

한 번에 끝내는 블록체인 개발 A to Z

Chapter 2

Blockchain 2.0 - Ethereum

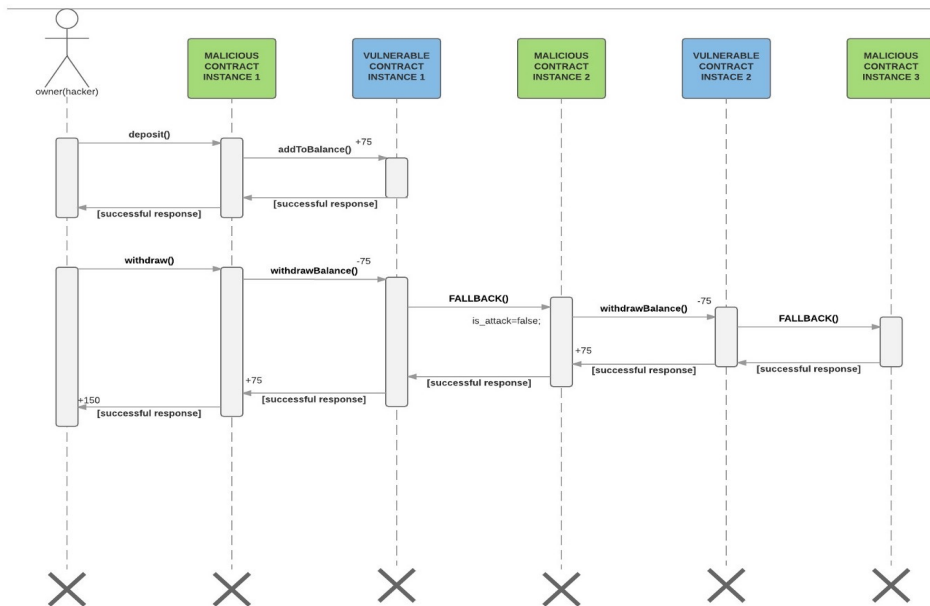
Chapter 2

Blockchain 2.0 - Ethereum

Ethereum History

THE DAO 해킹사건

- Slock.it 기업에서 Ethereum 네트워크 상에서 운영을 위해 구성중이던 THE DAO의 모집 자금이 해킹당한 사건이다.
- 공격자는 THE DAO의 코드 취약점을 파악하고 환불 요청을 무한정 반복하는 코드를 실행하여 예치한 자산 보다 훨씬 큰 자금을 획득하였다.
- 약 360만개 ETH(600억 상당)의 금액이 해킹당하고 HardFork로 이 거래를 롤백하였다.



(출처 : <https://medium.com/@MyPaoG/explaining-the-dao-exploit-for-beginners-in-solidity-80ee84f0d470>)

ICON

컨트랙트 정지

- 국내 대표적인 블록체인 기업인 ICON의 ERC20 컨트랙트에 치명적인 취약점이 발견되었다. 이 취약점은 사용자 누구든지 컨트랙트 상의 모든 토큰 전송을 중지시키는 문제였다.
- 문제의 원인은 == 을 사용해야 곳에 개발자의 실수로 !=을 사용한 것이 문제였다.
- 이를 통해서 개발사들의 컨트랙트 Audit이 필수적으로 요구되고 있다.

```
contract IcxToken is ERC20, Lockable {
    using SafeMath for uint;

    mapping( address => uint ) _balances;
    mapping( address => mapping( address => uint ) ) _approvals;
    uint _supply;
    address public walletAddress;

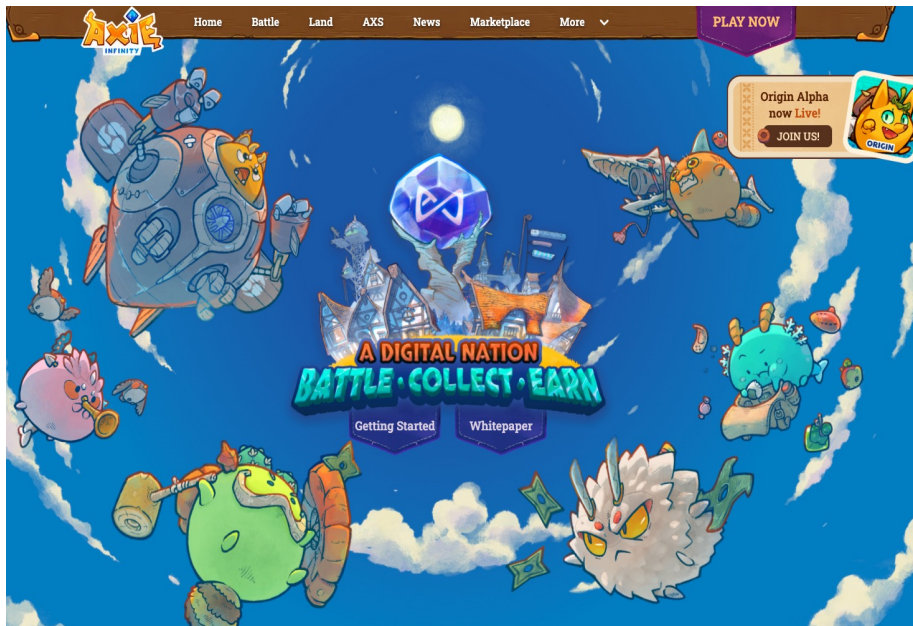
    //event TokenMint(address newTokenHolder, uint amountOfTokens);
    event TokenBurned(address burnAddress, uint amountOfTokens);
    event TokenTransfer();

    modifier onlyFromWallet {
        require(msg.sender != walletAddress);
        _;
    }
}
```

