Understanding Cross Chain interoperability Solutions- part1

shymaa arafat

In my 2nd DeFi attacks article (https://medium.com/@shymaa.arafat/defi-attacks-part-2-45c7e2c9c00) I said that “bridges" is an area I haven’t touched yet, so I can’t tell you much about its vulnerabilities except quotes from other people. According to chainalysis report [1], ***64% of DeFi stolen money*** *this year 2023 happened through cross-chain protocols* (DeFi itself was responsible of 82% instead of 73.3% in 2022); I also found out that CBDC interoperability solutions depend very much on bridging [2].

Hence, it seemed like a “must know" area, and the very last lectures & talks of the ZKP MOOC course [3,4] I was taking gave me a good starting point to gather more material and explore the whole area; so let me tell you what I found…

Now, let’s setup some terminology before we go any further:

1-From this must read survey paper [5], be aware that there are different areas to be addressed in interoperability; Fig.1

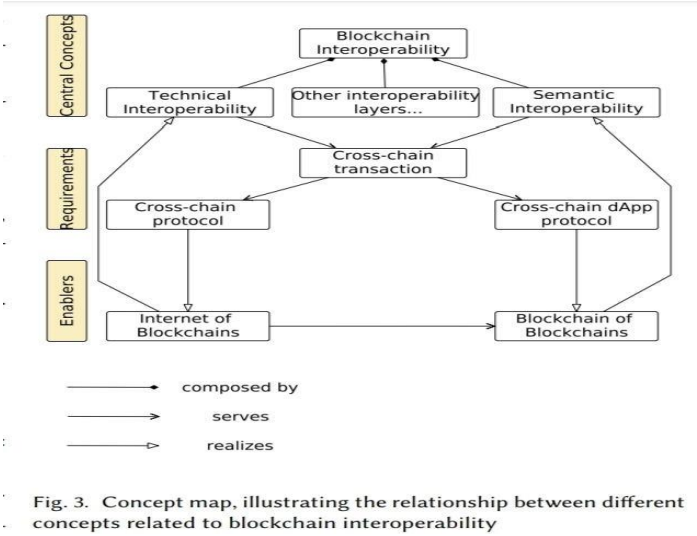

Fig. 3. Concept map, illustrating the relationship between different concepts related to blockchain interoperability

Fig.1: different interoperability areas, from [5]

- ***Regulations interoperability*** for example; like different taxes applied to each blockchain, or different regulations for source & target CBDC,…etc.
- ***Technical interoperability***, what we are mostly concerned about, which refers to the infrastructure that handles all kinds of messages passing between blockchains (verifying signatures, checking confirmations & finality in the sending Blockchain,…etc.
- ***Semantic interoperability*** which refers to the management of accepted (verified) TXs crossing borders, like ordering them in blocks, checking for conflicts,…etc; *Chimera Chains* is an example I've read recently where heterogenous *Paxos* is a consensus algorithm for ordering [6]. I believe it's the same problem solved by *shared sequencers* and solutions used by Ethereum L1 to construct blocks from its different L2 roll-ups or shards. Another simpler example is think how will a DEX order exchange TXs coming almost simultaneously from different blockchains (Ethereum, BNB,…etc); ie, what if their smart contracts are trying to perform overlapping tasks like liquidating the same resource in part of the code?

2-Differentiate between (still from [5])

- **Cross-Chain** usually abbreviated as **CC** (**CC-TX**, or **CCCP** for cross-chain communication protocol) refers to connecting ***homogeneous Blockchains***. That 's what we're going to discuss through this article since it is mostly concerned with DeFi as a start; ie all Blockchains are EVM-like, even Bitcoin is public permissionless.
- **Cross Blockchain**, abbreviated as **CB (CBCP** for the protocols**)**, refers to connecting ***heterogeneous blockchains***; ie, for example if you tried paying to a permissioned energy trading blockchain using your cryptocurrency stored at a public permissionless blockchain, you probably have heard about Hyperledger Fabric. We will defer this kind to a following article.

3-Wether CC or CB, you have to understand that we are now having at ***least two TX fees*** to pay (one in each Blockchain, one or more for the intermediate platform if there's one [7]); the TX *finality* or *escrow time* (to be confirmed such that probability of double spending or forking the block containing it approaches zero) is now ***at least the sum of both blockchains times*** (with additional delay ***time*** we wish to minimize ***for the crossing borders steps***); and the TX is at most ***as secure as the weakest*** of the two blockchains and the interconnection solution used (some solutions deploy a security boost option, ex: https://youtu.be/QNRUXXoQf5U&t=29m35s, but this is beyond the scope of this article). Be aware also that the interconnection scheme must take care of any ***difference in the cryptographic algorithms*** (or their parameters) ***used*** by both chains; [4] talks about the *Schnorr* overhead of field transformation between different elliptic curves , also there are chains that uses different implementations than *ECDSA* like *EdDSA*, or even completely different algorithms like signatures used by Bitcoin taproot.

4-Those CC or CB transactions were at the beginning only money transfer or payment TXs; either BTC or ERC-20 like tokens or maybe some form of CBDC token where a *lock/burn* happens in one side and a *mint/unlock* happens at the other. More needs and capabilities have evolved with the advancement of dApps and smart contracts, this can be simply achieved by adding more functionality in the smart contract deployed in the target blockchain; this includes [4] different kinds of message passing for registration, governance, access rights,…etc; also

Commented [DA1]: Specifically, [4] mentioned that in POS chains Cosmos uses ***EdDSA*** *(Edward curve Digital Signature Algorithm)* on *Curve25519* while Ethereum supports *BN254*, and that circuit that transform a Cosmos signature in the field supported by Ethereum involves 2m gates. Also Fusion that we talk about late in the article [28] mentions in its yellow paper that they currently support ***ECDSA*** *(Elliptic Curve Digital Signature Algorithm)* which is used by 80% of cryptocurrencies, but still they prepare to support *Schnorr* signatures (at that time, it wasn't officially used by Bitcoin Taproot) and *Stellar Ed25519* (Edward Stellar) in their next phase.

