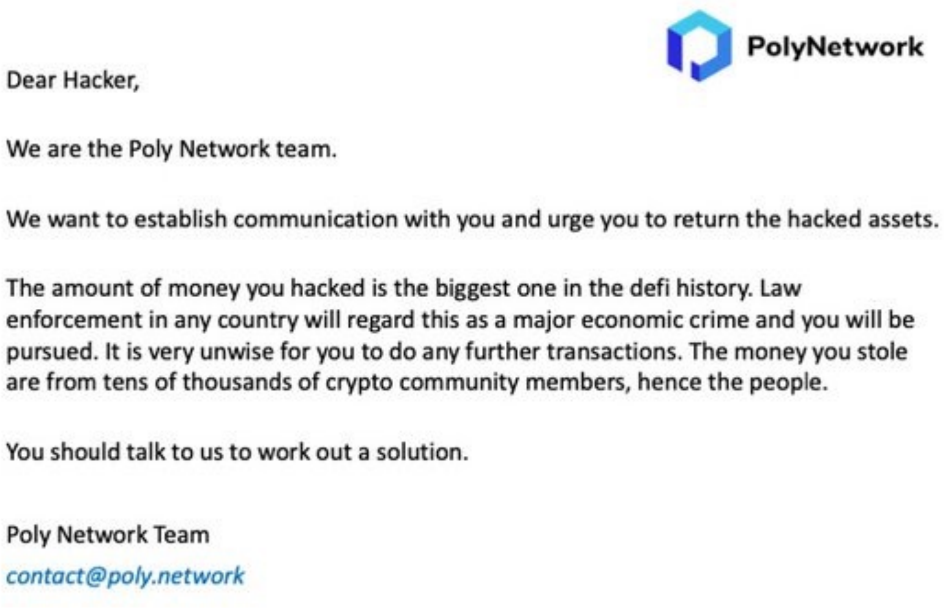
Poly Network Hack

PolyNetwork – 600M $

- Biggest hack ever in the history of cryptocurrency
- Multi chain hack:
    - Ethereum
    - Binance Smart Chain
    - Polygon Network



PolyNetwork

Dear Hacker,

We are the Poly Network team.

We want to establish communication with you and urge you to return the hacked assets.

The amount of money you hacked is the biggest one in the defi history. Law enforcement in any country will regard this as a major economic crime and you will be pursued. It is very unwise for you to do any further transactions. The money you stole are from tens of thousands of crypto community members, hence the people.

You should talk to us to work out a solution.

Poly Network Team
contact@poly.network

https://twitter.com/PolyNetwork2/status/1425123153009803267

Poly Network Hack

Who was the attacker? **His address(es)**

Attacker ETH:
0xc8a65fadf0e0ddaf421f28feab69bf6e2e589963

Attacker BSC:
0x0D6e286A7cfD25E0c01fEe9756765D8033B32C71

Attacker Polygon:
0x5dc3603C9D42Ff184153a8a9094a73d461663214

Which contracts were exploited?

Contract ETH
0x250e76987d838a75310c34bf422ea9f1ac4cc906

Contract BSC
0x05f0fDD0E49A5225011fff92aD85cC68e1D1F08e

Contract Polygon
0x28FF66a1B95d7CAcf8eDED2e658f768F44841212

https://rekt.news/polynetwork-rekt/

Poly Network – Stolen Funds Breakdown

Ethereum Blockchain

	Quantity stolen
USDC	96,389,444
WBTC (wrapped Bitcoin)	1,032
DAI	673,227
UNI (Uniswap)	43,023
SHIBA	259,737,345,149
renBTC	14.47
USDT	33,431,197
wETH (wrapped Ether)	26,109
FEI USD	616,082

Binance Smart Chain

	Quantity stolen
BNB	6,613.44
USDC	87,603,373
ETH	299
BTCB	26,629
BUSD	1,023

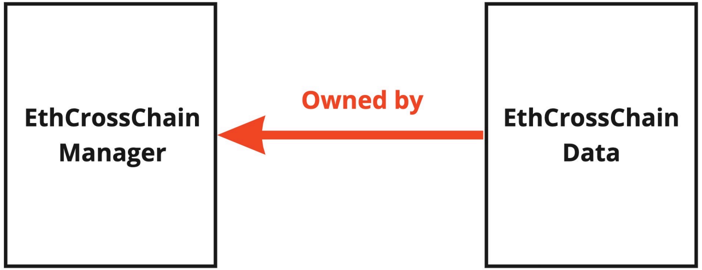
Polygon Blockchain

	Quantity stolen
USDC	85,089,610

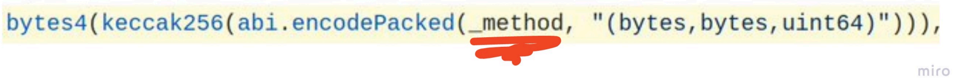
PolyNetwork Hack – The 2 exploited vulnerabilities

Mismanagement of access rights between two contracts

EthCrossChainManager is an owner of EthCrossChainData,
= EthCrossChainManager can execute privileged functions!



_method is user defined
= can be set at will.



```
bytes4(keccak256(abi.encodePacked(_method, "(bytes,bytes,uint64)"))),
```

Solidity Code

Poly Network – The vulnerable contracts

Vulnerable Contract 1: `EthCrossChainManager`

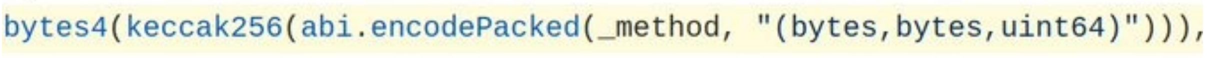
➔ Can be called by anyone
Allows to trigger messages from another chain to the Poly chain

Vulnerable function: `verifyHeaderAndExecuteTx`

Execute a cross chain transaction by:

- ○ Specifying a target contract (on Poly network)
- ○ Run a specific function in the target contract, using its “**Solidity function id**” [1]

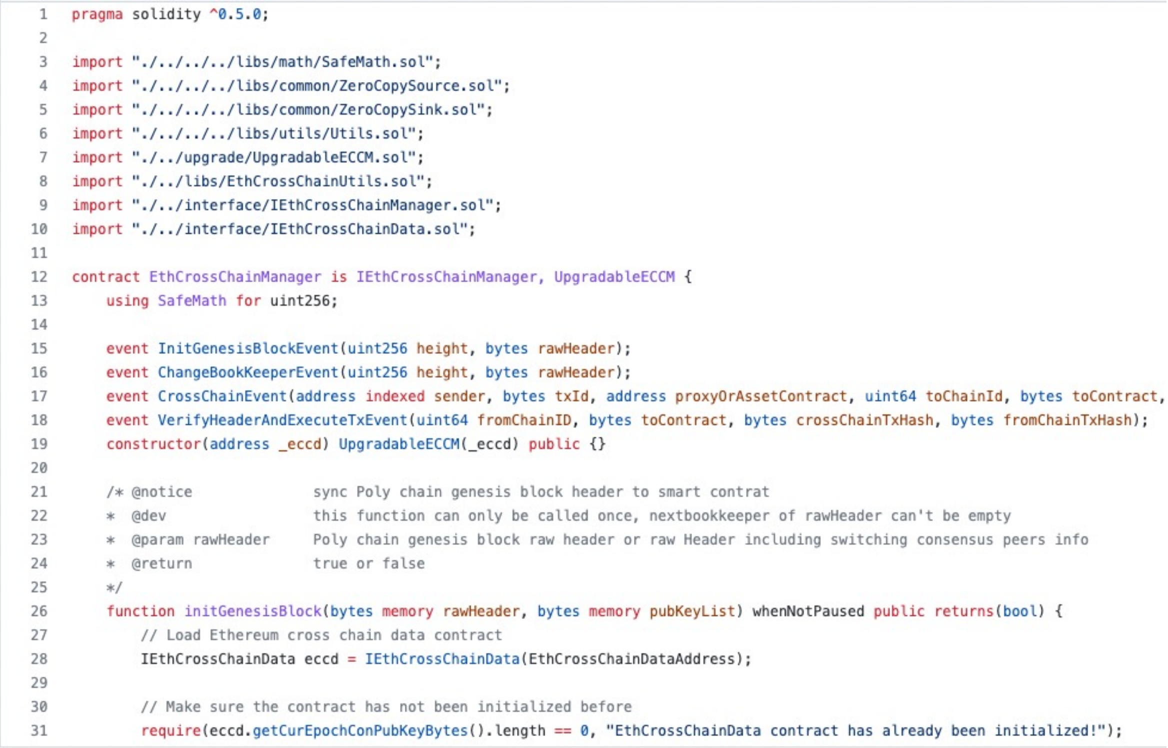
Solidity function id =



```
bytes4(keccak256(abi.encodePacked(_method, "(bytes,bytes,uint64)"))),
```

