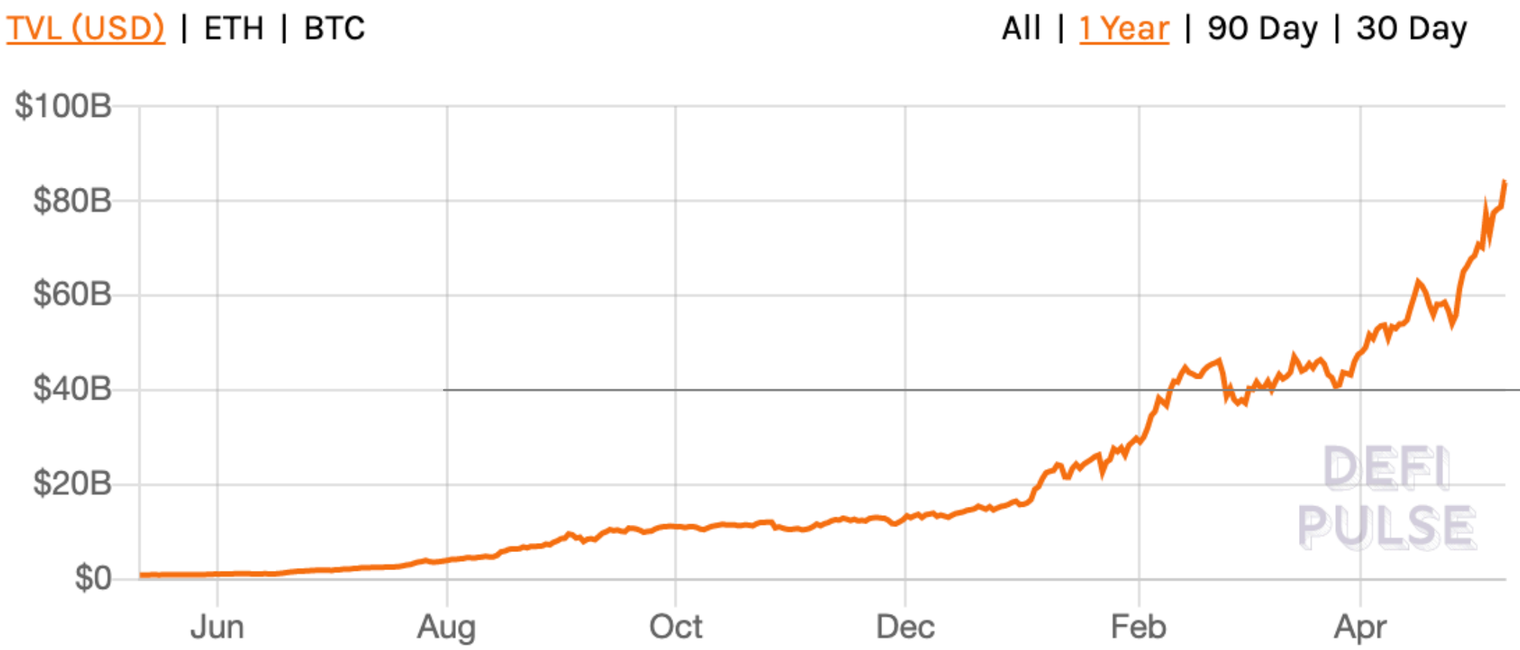
Total Value Locked (USD) in DeFi



1.	Maker	Ethereum	Lending	$14.30B	7.27%
2.	Aave	Ethereum	Lending	$11.08B	-0.97%
3.	Compound	Ethereum	Lending	$11.05B	6.91%
4.	Uniswap	Ethereum	DEXes	$7.90B	4.58%
5.	Curve Finance	Ethereum	DEXes	$7.82B	6.00%
6.	SushiSwap	Ethereum	DEXes	$5.47B	2.06%

(2021-05-09, DeFi Pulse 기준)