Commented [DA2]: It's written in *Zetachain* (https://blog.zetachain.com/introducing-omnichain-accounts-ee49392ffe28) that they add the coding facility to a script blockchains like Bitcoin (to perform any needed functionality without a smart contract) by writing the required code in the OP_RETURN field in the Bitcoin TX; then the Zeta client parses it and invokes a *Zetaprocess* function inside the smart contract.

NFTs it's not just passing an ERC-721 token, you may want to lock the ownership of an NFT and only pass its utility or rent it or….etc. (I noticed many 2023 Blockchain interoperability papers appearing in Metaverse specialized conferences).

5-If you started by exploring comparison articles [8,9] and block diagrams of famous platforms (like I did), you will find the terms "**routers**" & "**gateways**" excessively used. ***These are all*** *nodes deploying* ***smart contracts*** *named that* (or maybe could be hard-coded in a ***TEE***); they're named this way following the convention in [10] (and other earlier papers) that made an analogy with the internet interoperability problem solved in the 90's, where the internet viewed each network as an *Autonomous System* **AS** that can have its own routing protocol and architecture and communicate through border routers & gateways. So here in Blockchains (Fig.2-a) we can build an *Internet of Blockchains* **IOB** as the underlying infrastructure for interoperability (Fig. 2-b)

Commented [DA3]: The authors in [10] use more of a communication & networking FATF terminology; so, X.509 is simply the PKI Public Key Infrastructure we use to verify certificates & signatures for a private-public key pair; VASP is the Virtual Asset Service Provider being passed cross Blockchains (ex. the CB issuing the CBDC).

- A **router** is a smart contracts that handles (part of handling) message passing between *homogeneous* blockchains; examples include Chainlink [11]
- While a **gateway** is a smart contract that is part of the communication system between *heterogeneous* blockchains; examples include Hyperledger Cacti [12].
- You may also find an Identity Management Smart Contract that resembles the **DNS** in the internet.

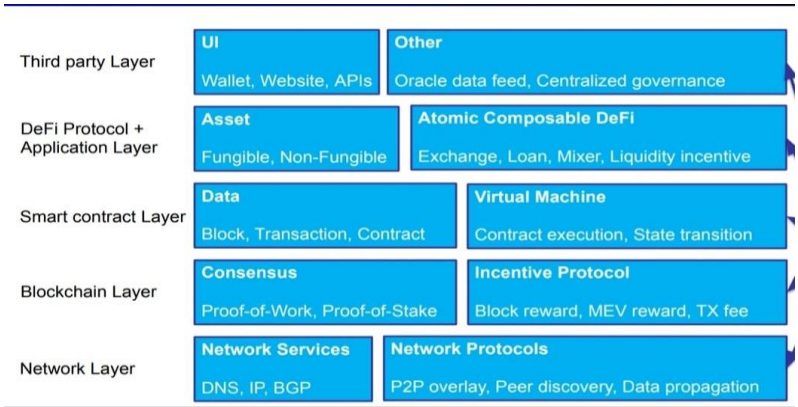

Fig.2-a: DeFi layers communication perspective, from Berkeley DeFi MOOC, lec13

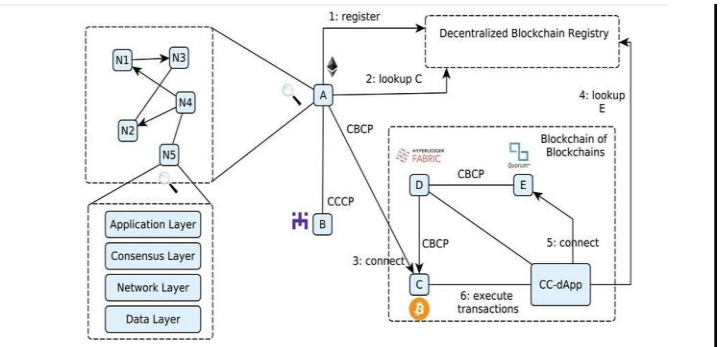

Fig. 6. Architecture for Interoperable Blockchains: a network comprised of five blockchains (A to E) and a cross-chain decentralized application (CC-dApp).

Fig.2-b from [5] Appendix: Blockchain interoperability viewed as Internet interoperability.

6-On the other hand the layers terminology used in naming "***Layer zero***" [13] refers to the DeFi stack layers in Fig.3 where we call Ethereum POS and roll-ups L2 (layer 2 in this diagram) and Ethereum POW as L1.

Commented [DA4]: ; a newer solution ***Hana*** (https://twitter.com/HanaNetwork, https://medium.com/hananetwork/introducing-hana-network-layer-0-for-privacy-2eb97b7bfd34) is said to be L0 (UTXO based) and uses *Bulletproofs* to provide *private* one chain TXs and cross-chain swaps & transfers, but I couldn't find their white paper to know more than that.