[1] This is similar to a function selector, except that the parameters types are already set up in stone as (bytes,bytes,uint64)

PolyNetwork – Vulnerable Contract (Solidity)

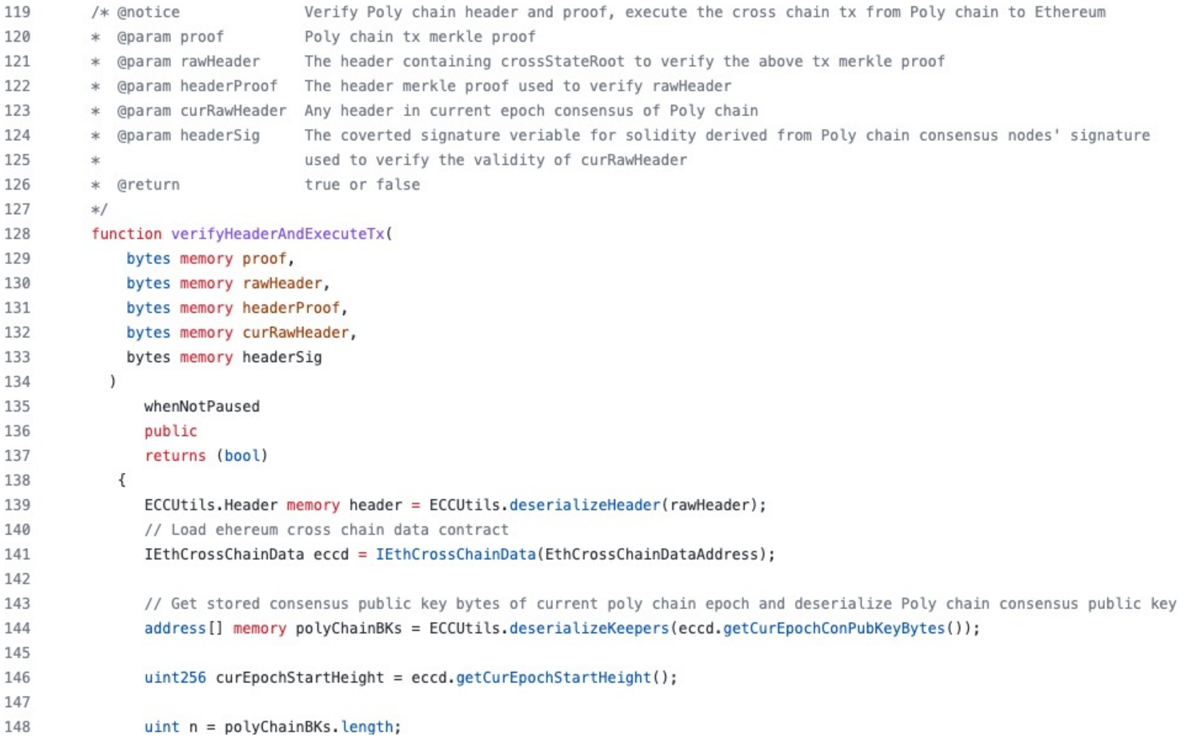


```solidity
pragma solidity ^0.5.0;

import "./../../../libs/math/SafeMath.sol";
import "./../../../libs/common/ZeroCopySource.sol";
import "./../../../libs/common/ZeroCopySink.sol";
import "./../../../libs/utils/Utils.sol";
import "./../upgrade/UpgradableECCM.sol";
import "./../libs/EthCrossChainUtils.sol";
import "./../interface/IEthCrossChainManager.sol";
import "./../interface/IEthCrossChainData.sol";

contract EthCrossChainManager is IEthCrossChainManager, UpgradableECCM {
    using SafeMath for uint256;

    event InitGenesisBlockEvent(uint256 height, bytes rawHeader);
    event ChangeBookKeeperEvent(uint256 height, bytes rawHeader);
    event CrossChainEvent(address indexed sender, bytes txId, address proxyOrAssetContract, uint64 toChainId, bytes toContract,
    event VerifyHeaderAndExecuteTxEvent(uint64 fromChainID, bytes toContract, bytes crossChainTxHash, bytes fromChainTxHash);
    constructor(address _eccd) UpgradableECCM(_eccd) public {}

    /* @notice              sync Poly chain genesis block header to smart contrat
    *  @dev                 this function can only be called once, nextbookkeeper of rawHeader can't be empty
    *  @param rawHeader     Poly chain genesis block raw header or raw Header including switching consensus peers info
    *  @return              true or false
    */
    function initGenesisBlock(bytes memory rawHeader, bytes memory pubKeyList) whenNotPaused public returns(bool) {
        // Load Ethereum cross chain data contract
        IEthCrossChainData eccd = IEthCrossChainData(EthCrossChainDataAddress);

        // Make sure the contract has not been initialized before
        require(eccd.getCurEpochConPubKeyBytes().length == 0, "EthCrossChainData contract has already been initialized!");
```

…

Source: *https://gist.github.com/CJ42/868003588f027619edac9938ce128b52*

PolyNetwork – Vulnerable Function (Solidity)



```
/* @notice              Verify Poly chain header and proof, execute the cross chain tx from Poly chain to Ethereum
*  @param proof         Poly chain tx merkle proof
*  @param rawHeader     The header containing crossStateRoot to verify the above tx merkle proof
*  @param headerProof   The header merkle proof used to verify rawHeader
*  @param curRawHeader  Any header in current epoch consensus of Poly chain
*  @param headerSig     The coverted signature veriable for solidity derived from Poly chain consensus nodes' signature
*                       used to verify the validity of curRawHeader
*  @return              true or false
*/
function verifyHeaderAndExecuteTx(
    bytes memory proof,
    bytes memory rawHeader,
    bytes memory headerProof,
    bytes memory curRawHeader,
    bytes memory headerSig
  )
      whenNotPaused
      public
      returns (bool)
   {
      ECCUtils.Header memory header = ECCUtils.deserializeHeader(rawHeader);
      // Load ehereum cross chain data contract
      IEthCrossChainData eccd = IEthCrossChainData(EthCrossChainDataAddress);

      // Get stored consensus public key bytes of current poly chain epoch and deserialize Poly chain consensus public key
      address[] memory polyChainBKs = ECCUtils.deserializeKeepers(eccd.getCurEpochConPubKeyBytes());

      uint256 curEpochStartHeight = eccd.getCurEpochStartHeight();

      uint n = polyChainBKs.length;
```

…

Source: *https://gist.github.com/CJ42/868003588f027619edac9938ce128b52#file-polynetwork-hack-sol-L128-L134*

