우리는 왜 해킹이라는 길을 가게 되었는가?





---

01

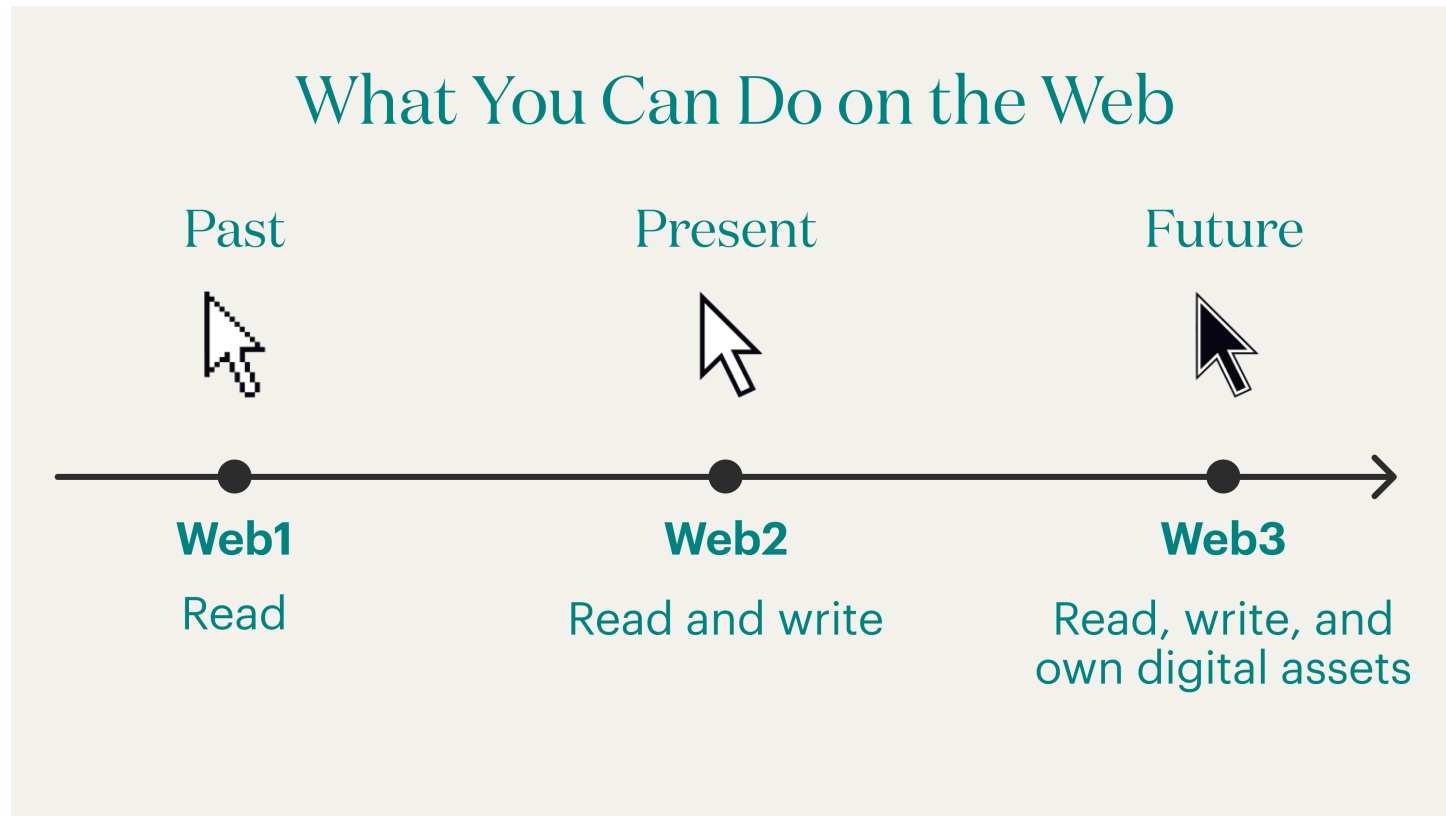
---

**Web3 너가 뭔데?**

---



## ■ Web3 너가 뭔데?



## ■ Web1 & Web2

Web1: 읽기만 가능한 인터넷!

Static HTML로 구성되어 있어 사용자는 읽기만 가능

Ex) Yahoo, Google...



Web2: 사용자가 콘텐츠를 직접 생성!

현재 대부분의 홈페이지

모든 데이터와 상호작용은 특정 기업(Google, Meta 등)이 소유하고 통제하는 **중앙화된 플랫폼**을 통해 이루어짐.

Ex) 페이스북, 유튜브, 위키피디아...





## ■ Web1: 읽기만 가능한 인터넷!

### World Wide Web

The WorldWideWeb (W3) is a wide-area [hypermedia](#) information retrieval initiative aiming to give universal access to a large universe of documents.

Everything there is online about W3 is linked directly or indirectly to this document, including an [executive summary](#) of the project, [Mailing lists](#) , [Policy](#).

#### [What's out there?](#)

Pointers to the world's online information, [subjects](#) , [W3 servers](#), etc.

#### [Help](#)

on the browser you are using

#### [Software Products](#)

A list of W3 project components and their current state. (e.g. [Line Mode](#) ,X11 [Viola](#) , [NeXTStep](#) , [Servers](#) , [Tools](#) , [Mail robot](#) , [Library](#) )

#### [Technical](#)

Details of protocols, formats, program internals etc

#### [Bibliography](#)

Paper documentation on W3 and references.

#### [People](#)

A list of some people involved in the project.

#### [History](#)

A summary of the history of the project.

#### [How can I help ?](#)

If you would like to support the web..

#### [Getting code](#)

Getting the code by [anonymous FTP](#) , etc.



