SoK: Crosschain Token Bridges and Risk

***Abstract*—Despite the importance of token bridging with $2 billion USD stolen from bridges in 2022, there is a gap in existing literature of token bridges and the risks they pose to the wider ecosystem from a financial standpoint. In this Systematization of Knowledge, we bridge the gap in literature with a focus on token bridging and Liquidity Networks (LNs). We provide an outline the token mechanisms, their risk profiles, and the potential contagion these mechanisms pose, and a review of potential methods to mitigate contagion in the case of token price damage.**

***Index Terms*—Bridges, Crosschain, Liquidity Networks, Tokens, Risk**

I. Introduction

According to Vitalik Buterin, in an increasingly crosschain world, the likelihood of "systemic contagion that threatens the economy on that entire ecosystem" increases [44]. The risk is exasperated with the involvement of multiple chains instead of pairwise crosschain communication [44]. The investigation of Token Bridges, which allow the transfer of tokens across chains, is key to understand risk transfer. In addition, the scale of damage due to insecure bridging is increasing - with $2 billion USD stolen from bridges in 2022, which is 69% of all funds stolen that year [75]. This Systemization of Knowledge presents formal definitions for token bridges and their token mechanisms, and the corresponding types of risk. As literature and formal exploration of risk from a financial perspective is lacking, with existing knowledge in sparse forms of company project pages, forums, blogs and documentation. The aim is for the SoK to act a framework to understand the spread of risk in the field of crosschain enabled ecosystem.

The secondary implications of these crosschain risks can lead to token devaluation, contagion to other protocols and perhaps even the downfall of a chain entirely. In addition, with increasing push for crosschain stablecoins, there is a need for a framework to understand risk from a financial perspective.

II. Bridge Background

Bridges, for the context of this SoK, encompasses both message based bridges and application level protocols (Liquidity Networks) - which are most widely used. Thus bridges can be considered as service or protocol which allows the transfer of tokens between chains.

A. Motivation for Bridging

One key sub issue of interoperability, is the non-transferability of tokens or assets across networks. A free movement of tokens between chains would increase liquidity and act as catalyst for enhanced DeFi applications or functionalities.

Demand for crosschain token transfer has been primarily driven by the following:

1. Transferability of liquidity across chains. Primarily from larger to smaller chains (L1s to L2s and Major L1s to alt-L1s)

2. Exposure to Bitcoin on Ethereum DApps. Alongside the ability to utilise BTC

3. Rise of L2s. Addressing scalability bottlenecks of Ethereum with L2s and utilising major tokens on L2s

4. ETH and other major ERC20 tokens on alt-L1s.

However, the demand for bridges surpasses purely token bridging or liquidity transfer to other potential use cases for interoperability between different blockchains. Atomic swaps, also allow for the transfer of assets across chains through swaps of two native assets [33]. Crosschain contracts, allow events occurring on one chain can trigger events on another. Other use cases include crosschain ownership, crosschain social recovery wallets [32], crosschain collateralisation where collateral can be staked on any chain to trigger events on another chain. For example crosschain lending with collateralisation on chain A and loans given out in alternate chain B.

B. Bridge Types

According to the Bridge Framework by [62], there are broadly two types of bridges.

1) Message based bridges, also referred to as *"true bridges"* are generalized message passing bridges allowing the transfer arbitrary data through passing of messages.
2) Liquidity Networks (LNs) are application level protocols which enable fast transfer of liquidity via swaps of native assets. LNs typically use pooled assets across chains and true bridges to mint the assets or rebalance the pools of assets.

As shown in Diagram 1, the Liquidity Networks utilise Message based bridges as part of their architecture.

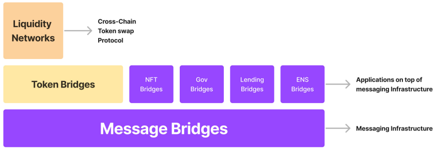

Fig. 1. Diagram of Bridge Types presented in the L2Bridge Framework from [62]

Message Bridge is the most primitive type of bridge facilitating any form of data transfer crosschain. *Token bridges* allow the transfer of tokens between chains. *Liquidity Networks* facilitate token transfer through swaps. Pools of assets on source and destination chain allow users to near instantaneous transfer via bonders or insurers who front liquidity for a fee.

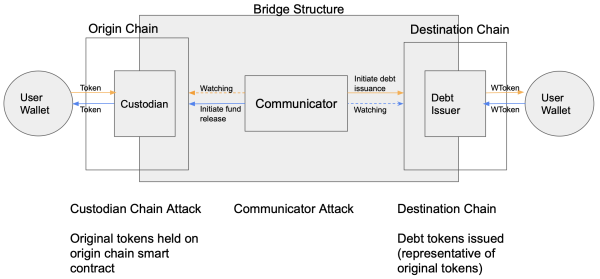

Fig. 2. Bridge Structure of Typical Lock and Mint Bridge based on Figures 2 and 3 from [37]

1) Message Based Token Bridges: Figure 2. shows the typical structure of a Lock and Mint Bridge. The user deposits a token on the origin chain bridge smart contract. The deposit is detected by the bridge, and the deposit triggers debt issuance of wrapped version of the token WToken.

The WTokens issued are backed on the custodial smart contract and can be retrieved when WTokens are sent to the Destination Chain contract to be burned.