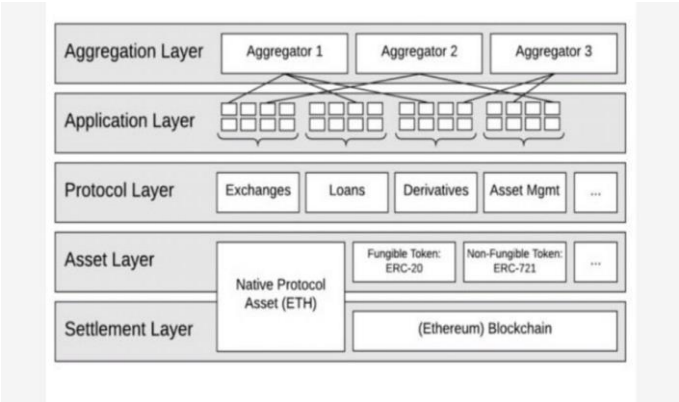

Fig.3: DeFi stack layers, from Nicosia University DeFi MOOC

So, we could say an L0 interoperability solution means to put your solution down in L0 and build upon it (Fig.4-a), while an L2 interoperability solution means to put your solution in a higher layer gathering CC-TXs from different blockchains (Fig.4-c). We'll get back to the differences between those platforms which is in the very fine technical details of how their smart contracts are written; maybe most of them classify as a *Blockchain Of Blockchains* (**BOB)** that we will explain more in the following article (Although ***Zetachain*** describes itself as an L1 *Blockchain **For** Blockchains* [14] (Fig. 4-b)).

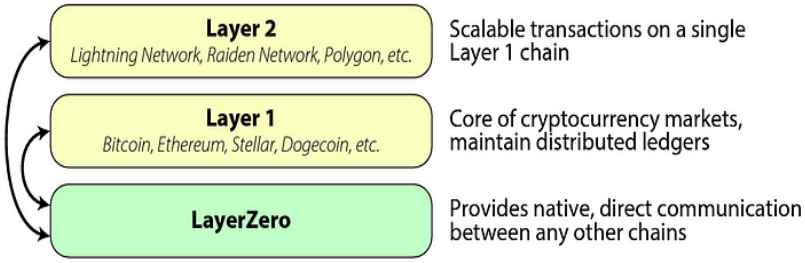

Fig.(4-a) Layer zero

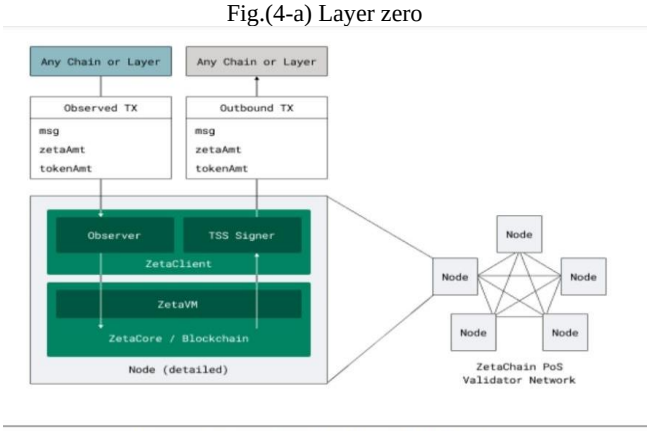

Figure 2. ZetaChain High Level Architecture.

Fig.(4-b): Zetachain [14] describes itself as L1 Omnichains solution

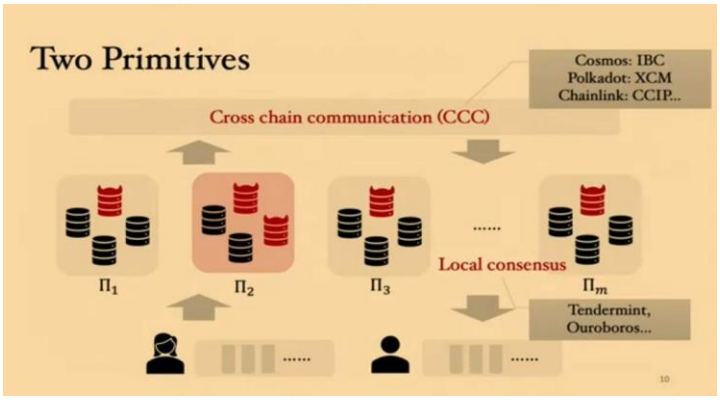

Fig (4-c): L2 CCC solutions from a newer paper (https://youtu.be/QNRUXXoQf5U&t=29m35s)

7-You may also find the term ***omni-chains*** kind of vague (as I did earlier); it was conceptually promoted [15] as enabling dApps to use a unified token belonging to the platform across different blockchains instead of different kinds of wrapped tokens for each interoperability solution which affects the fungibility of the original assets while crossing borders (meaning that different wrapped solutions may have different values for the same asset value).

Omnichains try to be a chain for all which is similar to idea of BOB in [5] if I understand correctly, let me just give some example details and wait till we reach BOB systems in detail:-

- L**ayer zero** ecosystem (LayerZero Labs) uses the unified token (**OFT** *Omnichain Fungible Token*) as an L0 standard token; meaning that even ERC-20 is on the layer L1 above it and can be treated as OFT within all included blockchains. However, ***bridges*** are still needed to handle non EVM-like blockchains (Aptos), BTC (BTC.b by Avalanche), Altcoins (Altitude) and USDC (built jointly between layer-zero & circlepay the original issuer of USDC).
- **Zetachain** (ZetaChain Blog) as L1 omnichain handles Bitcoin by generating a Bitcoin key and use it to transfer the asset with whatever programmable functionality needed written in the *OP-RETURN* part; the zeta client then parses the code into a function inside the smart contract, the BTC is locked and an equivalent amount of the standard token **ZRC-20** is generated (here it's an L1 token so it's an extension of ERC-20).
- **Omniledger** (https://ieeexplore.ieee.org/document/8418625) is an L2 omnichain but has nothing to do with interoperability, it's for sharding & scaling purposes only (like L2 roll-ups but was much earlier in 2018)

That was a grasp of notes about scattered terms here & there the reader may have found vague or confusing. Now let's delve into the mostly used classification of Blockchain interoperability solutions…

(if you're interested only in BOB famous solutions like Chainlink, Hyperledger, Cosmos, Polkadot, Zetachain,…etc wait for the following article, I will put its link here when it's ready)