## ■ Web2: 사용자가 콘텐츠를 직접 생성!

The screenshot shows a GitHub profile for the user 'wiimdy'. The profile includes a circular avatar with a raccoon and the text 'IT FUCKEN WIMDY!', the username 'wiimdy', and a bio 'hi'. Below the profile information, there are statistics: '5 followers · 10 following' and a link to 'wiimdy.kr'. The 'Highlights' section is also visible. The main content area displays a list of repositories:

- web2** (Public): PHP, Updated last week. Includes a 'Star' button and a commit history graph.
- blog** (Public): HTML, MIT License, Updated last week. Includes a 'Star' button and a commit history graph.
- bearmoon** (Public): Solidity, 1 commit, Updated on Jul 22. Includes a 'Star' button and a commit history graph.
- beraborrow** (Public): Solidity, 1 commit, Updated on May 30. Includes a 'Star' button and a commit history graph.

<https://github.com/wiimdy?tab=repositories>

## ■ Web3!

**Web3:** 사용자는 자신의 데이터와 디지털 자산을  
누구의 허락도 없이 완벽하게 통제하고 소유

블록체인 기술을 기반으로, 특정 기업이 아닌 사용자가 직접  
자신의 데이터와 디지털 자산을 소유하고 관리하는 새로운 인터넷입니다.

Web3의 특징: 탈중앙성, 퍼블릭 블록체인, 투명성..





## ■ Web3 세줄 요약

### 1. 탈중앙성

- 중앙 서버나 관리 주체 없이, 네트워크 참여자들이 **공동으로 시스템을 운영**하고 검증.

### 2. 투명성과 불변성

- 모든 소스 코드와 거래 기록이 **블록체인에 영구적**으로 공개.

### 3. 사용자 소유권과 직접적인 가치 이동

- 사용자는 자신의 디지털 자산을 지갑에 **직접 소유**하며, 은행 같은 중개자 없이 가치를 주고받음.



## ■ 퀴즈 1.

- Q1: Web3 서비스에서 사용자의 데이터(예: 거래 기록)는 기본적으로 어디에 저장될까요?

1. 새 서비스를 운영하는 회사의 중앙 데이터베이스
2. 여러 컴퓨터에 분산되어 모두가 공유하는 블록체인
3. 사용자의 개인 컴퓨터 하드 드라이브
4. 클라우드 서버 (예: AWS, Google Cloud)



## ■ 퀴즈 1.

- Q1: Web3 서비스에서 사용자의 데이터(예: 거래 기록)는 기본적으로 어디에 저장될까요?

1. 새 서비스를 운영하는 회사의 중앙 데이터베이스

2. 여러 컴퓨터에 분산되어 모두가 공유하는 블록체인

3. 사용자의 개인 컴퓨터 하드 드라이브

4. 클라우드 서버 (예: AWS, Google Cloud)





---

02

---

# Web3 보안 맛보기

---



## ■ 이더리움의 스캔 사이트

ETH Price: \$4,608.64 (+7.83%) Gas: 12.976 Gwei

Etherscan

HomeBlockchainTokensNFTsResourcesDevelopersMoreWIIMDY

The Ethereum Blockchain Explorer

Ad

All Filters Search by Address / Txn Hash / Block / Token / Domain Name

Sponsored: Rollbit: Trade 30+ Crypto - BTC, ETH, SOL, MOG, WIF. 1,000x leverage, instant execution! Trade Now!

ETHER PRICE

\$4,608.64 @ 0.03978 BTC (+7.83%)

TRANSACTIONS

2,954.55 M (19.9 TPS)

MED GAS PRICE

12.976 Gwei (\$1.26)

MARKET CAP

\$556,298,056,572.00

LAST FINALIZED BLOCK

23197180

LAST SAFE BLOCK

23197244

TRANSACTION HISTORY IN 14 DAYS

1 900k  
1 500k  
Aug 7 Aug 14 Aug 21

Latest Blocks

Customize

23197273

18 secs ago

Miner Titan Builder

253 txns in 12 secs

0.04106 Eth

23197272

30 secs ago

Miner Titan Builder

278 txns in 12 secs

0.08278 Eth

Latest Transactions

Customize

0xbd995cd0ac...

18 secs ago

From 0x4838B106...B0BAD5f97

To 0x388C818C...7ccB19297

0.03499 Eth

0x21b69dc0cc...

18 secs ago

From 0x08F9F14f...1878f1D11

To 0x3A75346f...12A6CfA83

0 Eth

<https://etherscan.io/>



## ■ ENS와 지갑 주소



Home Blockchain ▾ Tokens ▾ NFTs ▾ Resources ▾ Developers ▾ More ▾ | ②

### Domain Name Lookup

wiimdy.eth



Domain names allow users to interact with other addresses on-chain using human-readable names instead of long and complicated address hashes.

[Learn more >](#)

**MEXC**  
**On-Chain Bounty**  
\$40,107,593 Airdrop Rewards Await  
[Join Now](#)

Result for: wiimdy.eth

[Domain Name Lookup](#) / Search

#### Overview of ENS

② Resolved Address:

0x00000000F2708738d4886Bc4aEdEFd8dD04818b0

② Expiration Date:

2027.02.24 at 11:34

② Registrant:

0xD4416b13d2b3a9aBae7AcD5D6C2BbDBE25686401

[Lookup names](#)

② Controller:


0xD4416b13d2b3a9aBae7AcD5D6C2BbDBE25686401

[Lookup names](#)

<https://etherscan.io/name-lookup-search?id=wiimdy.eth>



## ■ 주소 조회하기

 **Address** 0x00000000F2708738d4886Bc4aEdEFd8dD04818b0

[Buy](#) [Presale](#) [Play](#) [Gaming](#)

Sponsored: [bc.game](#) - INVITE FRIEND & GET BONUS! 15% COMMISSION [Play Now](#)

[wiimdy.eth](#)

[☆](#) [</> API](#) [≡](#)

**Overview**

ETH BALANCE  
0.006588600705485999 ETH

ETH VALUE  
\$30.35 (@ \$4,605.80/ETH)

TOKEN HOLDINGS  
\$18.20 (15 Tokens)

**More Info**

PRIVATE NAME TAGS  
[+ Add](#)

TRANSACTIONS SENT  
Latest: 1 day ago ↗ First: 120 days ago ↗

FUNDED BY  
[0xB42F812A...759EbEAD6](#) | 120 days ago

**Multichain Info**

\$69.61 (Multichain Portfolio)