Wrapped Tokens are representative tokens issued by the bridge provider. Wrapped tokens are also referred to as derivative tokens for this SoK, as their value is derived on the asumption of 1-to-1 backing.

a) L1 to L1 Bridges: Inter-L1 bridges, are bridges which bridge between two heterogeneous L1s. For example, a bridge from Ethereum to Bitcoin. These are also known as **Intercluster Bridges**, [63] are similar to interchain bridges. They connect chains from two different clusters. **Any-to-any bridges**, such as Wormhole, allow bridging between two heterogeneous chains. The tokens for each contract can be created without permission for any token.

b) Native Bridges: Native bridges "bootstrap liquidity of a specific chain i.e to seamlessly onboard users /moves funds into the ecosystem" [57] such as the Avalanche Bridge for the Avalanche chain. **Canonical Bridges** is a term typically used to refer to L1 to L2 bridges, though they have a similar meaning to Native Bridges. Canonical or native bridges, typically take a longer period of time to bridge assets than liquidity networks as they require a time period for finality to be established, such as the challenge period for optimistic rollups.

c) Validator or Oracle-based Bridges: "rely on a set of external validators or oracles to validate cross-chain transfer" [57] such as multichain and across.

d) Cross rollup bridges: facilitate L2 to L2 transfer of assets. Examples include Hop Protocol.

e) Validating Bridges: Validating Bridges are bridges between Ethereum and a rollup [64], where the bridge contract verifies the state updates proposed by the offchain system.

f) Other Bridge Type Definitions: Others define **Intracluster Bridges** [63], referring bridges between EVM based chains. This requirement means bridges are able to read the state of all of the chains in the same manner.

Others bridge types are **Token Specific** (such as WBTC), or **Application Specific**, bridging from a specific chain (Polygon PoS, Optimism Bridge), or bridging for a specific protocol.

There are also **Sidechain bridges**, which bridge from the main L1 to the sidechain such as Gnosis from Ethereum [65].

2) Liquidity Networks and Token Swaps:

a) Liquidity Networks (LNs): provide near instantaneous bridging at a premium. Liquidity Providors, known as Bonders or Routers, front the liquidity for the user, taking on the temporary risk of the transaction should it suffer from disputes or rollbacks. Not only is the user paying for the underlying bridging services, but also the insurance premium for the risk taken on by the Bonder. Thus, the fees need to linearly increase with the transaction size as the Bonder is taking on greater risk (whereas true bridges have a set fee per transaction). Typically, Liquidity Pools and Automated Market Makers (AMMs) are used on either chain of the transaction to deliver instant liquidity. Compared to traditional bridges, they allow swapping of native assets as opposed to the minting of wrapped assets. Centralised Exchanges can be considered as Liquidity Networks.

b) Hash Timelock Contracts (HTLC): facilitates atomic swaps of two native assets across chain between two users securely. Users deposit their tokens onto HTLC contracts and the swap is performed correctly and the user is able to unlock the target token or the user can re-retrieve their orginal locked token.

3) Interoperability Platforms: Interoperability Platforms are general Crosschain Communication (CCC) protocols such as LayerZero [69], Polkadot [68], Cosmos (IBC) [67] and Chainlink's CCIP [66], which allow generic messaging and interoperability between any chains. These interoperability platforms can be used for token bridging directly, or as a foundation to build a token bridge (as with Stargate [70] built on LayerZero).

C. Bridge Architecture & Features

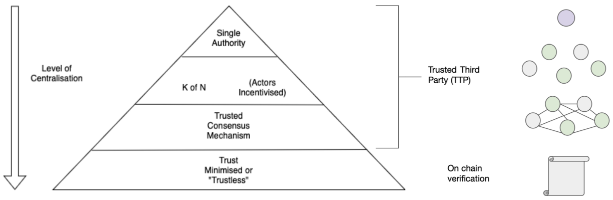

Fig. 3. Levels of Trust

1) Levels of Trust: Figure 3. shows the levels of trust of the offchain element of the bridge, with decreasing level of centralisation lower on the pyramid. The first three levels (Single Authority, K of N and Trusted Consensus Mechanisms) are a type of Trusted Third Party (TTP) with varying degrees of centralisation, where the bridge contracts trusts the external component for approving bridge transfers. Trust minimized or "trustless" bridges, verify the correctness of the update proposed by the offchain actor on chain.

Single Authority consists of a single person or wallet controlling the release of funds in the bridge.

K of N refers to a set of multi signature wallets which need to sign off on the transactions. A threshold value of K participants must sign for the transaction to go through. Participating actors can be incentivised by a requirement to stake collateral. Staked collateral is bonded or insured. Insured collateral insures the staked collateral will be returned to the user if malicious behaviour occurs and the stake is slashed. Bonded collateral is returned to the protocol in cases of misbehaviour. The types of collateral may further impact the level of security, in the case of tokens endogenous to the system. These bridges are semi-centralised, with the trust assumption of independence of participating actors with the majority not colluding. If actors collude or multiple wallets owned by the same organisation are compromised, funds may be stolen. The set of K actors may be randomly and dynamically selected to ensure a more decentralised process [55].

Trusted Consensus Mechanism. A middle consensus mechanism acts as the trusted authority which the bridge contract relies on to sign off on the transactions. For example, a third blockchain. The security of these bridges depend on the security of the consensus mechanism. The level of decentralisation also depends on the level of decentralisation of the consensus mechanism, but is significantly more decentralised than the K of N authorities or single trusted authorities structure. The bridge contract does not validate the transactions so the security is reliant on trusting the off chain system. The mechanism must also be available and online or the users may not be able to withdraw.

