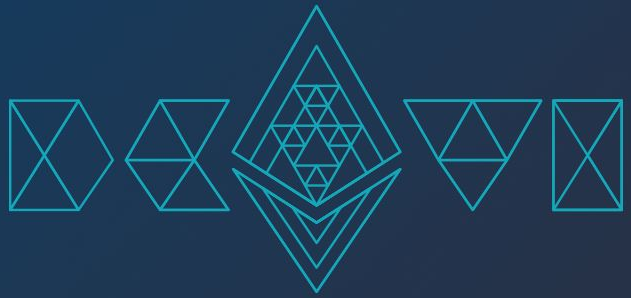


Securing Cross-chain Communication

Nithin Eapen

Router Protocol

All the attention for Cross Chains Swaps/Bridges

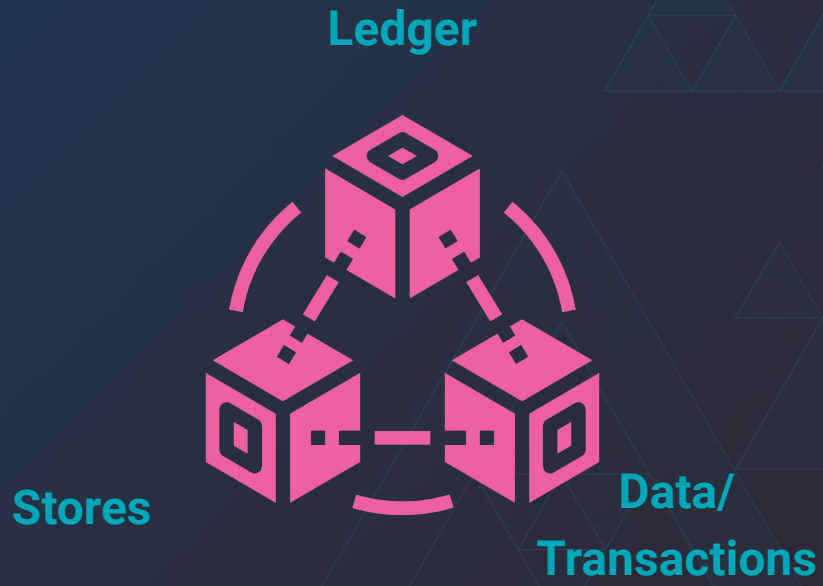
Raises

- **Layer Zero** 135 million $
- **HashFlow** 25 million $
- **Nomad** 22 million $

Hacks

- **Ronin Bridge** 600+ million $
- **Wormhole** 325 million $
- **Harmony Bridge** 100 million $

Blockchain?