DeFi와 보안

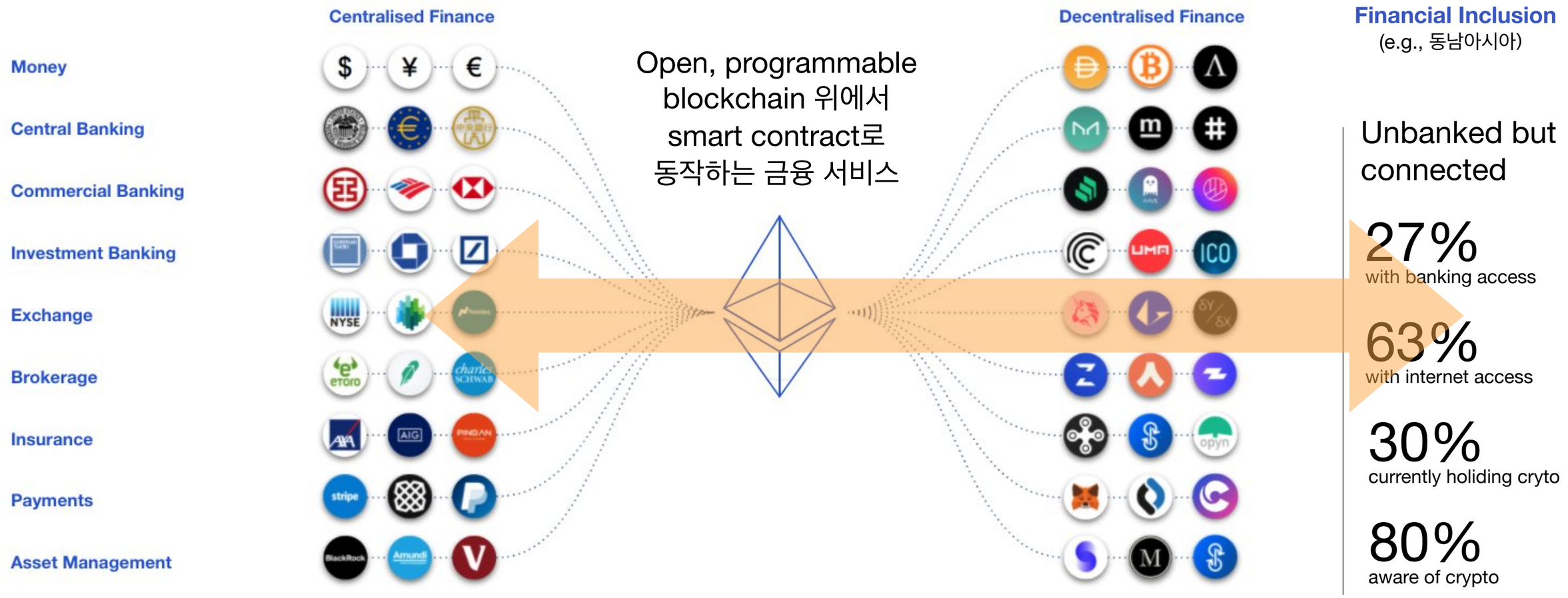
2021-05-20

이종협

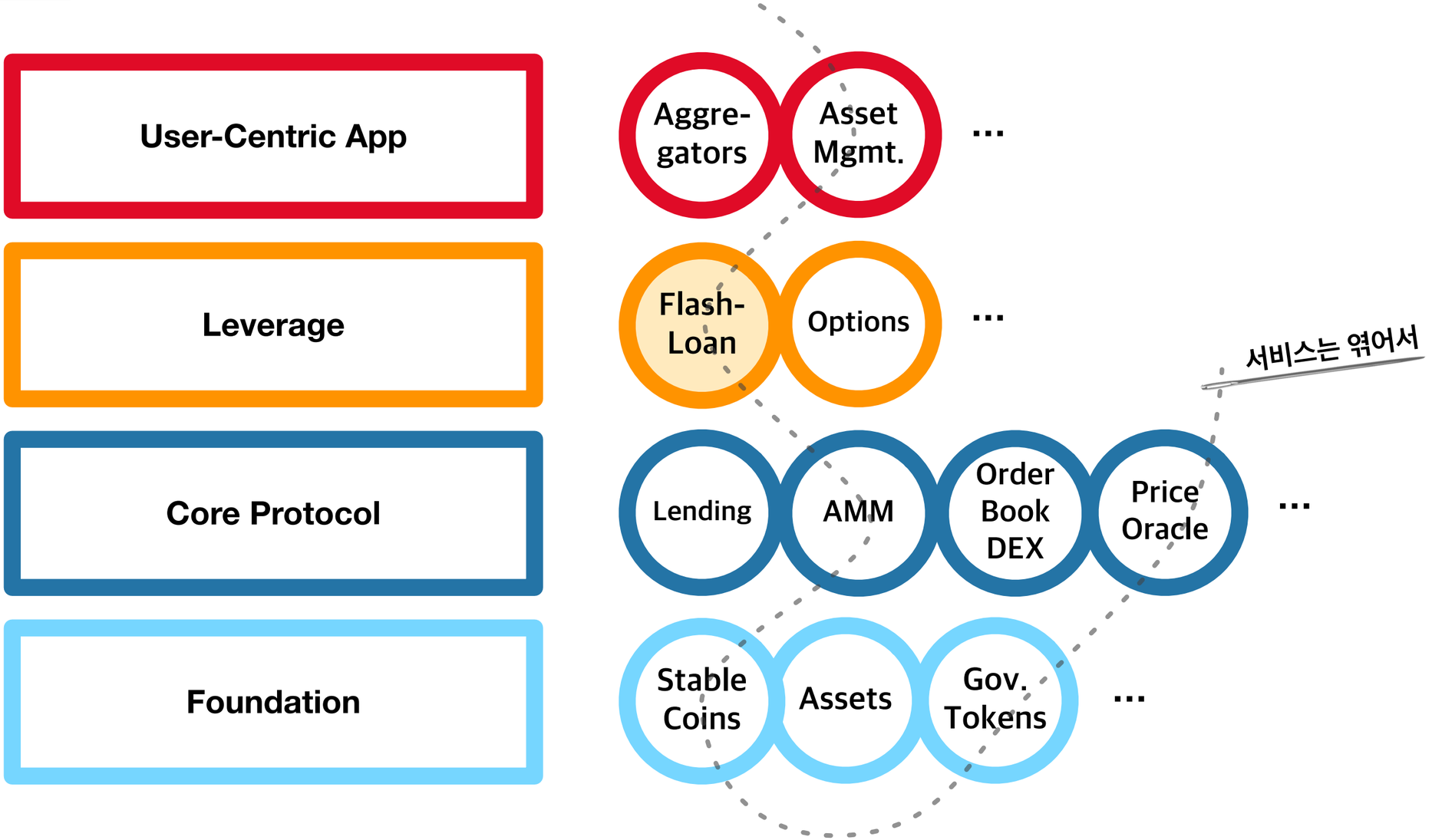
Rekt Leaderboard

1. **EasyFi - REKT** *Unaudited*
   $59,000,000 | 19 Apr 2021
2. **Uranium Finance - REKT** *Unaudited*
   $57,200,000 | 28 Apr 2021
3. **Kucoin - REKT** *Internal audit*
   $45,000,000 | 29 Sep 2020
4. **Alpha Finance - REKT** *Quantstamp, Peckshield*
   $37,500,000 | 13 Feb 2021
5. **Meerkat Finance - BSC - REKT** *Unaudited*
   $32,000,000 | 04 Mar 2021
6. **Spartan Protocol - REKT** *Certik*
   $30,500,000 | 02 May 2021
7. **Paid Network - REKT** *Unaudited*
   $27,000,000 | 05 Mar 2021
8. **Harvest Finance - REKT** *Haechi, Peckshield*
   $25,000,000 | 26 Oct 2020
9. **Pickle Finance - REKT** *MixBytes, Haechi*
   $19,700,000 | 22 Nov 2020
10. **Rari Capital - REKT** *Unaudited*
    $15,000,000 | 8 May 2021
11. **Furucombo - REKT** *Haechi*
    $14,000,000 | 27 Feb 2021
12. **Compounder Finance - REKT** *Solidity Finance*
    $12,000,000 | 02 Dec 2020
13. **Value DeFi - REKT 3** *Unaudited*
    $11,000,000 | 7 May 2021
14. **Yearn - REKT** *Unaudited*
    $11,000,000 | 05 Feb 2021
15. **Value DeFi - REKT 2** *Unaudited*
    $10,000,000 | 5 May 2021
16. **Cover - REKT** *Arcadia Group*
    $9,400,000 | 29 Dec 2020
17. **Hack Epidemic (Origin Protocol - REKT)** *Unaudited*
    $8,000,000 | 17 Nov 2020
18. **Warp Finance - REKT** *Hacken*
    $7,800,000 | 18 Dec 2020
19. **Value DeFi - REKT** *Peckshield*
    $7,000,000 | 14 Nov 2020
20. **Roll - REKT** *Unaudited*
    $5,700,000 | 14 Mar 2021
21. **DODO - REKT** *Unaudited*
    $2,000,000 | 09 Mar 2021
22. **Akropolis - REKT** *CertiK, SmartDec*
    $2,000,000 | 12 Nov 2020