4 addresses found via [Blockscan](#)

[Transactions](#) [Internal Transactions](#) [Token Transfers \(ERC-20\)](#) [NFT Transfers](#) [Analytics](#) [Assets](#) [Cards](#) [New](#)

[Advanced Filter](#)

Latest 25 from a total of 91 transactions

[Download Page Data](#)

Transaction Hash	Method	Block	Age	From	To	Amount	Txn Fee
<a href="#">0x9ce812abe1...</a>	Deposit Native	23187264	33 hrs ago	<a href="#">wiimdy.eth</a>	<a href="#">0x4cD00E38...62338BC31</a>	0.00116545 ETH	0.00002395
<a href="#">0x0bf0c4a4df0...</a>	Multicall	23187256	33 hrs ago	<a href="#">wiimdy.eth</a>	<a href="#">0xF5042e6f...D8eB9e222</a>	0.00116521 ETH	0.00022024

<https://etherscan.io/address/0x00000000F2708738d4886Bc4aEdEFd8dD04818b0>




## ■ 주소 거래내역 분석

### Transaction Details

< >

Overview Logs (1) State

 TRANSACTION ACTION

Call Deposit Native Function by [wiimdy.eth](#) on [0x4cD00E38...62338BC31](#)

Transaction Hash:

0x9ce812abe17241444c9bbbe2b3e10bbd9dee00e2a47a3d9f1da9293a43d3cf4d

Status:

Success

Block:

23187264 23512 Block Confirmations

Timestamp:

3 days ago (Aug-21-2025 05:06:59 AM UTC)

From:

[wiimdy.eth](#)

To:

[0x4cD00E387622C35bDDB9b4c962C136462338BC31](#)

Value:

0.001165453521815527 ETH \$5.53

Transaction Fee:

0.000023956120065576 ETH \$0.11

Gas Price:

0.966908301 Gwei (0.000000000966908301 ETH)

<https://etherscan.io/tx/>



## ■ 주소 거래내역 분석

❓ Ether Price:	\$4,224.96 / ETH
❓ Gas Limit & Usage by Txn:	32,650   24,776 (75.88%)
❓ Gas Fees:	Base: 0.234888175 Gwei   Max: 0.966908301 Gwei   Max Priority: 0.734584134 Gwei
❓ Burnt & Txn Savings Fees:	<div> Burnt: 0.0000058195894238 ETH (\$0.03)</div> <div> Txn Savings: 0 ETH (\$0.00)</div>

❓ Other Attributes: Txn Type: 2 (EIP-1559) Nonce: 81 Position In Block: 73

❓ Input Data:

Function: depositNative(address depositor,bytes32 id) \*\*\*

MethodID: 0x49290c1c

[0]: 00000000000000000000000000000000f2708738d4886bc4aedefd8dd04818b0

[1]: 5e2d158d1101bf629497edf26a0c83251927aac1afec6a581a0c4837841d9e08

View Input As ▾

Decode Input Data

View In Decoder

Advanced Filter

Write Contract

More Details:

— [Click to show less](#)



## ■ Web3의 활동 내역 분석

← → ↻ etherscan.io/address/0x4cd00e387622c35bddb9b4c962c136462338bc31#code

ETH Price: \$4,625.74 (+8.23%) Gas: 11.024 Gwei

Search by Address / Txn Hash / Block / Token / Domain Name

Contract Name:	RelayDepository	Optimization Enabled:	No with 200 runs
Compiler Version	v0.8.28+commit.7893614a	Other Settings:	cancun EvmVersion

Contract Source Code (Solidity Standard Json-Input format) Open In

File 1 of 7 : RelayDepository.sol Outlin

```
1 // SPDX-License-Identifier: MIT
2 pragma solidity ^0.8.23;
3
4 import {Ownable} from "solady/auth/Ownable.sol";
5 import {ERC20} from "solady/tokens/ERC20.sol";
6 import {EIP712} from "solady/utis/EIP712.sol";
7 import {SafeTransferLib} from "solady/utis/SafeTransferLib.sol";
8 import {SignatureCheckerLib} from "solady/utis/SignatureCheckerLib.sol";
9
10 import {Call, CallRequest, CallResult} from "./utis/RelayDepositoryStructs.sol";
11
12 /// @title RelayDepository
13 /// @author Relay
14 - contract RelayDepository is Ownable, EIP712 {
15 -     using SafeTransferLib for address;
16     using SignatureCheckerLib for address;
17
18     /// @notice Revert if the address is zero
19     error AddressCannotBeZero();
20
21     /// @notice Revert if the signature is invalid
22     error InvalidSignature();
23
24     /// @notice Revert if the call request is expired
25     error CallRequestExpired();
```

File 2 of 7 : Ownable.sol Outlin

```
1 // SPDX-License-Identifier: MIT
2 pragma solidity ^0.8.4;
3
4 /// @notice Simple single owner authorization mixin.
5 /// @author Solady (https://github.com/vectorized/solady/blob/main/src/auth/Ownable.sol)
6 ///
```

<https://etherscan.io/address/0x4cd00e387622c35bddb9b4c962c136462338bc31#code>



## ■ 실제 해킹 사건 분석

**PeckShield Inc.** @peckshield

.@GMX\_IO has been exploited for ~\$42M. The exploiter has bridged ~\$9.6M worth of cryptos to #Ethereum.