(출처 : etherscan)

P2E











- Play to Earn(P2E)란 기존 게임산업과는 달리 사용자가 게임을 하면서 돈을 벌 수 있는 형태이다.
- 동남아시아에서 출발하여 이 게임을 통해서 생활비를 마련하는 사람들이 생기면서 급격한 성장이 이루어졌다. (21년 매출 13억달러)
- 국내 게임사들이 이를 통해서 NFT와 P2E 진출을 선언하였고, 대표적인 게임사가 위메이드이다.



(출처 : <https://axieinfinity.com/>)

Ronin Bridge 해킹

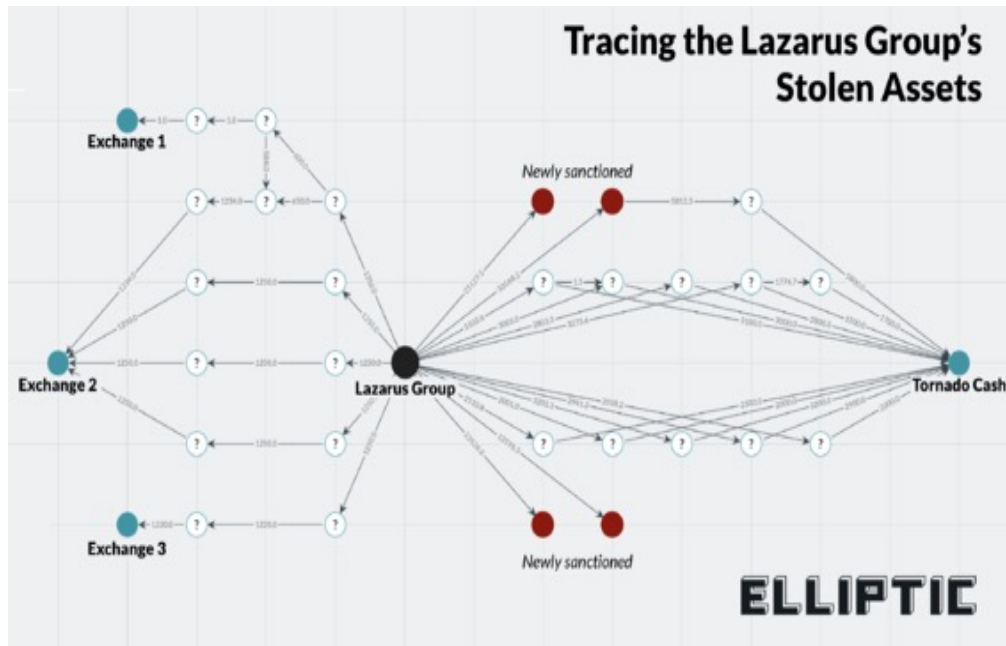
- Axie Infinity가 운영되는 Ronin Network는 Ethereum의 사이드체인이다.
- Ronin Bridge를 통해서 Ethereum과 Ronin 사이에 자산의 이동이 가능해졌다.
- 22년 3월 Ronin Bridge의 POOL에서 7000억 상당의 자금이 북한 해커에 의해서 탈취되었다.
- Ronin Network에는 9개의 검증 노드가 운영중이며 5개 이상의 키가 있어야 동작을 하는데 해커가 5개 이상의 키를 해킹하여 해킹에 성공하였다.