Poly Network – The vulnerable contracts

Vulnerable Contract 2: `EthCrossChainData`

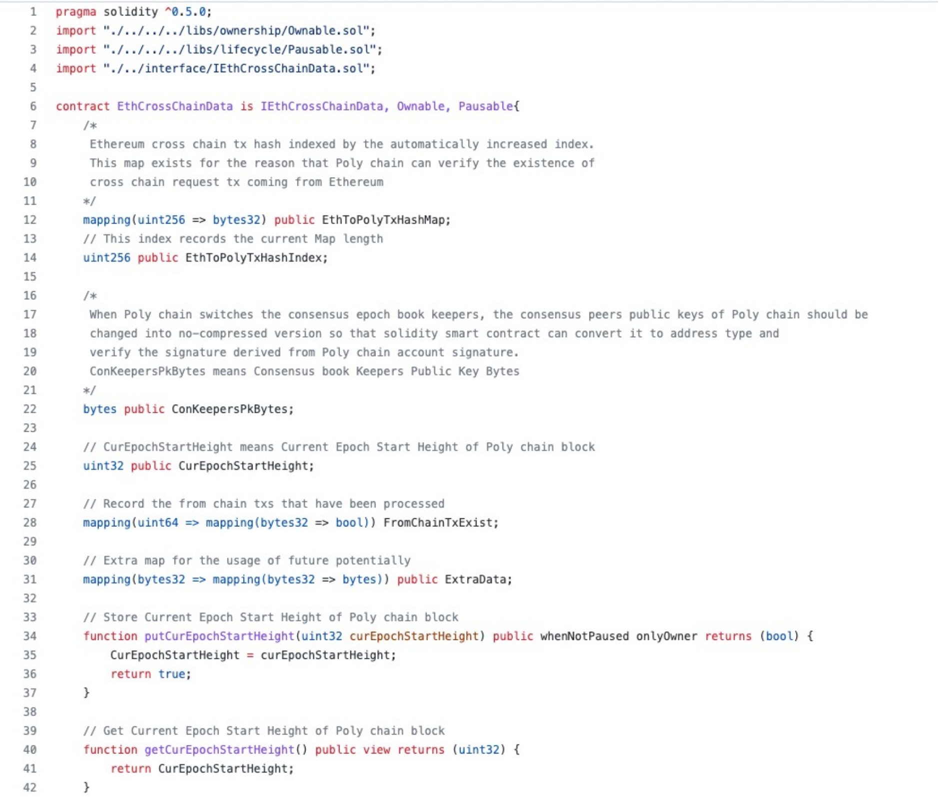
Very High Privileged contract ! ➔ Can only be called by its owners.

Set + manage list of **"Keepers"**
= list of public keys that manage the wallets in the underlying liquidity chain

➔ **Keepers have the right to execute large transactions,** transfer large amounts to other wallets.

Vulnerable function: *putCurEpochConPubKeyBytes*
= become a **"Keeper"**
Set the public key (passed as parameter) as a Keeper

PolyNetwork – Vulnerable Contract (Solidity)

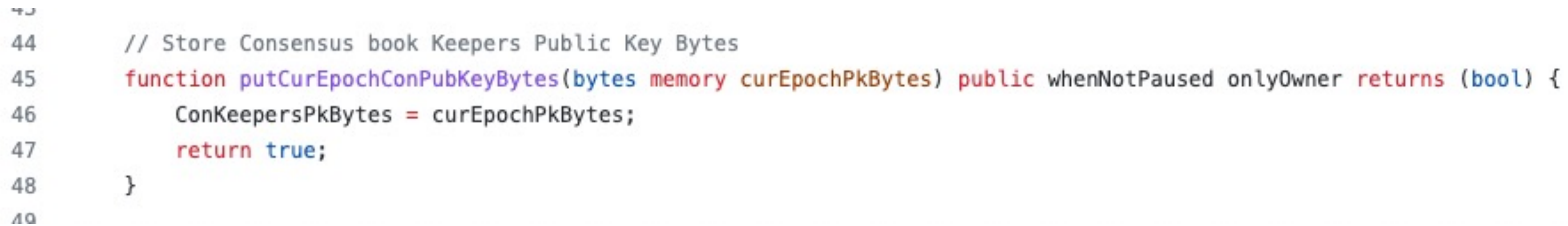


```solidity
pragma solidity ^0.5.0;
import "./../../../libs/ownership/Ownable.sol";
import "./../../../libs/lifecycle/Pausable.sol";
import "./../interface/IEthCrossChainData.sol";

contract EthCrossChainData is IEthCrossChainData, Ownable, Pausable{
    /*
     Ethereum cross chain tx hash indexed by the automatically increased index.
     This map exists for the reason that Poly chain can verify the existence of
     cross chain request tx coming from Ethereum
    */
    mapping(uint256 => bytes32) public EthToPolyTxHashMap;
    // This index records the current Map length
    uint256 public EthToPolyTxHashIndex;

    /*
     When Poly chain switches the consensus epoch book keepers, the consensus peers public keys of Poly chain should be
     changed into no-compressed version so that solidity smart contract can convert it to address type and
     verify the signature derived from Poly chain account signature.
     ConKeepersPkBytes means Consensus book Keepers Public Key Bytes
    */
    bytes public ConKeepersPkBytes;

    // CurEpochStartHeight means Current Epoch Start Height of Poly chain block
    uint32 public CurEpochStartHeight;

    // Record the from chain txs that have been processed
    mapping(uint64 => mapping(bytes32 => bool)) FromChainTxExist;

    // Extra map for the usage of future potentially
    mapping(bytes32 => mapping(bytes32 => bytes)) public ExtraData;

    // Store Current Epoch Start Height of Poly chain block
    function putCurEpochStartHeight(uint32 curEpochStartHeight) public whenNotPaused onlyOwner returns (bool) {
        CurEpochStartHeight = curEpochStartHeight;
        return true;
    }

    // Get Current Epoch Start Height of Poly chain block
    function getCurEpochStartHeight() public view returns (uint32) {
        return CurEpochStartHeight;
    }
```

…

Source: *https://gist.github.com/CJ42/868003588f027619edac9938ce128b52*

PolyNetwork – Vulnerable Function (Solidity)



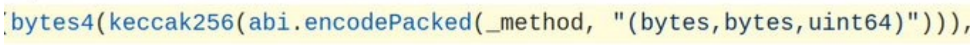
```
    // Store Consensus book Keepers Public Key Bytes
    function putCurEpochConPubKeyBytes(bytes memory curEpochPkBytes) public whenNotPaused onlyOwner returns (bool) {
        ConKeepersPkBytes = curEpochPkBytes;
        return true;
    }
```

…

Source: https://gist.github.com/CJ42/868003588f027619edac9938ce128b52#file-polynetwork-hack-sol-L128-L134

PolyNetwork Hack – The attack in 3 steps

Step 1: brute force "_method" field in



```
bytes4(keccak256(abi.encodePacked(_method, "(bytes,bytes,uint64)"))),
```

Objective = match function signature of `putCurEpochConPubKeyBytes(bytes)`

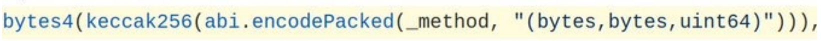
Step 2: make a **cross chain transaction** from Ethereum to Poly Network

contract	EthCrossChainManager	EthCrossChainData
method	`verifyHeaderAndExecuteTx(…)`	`putCurEpochConPubKeyBytes(…)`
network	Ethereum	PolyNetwork

Step 3: register attacker's public key as **Keeper** via step 2 = **Drain Funds**

Step 1: Brute Force "_method"

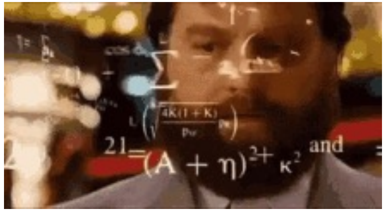
Function signature of



```
bytes4(keccak256(abi.encodePacked(_method, "(bytes,bytes,uint64)"))),
```

=

`putCurEpochConPubKeyBytes(bytes)`



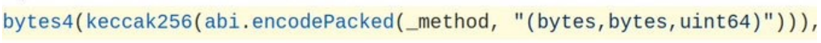
=

0x41973cd9

Step 1: Brute Force “_method”

Hash Collision found !

