What Happened to PolyNetwork?2021 then 2023

shymaa arafat

Preface

If you ever read a survey about Blockchain Interoperability solutions, you will probably find PolyNetwork under ***side chain*** bridges. Those kind of solutions originated from the very old idea of having side chains pegged to the Bitcoin Blockchain to perform small value off-chain TXs between 2 parties (for example a customer & Marchant) faster and cheaper [1]; the pegged chain starts with one online TX signed by both parties then either timed out and reverted (HTLC script in Bitcoin) or sealed by the target signing the final withdrawal amount. The idea was then extended to perform cross-chain atomic swaps [2] instead of a centralized exchange in 2014 (Before Ethereum); Fig.1 (a,b).

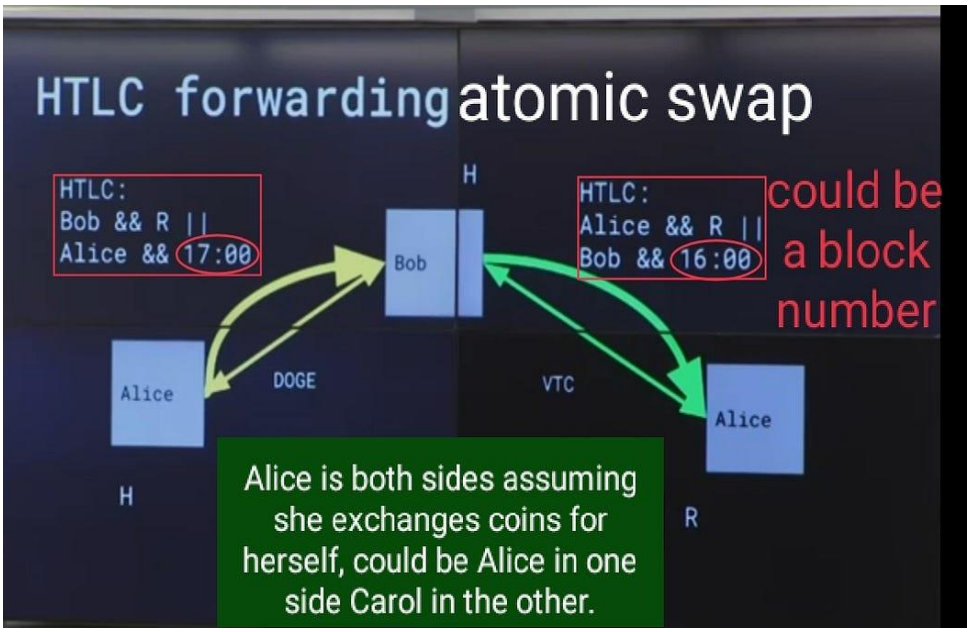

Fig.1-a from MIT lecture

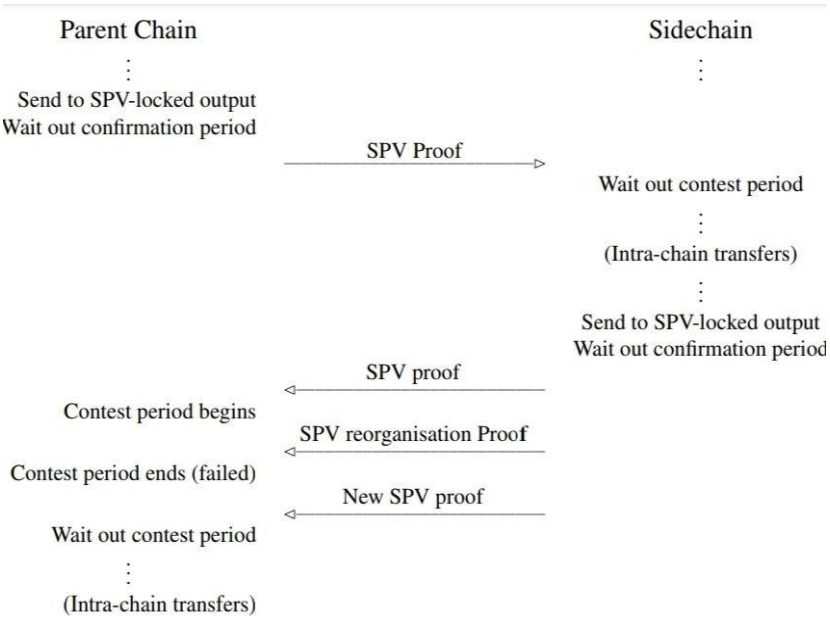

Fig. 1-b from [2] where SPV=Simple Payment Verifier which is the Merkle proof witness of the TX