Public Connectors

1-Side Chains & HTLC

Most material will direct you to 2016 Vitalik Buterin technical report [16] that summarizes all in this category, but let me suggest you also revisit the origins of that in Bitcoin where **HTLC** (*Hash Time Lock Contract*) was added to the Bitcoin instruction set as a TX that starts (on-chain) an exchange between a sender Alice & a receiver Bob. After that Alice & Bob can interact as much as they want off-chain without extra cost and without burdening the Blockchain; the communication thread (**payment channel** or **side chain**) ends by either being sealed with a TX (on-chain) signed by Bob signature confirming taking the money, or being reverted and all money back to Alice if the lock deadline (could be time *CHECKLOCKTIMEVERIFY* or block number *CHECKSEQUENCEVERIFY* [17]) was reached without an on-chain TX signed by Bob. The name "***side chains***" came because this off-chain interaction thread between Alice & Bob is

Commented [DA5]: The word "*Omni*" came from a Latin word that meant "all" or "everything"; meaning now "*a combining form of all things*"

like a pegged chain to the main Bitcoin chain; side chains were possible to cascade as ***DAG*** to provide fast and cheap ***n-party off-chain*** communication channels and were mostly used as a scalability solution for Bitcoin if without HTLC (ending with a multi-signature TX) [17,18].

Could be the first cross-chain attempt and considered innovative at the time, 2014, when HTLCs and side chains were used to perform atomic swaps and facilitate Bitcoin exchange with other altcoins without using a centralized exchange (Fig. 5-a from [18], Fig.5-b from [19]). Then when Ethereum and it's fellow EVM-like chains appeared, HTLC and side chains were coded into smart contracts with more extendable functionality for Bitcoin or like altcoins to communicate with DeFi in a tokenized representation. **BTC-Relay** [20] with its *WBTC* is an example, probably the first in 2016, where the smart contract stores a Merkle of block headers sometimes called a *history tree* to verify the Simple Payment Verifier *SPV* Merkle proof against the last block header; **Peace-Relay** is a bi-directional one connecting Ethereum to Ethereum Classic [21], of course using Merkle Patricia proofs this time due to the different Ethereum state storage design. HTLCs and side chains could be used also to connect either two private blockchains (Fig. 5-c from [22]), or a private blockchain to public cryptocurrency one for payment purposes [23]; the main idea remains the same as you can see the logic in Fig.5 a,b,c is not very much different. Maybe here it's a suitable place to mention that according to [5], **WanChain** [24] was from the early ones (2019) that added more functionality by facilitating coding in *Web Assembly* ***WASM*** not just Solidity/Rust/… and other high level languages; *WASM* as a lower level language gives more efficiency needed in web3 applications.

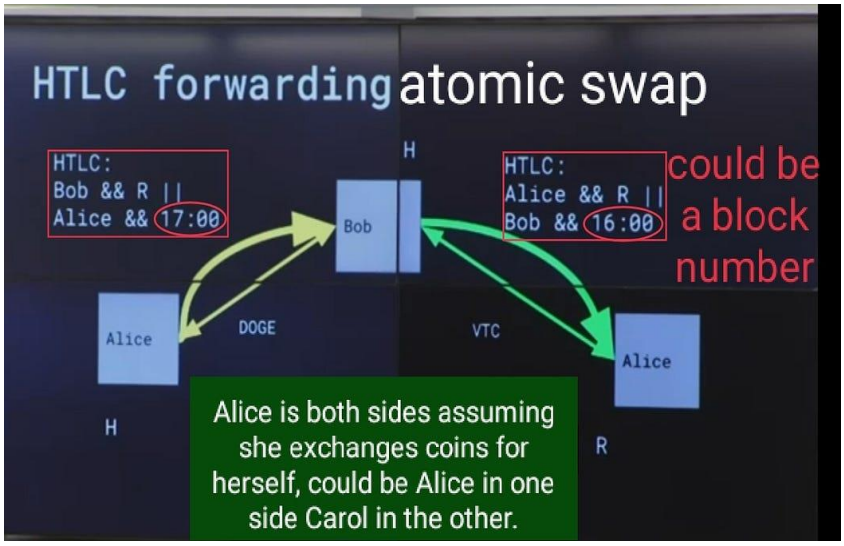

Fig.5-a: HTLC usage in atomic swaps as explained in MIT 2018 lecture[18] (annotated): the deadline in Bob TX must be smaller than the original one by Alice for the HTLC to work properly

Commented [DA6]: A vulnerability named ***HTLC replacement cycling*** against HTLC usage in lightning networks was discussed in the last Bitcoin newsletter 25/10/2023 when Alice replaces the first TX with another after Bob writes his TX in an n-payment channel. I think most cross-chain communication techniques are not susceptible to this exploit since most of them are already cautious about finality or escrow time; ie, no TX at the target chain before reaching confirmation at the source chain.

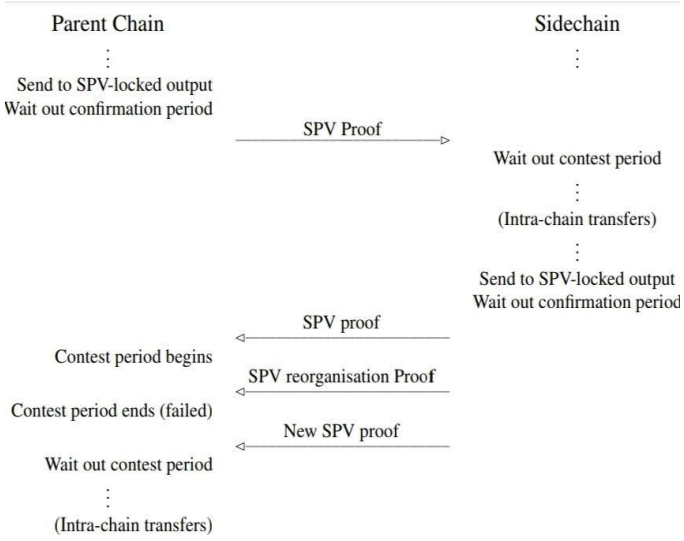

Fig. (5-b) a 2-way peg side chain in its original paper [19], BTC-Relay in [20] is not very much different, only it works in one direction since ERC-20 and a similar tokens cannot be processed in the Bitcoin blockchain.