Trustless Bridges Custodial smart contracts self verify the correctness of the state update proposed by off chain actors. Ideal trustless bridges should allow permissionless participation in the validation and operation of the bridge and guarantee methods for operation in case of downtime of actors. They should also be resistant to censorship. If implemented well, security of trustless bridges is virtually equivalent to the security of the involved chains.

2) Verification Types: As presented in the L2Framework [62], there are various types of security mechanisms.

a) External Verification: An off chain Trusted Third Party (TTP) watches the events on one chain, verifies the validity of the events and communicates them to the destination chain, authorising the release of assets. The TTP can be a completely centralised single actor, multi-sig wallet or a consensus mechanism.

b) Native Verification: Native verification, also known as Light Client verification [62], involves verification on chain (destination chain).

1) Verification of validity of state (zk state proof or fraud proof with dispute mechanism)
2) Verification of consensus

c) Optimistic Validation: Submitted transactions are assumed to be valid. Honest actors can submit fraud proofs within a specified time period for fraudulent transactions.

III. Issues with Bridges

A. No Natural Fungibility

Since chains developed in silos, tokens are not naturally fungible between chains by design. Every token thus has a "home" chain, where the original token is created. To make a token fungible across chains, token project owners can create token contracts on all the chains, and provide an offchain bridge which allows for the "transfer" of tokens by locking and minting or burning and minting [71], [72]. For general any-to-any chain bridge solutions, there is always the creation of a representative token on the destination chain.

The commonly used Lock and Mint style mechanism, creates multiple variations of tokens based on which bridge issued them. For example, the bridged USDC variations include USDC.e, USDC.bC and axlUSDC [73]. The downside to any bridge being able to create any representative tokens, is the following:

1) Liquidity Fragmentation
2) Poor User Experience and User Fragmentation
3) Reduced Transparency

Liquidity must exist separately for every variation, with lesser used variations with little to no liquidity. There are too many variations created by large number of different bridges. Given the variety of tokens supported by different blockchain networks, each with different values and transaction rules, "accurate identification and verification of token types are necessary when conducting cross-chain transactions" [38]. The user is burdened with the responsibility to choose which variation to use. In addition, it is more difficult for the token issuer to track tokens due to the amount of variations created [73], reducing the transparency of tokens on each chain and variants are not always exchangeable to non variants on DEXes.

In this environment, platform approved tokens guide users to which are "official" tokens. Platform approval can be listed tokens on a DEX or listed on wallets without manually adding them.

There is also a significant advantage to chain projects developing bridges, also called "native bridges". Native bridges are considered the official means to transfer tokens between chains, more commonly used with Ethereum to L2 bridges such as Optimism. Wallets recognise as natively bridged, fungible representative, and there is liquidity support for token as the main token used on the chain. This chain approval also applies for non native bridges, where tokens are considered as the main fungible representative to be used on that chain.

TABLE I
BUSD TOKEN FRAGMENTATION

Bridge Provider	**Polygon**	**Arbitrum**	**Solana**	**BSC**	**Ethereum**
Multichain	anyBUSD			BUSD, BUSD (peg)	BUSD
Allbridge			abBUSD		
Portal		BUSDet, BUSDbs	BUSDet, BUSDbs		
Wormhole	BUSD		BUSD	BUSD	BUSD
Binance	BUSD (peg)			BUSD (peg)	
Paxos					BUSD

B. Token Fragmentation for Any to Any Bridges

Table I. shows the stablecoin BUSD and wrapped variants of BUSD across multiple chains and issued by multiple different bridge providers. Paxos is the orginal issuer of BUSD, a USD backed stablecoin, with partnership with Binance Exchange and previously approved by the New York State Department of Financial Services (NYDFS). Since the SEC charges against Paxos, Paxos has seized its partnership with Binance and halted minting of new BUSD coins but allowed for existing minted BUSD to be exchanged for alternatives [43]. Binance issued BUSD, also known as Binance-peg BUSD is a separate to Paxos' BUSD [42]. Since the severance of Paxos BUSD, Binance has also planned a phased halt in the use of BUSD from its exchanges.

As seen on Table I., liquidity and user fragmentation is caused by the multitude of variations created by each provider on each chain. DEXes treat each variant as a separate asset, with oracalised price tracking of BUSD. This frequently leads to little to no liquidity in these smaller token pools.

Due to the fragmentation issue, there is an increasing trend for native circulation of tokens, through the introduction of individual smart contracts on each chain for the token. USDC added native smart contracts for the token for 7 new chains since last year - with a total of 15 chains as of November 2023 [77]. In addition, Circle have created a bridged contract standard for third party bridged USDC allowing new chains to issue native USDC. A single companies such as Circle effectively delegate out minting licenses to various bridges, allowing the centralised control of tokens and unifying the endless creation of minted derivatives.

TABLE II
WORMHOLE OFFICIATED BRIDGED TOKENS

Destination	Total	Native Available	Multi-bridged	Bridged from Ethereum
Ethereum	25	8	1	N.A.
Solana	108	10	2	87
Avalanche	17	6	1	2

Table II. shows the official tokens bridged via the Wormhole bridge (also known as Portal) found on Wormhole's token list [48], [49]. The issue of liquidity fragmentation is exasperated by tokens being wrapped by different bridge providers.