**Transaction Details:**

- 0x31826f095691e4e48f228bc7975f943f4b04228c7acdc9a3262ef
- 355860237 42111 Block Confirmations
- 1 hr ago (Jul-09-2025 12:30:11 PM +UTC)
- 0x42666f8f377405429EE18559e548970d69160f3
- 0x75E42e0f01baf1D402238a82A287749f9b4A0c (GMX: Position Manager)

**Transfers:**

- Transfer 0.009976117799240672 ETH (\$26.51) From Wrapped Ether To GMX: Order Book
- Transfer 0.009976117799240672 ETH (\$26.51) From GMX: Order Book To 0x7038D503...6771cc355
- Transfer 0.003 ETH (\$7.97) From Wrapped Ether To GMX: Order Book
- Transfer 0.003 ETH (\$7.97) From GMX: Order Book To 0x42666f8f...9D49160F3

**Wallet:**

Token	Price	Amount	USD Value
Legacy Trax Dollar	\$0.9674	10,548,626.3042	\$10,416,056
WBTC	\$109,141.34	88.1734	\$9,623,359
WETH	\$2,651.84	2,205.4992	\$5,848,631
DAI	\$1	4,999,278.8246	\$4,999,279
USDC	\$0.9999	4,282,959.0743	\$4,282,531
ETH	\$2,652.18	999.7329	\$2,651,472
USDC	\$0.9999	1,999,447.4495	\$1,999,248
DAI	\$1	1,338,385.1379	\$1,338,385
UNI	\$8.1608	65,479.2414	\$534,363.86
LINK	\$14.075	23,806.2093	\$334,187.77
ETH	\$2,651.84	0.5707	\$1,529.22

11:04 PM · Jul 9, 2025 · 165.5K Views

<https://x.com/peckshield/status/1942947860645134450>





지엠엑스   
@GMX\_IO



**Arbitrum의 GMX V1 GLP 풀에서 취약점 공격이 발생했습니다. 약 4천만 달러 상당의 토큰이 GLP 풀에서 알 수 없는 지갑으로 이체되었습니다.**

GMX는 보안을 최우선으로 생각했으며, GMX 스마트 컨트랙트는 최고 보안 전문가들의 수많은 감사를 거쳤습니다. 따라서 이번 조사에서 모든 핵심 참여자는 조작이 어떻게 발생했는지, 그리고 어떤 취약점이 이를 가능하게 했는지 조사하고 있습니다. 보안 파트너들도 적극적으로 참여하여 발생한 사건을 철저히 파악하고 관련 위험을 최대한 신속하게 최소화하고 있습니다. Arbitrum의 주요 목표는 복구와 문제의 근본 원인 파악입니다.

#### **조치 사항:**

추가 공격 벡터를 차단하고 사용자를 추가적인 부정적 영향으로부터 보호하기 위해 Arbitrum과 Avalanche 모두에서 GMX V1 거래, GLP 발행 및 상환을 비활성화했습니다.

**취약점 범위:** 이 취약점 공격은 GMX V2, 해당 마켓, 유동성 풀, 그리고 GMX 토큰 자체에는 영향을 미치지 않습니다.

이용 가능한 정보에 따르면 해당 취약점은 GMX V1 및 GLP 풀에 국한됩니다. 더욱 완전하고 검증된 정보가 확보되는 대로 자세한 사고 보고서를 발표하겠습니다.

오후 11시 35분 · 2025년 7월 9일 · **325.7K** 조회수

[https://x.com/GMX\\_IO/status/1942955807756165574](https://x.com/GMX_IO/status/1942955807756165574)



## ■ 공격 로그 분석

```
[Sender] 0xd4266f8f82f7405429ee18559e548979d49160f3
0 0 → CALL [Receiver] GMX: Position Manager.executeDecreaseOrder [Calldata] (_account=GMX Exploiter 1, _orderIndex=5, _feeReceiver=[Sender]0xd4266f8f82f74
1 1 → STATICCALL GMX: Vault.gov [Calldata] () ▶ (Timelock)
2 1 → STATICCALL GMX: Order Book.getDecreaseOrder [Calldata] (_account=GMX Exploiter 1, _orderIndex=5) ▶ (collateralToken=WETH, collateralDelta=26,51
3 1 → STATICCALL GMX: Vault.getMinPrice [Calldata] (_token=WETH) ▶ (2,661,295,000,000,000,000,000,000,000,000)
11 1 → CALL ShortsTracker.updateGlobalShortData [Calldata] (_account=GMX Exploiter 1, _collateralToken=WETH, _indexToken=WETH, _isLong=true, _sizeDelta=
12 1 → CALL Timelock.enableLeverage [Calldata] (_vault=GMX: Vault) ▶ ()
23 1 → CALL GMX: Order Book.executeDecreaseOrder [Calldata] (_address=GMX Exploiter 1, _orderIndex=5, _feeReceiver=[Sender]0xd4266f8f82f7405429ee18559e
24 2 → STATICCALL GMX: Vault.getMinPrice [Calldata] (_token=WETH) ▶ (2,661,295,000,000,000,000,000,000,000,000)
32 2 → CALL GMX: Router.pluginDecreasePosition [Calldata] (_account=GMX Exploiter 1, _collateralToken=WETH, _indexToken=WETH, _collateralDelta=26,517
89 2 → CALL WETH.withdraw [Calldata] (amount=9,976,117,799,240,672) ▶ ()
93 2 → CALL value: 0.009976117799240672 Ether GMX Exploiter 1.fallback(raw data) ▶ ()
94 3 → STATICCALL GMX: GlpManager.getGlobalShortAveragePrice [Calldata] (_token=WBTC) ▶ (1,913,705,482,286,167,437,447,414,747,675,542)
97 3 → STATICCALL GMX: Vault.getMaxPrice [Calldata] (_token=WBTC) ▶ (109,500,940,000,000,000,000,000,000,000,000)
```

<https://app.blocksec.com/explorer/tx/arbitrum/0x03182d3f0956a91c4e4c8f225bbc7975f9434fab042228c7acdc5ec9a32626ef>



## ■ 실제 취약점 코드

```
gmx-contracts / contracts / core / OrderBook.sol

Code Blame 984 lines (881 loc) · 31.6 KB

864         order.collateralToken,
865         order.indexToken,
866         order.collateralDelta,
867         order.sizeDelta,
868         order.isLong,
869         address(this)
870     );
871
872     // transfer released collateral to user
873     if (order.collateralToken == weth) {
874         _transferOutETH(amountOut, payable(order.account));
875     } else {
876         IERC20(order.collateralToken).safeTransfer(order.account, amountOut);
877     }
878
```