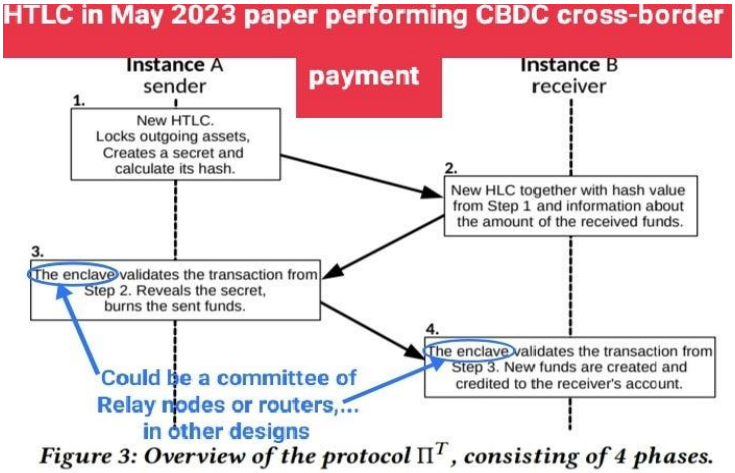

Fig.5-c: usage of HTLC in CBDC atomic swaps (annotated from [22]); Merkle proofs similar to SPV are exchanged & verified here too.

True the name “public" connectors came from their usage (and original design) to connect public permissionless blockchains; however, HTLCs are more used to either connecting Bitcoin and like altcoins to DeFi (**X-Claim** [25] builds kind of a faster non-interactive version of BTC-Relay); or to connect private blockchains (CBDCs [22], or IoT [23]); [26] generalize to a heterogenous (public & private/consortium) but just Ethereum like blockchains(EVM). **Atomic Loans** the 2019 paper [27] maybe was the first to propose the use of atomic swaps in over-collateralized DeFi loans including stable coins and fiat currency, although all references of the project and the company investments afterwards refers to facilitating Bitcoin usage in DeFi and payments (https://www.crunchbase.com/organization/atomic-loans, https://consensys.io/diligence/audits/2019/09/atomic-loans/). **Fusion** [28] (based on 2017 paper) uses a variant of HTLC that add *time slices* where participants can earn interest on their locked money during a time slice which is more profitable; I also found another paper [29] that connects Ethereum to Tron using HTLCs (Peace-Relay in [21] use side chains only without HTLC). Other crypto HTLC solutions follow the Bitcoin Lightning Networks idea; ie, they aim to provide off-chain TXs as a scalability solution similar to ***Lightning Networks LN***. Examples include **Commit-chains** [30] that allow secure payments for lightweight Ethereum clients in ~46 KB on mobile devices; maybe **Elements** [31] as an L2 over Bitcoin target functionality & privacy more than scalability, but still do not target interoperability.

>>> A side note here, is that lightweight and off-chain TXs are very much desirable bonus properties in the CBDC case or Financial systems in general. As for interoperability, those are usually private permissioned by nature which makes them suitable for this type of interoperability solutions; an additional condition from [10, sec 6] that HTLCs can connect private blockchains only if there’s a 3rd party public blockchain as an intermediary and also in a *semi-trusted* environment (which is the case in [22]), or if all candidates are registered in both chains.

2-Intermediary Systems

We ended our discussion on HTLCs & side chains by the fact that their usage in private permissioned blockchains requires writing at least succinct proofs on a public blockchain periodically. Another fact I’ve learned it’s proved from [5] is that asynchronous protocols cannot tolerate misbehaving nodes *without a trusted third party*; practically recording every step on a public blockchain will cost a huge amount of gas [4] (up to 64M gas; ie. nearly 6300$ when tried by *Near* rainbow bridge & others). So, it is either done periodically as snapshots like in [22], or through decentralization in the usual crypto manner:

1)the repetition of tasks by a number of independent nodes, 2) incentivized to participate according to some rewarding mechanism, 3) to verify passing data according to some cryptographic rules (written as a smart contract), and 4) reach a decision through some consensus protocol (usually a variant of BFT). We generally call that a ***bridge*** (an intermediary system that contain a number of ***relay nodes*** who choose to “relay or not relay” the messages they receive from the communicating blockchains).

Commented [DA7]: Vitalik public connectors TR was first published by r3 corda paper in 2016, r3 Corda participated recently in newer CBDC interoperability designs with Quorom & Swift (https://www.swift.com/news-events/news/successful-testing-paves-way-cbdc-use-cross-border). Fusion is also promoted to be for financial systems, Chainlink just completed a project with swift (not CBDC) and Hyperledger is on the Hamilton CBDC project; more about this in next articles.

Commented [DA8]: The author in [10] (2021) describe the node that writes to the 3rd public blockchain as a “gateway", since the two connecting chains are permissioned (or could be anything not necessarily homogenous with the 3rd public); the term ”gateway” is also used by Hyperledger Cacti platform connecting heterogenous blockchains.