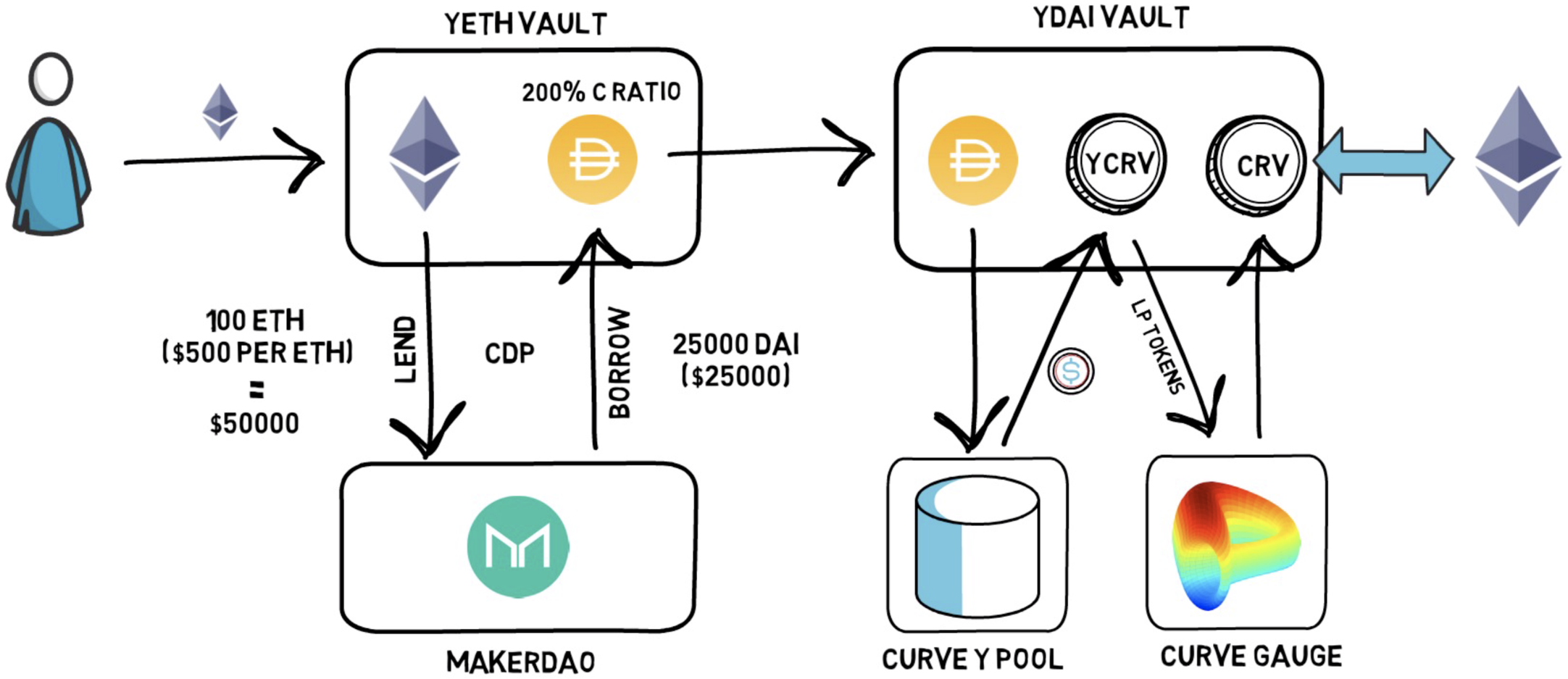
DeFi - 양면의 존재


Centralised Finance
Money
Central Banking
Commercial Banking
Investment Banking
Exchange
Brokerage
Insurance
Payments
Asset Management
Open, programmable blockchain 위에서 smart contract로 동작하는 금융 서비스
Decentralised Finance
Financial Inclusion
(e.g., 동남아시아)
Unbanked but connected
27%
with banking access
63%
with internet access
30%
currently holiding cryto
80%
aware of crypto

DeFi Stack


User-Centric App
Leverage
Core Protocol
Foundation
Aggre-gators
Asset Mgmt.
...
Flash-Loan
Options
...
Lending
AMM
Order Book DEX
Price Oracle
...
Stable Coins
Assets
Gov. Tokens
...
서비스는 엮어서

Money Lego - Composability



(e.g. ETH Vault)

DeFi 보안의 고민거리

Smart contracts

전통적 문제

Domain Knowledge

금융+기술의 이해

초고속성장하는 산업

시장 > 기술

Control dependency가 높은 시스템의 안전성은?

Money lego = security model lego

```
function withdraw(
    address underlying,
    address tokenX
) public {
    uint256 underlyingAmount = IERC20(underlying).balanceOf(address(this));
    // call to FakeUnderlying
    tokenX.transfer(msg.sender, underlygingAmount);
}
```

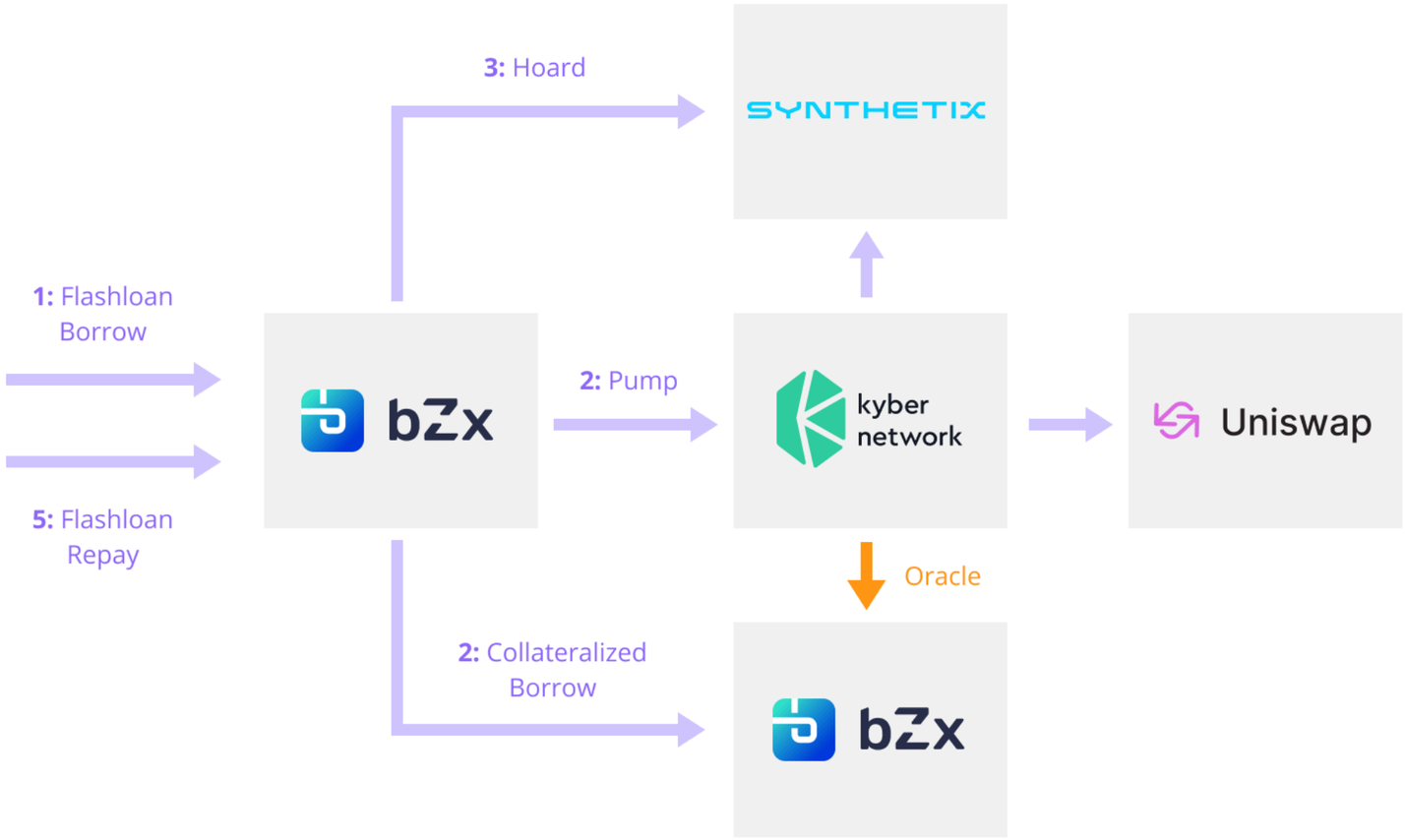
(너무나 당연하게도) 무엇이 도사리고 있는지 모릅니다.