Function signature of



```
bytes4(keccak256(abi.encodePacked(_method, "(bytes,bytes,uint64)"))),
```

=

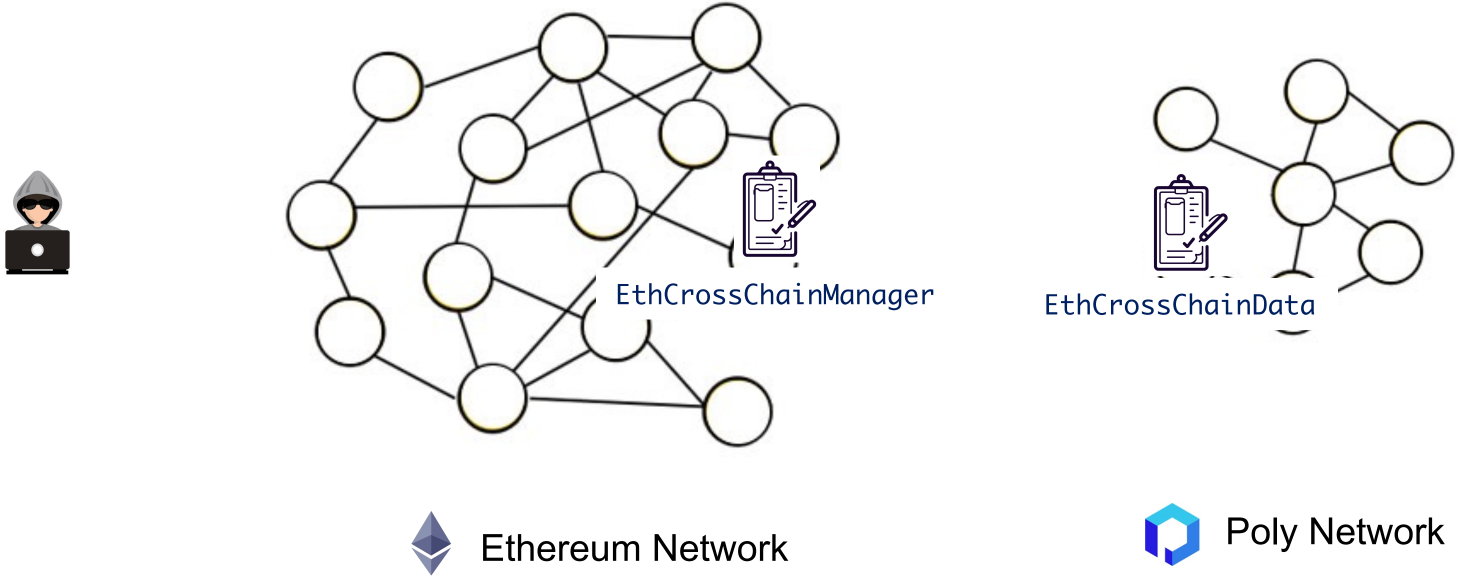
putCurEpochConPubKeyBytes(bytes)

f1121318093(bytes,bytes,uint64)

=

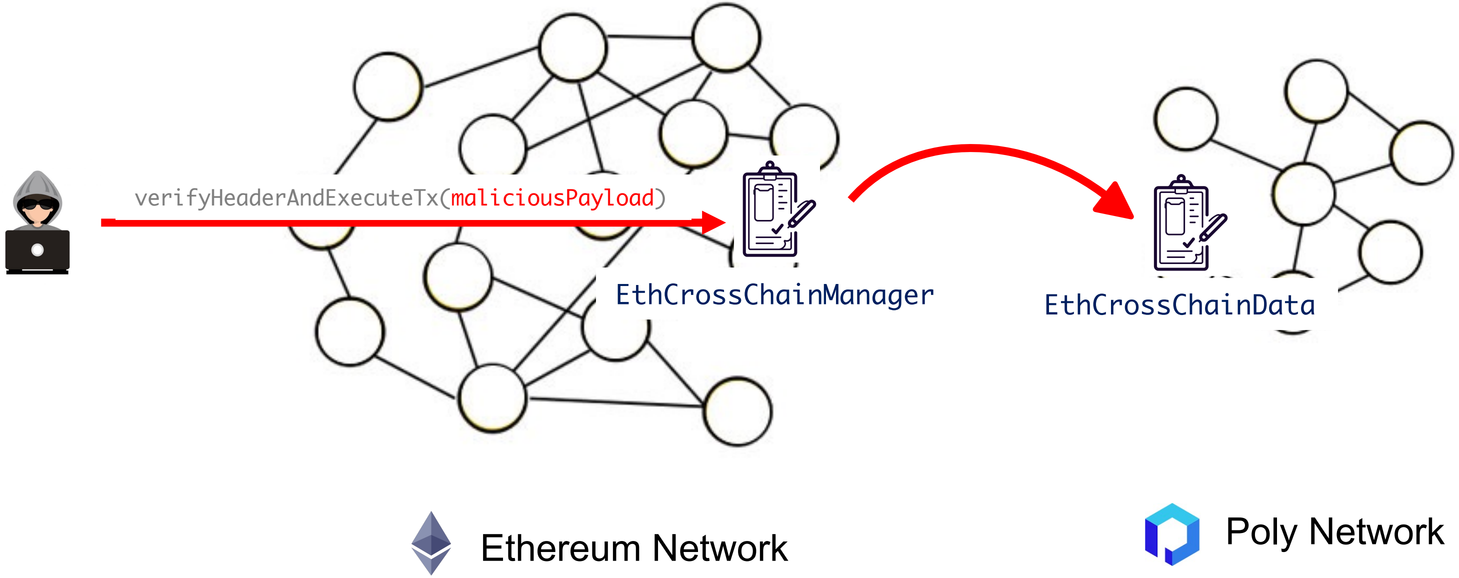
0x41973cd9

Step 2: Make a cross-chain transaction



Step 2: Make a cross-chain transaction

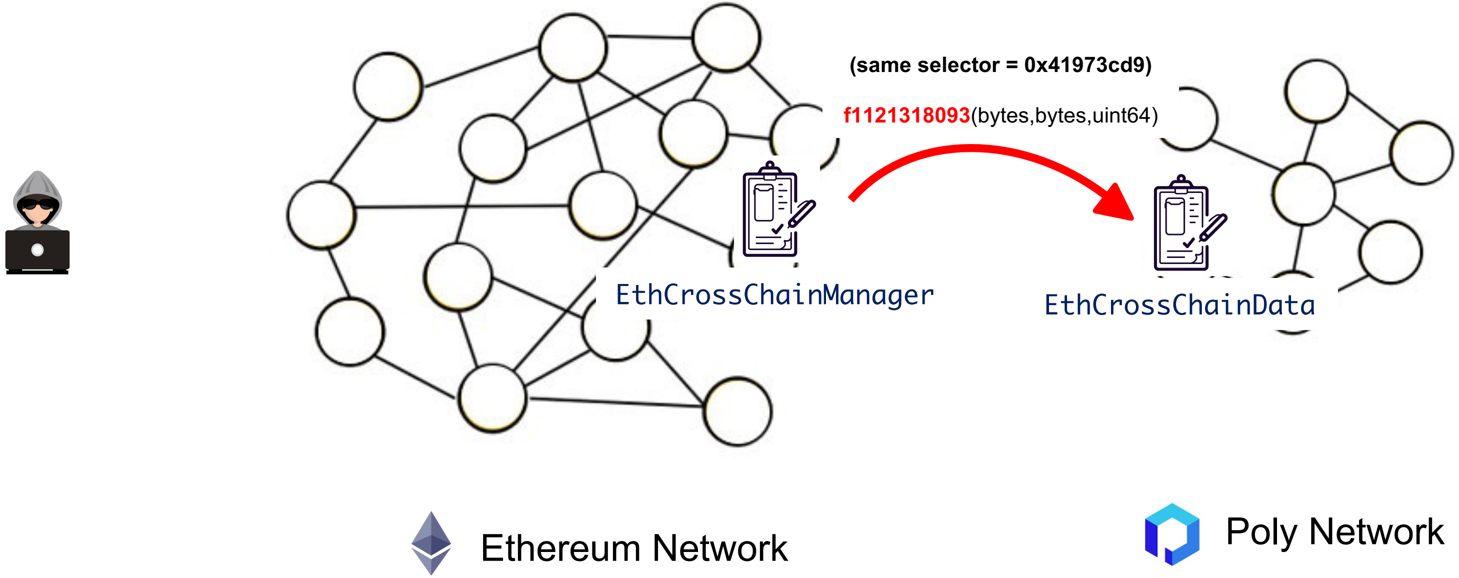
maliciousPayload = f1121318093(bytes,bytes,uint64)