Data & Transactions = Value

450 billion USD

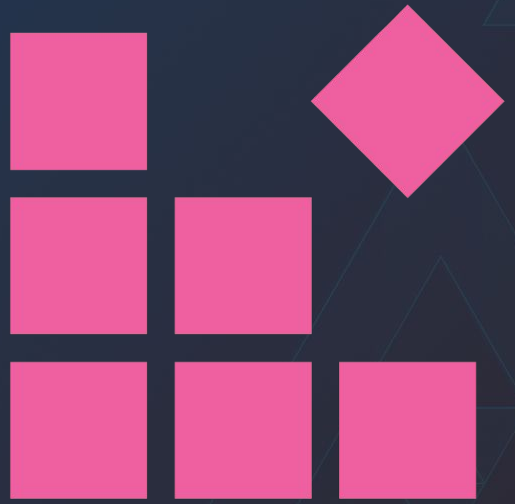
200 billion USD

50 billion USD

Total Market Cap

1 Trillion $

Fragmented

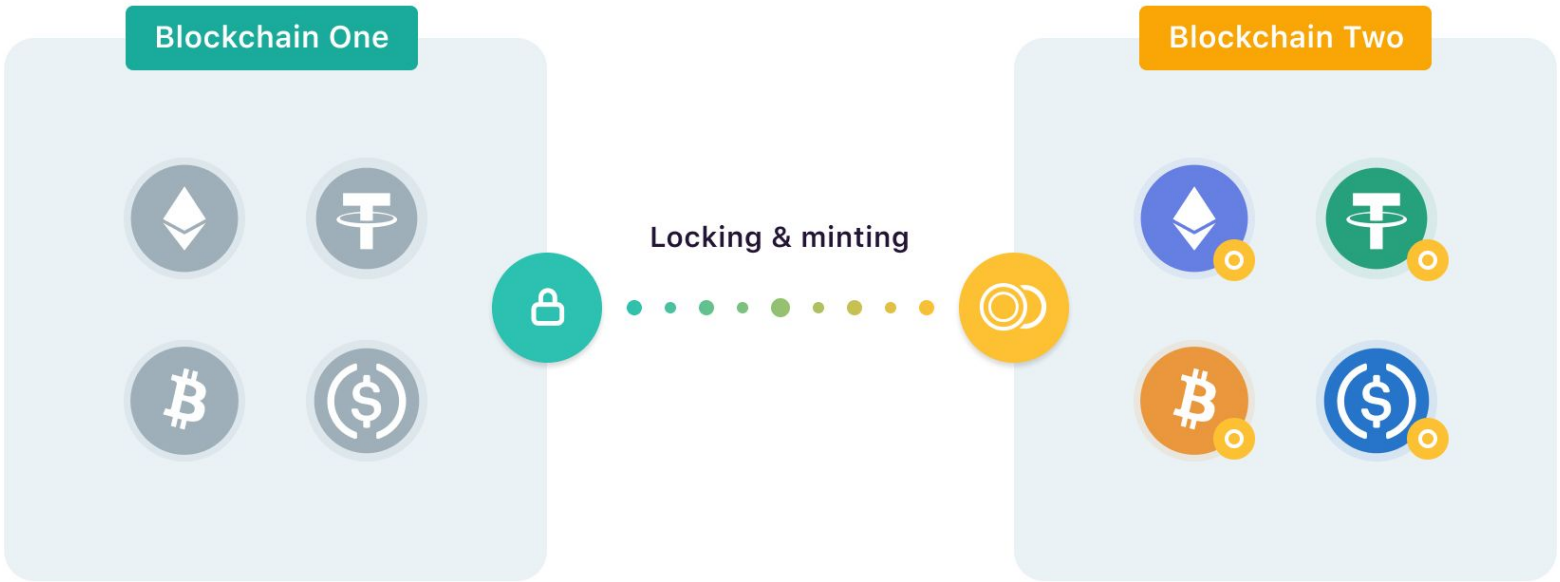


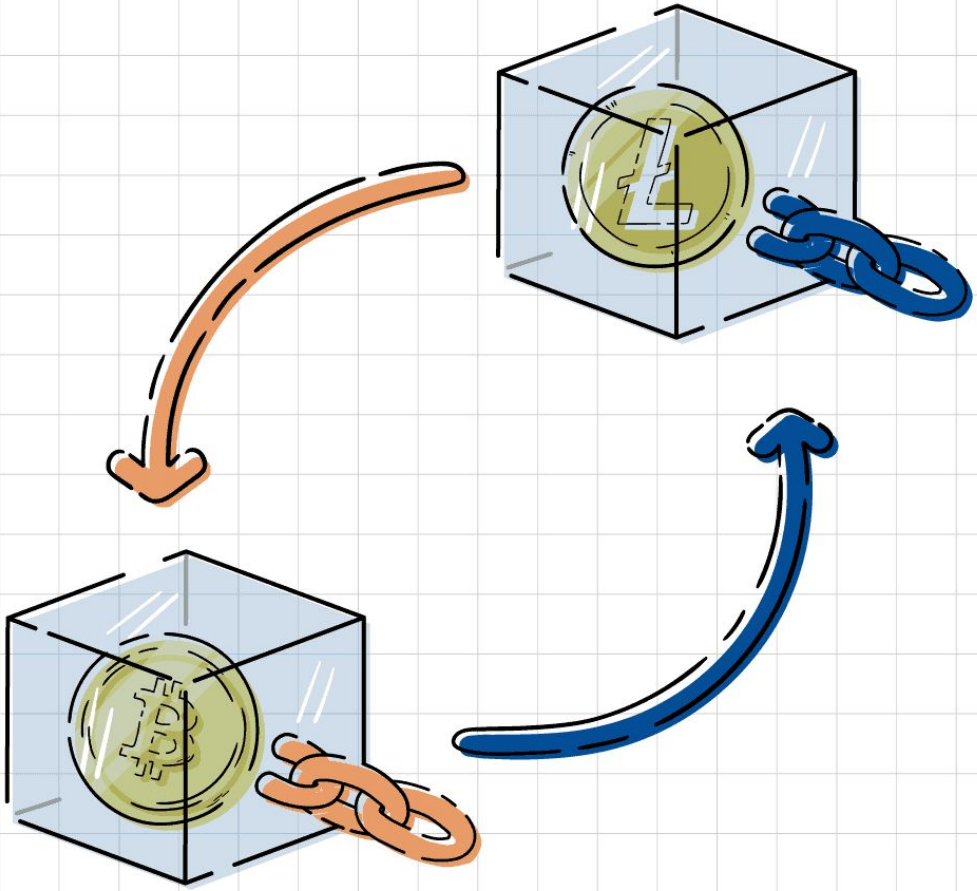
Blockchains are disparate walled islands of value