아마도 balance를 return?

DeFi의 component를 제대로 이해하고 있는가?

Flashloan을 이용한 (oracle) 시세 조작

Five Composable DeFi Protocols in bZx Hack II



1. Deposit collateral and take 7,500ETH flash loan on bZx	🡅 7,500 ETH
2. Convert 3518 ETH to sUSD using Synthetix	🡇 3,518 ETH
3. Use 900 ETH to manipulate the sUSD price to 2.5$ on Kyber	🡇 900 ETH
4. Deposit sUSD to bZx as collateral to borrow more ETH	= 3,083 ETH
5. Thanks to DeFi protocols pricing sUSD at $2.5, bZx will think the 3,518 ETH you spent on sUSD is actually worth 8,795 ETH. So the protocol will think it is safe to lend you 6,796 ETH, for something you bought only 3,518 ETH	🡅 6,796 ETH = 9,879 ETH
6. Use your new loan and left-overs from your original balance to pay back the initial 7,500 ETH, take back your collateral and enjoy 2,379 ETH in gross profit	🡇 7,500 ETH 🏆 2,379 ETH
Total value locked in bZx dropped from $19.06M to $12.33M.	

시장의 성장이 기술의 성숙보다 우선시 되면 어떻게 되는가?

깊은 이해없이 코드를 fork해서 사용하면서 문제 발생

```
        uint balance0;
        uint balance1;
        { // scope for _token{0,1}, avoids stack too deep errors
        address _token0 = token0;
        address _token1 = token1;
        require(to != _token0 && to != _token1, 'UraniumSwap: INVALID_TO');
        if (amount0Out > 0) _safeTransfer(_token0, to, amount0Out); // optimistically tr
ansfer tokens
        if (amount1Out > 0) _safeTransfer(_token1, to, amount1Out); // optimistically tr
ansfer tokens
        if (data.length > 0) IUraniumCallee(to).pancakeCall(msg.sender, amount0Out, amou
nt1Out, data);
        balance0 = IERC20(_token0).balanceOf(address(this));
        balance1 = IERC20(_token1).balanceOf(address(this));
        }
        uint amount0In = balance0 > _reserve0 - amount0Out ? balance0 - (_reserve0 - amo
unt0Out) : 0;
        uint amount1In = balance1 > _reserve1 - amount1Out ? balance1 - (_reserve1 - amo
unt1Out) : 0;
        require(amount0In > 0 || amount1In > 0, 'UraniumSwap: INSUFFICIENT_INPUT_AMOUN
T');
        { // scope for reserve{0,1}Adjusted, avoids stack too deep errors
        uint balance0Adjusted = balance0.mul(10000).sub(amount0In.mul(16));
        uint balance1Adjusted = balance1.mul(10000).sub(amount1In.mul(16));
        require(balance0Adjusted.mul(balance1Adjusted) >= uint(_reserve0).mul(_reserve
1).mul(1000**2), 'UraniumSwap: K');
        }

        _update(balance0, balance1, _reserve0, _reserve1);
        emit Swap(msg.sender, amount0In, amount1In, amount0Out, amount1Out, to);
    }