## ■ Root cause 분석

1. 공격자가 이 함수 실행

```
function executeDecreaseOrder(  
    // transfer released collateral to user  
    if (order.collateralToken == weth) {  
        _transferOutETH(amountOut, payable(order.account));  
    } else {  
        IERC20(order.collateralToken).safeTransfer(order.account, amountOut);  
    }  
)
```

2. receiver를 인자로 넘김

```
function _transferOutETH(  
    uint256 _amountOut,  
    address payable _receiver  
) {  
    IWETH(weth).withdraw(_amountOut);  
    sendValue(_receiver, _amountOut);  
}
```

3. receiver(exploiter) 코드를 실행

```
function sendValue(address payable recipient, uint256 amount) {  
    require(address(this).balance >= amount, "Address: insufficient balance");  
  
    // solhint-disable-next-line avoid-low-level-calls, avoid-call-value  
    (bool success, ) = recipient.call{value: amount}("");  
    require(  
        success,  
        "Address: unable to send value, recipient may have reverted"  
    );  
}
```



## ■ Root cause 분석

exploiter를 call 하면 어떻게 되는가?

=> exploiter가 원하는 함수 실행 가능

=> 이게 왜 문제?

=> 실행 흐름이 exploiter에게 넘어가서 거래소의 가격을 바꿀수 있음  
(레버리지 숏 포지션을 열며..)



## ■ Root cause 분석

공격자에게 실행 흐름이 넘어 갔을 때

```
2 → CALL value: 0.009976117799240672 Ether GMX Exploiter 1.fallback(raw data) ▶ ()
3 → STATICCALL GMX: GlpManager.getGlobalShortAveragePrice [calldata] (_token=WBTC) ▶ (1,913,705,482,286,167,437,447,414,747,675,542)
3 → STATICCALL GMX: Vault.getMaxPrice [calldata] (_token=WBTC) ▶ (109,500,940,000,000,000,000,000,000,000,000)
3 → STATICCALL GMX: Vault.reservedAmounts [calldata] (0xaf88_USDC) ▶ (27,855,857,410)
3 → STATICCALL GMX: Vault.poolAmounts [calldata] (0xaf88_USDC) ▶ (10,013,532,053,118)
3 → STATICCALL GMX: Vault.usdgAmounts [calldata] (0xaf88_USDC) ▶ (10,013,364,877,641,887,807,943,993)
3 → STATICCALL GMX: Vault.maxUsgAmounts [calldata] (0xaf88_USDC) ▶ (16,898,185,277,151,228,065,200,623)
3 → CALL UniswapV3Pool.flash [calldata] (recipient=GMX Exploiter 1, amount0=0, amount1=7,538,567,619,570, data=(long param)) ▶ ()
```



## ■ Root cause 분석

어느정도 GLP에 돈을 맡기고 레버리지 샷을 한다.

```
4 → CALL GMX Exploiter 1.uniswapV3FlashCallback (calldata) (fee0=0, fee1=3,769,283,810, data=(long param)) ▶ ()
+ 5 → CALL 0xaf88_USDC.approve (calldata) (spender=GMX: GlpManager, value=6,000,000,000,000) ▶ (true)
+ 5 → CALL GMX: Reward Router V2.mintAndStakeGlp (calldata) (_token=0xaf88_USDC, _amount=6,000,000,000,000, _minUsdg=0, _minGlp=0) ▶ (4,129,578,056,417,997,08)
+ 5 → CALL 0xaf88_USDC.transfer (calldata) (to=GMX: Vault, value=1,538,567,619,570) ▶ (true)
+ 5 → STATICCALL GMX: Vault.getMaxPrice (calldata) (_token=0xaf88_USDC) ▶ (1,000,000,000,000,000,000,000,000,000)
+ 5 → CALL GMX: Vault.increasePosition (calldata) (_account=GMX Exploiter 1, _collateralToken=0xaf88_USDC, _indexToken=WBTC, _sizeDelta=15,385,676,195,700,000,000)
```

레버리지: 거래소에 돈을 빌려서 투자를 하는 기술

샷: 하락에 배팅하기 (가격이 떨어질 것이라 예상)



## ■ Root cause 분석

GLP의 가격이 급격히 올라 다시 GLP를 판다.

```
+ 5 → CALL GMX: Reward Router V2.unstakeAndRedeemGlp [calldata] (_tokenOut=WBTC, _glpAmount=386,498,977,301,112,432,466,652, _minOut=0, _receiver=GMX Exploiter)
+ 5 → STATICCALL GMX: GlpManager.getAum [calldata] (maximise=false) ▶ (908,179,662,530,938,665,952,483,378,294,110,666,923)
5 → STATICCALL GLP.totalSupply [calldata] () ▶ (36,067,854,524,500,331,097,383,663)
5 → STATICCALL GMX: Vault.reservedAmounts [calldata] (WETH) ▶ (410,917,754,896,704,777,625)
5 → STATICCALL GMX: Vault.poolAmounts [calldata] (WETH) ▶ (3,646,154,583,342,333,502,942)
+ 5 → STATICCALL GMX: Vault.getMinPrice [calldata] (_token=WETH) ▶ (2,661,295,000,000,000,000,000,000,000,000)
+ 5 → CALL GMX: Reward Router V2.unstakeAndRedeemGlp [calldata] (_tokenOut=WETH, _glpAmount=341,596,270,985,668,652,106,658, _minOut=0, _receiver=GMX Exploiter)
```

왜 GLP의 가격이 급격히 올랐는가?