Step 3: Register Attacker’s public key as **Keeper**

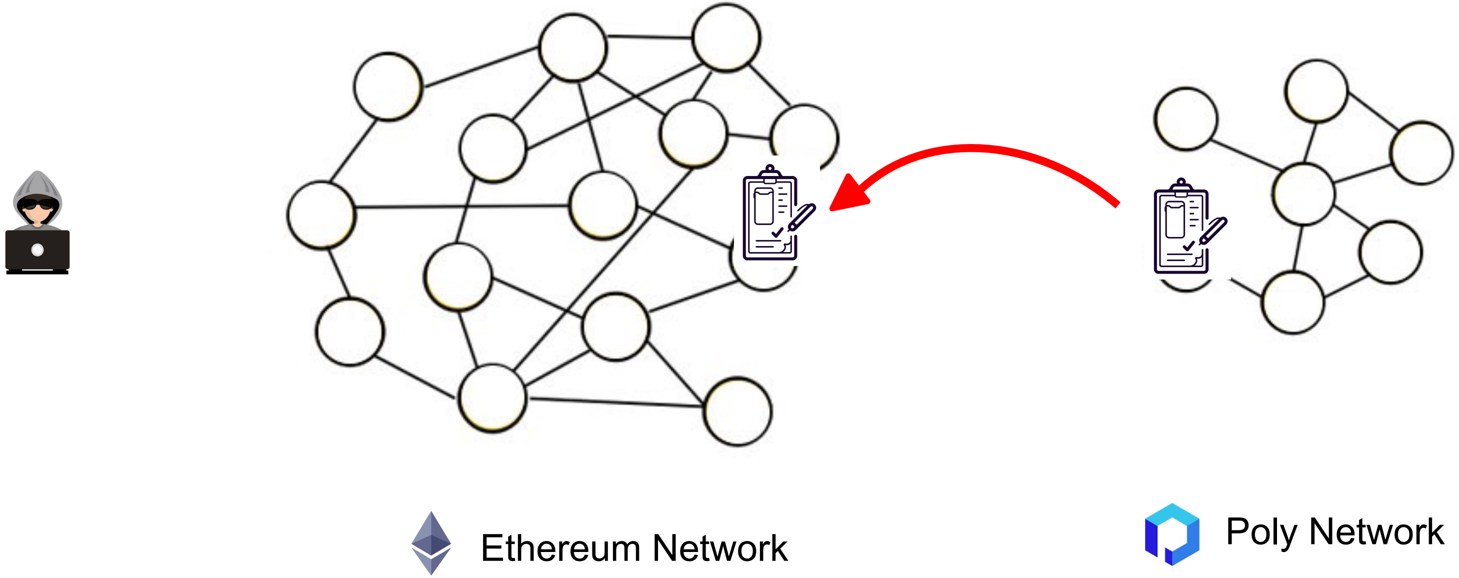
EthCrossChainData thinks that this **payload** calls `putCurEpochConPubKeyBytes(bytes)` (same function selector)