```

```
        uint balance0;
        uint balance1;
        { // scope for _token{0,1}, avoids stack too deep errors
        address _token0 = token0;
        address _token1 = token1;
        require(to != _token0 && to != _token1, 'UniswapV2: INVALID_TO');
        if (amount0Out > 0) _safeTransfer(_token0, to, amount0Out); // optimistically tr
ansfer tokens
        if (amount1Out > 0) _safeTransfer(_token1, to, amount1Out); // optimistically tr
ansfer tokens
        if (data.length > 0) IUniswapV2Callee(to).uniswapV2Call(msg.sender, amount0Out,
amount1Out, data);
        balance0 = IERC20(_token0).balanceOf(address(this));
        balance1 = IERC20(_token1).balanceOf(address(this));
        }
        uint amount0In = balance0 > _reserve0 - amount0Out ? balance0 - (_reserve0 - amo
unt0Out) : 0;
        uint amount1In = balance1 > _reserve1 - amount1Out ? balance1 - (_reserve1 - amo
unt1Out) : 0;
        require(amount0In > 0 || amount1In > 0, 'UniswapV2: INSUFFICIENT_INPUT_AMOUNT');

        { // scope for reserve{0,1}Adjusted, avoids stack too deep errors
        uint balance0Adjusted = balance0.mul(1000).sub(amount0In.mul(3));
        uint balance1Adjusted = balance1.mul(1000).sub(amount1In.mul(3));
        require(balance0Adjusted.mul(balance1Adjusted) >= uint(_reserve0).mul(_reserve
1).mul(1000**2), 'UniswapV2: K');
        }

        _update(balance0, balance1, _reserve0, _reserve1);
        emit Swap(msg.sender, amount0In, amount1In, amount0Out, amount1Out, to);
    }

```

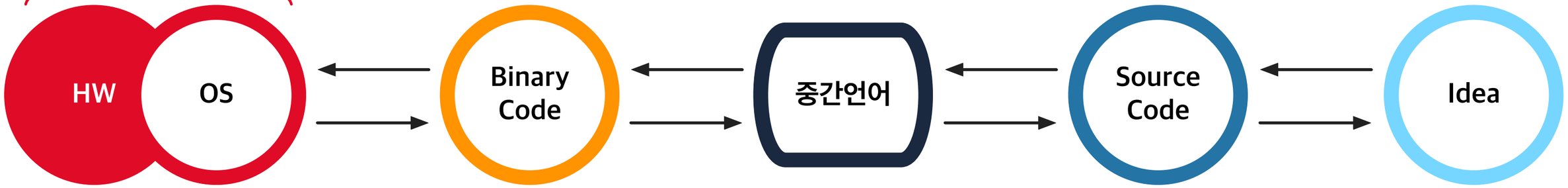
어느 쪽이 original code 일까요?

1. **EasyFi - REKT** *Unaudited*
   $59,000,000 | 19 Apr 2021
2. **Uranium Finance - REKT** *Unaudited*
   $57,200,000 | 28 Apr 2021
3. **Kucoin - REKT** *Internal audit*
   $45,000,000 | 29 Sep 2020
4. **Alpha Finance - REKT** *Quantstamp, Peckshield*
   $37,500,000 | 13 Feb 2021
5. **Meerkat Finance - BSC - REKT** *Unaudited*
   $32,000,000 | 04 Mar 2021
6. **Spartan Protocol - REKT** *Certik*
   $30,500,000 | 02 May 2021
7. **Paid Network - REKT** *Unaudited*
   $27,000,000 | 05 Mar 2021
8. **Harvest Finance - REKT** *Haechi, Peckshield*
   $25,000,000 | 26 Oct 2020
9. **Pickle Finance - REKT** *MixBytes, Haechi*
   $19,700,000 | 22 Nov 2020
10. **Rari Capital - REKT** *Unaudited*
    $15,000,000 | 8 May 2021
11. **Furucombo - REKT** *Haechi*
    $14,000,000 | 27 Feb 2021
12. **Compounder Finance - REKT** *Solidity Finance*
    $12,000,000 | 02 Dec 2020
13. **Value DeFi - REKT 3** *Unaudited*
    $11,000,000 | 7 May 2021
14. **Yearn - REKT** *Unaudited*
    $11,000,000 | 05 Feb 2021
15. **Value DeFi - REKT 2** *Unaudited*
    $10,000,000 | 5 May 2021
16. **Cover - REKT** *Arcadia Group*
    $9,400,000 | 29 Dec 2020
17. **Hack Epidemic (Origin Protocol - REKT)** *Unaudited*
    $8,000,000 | 17 Nov 2020
18. **Warp Finance - REKT** *Hacken*
    $7,800,000 | 18 Dec 2020
19. **Value DeFi - REKT** *Peckshield*
    $7,000,000 | 14 Nov 2020
20. **Roll - REKT** *Unaudited*
    $5,700,000 | 14 Mar 2021
21. **DODO - REKT** *Unaudited*
    $2,000,000 | 09 Mar 2021
22. **Akropolis - REKT** *CertiK, SmartDec*
    $2,000,000 | 12 Nov 2020

DeFi 보안의 현재는?

Software security에서의 (기존) 접근 방법

실제 사고는
여기에서 일어난다.



Reverse code engineering (decompiler, manual)

Design verification

ASLR

DEP, W^X

Fuzzing

Static Analysis

Ref monitors

CFI, SFI, …
(Rewriting)

New PLs.