=> GLP 가격 = (user\_GLP / total\_GLP\_supply) \* AUM (이놈이 급격히 상승)

AUM = (금고에 있는 모든 코인 총합) + (\*\*샷 포지션의 손실) - (샷 포지션의 이익)





## ■ 그래서 어떻게 되었는가?



지엠엑스    
@GMX\_IO



GMX V1 익스플로잇의 책임자와 연락을 취하기 위해 이 메시지를 게시합니다. 익스플로잇을 성공적으로 실행하셨으며, **익스플로잇 거래를 조사하는 모든 사람에게 귀하의 능력이 명백하게 드러났습니다.** 500만 달러 규모의 화이트햇 버그 바운티는 계속 이용 가능합니다. 이 바운티를 수락할지, 아니면 악용된 자금을 유지할지 결정하는 것은 자금을 자유롭게 사용할 수 있느냐, 아니면 자금을 얻기 위해 추가적인 위험을 감수하느냐의 차이입니다. 화이트햇 버그 바운티를 선택할 경우, 500만 달러는 지금 당장 자유롭게 사용할 수 있다는 점을 다시 한번 강조드립니다. 필요한 경우 자금 출처 증명을 제공할 수 있습니다. **이 문제에 대한 합의가 이루어지면 500만 달러는 합법적으로 화이트햇 바운티로 분류될 것입니다.** GLP 사용자는 전액 보상을 받게 되며, 500만 달러의 차액은 재무부에 할당된 버그 바운티 기금으로 충당되므로 추가 조치의 근거는 없습니다. 문의 사항: 이메일: security@gmx.io 온체인: (GMX 배포자: 0x5F799f365Fa8A2B60ac0429C48B153cA5a6f0Cf8) Immunefi: ([https://immunefi.com/bug-bounty/gmx ...](https://immunefi.com/bug-bounty/gmx...))

[https://x.com/GMX\\_IO/status/1943342382503567586](https://x.com/GMX_IO/status/1943342382503567586)



## ■ 해피엔딩...



지엠엑스   
@GMX\_IO



GMX V1 코드베이스에 보안 취약점이 발견되어 공개되었습니다. GMX V1 포크에도 안전하게 통보되었습니다. 이번 복구 과정에서 0xDF3340A436c27655bA62F8281565C9925C3a5221의 행위를 인지하고 있습니다. GLP 보유자 소유의 4,200만 달러 상당의 잠재적 악용 가능 자산이 확보되었습니다. **사용자에게 500만 달러의 포상금이 지급된 후,** 나머지 자금은 현재 GMX 보안 멀티시그에 안전하게 보관되어 있습니다. 참여자들은 GMX DAO에 제출할 배포 계획을 수립 중이며, 곧 더 자세한 정보를 공유할 예정입니다.

오후 9시 53분 · 2025년 7월 11일 · **110.6K** 조회수

[https://x.com/GMX\\_IO/status/1943654914749534380](https://x.com/GMX_IO/status/1943654914749534380)



## ■ 왜 Web3가 재밌는가?

오픈된 코드, 오픈된 로그 => 해킹 사건들에 대해 모든 정보가 공개되어 있음  
분석이 가능하고 취약점 공부 재밌음

**\$40M GMX EXPLOIT**

**\$40M GMX Exploit: AUM Manipulation**

BlockSec  
@BlockSecTeam · Jul 10 · 📍

6 60 217 37K

GMX was hacked with more than 40M loss. The attacker leveraged a vulnerability with opening a short position while leverage was enabled in the contract.

42m dollars

전체 금융 이미지 쇼핑 뉴스 동영상 짧은

42,000,000 미국 달러 =

**58,398,269,160.00**

**대한민국 원**

8월 29일 오후 2:59 UTC · Morningstar 제공 · 면책조항

42000000 미국 달러 ▼

58398269160. 대한민국 원 ▼

<https://x.com/BlockSecTeam/article/1942990338731229379>



## ■ 결론

영어 실력과 코드를 이해할 수 있는 **solidity 실력**을 갖춘다면  
모든 해킹 사건들을 분석할 수 있다.

=> 모든 해킹 사건들을 그때 환경으로 세팅으로 해서 exploit 코드를 작성할 수 있다!

티오리의 Web3 팀인 chainlight에서 작성한 해킹 사건 모음집

<https://drive.google.com/file/d/1zt30caMFy64RehSFCA4P-jP-31IST9LD/view>



---

# 03

---

**Web3 보안, 어떻게 시작할까?**

---



## ■ 어떻게 공부할 수 있는가? - 드림핵



### Smart Contract Security

★ 10.0 (1)

Tier 2

Easy

Skill Path

Blockchain

본 Path에서는 이더리움과 Solidity 기반 스마트 컨트랙트의 구조와 보안 취약점을 학습하고 실습을 통해 실제 보안 사고로 이어진 핵심 취약점들을 직접 분석합니다. 스마트 컨트랙트에서 자주 발생하는 보안 문제를 중심으로 Reentrancy, Integer Overflow, Storage 조작 등 실전 공격 기법과 방어 전략을 학습합니다. 본 Path를 모두 완료하면 스마트 컨트랙트 감사(Audit)에 필요한 기초 지식을 함양하여 Web3 분야의 버그 바...

학습목표 Unit 구성 수강 후기 1

#### 이런 이유로 이 Path를 추천해요

블록체인에서 스마트 컨트랙트는 단 한 줄의 코드에만 실수가 있어도 수백억 원 규모의 자산 손실로 이어질 수 있을 만큼, 보안이 무엇보다 중요한 분야입니다. 특히 재진입성(Reentrancy), Fallback 함수 등으로 인해 발생하는 취약점은 실제 해킹 사례에서도 자주 등장하고 있습니다. 본 Path에서는 이더리움 네트워크와 EVM의 구조를 이해하는 것부터 시작해서 Solidity 기반 컨트랙트에서 발생하는 보안 취약점을 실습용 컨트랙트 환경에서 실제로 실습해볼 수 있도록 구성되어 있습니다. 블록체인 보안 연구원, 스마트 컨트랙트 감사자(Auditor)와 같은 커리어에 필요한 역량을 쌓고자 하시는 분들을 위한 Path입니다.