Result ➔ register public key passed in parameters as **Keeper**



<u>Step 3:</u> Register Attacker’s public key as **Keeper**

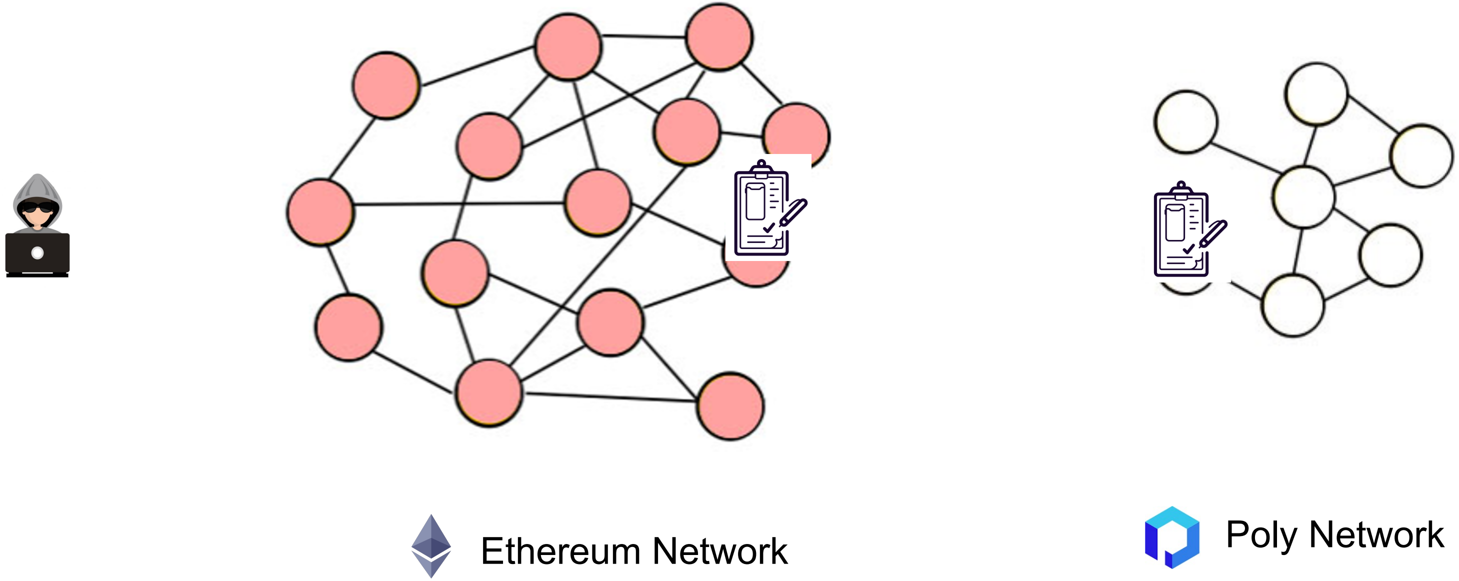
Cross-chain contracts call return



Ethereum Network

Poly Network

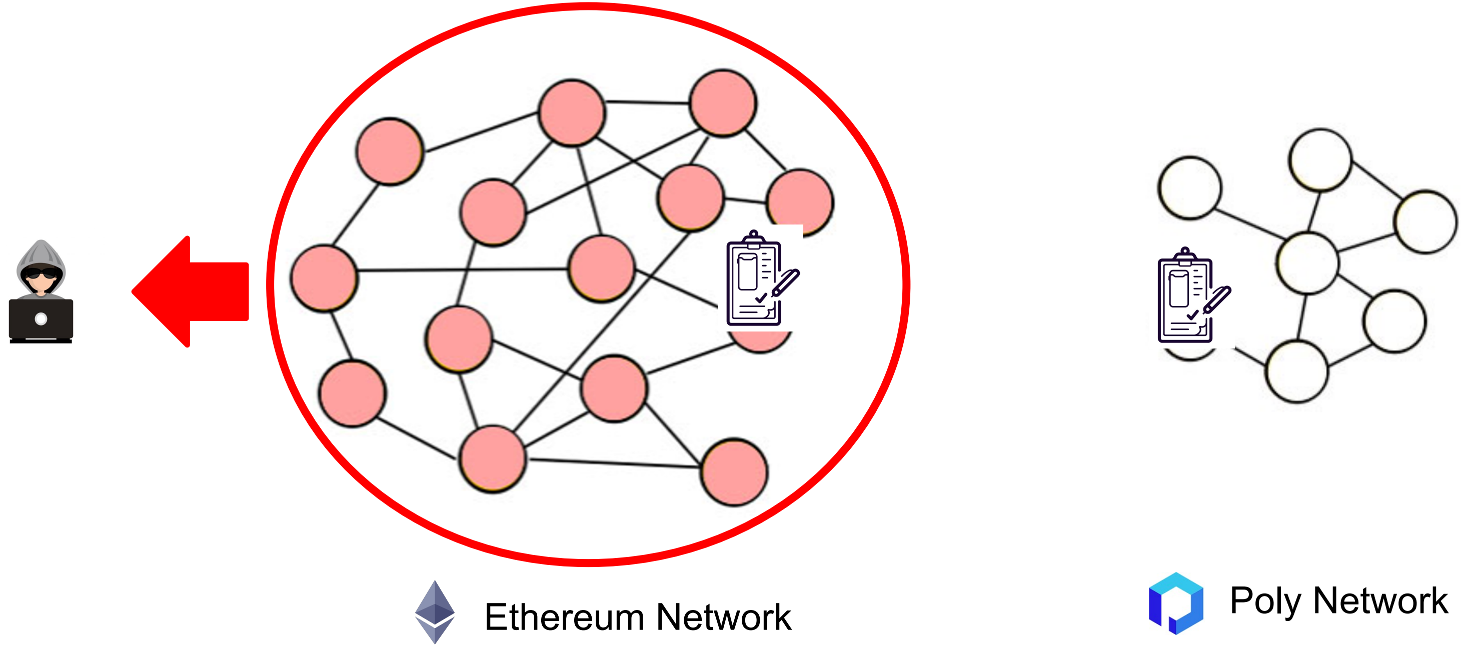
The attacker has now control over the wallets…



Ethereum Network

Poly Network

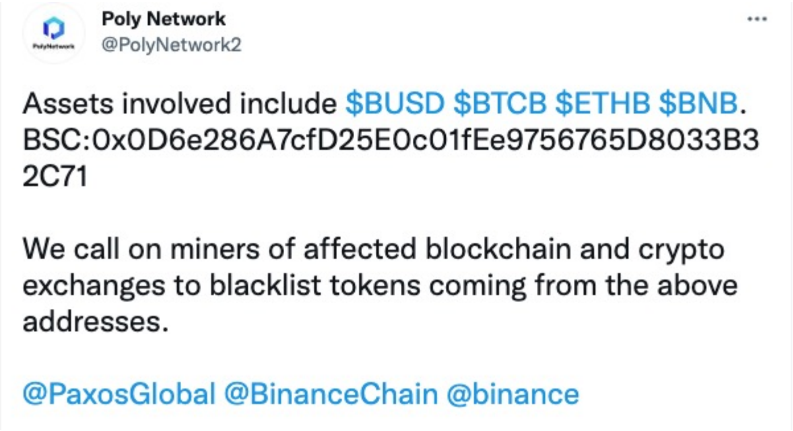
… and **start draining funds**



Final Step

Repeat for other liquidity wallets
(Binance, Tether, etc…)

Soon after the exploit is discovered, Polynetwork ask exchanges to block the funds



Poly Network
@PolyNetwork2

Assets involved include $BUSD $BTCB $ETHB $BNB.
BSC:0x0D6e286A7cfD25E0c01fEe9756765D8033B32C71

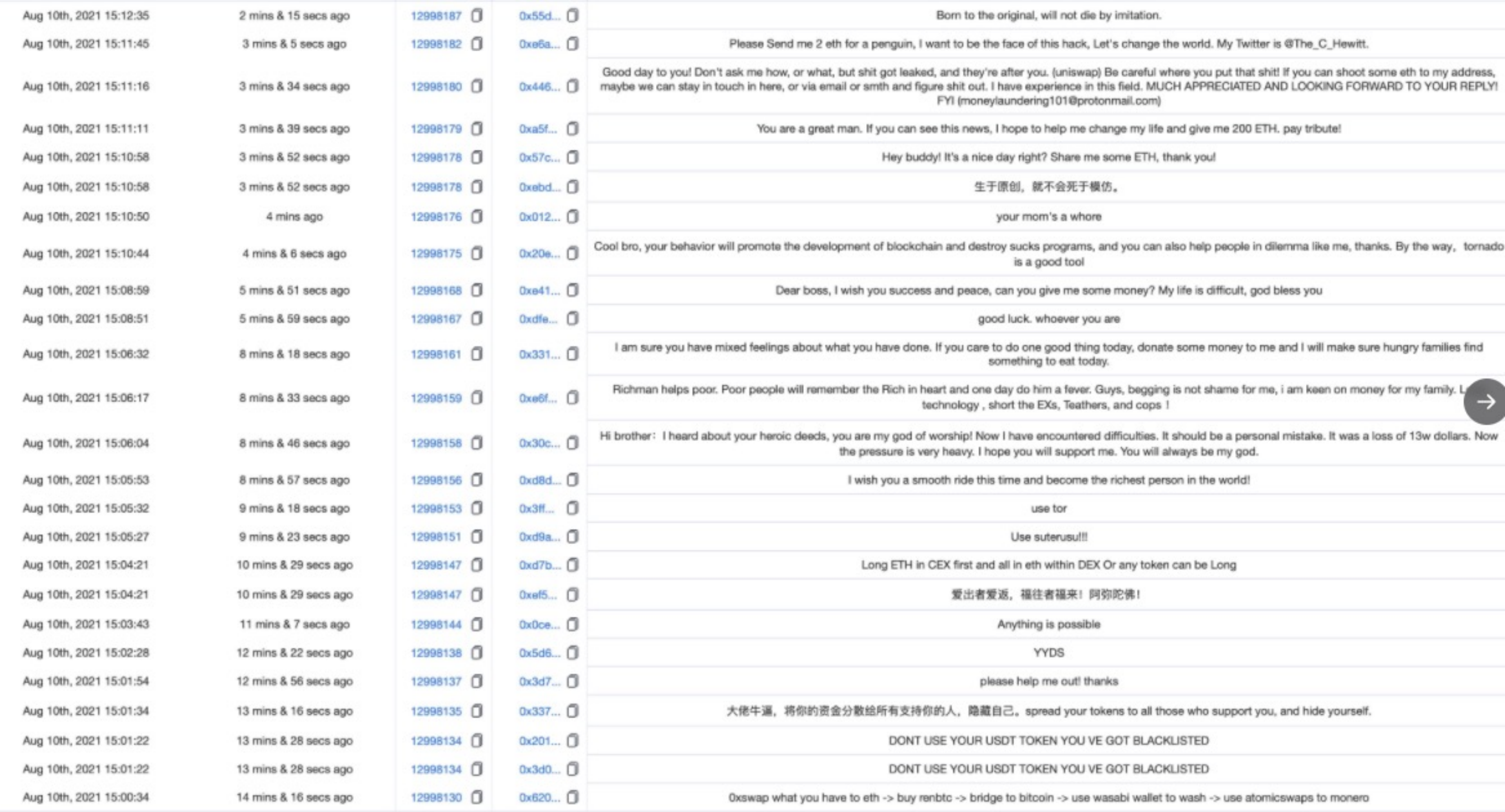
We call on miners of affected blockchain and crypto exchanges to blacklist tokens coming from the above addresses.