If there is no direct bridging available, the tokens will "traverse through intermediate chains before reaching the destination chain" [41]. Bridge aggregators, such as Bungee [40], allow users to "choose a preferable route in terms of cost, speed, effectiveness, or even security" [41] when bridging. Bridge aggregators use a combination of DEXes and native bridges to facilitate bridging of any-to-any tokens by finding an optimal route [39], [40].

For example, a direct bridging from Ethereum to Avalanche may lead to WETH.e, but bridging via Polygon Proof of Stake Bridge en route leads to a different variation WETH.e (PoS). This results to "double-wrapped" tokens [50]. Double bridging using the same bridge (in the case for Wormhole), leads to the appearance of a single bridged token and the origin of the token is stated as the origin of the first bridging.

Furthermore, Wormhole's any-to-any type bridging leads to the creation of unnecessary derivatives, when native equivalent tokens are available. For example, the existence of USDTso when USDT is natively available on Ethereum. The fragmentation in liquidity and in user experience has increasingly been flagged as a concern from various members of the development community [58], [77].

1) Lack of Pricing Markets for Wrapped Tokens: Applications utilising wrapped representative tokens, such as DEXes, use the pricing of the original asset via oracle as opposed to the pricing of the wrapped derivative. This means if a wrapped token were to fail, there could be undercollateralised loans due to incorrect pricing.

Pricing of the wrapped tokens should deviate from the pricing of the original in the case of a bridge hack or bridge system failure. Due to the multitude of tokens and lack of liquidity in smaller wrapped versions, applications utilise the pricing of the original as opposed to the derivative token.

C. Finality and Time to Unlock

1) Finality: A core reason of why "bridges are fraught with inherent peril", is that it is "impossible to be assured of finality" [30]. Chains which differ at L1, have different thresholds for what is defined as "final", or 100% recognized as a immutable transaction of the past. There have been reports of issues with finality on certain chains with reorgs of double digit blocks [9]. For creators of bridges, and for users keen on security, finality is a key issue not to be overlooked.

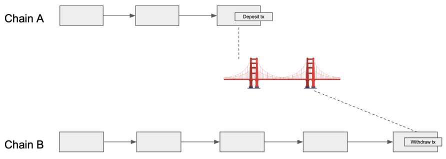

Fig. 4. Deposit event on Chain A triggers funds release on chain B

For two asynchronous probabilistic finality chains, there is always the risk of a 51% attack or a chain reorganisation,

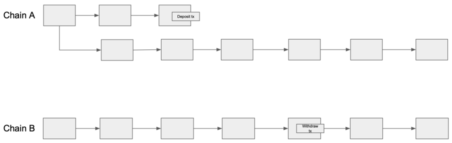

Fig. 5. Block reorg or 51% attack leads to deposit transaction being reversed on chain A

creating the risk for “double-spend”. Figures 4. and 5. illustrates how a deposit reversal on one chain, could lead to the duplication of the user’s funds in a bridging transaction.

In Figure 4, the user initiates a bridging transaction for her tokens from chain A to chain B through a deposit transaction. This is recognized by the bridge, and the user’s tokens are released on chain B. Some time thereafter, the block including the deposit transaction is deemed invalid due to a chain reorg or 51% attack (Figure 5). Since the deposit transaction has been reversed, but not the withdrawal transaction, the user duplicated their tokens, having tokens on both chains.

However, some L2 rollups are not exposed to 51% attack, as any rollback in the fundamental L1, will also happen in L2. “If Ethereum gets 51% attacked and reverts, Arbitrum and Optimism revert too, and so “cross-rollup” applications that hold state on Arbitrum and Optimism are guaranteed to remain consistent even if Ethereum gets 51% attacked” [44].

Despite propositions of ZK-SNARKS based decentralised bridges such as in [36], Buterin states “Even if there’s a perfect ZK-SNARK-based bridge that fully validates consensus, it’s still vulnerable to theft through 51% attacks like this” [44].

2) Cost for 51% attack: The risk of 51% attacks exist for all Proof of Work (PoW) chains, where miners solve difficult problems to produce blocks. Estimations based on NiceHash [34] [35] shows how the cost for PoW chains to be 51% attacked. $6.7 million USD have been stolen as a result of three 51% attacks on Ethereum Classic, ZenCash and PegNet [31]. The cost of a 51% attack is estimated to be $600k on Ethereum for an attack duration of one hour [37].

The risk of transaction reversal is one major contributor to risk in holding wrapped representative tokens. The holding of native tokens is safer than bridged backed representative tokens [44].

3) Time to Unlock: For True Bridges, as opposed to Liquidity Networks, the time to unlock the tokens at the destination once the tokens are sent from the origin chain depends on the security mechanisms of the chains involved. The time to transfer is also highly dependant on the time it takes for a transaction to be considered “final”. For fraud proof based, optimistic systems, the challenge period must pass in order for a transaction to be deemed final which is 7 days for Optimism [24] and Arbitrum [25].

TABLE III
TIME TO UNLOCK - CANONICAL BRIDGES

Chain	L1 to L2 Deposit	L2 to L1 Withdrawals
Optimism	1 minute (5 block re-orgs)	7 days (challenge period)
zkSync	1-5 minutes	10 mins-7 hours (depending on activity level)
Arbitrum	15-30 minutes (depending on congestion)	7 days (challenge period)

Liquidity Networks, other decentralised applications and any-to-any bridges, use adjustable“Peg Zones”, which apply an “finality threshold at some arbitrary number of blocks” [28] to determine finality for probabilistic finality chains. The longer the wait, the safer. However, the safety is traded off against speed, and thus usability for some applications.