#### 이런 내용을 배워요

- ✓ 이더리움 및 EVM (Ethereum Virtual Machine) 구조 이해
- ✓ Solidity 문법과 스마트 컨트랙트 개발 기초

권장 소비자 가격

1250 코인

판매가

1250 코인

Pro 구독하면

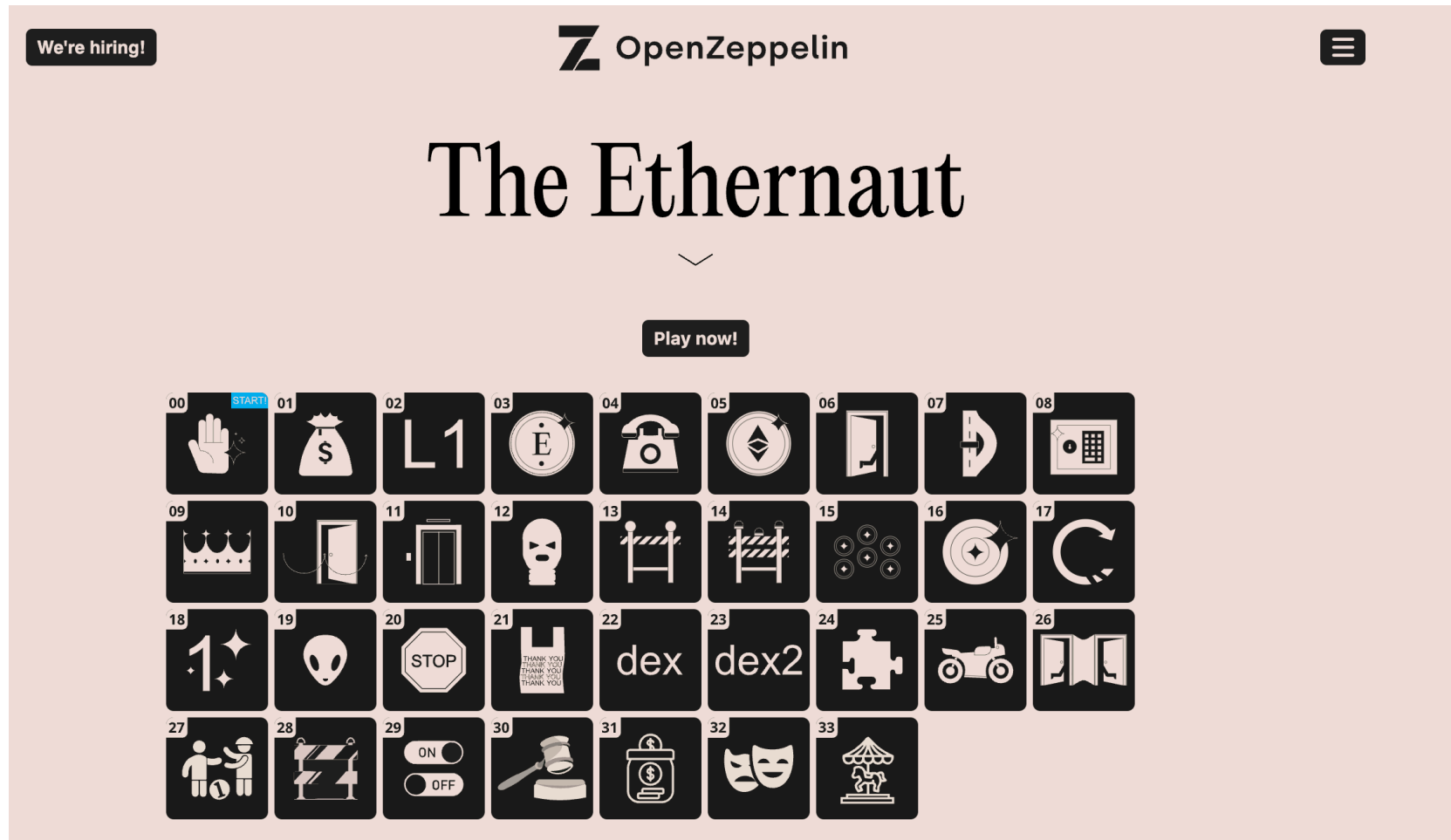
무료

구독하고 무제한 수강하기

1250 코인으로 구매하기



## ■ 어떻게 공부할 수 있는가? - Ethernaut





## ■ 어떻게 공부할 수 있는가? - Ethernaut

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.6.12;

import "openzeppelin-contracts-06/math/SafeMath.sol";

contract Reentrance {
    using SafeMath for uint256;

    mapping(address => uint256) public balances;

    function donate(address _to) public payable {
        balances[_to] = balances[_to].add(msg.value);
    }

    function balanceOf(address _who) public view returns (uint256 balance) {
        return balances[_who];
    }

    function withdraw(uint256 _amount) public {
        if (balances[msg.sender] >= _amount) {
            (bool result,) = msg.sender.call{value: _amount}("");
            if (result) {
                _amount;
            }
            balances[msg.sender] -= _amount;
        }
    }