Anti Virus

AEG (init)

Binary AEG (Mayhem)

반복되는
창과 방패의 싸움

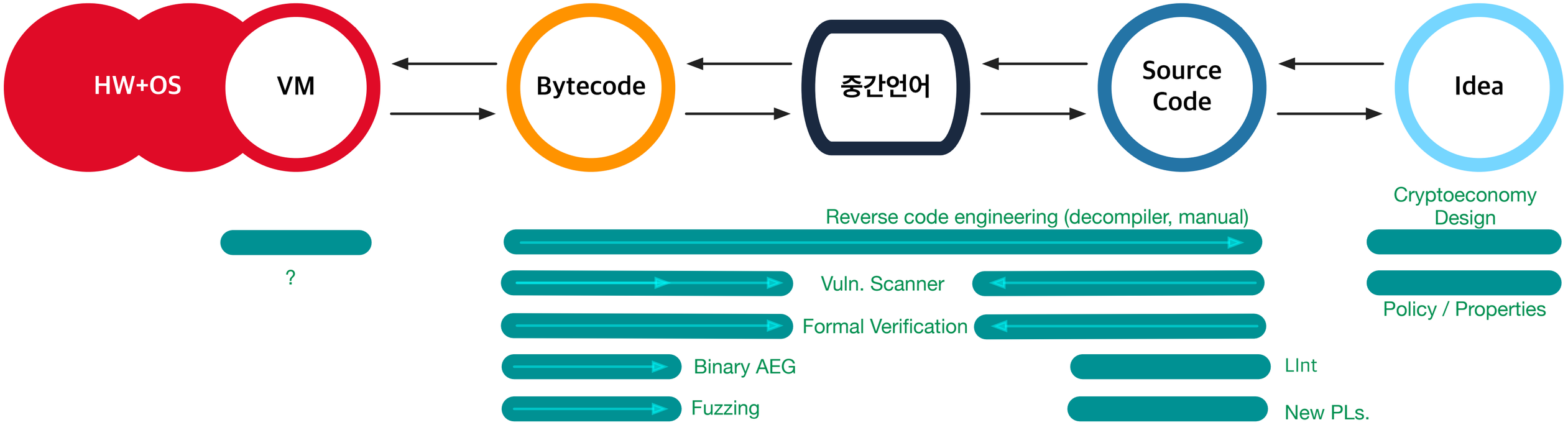
실제 문제는 여기에
있으나 너무 복잡하다.

Binary
분석의
마지노선

기존의 강자가
너무 쎄다.
(Parsing도 어렵다)

Mind
the gap!

Blockchain Service에 대한 보안 접근 방법



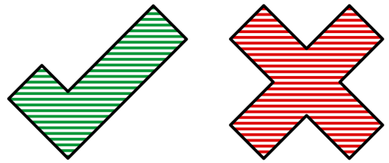
Binary Symbolic Exeuction!

얼마나 필요한가?

새로운 환경에 맞는 새로운 모델이 필요

Macro와 Micro적인 생각을 동시에 해야 한다.