Interchain consensus protocols, are solutions to mitigate the 51% attack risk and the risk of transaction reversal due to chain re-orgs. These proposed solutions include crosschain timestamping and crosschain checkpointing [6]–[8]. Crosschain checkpointing can be used to increase the security of crosschain network, even with chains with weaker security guarantees [6]. “Cross-staking” allowing validators to stake collateral on other chains which aren’t their native chains with IBC channels allow cross verification of blocks [8].

Bridges are also a retrofitted solution in response to a multi chain interoperability problem [14]. Perhaps due to the retrofitted approach, there is a tendency for fragmentation of approaches and of liquidity with the existing bridges. Especially for any to any bridges, liquidity fragmentation causes many virtually illiquid tokens. From a systemic risk perspective, the types of tokens able to be transferred across different clusters (L1s), should be minimized, for example, only allowing major tokens to be transferred. Allowing every token between clusters, increases interconnectedness and risk.

D. Risk by Size of chain

In general, the smaller the chain (in terms of participants, activity and TVL), the riskier the chain; not due to its inherent security properties, but because the less battle tested the smart contract practices, economic incentives and other aspects of the chain - leading it to be less robust to attacks.

Similarly, the more chains involved, the riskier. The risk for protocol failure increases with the incorporation of more chains. The combination of multiple attack vectors mean new avenues for attack are created [44].

Alternate forms of crosschain DApps are increasingly prominent, with the rise of crosschain governance, DAOs and lending. Since DAOs can control parameters of protocols, the implementation of crosschain governance is likely to increase the available attack vectors versus single chain governance system. As exemplified in the Beanstalk hack [11], even single chain governance can be exploited in combination of other attacks to compose a successful hack. Ensuring crosschain governance is robust, is essential for the health of any protocol. Protocols have also abandoned products relying on certain bridges. For example, Fantom have avoided certain Decentralized Applications dependant on bridges, due to the continued breaches. In a community proposal presented and approved to freeze access to Aave V3 services on Fantom, it was stated due to the "Harmony bridge event and the recent Nomad bridge exploit, the aave community should consider the risk/benefits of keeping an active Aave V3 market on fantom as this network is dependent of anyswap (multichain) bridge" [12]. The security risks of crosschain applications are significantly more prominent.

E. Types of Attacks

[37] provides classification for the types of attacks on bridges. Classical lock-and-mint style bridges have suffered several types of attacks classified by [37]; Custodial attacks on the origin chain, including the unlocking of custodied assets, Debt Issuer attacks which are attacks on Destination chain, including unauthorised minting of assets, and Communicator Attacks (such as polluting the data source of an oracle).

1) Lack of State Consistency Checks: State consistency checks refers to the checking of balances across bridge smart contracts and the monitoring for unusual transactions. In the event of a hack, consistency checks can help identify hacks in real time so that teams behind bridge protocols can act in response. The lack of consistency checks on balances means there is a lack of awareness of hacks in real time, until some time passes. This has been the case for certain hacks, raising the issue of lack of balance checks for these bridges.

IV. Bridge Token Mechanisms and Risk Profiles

A. Bridge Token Mechanisms

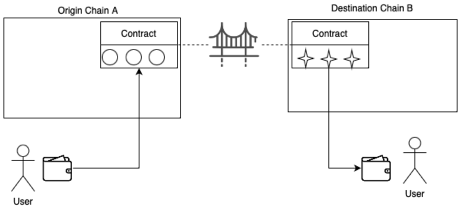

Fig. 6. Classical lock and mint mechanism

1) Lock and Mint: Figure 6 shows the classical lock and mint mechanism where a user deposits a token into the bridge's contract on the origin chain A and receives a minted, synthetic representative token on the destination chain B. The synthetic wrapped token can be deposited in the destination chain B, which will be burned for the original tokens to be unlocked.

For canonical bridges, the origin chain A is the L1 and destination chain B would be an L2, with only native tokens deposited in chain A. For any to any bridges, chain A and B are heterogenous chains with no requirement on the type of token deposited on chain A, including already wrapped tokens.

2) Burn and Mint: Mint and Burn, as shown in Figure. 7, allows tokens to be burnt when leaving chain A and virtually equivalent tokens to be minted on chain B. In Mint and Burn systems, the bridge is provided by the token creator (such as CCTP for USDC [56]) or authorised by the token creator to operate the burning and minting of the USDC when users move their USDC across chains.

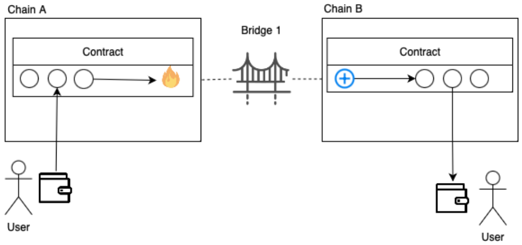

Fig. 7. Mint and Burn mechanism

3) Liquidity Network (LN): Liquidity Networks are application level protocols which enable near instantaneous liquidity transfer across chains. LNs typically use continuous liquidity pools to provide instantaneous liquidity to the user and front liquidity to the user for a fee. True bridges or native bridges can be used to settle the balances after the transaction has occurred. For some LNs, the use of true bridges is indirect - to create the pools of assets in the first place [70] or for arbitrageurs and independent liquidity providers to deliver liquidity to users at a profit [17].