    receive() external payable {}
}
```





## ■ 어떻게 공부할 수 있는가? - Ethernaut

```
function withdraw(uint256 _amount) public {  
    if (balances[msg.sender] >= _amount) {  
        (bool result,) = msg.sender.call{value: _amount}("");  
        if (result) {  
            _amount;  
        }  
        balances[msg.sender] -= _amount;  
    }  
}
```



## ■ 어떻게 공부할 수 있는가? - Competitive audit


### Competitive audits

Search

#### Active

● ENDS IN 33 DAYS

AUDIT



**Flare - FAsset**  
The blockchain for data. The platform for non smart contract asset DeFi. Built on enshrined data protocols.

◆ EVM


Solidity

20 Aug 5:00 AM - 24 Sep 5:00 AM

\$190,000 in USDC

● ENDS IN 4 DAYS

AUDIT



**Morpheus**  
Morpheus is for Builders of Smart Agents. Empowering them with Capital, Code & Compute.

◆ EVM

Solidity


16 Aug 5:00 AM - 26 Aug 5:00 AM

\$20,000 in USDC

#### Upcoming

● STARTS IN 18 DAYS

AUDIT



**Fluid**  

≡ Solana


Rust

09 Sep 5:00 AM - 30 Sep 5:00 AM

\$93,500 in USDC

● STARTS IN 6 DAYS

AUDIT



**GTE Perps and Launchpad**  
GTE is the world's fastest decentralized exchange. We've vertically integrated every aspect of trading - from token creation, to spot and perps - to give you the best o...

◆ EVM

Solidity

28 Aug 5:00 AM - 25 Sep 5:00 AM

\$103,250 in USDC



## ■ 어떻게 공부할 수 있는가? - Upside Academy

### 교육과정

업사이드 아카데미에서 교육하는 단계별 과정을 소개합니다.



1 단계

기본 교육

Blockchain 개요

EVM Basic

DeFi Basic

Solidity Basic

암호학 Basic

Staking

화폐현상

정보보안개론



2 단계

심화 교육

EVM Advanced

DeFi Advanced

Solidity Advanced

NFT

Solana

Cosmos

암호학02

K8s


Multichain & L2


Crosschain





## ■ 어떻게 공부할 수 있는가? - Upside Academy

← → ↻ 🌐 bearmoon.gitbook.io/bearmoon/


 **BearMoon** 🔍 Search... # K


BearMoon\_en ▾  **Introduction** 📄 Copy ▾


 **Introduction**

 Berachain PoL Overview


**THREAT MODELING**


 Threat Modeling Terminology


 PoL Threat Modeling

 dApp Threat Modeling

**SECURITY GUIDELINES**

 Impact Classification

 PoL Security Guidelines >


 dApp Security Guidelines >


**APPENDIX**

Glossary

External Resources

References

 Powered by GitBook



This document provides a comprehensive security analysis of Berachain's Proof of Liquidity (PoL) system, identifying potential threats and presenting practical guidelines to mitigate them.

<https://bearmoon.gitbook.io/bearmoon/>



## ■ 어떻게 공부할 수 있는가? - Upside Academy

### 지원혜택

교육생들의 성장에 도움이 될 수 있는 다양한 지원이 제공됩니다.

#### 교육 및 멘토링

두나무 x 티오리 현직 탭티어  
멘토들의 교육 및 멘토링 진행



#### 최신형 장비 지원

최신 사양의 MacBook Pro M4  
14인치 지급 및 모니터 지원



#### 교육 지원금 지급

교육지원금(4개월간) 팀 활동비  
별도 지급, 교육생 전원 안전 보험  
가입



#### 아카데미 전용 교육장 Up space

개인 전용석 / 강의실 지원 팀별  
프로젝트 룸



#### 전용 스낵바 제공

각종 간식 및 음료 무료 제공



#### 인증서 발급

교육 수료 시 인증서 발급



#### 수료 후 후속연계 지원

업사이더 Alumni Community  
지원, 후속 프로젝트 및 연구 지원



<https://upside.center/apply>



## ■ 어떻게 공부할 수 있는가? - 번외

← **MegaETH** 778 posts **Following**

**MegaETH** @megaeth\_labs · 14h  
MegaETH is ruthlessly pragmatic, tuned for performance and UX.

This is evident in all of our architectural decisions.

For settlement, we leverage both optimistic and ZK proofs to create efficient security for the entire chain.

You will see this same decision adopted by others

**MEGAETH** SECURED BY ZK

108 171 820 19K

**MegaETH** @megaeth\_labs · Aug 19  
MegaETH has several key innovations that let us push scalability to the extreme.

**Four Pillars Research (KR)**  
2,464 subscribers

**비장의 카드를 꺼내 든 모나드**

[[ FOUR PILLARS ]]

: : [이슈] 비장의 카드를 꺼내 든 모나드  
작성자: 시원

- 모나드는 8월 20일 다양한 역할군(OG, 빌더, KOL)에 걸친 5,000개의 영향력 있는 계정을 수동으로 선별, "모나드 카드"를 배포했다. 이러한 선별적 접근법은 대형 오피니언 리더들의 마인드웨어를 확보하는 동시에, 이어지는 할당에 대한 추천 시스템과 결합되어 대규모의 포모를 형성해냈다.

- 모나드는 비판자와 회의론자들을 선제적으로 포용하고, 많은 수의 중형 오피니언 리더들에 대해 인정을 부여함으로써 커뮤니티 구성원으로 전환시켰다. 이러한 "적을 최소화하는" 접근법은 포용성이 방어적인 부족주의보다 더 강력할 수 있음을 입증했다.

- 소규모 프로젝트들이 효율적인 커뮤니티 구축을 위해 카이토와 같은 정량적 플랫폼을 계속 활용하는 반면, 대규모 프로젝트들은 수동적이고 정성적인 큐레이션으로 방향을 전환할 것으로 전망한다. 5,000명의 수령자를 선정하기 위해 수많은 계정을 검토했음 모나드의 노동집약적 접근법은 진정성과 진심 어린 배려가 자동화된 포인트 시스템보다 더 큰 반향을 일으킨다는 신호를 보낸다.

[이슈 아티클 전문 \(포스트\)](#)  
[이슈 아티클 전문 \(웹사이트\)](#)

[FP Website](#) | [Telegram \(EN / KR\)](#) | [X \(EN / KR\)](#)  
2.7K 18:04



## ■ 퀴즈 2.

- Q2: 이더리움에서 지갑 주소 및 거래 기록을 검색할 수 있는 사이트는?

1. 이더로그 (Etherlog)
2. 이더스캔 (Etherscan)
3. 이더서치 (Ethersearch)
4. 이더익스 (Etherex)





## ■ 퀴즈 2.

- Q2: 이더리움에서 지갑 주소 및 거래 기록을 검색할 수 있는 사이트는?

1. 이더로그 (Etherlog)

2. 이더스캔 (Etherscan)

3. 이더서치 (Ethersearch)

4. 이더익스 (Etherex)







---

04

---

정리

---

## ■ Do not fear!



## ■ Do not fear!

Web3 솔직히 한번 해보고 싶은데 용어 같은게 너무 어렵다..

뭐 어떻게 배워야 하는지도, 해야하는지 모르겠다..



과거의 나



## ■ Do not fear!

하지만! 우리는 해커다!

Web3 한번 맛보면 다시 못 나간다.

재밋다.. 멋있다..



현재의 나



---

# Q&A

[cwm912@korea.ac.kr](mailto:cwm912@korea.ac.kr)

---