@PaxosGlobal @BinanceChain @binance

The attacker tries to move some funds to Curve, Tether manages to freeze his funds (9 blocks before they move.)

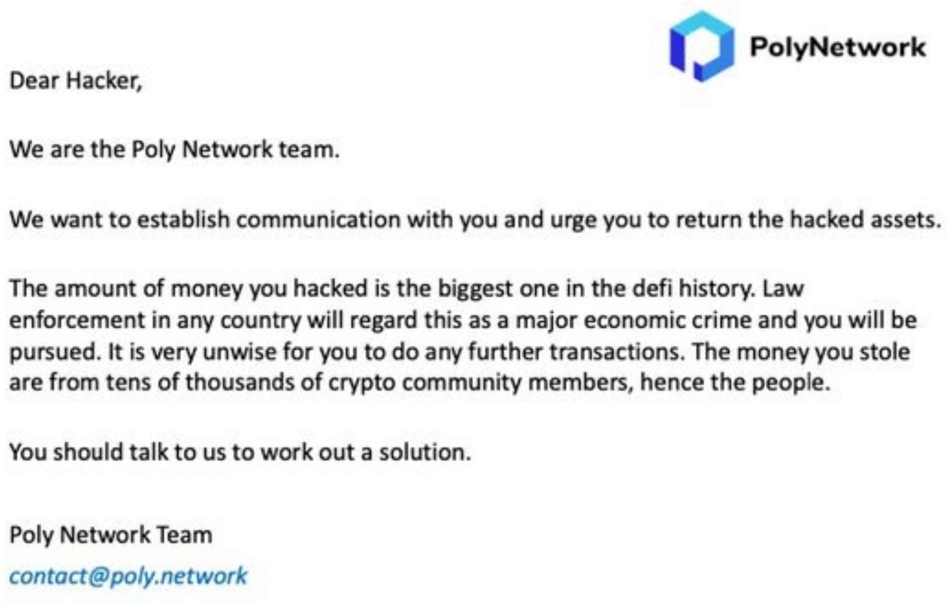
Others start to message the attacker by adding messages to transactions

hanashiro.eth warns ‘DONT USE YOUR USDT TOKEN YOU VE GOT BLACKLISTED’ and is rewarded with 13.37 ETH
This is followed by a slew of messages



Aug 10th, 2021 15:12:35	2 mins & 15 secs ago	12998187	0x55d...	Born to the original, will not die by imitation.
Aug 10th, 2021 15:11:45	3 mins & 5 secs ago	12998182	0xe6a...	Please Send me 2 eth for a penguin, I want to be the face of this hack, Let's change the world. My Twitter is @The_C_Hewitt.
Aug 10th, 2021 15:11:16	3 mins & 34 secs ago	12998180	0x446...	Good day to you! Don't ask me how, or what, but shit got leaked, and they're after you. (uniswap) Be careful where you put that shit! If you can shoot some eth to my address, maybe we can stay in touch in here, or via email or smth and figure shit out. I have experience in this field. MUCH APPRECIATED AND LOOKING FORWARD TO YOUR REPLY! FYI (moneylaundering101@protonmail.com)
Aug 10th, 2021 15:11:11	3 mins & 39 secs ago	12998179	0xa5f...	You are a great man. If you can see this news, I hope to help me change my life and give me 200 ETH. pay tribute!
Aug 10th, 2021 15:10:58	3 mins & 52 secs ago	12998178	0x57c...	Hey buddy! It's a nice day right? Share me some ETH, thank you!
Aug 10th, 2021 15:10:58	3 mins & 52 secs ago	12998178	0xebd...	生于原创，就不会死于模仿。
Aug 10th, 2021 15:10:50	4 mins ago	12998176	0x012...	your mom's a whore
Aug 10th, 2021 15:10:44	4 mins & 6 secs ago	12998175	0x20e...	Cool bro, your behavior will promote the development of blockchain and destroy sucks programs, and you can also help people in dilemma like me, thanks. By the way，tornado is a good tool
Aug 10th, 2021 15:08:59	5 mins & 51 secs ago	12998168	0xe41...	Dear boss, I wish you success and peace, can you give me some money? My life is difficult, god bless you
Aug 10th, 2021 15:08:51	5 mins & 59 secs ago	12998167	0xdfe...	good luck. whoever you are
Aug 10th, 2021 15:06:32	8 mins & 18 secs ago	12998161	0x331...	I am sure you have mixed feelings about what you have done. If you care to do one good thing today, donate some money to me and I will make sure hungry families find something to eat today.
Aug 10th, 2021 15:06:17	8 mins & 33 secs ago	12998159	0xe6f...	Richman helps poor. Poor people will remember the Rich in heart and one day do him a fever. Guys, begging is not shame for me, i am keen on money for my family. L technology , short the EXs, Teathers, and cops !
Aug 10th, 2021 15:06:04	8 mins & 46 secs ago	12998158	0x30c...	Hi brother：I heard about your heroic deeds, you are my god of worship! Now I have encountered difficulties. It should be a personal mistake. It was a loss of 13w dollars. Now the pressure is very heavy. I hope you will support me. You will always be my god.
Aug 10th, 2021 15:05:53	8 mins & 57 secs ago	12998156	0xd8d...	I wish you a smooth ride this time and become the richest person in the world!
Aug 10th, 2021 15:05:32	9 mins & 18 secs ago	12998153	0x3ff...	use tor
Aug 10th, 2021 15:05:27	9 mins & 23 secs ago	12998151	0xd9a...	Use suterusu!!!
Aug 10th, 2021 15:04:21	10 mins & 29 secs ago	12998147	0xd7b...	Long ETH in CEX first and all in eth within DEX Or any token can be Long
Aug 10th, 2021 15:04:21	10 mins & 29 secs ago	12998147	0xef5...	爱出者爱返，福往者福来！阿弥陀佛！
Aug 10th, 2021 15:03:43	11 mins & 7 secs ago	12998144	0x0ce...	Anything is possible
Aug 10th, 2021 15:02:28	12 mins & 22 secs ago	12998138	0x5d6...	YYDS
Aug 10th, 2021 15:01:54	12 mins & 56 secs ago	12998137	0x3d7...	please help me out! thanks
Aug 10th, 2021 15:01:34	13 mins & 16 secs ago	12998135	0x337...	大佬牛逼，将你的资金分散给所有支持你的人，隐藏自己。spread your tokens to all those who support you, and hide yourself.
Aug 10th, 2021 15:01:22	13 mins & 28 secs ago	12998134	0x201...	DONT USE YOUR USDT TOKEN YOU VE GOT BLACKLISTED
Aug 10th, 2021 15:01:22	13 mins & 28 secs ago	12998134	0x3d0...	DONT USE YOUR USDT TOKEN YOU VE GOT BLACKLISTED
Aug 10th, 2021 15:00:34	14 mins & 16 secs ago	12998130	0x620...	0xswap what you have to eth -> buy renbtc -> bridge to bitcoin -> use wasabi wallet to wash -> use atomicswaps to monero

PolyNetwork then ask for their money back



PolyNetwork

Dear Hacker,

We are the Poly Network team.

We want to establish communication with you and urge you to return the hacked assets.

The amount of money you hacked is the biggest one in the defi history. Law enforcement in any country will regard this as a major economic crime and you will be pursued. It is very unwise for you to do any further transactions. The money you stole are from tens of thousands of crypto community members, hence the people.

You should talk to us to work out a solution.