They are more useful when you can move these assets across

Bridges help move cargo from one island to another

Cross Chain Bridges





Cross Chain Swaps

Exchange a token on one blockchain for a different token on another chain

Fragmented users and value to move across chains without friction

You should not be send your ETH from your Dapp to coinbase to sell ETH, then buy Solana with USD and transferring it to your Solana Dapp

Critical Infrastructure for DeFi

- **Moving between proprietary blockchains**
  (Token on solana slp standard to Bsc BEP-20)

- **Transferring assets between Layer 2s**
  (Arbitrum to Optimism)

- **Both requires time and effort and idea of bridge is do transfers easy, quick, safe and trustless**

Architecture

- **Bridge Transfer information** (assets, contract calls from one blockchain to another)
- **A node monitors state of original chain.** (validator)
- **Transmits information from source chain to destination chain**
- **Check process requiring consensus among validators**
- **Signature**
- **Validator on destination chain verifies and issues IOU or sends to liquidity pool**

Various Types of Bridges and Mechanisms

POA Bridge

- Small set of outside actors listen to events on source chain, validate them and relay to destination chain
- Incentivization and slashing mechanisms to ensure integrity of these actors
- Pros : Few validators so consensus fast, low latency message transfers, adding new chains straightforward
- Cons: Trust based, collusion possibility,

POS Bridge

- Similar to POA Bridge node with large amount of token balance executes, verifies and signs
- Cons: Security depends on price of token

Light Client Bridge

- Example Rainbow Bridge
- A SC with ETH light client functionality is deployed on NEAR and SC with NEAR light client functionality deployed on Ethereum
- Verification is done by both chains calculating merkle roots from merkle tree and verifying it matches header
- No need of a node/validator besides miner
- High Implementation Costs. It requires SmartContract development to hold light client on each Blockchain
- Batching headers long wait time from Near to Ethereum

ULN with Oracle Bridge Adapters

- Does not keep track of headers
- It cannot compute transaction proof depends on external actor
- Oracles used to relay block headers and relayers to forward proofs
- Cons: Assumption is Oracles and Relayers wont collude

Custodial Bridge

- wBTC only from BTC to ETH

Decentralized Bridge

- Wormhole

Unidirectional Bridge

- wBTC all held by BitGo

Multidirectional Bridge

- Wormhole and Multichain

Lock, Mint & Burn

- To move N Token Z from blockchain A to blockchain B
- Lock N Token Z into bridge contract on blockchain A
- Bridge then Mints N Token Z or wrapped token Z on blockchain B
- To unlock or get the original tokens on blockchain A back, the token owner should burn the blockchain B tokens or wrapped tokens
- Once verified bridge will release Token Z on blockchain A

Poly Network Hack

- 2021 ...600 Million $+
- A master wallet for each Layer 1 , each containing certain funds
- A set of Smart Contracts that execute user instructions
- A Blockchain chain layer that these Smart Contracts run. Large amount in wallets for liquidity
- Hack was possible by access rights on SCs ETHCrossChainManager EthCrossChainData
- Hackers key registered as Keeper

Wormhole Hack

- Leaderless , Guardian nodes, ⅔ Approval , All guardians have equal weight
- Bypass verification using a deprecated function to mint wrapped ETH tokens on solana network without putting up any Solana . Then exchanged for ETH in their account
- Problem was detected by devs and uploaded to github but before it was deployed the hacker could use that problem
- Basically could issue gold certificates without having gold in the vault
- Losses were backed by JumpCrypto.