The Liquidity Provider (LP) takes on the temporary risk until the transaction is fully settled via true bridges (which can take up to 7 days for Optimism, due to the challenge period). Across [60], utilises a centralised pool of assets held in L1, and Liquidity Providers receive a refund after the bridging transaction has occurred. Others such as Hop [61] utilise Bonders who front liquidity and allow L2 to L2 (Spoke) bridging via routing through the L1 (Hub) using native bridges.

The Liquidity Provider acts as the insurer receiving payment for covering for two risk types whilst the transaction is in progress; transaction reversal and the risk of cross-chain messaging infrastructure failure [18]. For continous liquidity pool based LNs, sufficient liquidity must be available for the bridge to operate - thus there is a liquidity limit - in contrast to Lock and Mint or Burn and Mint true bridges or peer to peer trading Liquidity Network.

Intermediary Settlement Assets are used to rebalance the imbalances in the liquidity pools on either chain caused when a transaction occurs - depleting one pool and adding to another. These settlement assets also acts as an intermediary exchange medium, enabling zero slippage during the crosschain operation as the same asset is swapped. These intermediary tokens are typically stablecoins or custom tokens (often derived from stablecoins). Examples of settlement intermediary assets include RUNE in THORChain [22], deUSDC in deBridge [13] or hETH in HOP when bridging Ethereum [27] amongst others [19], [20].

Table IV. shows the various types of LNs. The most common type consist of two liquidity pools on either chain, with an optional additional AMM step to enable any-to-any token transfer. True bridging is used to resettle the balances after the liquidity is provided to the user upfront.

	Single Intermediary Medium		Native Tokens
	Stablecoin	Custom Token	
P2P Direct Trading			deSwap LN (DLN) by deBridge [17]
Continous Liquidity Pools (with optional AMM)	Stargate [70], deBridge [13], celer's xLiquidity [21] (Figure. 8)	HOP [3], Squid (Axelar) [19], THORChain [22] (Figure. 9)	
Burn & Mint Resettlement	MakerDAO Wormhole DAI [3]	HOP [3], connext [20]	

TABLE IV
LIQUIDITY NETWORK TYPES

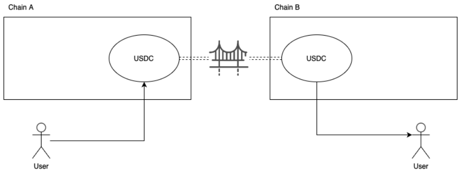

Fig. 8. Swap via intermediary stablecoin

a) Continuous Liquidity Pools (CLP): The majority of Liquidity Networks consist of two liquidity pools of assets - one on the source and the other on the destination chain of the transfer transaction (Figure 8). In this structure, intermediary token acts as an exchange medium allowing accurate amounts of the final token to be transferred to the user and to rebalance the pools once a transaction has occurred. The intermediary token can be created by the bridge project, such as RUNE in Thorchain, or stablecoins can be used such as USDC in Stargate.

Figure 8. shows a Liquidity Network based on pools of stablecoins such as USDC. The user deposits USDC on chain, to release the equivalent amount of chain B compatible USDC [3], [10] which can be native or existing bridged stableoins (such as Polygon PoS bridge). True bridging may or may not be used as a part of the LN architecture, using existing stabelcoins native to the chain or wrapped via native bridges.

This structure is often extended to use an AMM on both sides of the swap to enable any-to-any bridging of tokens shown in the following figure (Figure 9).

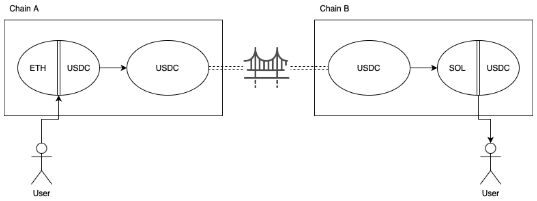

Fig. 9. Swap via intermediary stablecoin with AMMs on either chain allowing any to any swap

b) Continuous Liquidity Pools (CLP) with AMMs: Liquidity pools can have an additional step of AMMs wither side of the pool to enable the transfer of any assets. Figure 9. shows how ETH is initially swapped into the intermediary token USDC, where the same amount in credited on chain B, to be swapped to the final desired token - SOL. This allows any asset to be transferred. Stargate [70], based on LayerZero, uses this mechanism of bridging, allowing native swaps of tokens across chains. AMMs can be third party providers or provided by the LN provider.

c) LNs with True Bridging: Liquidity Networks utilise true bridging to rebalance the imbalances in the pools or as a method of no slippage accreditation of value across chains. Hop protocol, uses both Lock and Mint (L1 to L2) and Burn and Mint (cross L2) bridges as a part of the Liquidity Network shown in Figures 10 and 11 respectively.

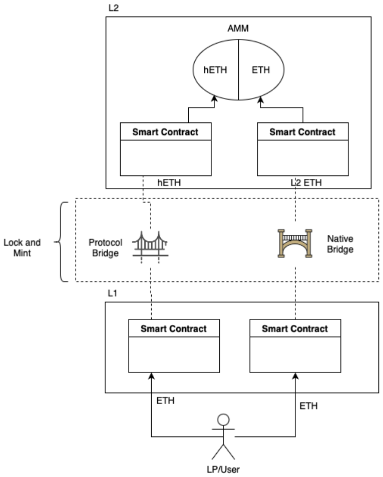

Fig. 10. L1 to L2 market of native to custom token in Hop protocol [26]

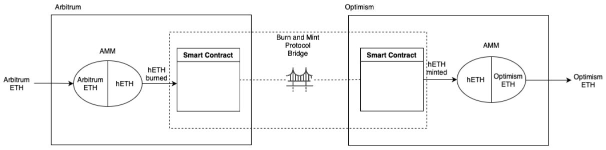

Fig. 11. Hop Cross rollup liquidity transfer with Burn and Mint resettlement mechanism [26]

Figure. 10 shows L1 to L2 LN on Hop protocol using two paths consisting of two Lock and Mint style bridges. One for the protocol hETH, and native ETH on the L2, both which are backed by the L1 native ETH on L1 smart contracts.