가정(assumption)의 파괴



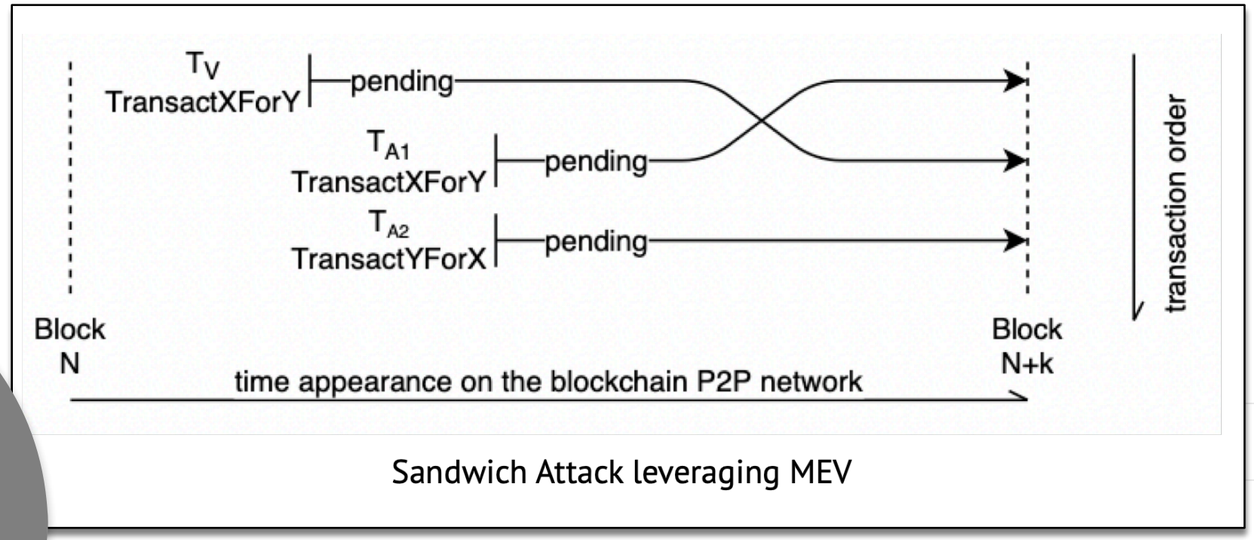
In Code We Trust 

Single security model 

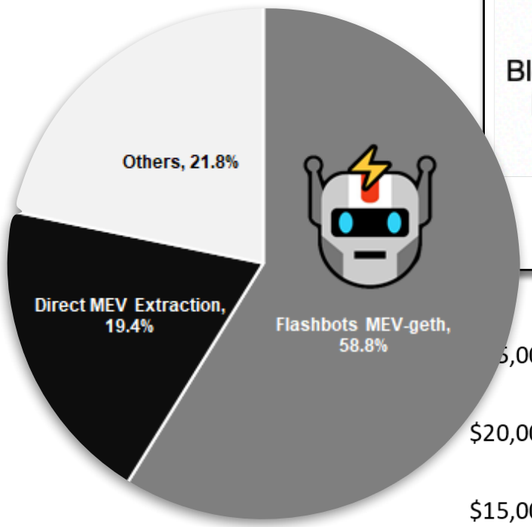
Static analysis가 중요하다 

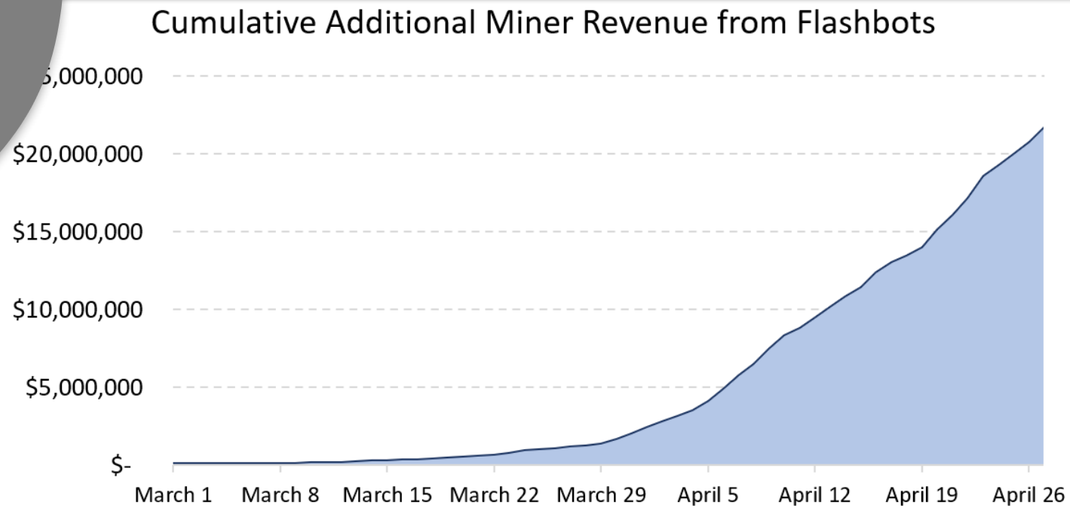
Audit을 많이 받으면 좋다
(+ formal verification) 

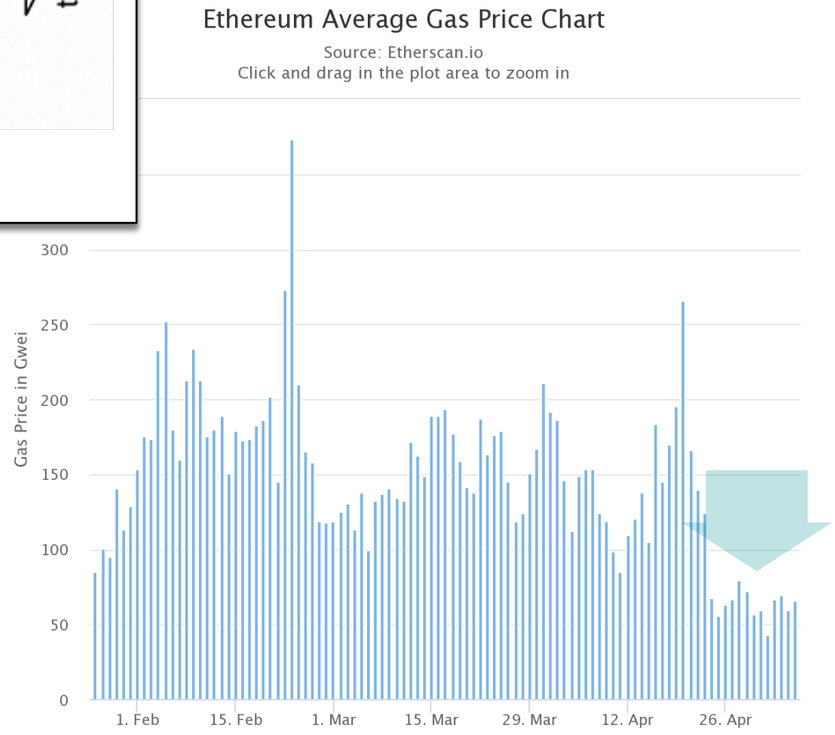
“Dark forest” - MEV / Flash bot



Sandwich Attack leveraging MEV







DeFi 산업이 무섭게 떠올라 누구나 혜택을 챙겨가겠지만,
(특히 보안은) 아직 허술하고 가꾸어나갈 부분이 많습니다.

이미 현재 보안의 가정과 모델은 잘 맞지 않습니다.
새로운 관점과 아이디어가 절실합니다.

최전선에서의 고민 — 너무 크고 재미있는 문제입니다.
협력을 구합니다!

jonghyup
@thebifrost.io
@pilab.co
@gachon.ac.kr