Commented [DA9]: Most DeFi applications we are used too, even the cryptocurrencies blockchains themselves, are considered “***Trustless***" because they use cryptographic techniques to prove and authenticate every step as opposed to other systems that use a trusted third party (which is considered a centralized solution to begin with), or to systems that hardcode (wire) the cryptographic function they use in what is called ***TEE*** *Trusted Execution Environment* or enclaves. TEE solutions were more common in private blockchains that already uses sensors (hardware) to measure physical parameters (water or energy for example) like Hyperledger Fabric so more hardware seems a natural choice; however, TEE solutions started to be more appealing to DeFi recently (https://decentralizedthoughts.github.io/2023-04-09-blockchainsplustees-day1-summary/, https://twitter.com/socrates1024/status/1700981955251286456)

Commented [DA10]: Using any form a centralized intermediary would introduce a single point of f ailure DeFi is trying to avoid all the time. Note that we consider cryptocurrency blockchains to be Δ synchronous (synchronization is achieved within time Δ), but I think any form of cross-chain interaction protocol will be event driven and hence asynchronous.

The number of those relay nodes constitutes a kind of dilemma; the more relayers the more security but the less time efficiency. Think of it as POS consensus because even if any node can become a relay it must be registered first, so the consensus here must be ***a variant of*** Byzantine Fault Tolerance ***BFT***; ie., ***at least 2/3 of the nodes must be honest*** (Not 51% as Nakamoto POW consensus, although Fusion white paper shows a 2-tier consensus one of them is POW). On the other hand reaching a consensus between a larger number of nodes is time consuming in such a time-critical environment as DeFi; take **RSK** [32] as an example (atomic swap bridge started with *RBTC* as tokenized BTC in Jan 2018, now include most EVM chains), in RSK medium value CC-TXs takes ~3hrs to confirm while large size ones may take a day.

You may find a little difference in terminology between Fig.6 from [3] (2023) and the famous survey paper [5] (2021), but you can still capture the details of each design with no contradiction or ambiguity. For example [5] call that design "*A federated 2-way peg*" considering it semi-centralized as the number of verifying relay nodes is much less than the number of full nodes in any cryptocurrency, it also says that there is no such thing as relay nodes without side chains.

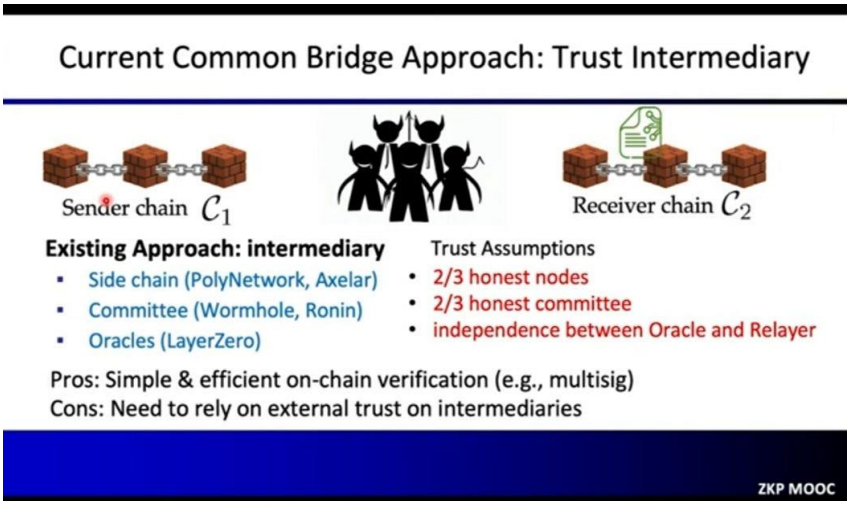

Fig. 6: from the ZK Berkeley MOOC [3], lec14.

Now delving into Fig.6, **PolyNetwork** [33] have 2 groups of relay nodes (sometimes called keepers) to relay data (provide a multi-signature on correctly authenticated data according to witness Merkle proofs) either in or out its intermediate *poly-chain*; while **Zendoo** [34] verify transmissions using *recursive ZK snarks*; **wormhole** [35] uses a governed set of guardian nodes that sign *Validator Action Approval VAA* while relayers pass VAAs off-chain; **Ronin** [36] started using *Proof of Authority PoA* consensus between limited validators to relay Axie Infinity players TXs through *Ronin-chains*; **Fusion** [28] uses *Ticketed Proof of Stake TPOS* consensus, where the validator participation is valid only for a ticket duration (this increases the number of validators to include those who can't have a working node all the time); **Wanchain** [24] uses *Galaxy POS* consensus (drawn from *Ouroboros POS* by IOHK) and claim to have 47 delegation validator

Commented [DA11]: *Zendoo* is part of the *Horizen* Blockchain for interoperability solutions (https://www.horizen.io/research/); Zendoo started between Bitcoin & IOHK for Cardano and the article here (https://hackernoon.com/zendoo-protocol-a-deep-dive) says it's only for UTXO-based Blockchains. Horizen uses the ***ZEN*** unified token and have more additional white papers *Latus* (details the rewarding incentive scheme for provers; [4] also mentioned the use of economic incentives in *Nomad* and *Near Rainbow* protocols but I haven't trace their papers yet) then *Darlin* (details the final recursive ZK-Snark proof).

nodes; **Layer zero** tries to add an extra security tier by using oracles from *Chainlink* for the oracle committee to be independent from the relay nodes (heard they're trying to make their own recently).

The paper [4] (2022) asserted the significance of ***key breaches*** (recall the number of relayers/validators dilemma we just discussed) through an attack on *Ronin* where the protocol required the signature of 5 out of 9 validators, so when 5 keys were compromised $624m were stolen; *Harmony's Horizon* bridge required 2 out of 4 and lost $100m (jun 2022) [37]; the recent attack on *PolyNetwork* (jul 2023) was also because 3 out of 4 signing EoAs were leaked through social engineering [38]; *Fusion* [28] is featured a distributed key storage mechanism since their original paper 2017 (like *arweave* if you are familiar with it) to avoid a single point of failure and minimize the effect of any penetration, but this does not prevent the threat of social engineering. Bridges are also suscept to ***code vulnerabilities*** like any DeFi construct, examples include (but not limited to [37]) the 610m$ *PolyNetwork* 2021 attack [38]; the 320m$ *wormhole* 2022 attack [39]; ignoring checking a link to be *nil* in the function parsing the Merkle tree to calculate and verify the proof "*ival*" led to the loss of 600m$ in *Binance* bridge (BNB token) 2022 (the hacker replaced the *nil* node in old leaves, the same fn was used by Cosmos but they had other checks) [40] ; the bug that led to *Nomad* attack was described by Samczsun [41] to be one of the most chaotic hacks (" you don't need to know about Solidity or Merkle Trees" he continued); also in the *Ronin* attack the key of the *Axie DAO* validator node were compromised through locating a backdoor (i.e., not through social engineering).