The setup of two bridge paths connected via AMM allows for a market where independent arbitrageurs can stabilise the hETH:L2 ETH exchange rate through exploiting the less taken path. Should the ETH/hETH rate become 1.005 [26], the arbitrageur has an incentive to swap L2 ETH for hETH, and redeem L1 ETH on L1 - effectively claiming ETH at a discount - and L1 ETH can be bridged back via native bridge to L2 ETH.

Figure. 11 shows the cross rollup LN mechanism, where a Burn and Mint bridge is used to transfer credit across chain. This is effectively the same structure as the Continous Liquidity Pools with AMMs and an intermediary token.

d) Peer-to-Peer (P2P) Crosschain Trading: P2P crosschain trading, such as deSwap LN (DLN) by deBridge [17], allows direct peer to peer trading where Makers submit requests to exchange an asset A on chain S for an asset B on chain D. Takers, whom have existing liquidity on the destination chain D, can choose to fulfill the order if the fee offered is favourable. An additional AMM step to exchange stablecoins into the target asset B to fulfill the order. Once proof of the order fulfillment is posted to the LN, the asset A is released to the Taker.

The benefit of P2P trading LN [17] is that the liquidity is not capped - which is the case or Continous Liquidity Pool LNs. P2P trading also removes the need to bootstrap pools with liquidity or run liquidity mining programs to maintain liquidity. It also removes the "unpredictable slippage" as the user can know in advance the exact amount they will be receiving.

B. Risk Profiles

TABLE V
BRIDGE RISK OVERVIEW

Token Mechanism	**Token Price Risk**	**Contagion**	**Risk Holder**
Lock & Mint	Firewalled	Compounding, Hierarchical	Wrapped Token Holder
Burn & Mint	Bi-directional	Weakest Link	All Token Holders
Liquidity Network			Liquidity Provider

TABLE VI
RISK OVERVIEW

Risk Type	**Token Mechanism**		
	Lock & Mint	***Burn & Mint***	***Liquidity Network***
AMM			✓
Crosschain Transfer Infrastructure	✓	✓	✓
Transaction Reversal	✓	✓	✓
System Failure during Transaction	✓	✓	✓
System Failure after Transaction	✓	✓	
Fee Model	Flat	Flat	Increases in proportion to tx size
Fees	Bridge + 2X Gas	Bridge + 2X Gas	DEX fees + Native Bridge + Liquidity Fee + Gas

Table. VI and V show the type of risk the token involved is exposed to in the case of a bridge failure. All types of token mechanisms are exposed to the risk of transaction reversal in probabilistic finality chains, with the exception of rollup bridges where any changes to L1 will also be rolled back on L2. Liquidity Networks involve crosschain swaps of native tokens, thus tokens are not exposed to price risk. However, liquidity providers carry the risk of pools of assets being stolen or in the case of a transaction reversal.

C. Lock and Mint

The risk profile for the lock and mint type bridge can be summarised as follows:

- Firewalled token price risk (one sided)
- Risk of bridge failure held by users of synthetic / representative tokens
- Serious incentives for attacks for custodied assets on origin chain

Classical lock and mint suffer from fragmented liquidity and risk of bridge failure at the responsibility of the user. As of today, bridges are retrofitted solutions to alt-L1s and rise of scalability boosting L2s. This leads to a lack of standards when it comes to wrapped tokens created.

The risk of the wrapped derivatives or representative tokens, can effectively be modelled like an exogenously backed, 1-to-1 stablecoin. Similar to how USDT claims to be backed 1-to-1 by the US Dollar, the wrapped tokens should be backed by the orginial in a 1-to-1 manner. The value of the wrapped derivative is considered the same as the value of the original, though this is not exempt from a "depegging" like event, if the wrapped is not backed as claimed.

The analogy of the 1-to-1 backed stablecoin also applies to compounded risk occurring for multi-bridged tokens. The second bridging of an already bridged token, is alike to a stablecoin backed by another stablecoin, backed by the native asset. Should any of the backing be missing in the chain of backings, the multi-bridged token will suffer from price "depegging".

a) Platform Approved Wrapped Tokens: For any to any bridges, the synthetic minted tokens need to be recognised and accepted by applications, DExes and Liquidity Pools for the minted token to be liquid and for it to have any utility in the destination chain. The advantage for native bridge providers, such as Optimism or Polygon PoS, is that the minted tokens are officially recognised by the chains themselves leading to wider adoption. Many tokens minted via any to any bridges have functionally no liquidity.

b) Firewall Risk: Typically, lock and mint mechanisms have a "firewall" or unidirectional risk. If tokens on origin chain A are stolen, or tokens on chain B are minted without any deposited tokens, the value of the synthetic token on destination chain B suffers from price drawdown but the tokens on chain A do not.