With the appearance of Ethereum, smart contracts coding added more flexibility & functionality both to the cross-
chain mechanism and to the possible programmability of the transaction crossing borders itself, also there was an essential need to connect Bitcoin & alike altcoins to DeFi. So, *smart contract versions* of the same idea like BTC-Relay, X-Claim, BTC.b,… started to appear; the necessity of avoiding a single point of failure and adding a rewarding incentive to verifiers led to the concept of *independent **relay** nodes* that reach a decision according to consensus (variant of BFT most of the time) we are familiar with in DeFi. PolyNetwork is one of those solutions

The PolyNetwork

A picture is better than thousand words, so let’s start with the main architecture from their white paper [3] ; Fig.2

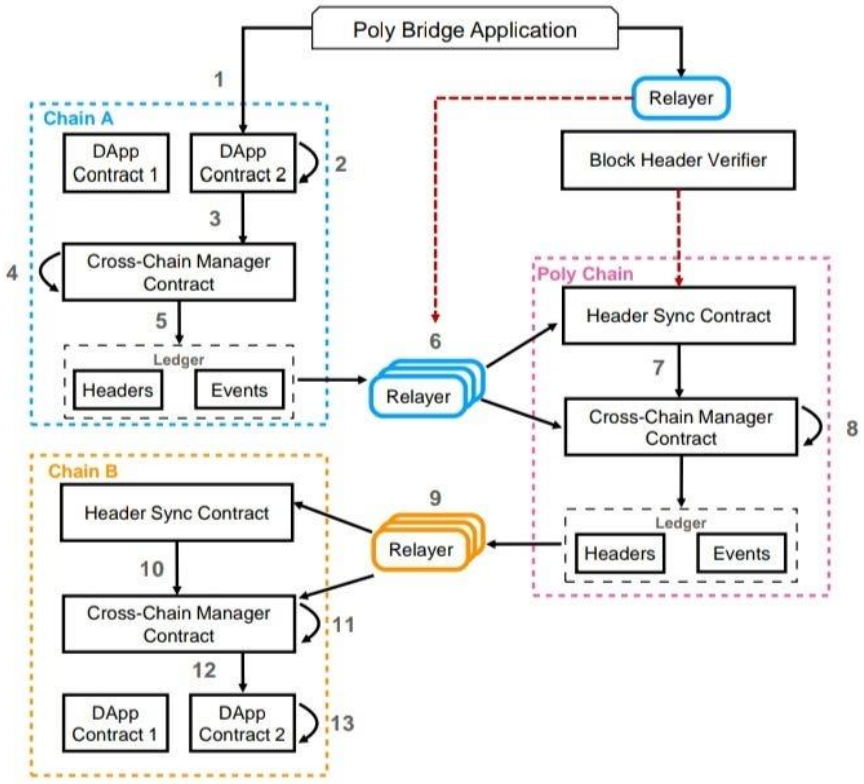

Fig. 1: The architecture design of Poly Bridge.

Fig.2 PolyNetwork Bridge architecture

As you can see from the block diagram, the Poly Bridge deploy a ***poly chain*** as an intermediary side chain between the sender & receiver chains. It use two groups of relayers (sometimes called ***gate keepers***) one in each direction (the blue verify data going into the poly-chain, and the orange out from it). From a developer point of view, you can find the main smart contract for the Ethereum chain "*EthCrossChainManager.sol*" or it's updates here
[4], and it will lead you to the main site [5].

The 610m$ Attack in 2021

Short & simple it is ***code vulnerability***, what I get from all resources [6,7,8] it is mostly due to:
1-*Not adjusting the access rights of the cross-chain function* such that it possessed all the rights of the cross-chain manager contract (you see it is the same contract deployed in the 3 chains and the CC-TX executes through it). Now, this contract is the one that is responsible of adding and/or removing (public-private key) entries of registered gate
keepers (https://github.com/polynetwork/eth-

contracts/blob/d16252b2b857eecf8e558bd3e1f3bb14cff30e9b/contracts/core/cross_chain_manager/data/EthCrossChainData.sol#L45); Fig.3.

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

```
// if we want to upgrade this contract, we need to invoke this method
function upgradeToNew(address newEthCrossChainManagerAddress) whenPaused onlyOwner public returns (bool) {
    IEthCrossChainData eccd = IEthCrossChainData(EthCrossChainDataAddress);
    eccd.transferOwnership(newEthCrossChainManagerAddress);
    return true;
}
```

Fig3: code screenshots taken from [6]

2-The signature guarding this specific critical function, although strong (Keccak256), is truncated to just 4 bytes **0x41973cd9** so that it was possible for the attacker to find a collision in at most ~2^{16} brute force trials (half the power due to Birthday attack).

So, the attacker used another function name with the same truncated hash to call, deleted all keepers, added only his key, and then withdrawn all liquidity.