Commented [DA12]: -Sadly *PolyNetwork* haven't completely recovered from this second attack yet (their twitter account says services are partially stored), the attack was able to mint tokens in many target blockchains without locked tokens in the source chains.

To avoid attacks, bridges usually use audits (example of security audit firms: Certik, SlowMist), deploy bug bounties, and evolve continuously by avoiding their own and others previous mistakes (vulnerabilities); *debridge* here [42] describes 10 cautionary guidelines.

So, *Harmony* now requires 4 out 5 key signatures and deployed 1m$ bug bounty; *Ronin* integrated Delegated Proof of Stake (DPOS) properties into its POA consensus, applied a strict reputation with tiers of slashing mechanisms, increased the number of validators to 22 (12,10) and required at least 8 of 9 signatures (instead of 5).

Axelar [43], which was recently chosen by *Lido* [44] (with *Neutron*) and *Uniswap* DAO bridge assessment committee for cross-chain governance message passing [45], 1)uses a rewarding POS incentive to have a *75 validator* nodes, 2)forces a periodic *key rotation* to minimize the risk of key leakages, and 3) puts a *limit on transacted money* in a certain time interval to cap any unexpected money draining attack; it also 4) avoid vote monopoly by using a *quadratic voting* mechanism to slow down (by the square root) the growth of a validator voting power with the increase of his stake due to the rewarding incentive scheme (for correct voting).

However, the excessive number of attacks remind the DeFi community with Vitalik Buterin words that "Bridges have fundamental security limits"; so *Blockchain Of Blockchain* systems (*BOB*) are gaining more ground everyday, or *Hybrid Systems* where bridges are deployed with them when needed like in DEXs for example.

3-**DEXs**

Vitalik in [16] followed by [5] both categorize exchanges, mostly DEXs we care about, under the

term *Notary Schemes* saying that they deploy a smart contract for each liquidity token they have a pool for, the SC uses oracles to determine price according to their used formula (the AMM formula), and a kind of manager smart contract above them probably to handle semantic interoperability we briefly mentioned above; we know from newer resources that DEXs deploy bridges to achieve technical interoperability.

- We just mentioned that ***Uniswap*** the highest market cap hired a committee to choose one for its governance messaging [45]; *Axelar* is a newer choice under testing, while *wormhole* is an earlier choice and is currently used on BNB, Gnosis, and MoonBeam deployments since Aug 2021. The report also talks about the *message sequence ordering* used by each choice (semantic interoperability according to my understanding) and that they do not favor the one used by *wormhole*. It's worth mentioning that wormhole has joined with COSMOS (a BOB system) recently [46] in Jul 2023.
- I found out that ***SushiSwap*** is now part of the *Layer-zero* ecosystem [47] and has built *SushiXSwap* which supports bridging of assets across Ethereum, Fantom, and about 5 other networks; it also utilizes *Stargate Finance Bridge* (part of Layer-zero too) to find the cheapest route for its users.
- ***Curve*** deploys different bridges for moving assets to different blockchains [48]. (Multichain bridge has stopped with no replacement yet)
- ***Aave*** has built its own bridge from Ethereum to Starknet [49]

Closure

Well, this was part-1 in my attempt to understand and summarize an up-to-date overview of blockchain interoperability solutions. I tried to the cover the necessary conceptual terminology first, then concentrated on public connectors which include all HTLCs, side chain based solutions and bridges. We saw at the end that many bridges are recently joining BOB systems to include more chains and have more security, which is going to be explained in part-2.

References

[1] https://www.chainalysis.com/blog/zetachain-security-halborn/, last accessed 8/9/2023.

[2] R. Auer, P. Haene, H. Holden, et al., *"Multi-CBDC Arrangements and The Future of Cross-Border Payments"*, BIS papers, 2021. (cross reference form "*CBDC Bridging between Hyperledger Fabric and Permissioned EVM-based Blockchains*", Mar 2023).
[3] Berkeley ZKP MOOC, 2023, "*ZK-bridges*", lec.14; https://youtu.be/0bKasr4G7OM?si=AA_7NNy1OYs-25Dn, last accessed 11/10/2023.
[4] Dawn Song et al., "zkBridge: Trustless Cross-chain Bridges Made Practical",2022, https://arxiv.org/abs/2210.00264

[5] "Blockchain Interoperability: past, present and future", 2021,

https://dl.acm.org/doi/10.1145/3471140

[6] https://anoma.net/blog/heterogeneous-paxos-and-multi-chain-atomic-commits; last accessed 12/10/2023.

[7] https://stackoverflow.com/questions/76871511/axelar-transaction-underpriced-error-on-token-deployment-for-bsc; last accessed 14/10/2023.

[8] Fil, "*Cosmos IBC, LayerZero, and Chainlink CCIP. Comparing Cross-Chain Solutions*", https://mirror.xyz/filarm.eth/vJG_FMayXVQeEkT6RGqhxk0ALGlSb3SGU9j7Y5pnZPo; last accessed 9/10/2023
[9] https://medium.com/coinmonks/layerzero-the-first-omnichain-interoperability-protocol-for-cross-chain-communication-e5d5e37b99a9; last accessed 9/10/2023.
[10] T. Hardjono, "*Blockchain Gateways, Bridges and Delegated Hash-Locks*", Feb 2021; https://arxiv.org/abs/2102.03933

[11] Chainlink, https://chain.link/; last accessed 9/10/2023.
[12] https://github.com/hyperledger/cacti/tree/main; last accessed 9/10/2023.