Poly Network Team
contact@poly.network

The attacker received a rather cryptic message
” Dont instant tornado funds, dont instant move blacklistable tokens to DAI/ETH? Insider confirmed!”

The attacker was looking at Tornado Cash and sent themselves a message
”Wonder why Tornado? Will miners stop me? Teach me please”

Then someone found a link between an address used by the attacker and some exchanges and tweeted

“Did the PolyNetwork Exploiter accidentally use the wrong sender address for this tx 0xb12681d9e? The sender address is tied to FTX, Binance, Okex accounts.”

The hacker’s attitude started to change, he suggested he could return *"some tokens"* or even abandon them, saying that they were *"not so interested in the money".*

Followed by a suggestion : “What if I make a new token and let the DAO decide where the tokens go”

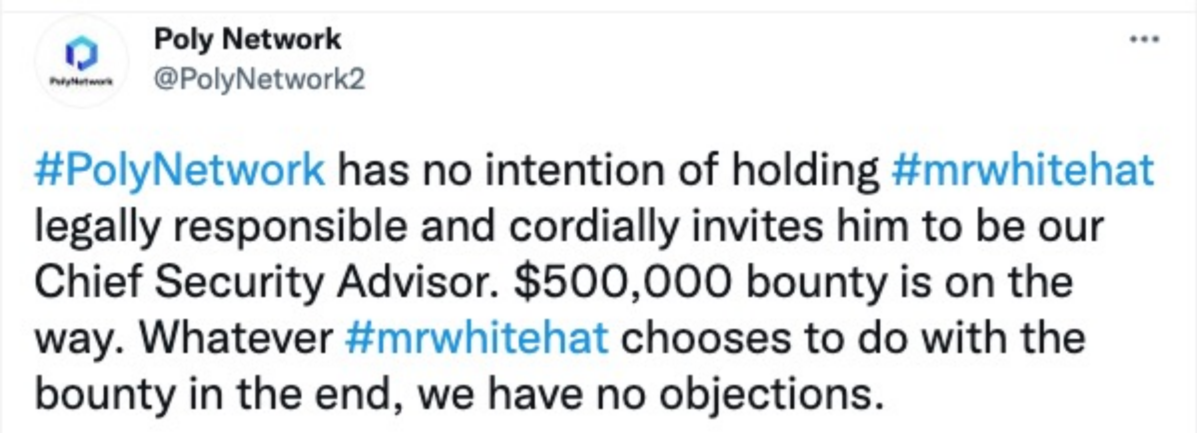
Finally the attacker messaged

”Ready to return the fund !”

See this spreadsheet for all communications

The attacker starts to return the funds

Polynetwork starts to refer to the attacker as ‘Mr White Hat’ and offer him a job and bounty



Poly Network
@PolyNetwork2

#PolyNetwork has no intention of holding #mrwhitehat legally responsible and cordially invites him to be our Chief Security Advisor. $500,000 bounty is on the way. Whatever #mrwhitehat chooses to do with the bounty in the end, we have no objections.

'Mr White Hat’ eventually signs off with rather a long message

DEAR POLY TEAM,

KEEP CALM AND THIS IS THE HAPPY ENDING! I HAVE TO ADMIT THAT MY WILD OR MAD BEHAVIORS HAVE LED CRISES TO YOUR PROJECT, YOUR TEAM AND EVEN YOUR LIVES. SORRY FOR THE INCONVENIENCE! IT MUST BE ONE OF THE MOST WILD ADVENTURES IN OUR LIVES.

THOUGH OUR COMMUNICATION IS NEVER PERFECT, WE ARE MOVING IN THE SAME DIRECTION: SETTLE DOWN THE MESS AND CHEER UP FOR THE FUTURE. I DIDN'T WANT TO LEAVE THE PROJECT IN RUINS SO I HAD MY PERSONAL PLAN TO TAKE THE RESPOSIBILITY OF SAVING THE PROJECT. MY ACTIONS, WHICH MAY BE CONSIDERED WEIRD, ARE MY EFFORTS TO CONTRIBUTE TO THE SECURITY OF THE POLY PROJECT IN MY PERSONAL STYLE. THE CONSENSUS WAS REACHED IN A PAINFUL AND OBSCURE WAY, BUT IT WORKS. SOME PEOPLE EVEN SUSPECT THAT THE WHOLE STORY IS A PR STUNT.

WHY DO WE FALL? SO WE CAN LEARN TO PICK OURSELVES UP. THIS INCIDENT MUST BE A SERIOUS LESSON TO MANY OF US, OR EVEN THE WHOLE DEFI COMMUNITY. PERSONALLY, I HAVE LEARNT AND PRACTISED A LOT. AND I TRIED TO POINT OUT SOME CRUCIAL FACTS ABOUT THIS CRAZY DEFI WORLD (PLEASE IGNORE MY BAD JOKES SINCE THE BEGINNING), AND HOPEFULLY MY PHILOSOPHY COULD BE INSPIRING, ESPECIALLY TO THOSE GEEKS WHO HAD MISBEHAVED ACCIDENTLY.

MY ACTIONS WERE DETERMINED SINCE I MADE THE FINAL DECISION, WHICH WAS TO MAKE IT PERFECT AND TO BE THE ETERNAL, INCLUDING PUBLISHING THE FINAL KEY TODAY. HOWEVER, ONE THING IS MISSING. DURING ALL THE NEGOTIATION, MY _ONLY_ REQUEST, WHICH WAS ALSO THE ONLY REASON FOR SLOW REFUND, WAS TO UNLOCK THE USDT. IN MY SELFISH VIEW, THE STORY IS TAINTED BY THE LOCKED USDT. IT WOULD HAVE BEEN A PERFECT EXAMPLE OF BUILDING TRUST BETWEEN ANONYMOUS "ADVERSARIES" BY LEVERAGING THE POWER OF SMART CONTRACT, IF WE HAD ANY CHANCE TO DEAL WITH THE USDT IN A NOT CENTRALIZED WAY. IT WAS JUST MY PREFERENCE OF SOLVING THE USDT ISSUE, AND IT MIGHT NEVER HAPPEN DUE TO THE UNSYNCHRONIZED COMMUNICATION. IT'S FAIR ENOUGH TO JUST LEAVE THE USDT HERE AS A SIN OF UNTRUST. WE DON'T HAVE TO WORRY ABOUT THE IMPERFECTIONS, BECAUSE THE COMMUNITY, THE MEDIA, THE CROWD AND YOU AND ME CAN'T WAIT FOR THE FINAL KEY, RIGHT? HERE IS THE KEY FOR _US_:

d3c0196b81dba3c2811c0a39536e4dc47d640e3099a9331821d40fd1d6ab66fb

I'M QUITING THE SHOW. BELIEVE IT OR NOT, I HAVE NEVER CONSIDERED THE SHARED WALLET AS THE "HOSTAGE" FOR RANSOM. AS YOU MAY HAVE NOTICED, I HAVE POURED YOUR BOUNTY AND MY COMPENSATION FUND FROM DONATIONS INTO THE SHARED MULTISIG WALLET. NOT SURE IF IT'S CONVENIENT, BUT DISTRIBUTING THE EXTRA ASSETS TO THE "SURVIVORS" WOULD BE THE LAST REQUEST FROM THIS MAN.

YOUR CHIEF SECURITY ADVISOR

Security – What to learn from Poly Network hack

Cross Chain calls Security

Cross-chain relay contracts: make sure they can’t be used to call special contracts.

Contracts with special privileges: make sure users can’t use cross-chain messages to call those special contracts.

References

Overview: https://blockworks.co/hackers-steal-over-600m-biggest-in-defi-history/

Technical: https://rekt.news/polynetwork-rekt/

Technical: https://research.kudelskisecurity.com/2021/08/12/the-poly-network-hack-explained/