Recovering

In addition to efforts tracing and returning the money [9], PolyNetwork [6,7,8]:

- limited the access rights of the cross-chain TX executing function.
- Limited the liquidity amount possible to withdraw in one TX.
- Added a Bug-Bounty and audit systems.
- I haven't read anything about changing the hash function signature, but I think if they added another value even with the same number of bits (call it ***m***) to be checked, for example by XORing the trimmed bits ***(n-m)*** into another ***m*** bits; this will add O(1) complexity but will make it much harder for a brute force trial to find 2 simultaneous collisions (~2^{32}).

The Jul 2023 Attack

Last July an
attacker was able to ***mint*** enormous number of ***tokens*** on target chains ***without locked assets*** (only the minimal possible amount to start a CC-TX).

I found conflicting reasons for the attack; Shark team (SharkTeam) [10] says the keeper keys was leaked through social engineering, Crypto daily [11] backs almost the same story specifying that exactly ***3*** *keeper* ***keys*** were traced,
but Halborn and Erhat [12] tell a different story.

-It’s important to note here that literature [13] always considered key breaching as a problem in side chains, since the BFT consensus requires at least 2/3 of the nodes to be honest (in this particular case there was ***only 4*** *signatures* needed and the attacker got ***3/4)***. The ***number of relay nodes*** (keepers) is a ***dilemma*** here between security and efficiency; it shouldn’t be too large to delay DeFi opportunities (in RSK medium value TXs need ~ 3hrs for confirmation, and large value TXs could take 1 day [14]) or too small to jeopardize security.

-Another precaution that may have prevented this attack is what [15] calls (strategy 2) “*checking consistency of protocol state*", it’s simply ***checking*** that (***Sum of input=Sum of output***) for each asset before confirming the mint of new tokens; I think if there were such a condition ***the protocol wouldn’t have minted those tokens ev en with the keepers signatures***. Strategy 7 may have helped also if there were a possibility to increase the number of signatures to 9 (with 6/9=2/3 not leaked) before minting this amount of tokens. Strategy 8 of applying fusion techniques is kind of similar approach to what I thought could add more security to the function signature in 2021 attack.

-Anyways, the partially good news is that the attacker wasn’t able to liquidate all the tokens he minted, only 41m$ liquidated out of billions worth tokens [16].

What now?

PolyNetwork (Poly Network) suspended all its activities after the last attack, but is trying to recover and its twitter account says services are partially stored and it will be back soon [17], but couldn’t trace any document on the changes they made to their design or code.

References

[1] MIT cryptocurrency, “Payment Channels and Lightning Networks”, lec13, 2018; https://youtu.be/Hzv9WuqIzA0?si=L-90NTSpUKtO_fA9, last accessed 11/10/2023.

[2] Andrew Miller, Peter Wuille, et. al, “Enabling Blockchain Innovations with Pegged Sidechains", 2014.

[3] PolyNetwork white paper.

[4] https://github.com/polynetwork/eth-contracts/tree/d16252b2b857eecf8e558bd3e1f3bb14cff30e9b/contracts/core/cross_chain_manager; last accessed 22/10/2023.

[5] https://github.com/polynetwork/poly; last accessed 22/10/2023.

[6] https://blog.kraken.com/product/security/abusing-smart-contracts-to-steal-600-million-how-the-poly-network-hack-actually-happened; last accessed 21/10/2023.

[7] https://research.kudelskisecurity.com/2021/08/12/the-poly-network-hack-explained/; last accessed 21/10/2023.

[8]https://slowmist.medium.com/the-analysis-and-q-a-of-poly-network-being-hacked-8112a35beb39; last accessed 21/10/2023.

[9]https://www.cnbc.com/2021/08/13/poly-network-hack-nearly-all-of-600-million-in-crypto-returned.html; last accessed 22/10/2023.

[10]https://medium.com/@sharkteam/sharkteam-polynetwork-attack-principles-and-asset-transfer-analysis-e8f6db9c8dbf; last accessed 21/10/2023.

[11]https://www.tradingview.com/news/cryptodaily:b8dae3a94094b:0-decoding-the-poly-network-exploit/; last accessed 22/10/2023.

[12]https://www.halborn.com/blog/post/explained-the-poly-network-hack-july-2023; (leads to Erhat tweet) last accessed 22/10/2023.

[13]Berkeley ZKP MOOC, 2023, “ZK-bridges", lec.14; https://youtu.be/0bKasr4G7OM, last accessed 11/10/2023.

[14]https://tokenbridge.rsk.co/; last accessed 22/10/2023.

[15]https://debridge.finance/blog/10-strategies-for-cross-chain-security/; last accessed 24/10/2023.

[16]https://decrypt.co/147059/poly-network-attack-conjures-billions-of-dollars-in-tokens-that-did-not-exist; last accessed 21/10/2023.

[17]https://twitter.com/PolyNetwork2/status/1714189964227825753; last accessed 22/10/2023.