[13] layer zero; https://layerzero.network/pdf/LayerZero_Whitepaper_Release.pdf

[14] https://blog.zetachain.com/zetachains-unique-approach-to-interoperability-329664e2d8ec; last accessed 9/10/2023.

[15] https://www.financemagnates.com/thought-leadership/why-omni-chain-is-the-future-of-dexs/; last accessed 9/10/2023.

[16] Vitalik Buterin,2016, Technical Report, "Chain Interoperability', https://allqantor.at/blockchainbib/pdf/vitalik2016chain.pdf
[17] https://github.com/bitcoin/bips/blob/master/bip-0112.mediawiki; last accessed 7/10/2023.

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

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

[20] BTC-Relay; https://github.com/ethereum/btcrelay/blob/develop/README.md; last accessed 12/10/2023.

[21]https://github.com/KyberNetwork/peace-relay; last accessed 18/10/2023.

[22] https://www.researchgate.net/publication/371124247_CBDC-AquaSphere_Interoperable_Central_Bank_Digital_Currency_Built_on_Trusted_Computing_and_Blockchain; last accessed 9/10/2023.

[23]https://www.researchgate.net/publication/372796024_A_Secure_Sidechain_for_Decentralized_Trading_in_Internet_of_Things

[24] WanChain, https://docs.wanchain.org/get-started/introduction; https://medium.com/wanchain-foundation/wanchain-roadmap-2020-9883f92fa0ab; last accessed 20/10/2023.

[25] "*XClaim: A framework for financially trustless blockchain interoperability"*, IEEE S&P 2019, https://www.xclaim.io/; last accessed 19/10/2019.

[26] P. Robinson & R. Ramesh, "*General Purpose Atomic Crosschain Transactions*",Nov 2020; https://arxiv.org/abs/2011.12783
[27]M. Black, T. Liu, and T. Cai, "*Atomic Loans: Cryptocurrency Debt Instruments*", Jan 2019;https://arxiv.org/abs/1901.05117

[28] Fusion, https://www.fusion.org/en; https://www.okx.com/learn/what-is-fusion ; last accessed 25/10/2023.

[29] M., Bahtia, and B. Singh, "*Hash time locked contract based asset exchange solution for probabilistic public blockchains*", 29/6/2022; https://link.springer.com/article/10.1007/s10586-022-03643-x

[30] "*Commit Chains: Secure, Scalable, Off-Chain Payments*", TR, https://eprint.iacr.org/2018/642.pdf, 2020; https://github.com/liquidity-network/nocust-contracts-solidity

[31] https://elementsproject.org/how-it-works; last accessed 19/10/2023. Liquid 2016 original paper for the interested reader, "*Strong Federations: An Interoperable Blockchain Solution to Centralized Third-Party Risks*", https://arxiv.org/abs/1612.05491

[32] RSK, https://tokenbridge.rsk.co/; last accessed 20/10/2023.

[33] PolyNetwork, https://www.poly.network/; last accessed 27/10/2023.

[34] "*Zendoo: a zk-SNARK Verifiable Cross-Chain Transfer Protocol Enabling Decoupled and Decentralized Sidechains*", IEEE 2020, https://ieeexplore.ieee.org/document/9355752

[35] Wormhole bridge design, https://everstake.one/blog/an-essential-guide-to-wormhole-and-the-portal-token-bridge; last accessed 23/10/2023.

[36] Ronin bridge, https://docs.roninchain.com/docs/basics/white-paper; https://docs.roninchain.com/docs/basics/dapps/ronin-bridge; last accessed 24/10/2023.

[37] https://limechain.tech/blog/biggest-blockchain-bridge-hacks/ ; last accessed 24/10/2023.
[38] PolyNetwork both attacks brief, https://medium.com/@shymaa.arafat/what-happened-to-polynetwork-2021-then-2023-2e991e29655b; last accessed 23/10/2023.

[39] Wormhole attack, https://extropy-io.medium.com/solanas-wormhole-hack-post-mortem-analysis-3b68b9e88e13; https://www.certik.com/resources/blog/1kDYgyBcisoD2EqiBpHE5l-wormhole-bridge-exploit-incident-analysis; last accessed 23/10/2023.

[40] BNB 600m$ attack, https://gist.github.com/samczsun/8635f49fac0ec66a5a61080835cae3db; last accessed 25/10/2023.

[41] Nomad, https://www.coindesk.com/tech/2022/08/02/nomad-bridge-drained-of-nearly-200-million-in-exploit/ ; last accessed 24/10/2023.

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

[43] https://axelar.network/blog/security-at-axelar-core; last accessed 14/10/2023.

[44] https://twitter.com/axelarcore/status/1702309307369615660; https://www.cryptotimes.io/Flido-chooses-axelar-and-neutron-for-wsteth-launch-on-cosmos/ ; last accessed 14/10/2023.

[45] https://uniswap.notion.site/Bridge-Assessment-Report-0c8477afadce425abac9c0bd175ca382; last accessed 14/10/2023.

[46] Wormhole join with Cosmos was announced in Jul (not Sep) https://wormhole.com/wormhole-foundation-engages-strangelove-for-cosmos-development-and-expansion/; last accessed 24/10/2023.

[47] Sushi-Swap in Layer-zero, https://www.coingecko.com/learn/layerzero-ecosystem; last accessed 15/10/2023.

[48] https://resources.curve.fi/multichain/bridging-funds/; last accessed 15/10/2023.
[49] https://app.aave.com/governance/proposal/127/; last accessed 15/10/2023.