Wormhole Hack

- **This is the source code that contains the security flaw. Notice it used deprecated load_current_index and load_instruction_at against the input of sysvars:instructions account without checking it is a real one.**
- **To summary Wormhole minting flow:**
    - Call a transaction with 2 instructions: secp256k1 with minting message and guardian.verify_signature to build a valid signature_set.
    - Call guardian.post_vaa with valid signature_set and message to build a valid message_acc.
    - Call token_bridge.complete_wrapped with valid message_acc to mint wrapped token.
- **The root cause**
  It is clearly that the Wormhole developers forget to check #4 input of function verify_signatures is a real and valid sysvar:instructions account.

Ronin Hack

- 2022 ...600 Million $+
- Really Web2 than a blockchain
- It interfaced with blockchain. It depended on 9 validator nodes which was compromised via social engineering
- Forgot to revoke access to Sky Mavis which now controlled 4 of 9 validators
- Scary part is they did not know this loss of 600 Million worth of ETH
- Then the hackers shorted Axie and RON tokens

Nomad Hack

- 2022 …150 Million $+
- Gave up security for simplicity or ease (Basically Light Clients)
- New update allowed users to spoof transactions or fake them withdrawing funds not theirs
- Multiple attackers

Fei Hack

- 80 million Dollar Hack
- ReEntrancy Bug

Beanstalk Hack

- 180 million Dollar Hack
- Flash Loans to accumulate assets to control governance protocol
- Hacker passed a proposal donating funds to Ukraine and taking off with the collateral

“If you’re trying to create a bridge between N different cryptocurrencies, the complexity of that is N squared,”
— which means N more chances for bugs to creep in.

Coding Practices

- **Web2 security practices first have to be followed …like phishing, running malware, spyware**
- **Stop making regular developer code a DeFi smart contract and then bring some security auditor.** (Like bank asking house building contractor to build their vault)
- **Centralized security to DeCentralized security is paradigm shift….not just code level security is important**
- **Common set of problems like ReEntrancy, Integer overflow etc should be known**
- **Updates or bugs if found cannot be uploaded in Github to alert hackers**

Coding Practices

- **Typos**
- **Uninitialized Implementation contracts** (Proxies)
- **Rounding Errors**
- **Unsafe Casting**
- **Smart Wallet Attacks**
- **Merkle Proof Mishandling**

Coding Practices

- Formal verification
- Testing ..Unit and Functional
- Fuzzing
- Documentation

Can we Stop Hacks?

- Hard Task
- Speed to scale and grow can cause vulnerabilities
- Hacking is easy but getting large amounts of money out is not easy anymore
- Chainanalysis to elliptic to Peckshield tracking them.
- Exchanges and USDT/USDC blocking funds
- Earlier in 2013 Exchanges were hacked...now its DeFi and Bridges

Mitigation & Response

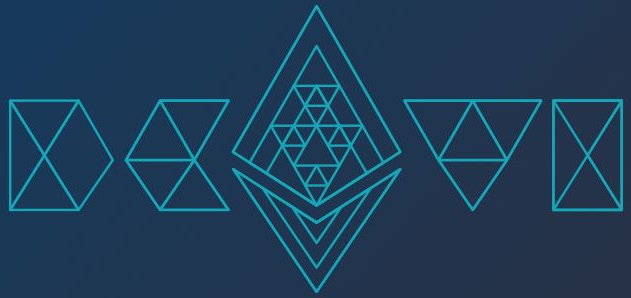
- **Audit and Bug Bounties** (Remember still though Auditors are not owners you are)
- **Prevent Contamination**
- **Fast Response**
- **Monitoring Systems and Reporting Guidelines**

Bridges Pros

- Collateral cross chain
- Scalability
- Efficiency

Bridges Cons

- Introducing some form of trust



Thank you!

Nithin Eapen

Router Protocol

nithin@routerprotocol.com

@neapen