Overview	Internal Txns	Logs (2)	State	Comments
Transaction Hash:	0xed2c72ef1a552ddaec6dd1f5cddf0b59a8f37f82bdda5257d9c7c37db7bb9b08 			
Status:	 Success			
Block:	14442840  749879 Block Confirmations			
Timestamp:	 121 days 17 mins ago (Mar-23-2022 01:31:04 PM +UTC)			
From:	0x098b716b8aaf21512996dc57eb0615e2383e2f96 (Ronin Bridge Exploiter) 			
Interacted With (To):	Contract 0x1a2a1c938ce3ec39b6d47113c7955baa9dd454f2 (Axie Infinity: Ronin Bridge)  			
Tokens Transferred:	» From Axie Infinity: Ronin... To Ronin Bridge Expl... For 25,500,000  (\$25,525,500.00)  USD Coin (USDC)			
Value:	0 Ether (\$0.00)			
Transaction Fee:	0.0219782 Ether  (\$35.40)			
Gas Price:	0.0000001 Ether (100 Gwei)			
Ether Price:	\$3,032.98 / ETH			

(출처 : etherscan.io)

Tornado.Cash

- Bitcoin에서는 Blender(Mixer)가 CoinJoin을 이용하였다면, Ethereum에서는 Smart Contract를 통해서 자금 세탁이 가능하다.
- 대표적인 Mixer인 Tornado Cash는 해커들이 자금 세탁을 하는 대표적인 통로이다.
- Ronin Bridge 해킹 자금도 이를 통해 세탁 후 해외 거래소로 이동하였을 것이라 보고 있다.



(출처 : <https://www.playtoearn.online/2022/03/30/ronin-bridge-hack-625-million-lost-in-the-biggest-defi-hack-to-date/>)

OverFlow 공격

- Ethereum Overflow 공격은 변수의 범위를 벗어나는 값을 입력하여 사용자가 가진 잔액보다 많은 금액을 송금하도록 하는 것이다.
- UINT8 인 변수의 최대값은 0~255이다. 0에서 -1을 하게 되면 -1이 되는 것이 아닌 255가 되는 것을 이용한 공격이다.
- Solidity 0.8 버전이상에서는 이를 자동으로 확인해주지만, 그 이전 버전은 Openzeppelin의 SafeMath Library를 사용하는 것이 일반적이다.

0x1abab4c8db9a30e703114528e31dee129a3a758f7f8abc3b6494aad3d304e43f

Success

5499035 (1588 block confirmations)

6 hrs 29 mins ago (Apr-24-2018 07:16:19 PM +UTC)

0xd6a09bdb29e1eafa92a30373c44b09e2e2e0651e

Contract [0x55f93985431fc9304077687a35a1ba103dc1e081](#) (SmartMeshICO)

▶ 65,133,050,195,990,400,000,000,000,000,000,000,000,000,000,000,000,0891004451135422463
(\$5,468,623,000,895,510,000,000,000,000,000,000,000,000,000,000,000) 🔗[ERC20 \(SmartMesh Token\)](#) from
[0xdf31a499a5a8358...to → 0xdf31a499a5a8358...](#)

▶ 50,659,039,041,325,800,000,000,000,000,000,000,000,000,000,000,000,693003461994217473
(\$4,253,373,445,140,950,000,000,000,000,000,000,000,000,000,000,000) 🔗[ERC20 \(SmartMesh Token\)](#) from
[0xdf31a499a5a8358...to → 0xd6a09bdb29e1ea...](#)

(출처 : <https://thenextweb.com/news/ethereum-smart-contract-integer-overflow>)

Smart Contract

취약점

① 접근권한 제어 문제

메시지 호출을 통해 다른 Contract Public 함수의 권한을 획득하는 것이다. 이를 통해 해당 함수를 공격자가 마음대로 이용할 수 있다.

② 짧은 주소 공격

EVM이 전체 자리수에서 부족한 자리에 0을 자동으로 추가함을 이용한 공격이다.

주소가 abcdef00일 경우 abcdef만 전송하여 뒤에 붙는 송금액 (0010)을 001000으로 바꿔 송금하게 하는 것이다.

③ 잔액 조건 무효화

함수가 특정 잔액이 이상이 있어야 실행이 되게 하는 조건이 있을 때, 공격자가 Fallback 함수를 Selfdestruct로 동작하지 않도록 하고 입금하여 공격 함수를 실행하게 할 수 있다.

④ DoS 공격

Loop 가 있는 함수의 Loop 횟수를 증가 시켜 컨트랙트 실행에 필요한 Gas Limit을 Block Gas Limit만큼 증가시켜 컨트랙트를 무력화 시키는 공격이다.