For any to any bridges, this risk can compound with every new representative token minted. Furthermore, in a network of any to any bridges, a unique Smart Contract implementation occurs for each chain pair $< C_1, C_2 >$. The number of synthetics created is also unlimited, as there are no restrictions for users to bridge and wrap any token.

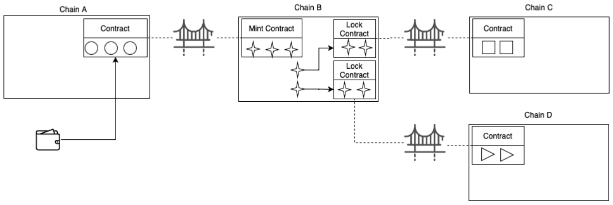

Fig. 12. Compounding risk on a series of any to any bridges

Figure 12. exemplifies how minted tokens backed by original tokens on chain A, is locked in further bridge contracts to create further representative tokens on chain C and D. The minted representative tokens on chain C is carries the risk of a multiple of bridges. This nature of this risk is hierarchical as the bridges earlier on the chain of bridging, can devalue all the tokens utilising the minted token downstream.

The majority of wrapped tokens in circulation, suffer from custodial risk due to their centralised structure. Concerns have been raised in the community, such as the Huobi bridge, with regards to the claims of a 1-to-1 lockup. Centralised bridge providers can in theory, remove all locked up tokens from the system.

1) Lock and Mint Contagion:

a) Multi-bridge Hierarchical Contagion: Similar to the weakest link contagion, hierarchical contagion refers to the tendency of established, benchmark tokens such as BTC and ETH being bridged into increasingly alt ecosystems. For example, Wrapped Bitcoin (WBTC) is bridged onto Ethereum, which is subsequently bridged to L2's and onto other L1's such as Solana and Avalanche.

As WBTC is a trusted bridge, with permissioned institutions holding the keys to authorise transactions, in theory, the BTC held may be removed by the custodians, leaving the Wrapped BTC unbacked.

b) WBTC Case Study: Wrapped Bitcoin (WBTC), is a bridge designed to enable the use of and exposure to Bitcoin on Ethereum. Considering two hypothetical scenarios, the contagious effects of a bridge breakdown can be understood.

Scenario 1) WBTC Bridge reservoir on the Bitcoin network is compromised, with $n\%$ of the supplied or bridged Bitcoin S, missing from the custodian.

Scenario 2) WBTC Bridge hacked by attacker to mint hypothetically infinite amount of WBTC m on Ethereum token issuer until a user notices the deposited Bitcoin does not match the issued WBTC after some time.

If the attacker chooses to rebridge the WBTC to BTC the maximum value which can be stolen is the BTC reservoir supply S in the Bitcoin network in Scenario 1. If the entire reservoir S is taken, the entire supply of WBTC on Ethereum would be valued at 0. Since WBTC on Ethereum is also "re-bridged" via alternative bridges to other chains, the derived synthetics backed by Ethereum WBTC would also be valued at 0, as the original backing supply no longer exists. However, the total damage would equal to S, as the backing is 1 to 1 so the total amount of derived synthetics should sum to S. From a bridge perspective, the damage is $2S$, as the original supply is gone, and the WBTC is valued at 0. The surrounding pools would likely be drained as users mass exit WBTC to other assets such as unrelated stablecoins. The price of WBTC bridged by the same provider on other chains with 100% backing would likely be impacted if WBTC bridge is severely affected.

If excess WBTC is minted by an attack, the attacker will seek to turn the minted WBTC into unaffected, reliable assets. One method would be to bridge back the WBTC which would be considered legitimate by the bridge, unlocking BTC to the attacker's wallet. Depending on the speed of the bridge, this may be unfavourable or the attacker, especially if the bridge protocol is centralised, and the bridge is able to stop the transaction.

To add to this, the lack of consistency checks on balances means there is a lack of awareness of hacks in real time, until some time passes. This has been the case for certain hacks, raising the issue of lack of balance checks for these bridges.

c) Undercollateralised Loans: According to Aave [59], there are 965.50 WBTC.e of value of $32.68M [1] supplied into the protocol. WBTC.e is a derivation of WBTC which is a backed by BTC. The loan health are calculated using a BTC/USD price feed. Should WBTC become undercollateralised by Scenario 1 or 2 given above, the loans would still be considered healthy. In effect, loans could be severely undercollateralised without liquidation.

These re-bridged tokens carry the counterparty risk of the original wrapped Bitcoin bridge in addition to the other bridges (eg. the Avalanche bridge). A failure of either bridge would could an issue to WBTC.e, but the impact of the failure of the wrapped Bitcoin bridge would cause greater damage.

2) Mitigating Lock and Mint Contagion: In order to reduce the hierchical spread of token price risk, tokens should be bridged as minimally as possible without re-wrapping. Furthermore, one can reduce fragmentation and risk by disallowing any-to-any third party bridging where arbitrary variations can be created by any user to any chain.

Established literature in traditional finance suggests the best design for minimizing the impact of bankruptcies between a network of banks is to design the network as loosely connected inter-cluster connections and closely connected intra-cluster connections. Similarly, Lock and Mint contagion can be mitigated by designing trust minimized intra-cluster communication, such as L1 to rollup, and trusted inter L1 communication also suggested by [5], [44].

[1] At time of writing in October 2023

D. Burn and Mint

The features of the Burn and Mint token mechanism can be described as follows:

- Potential for token price risk spread across all chains (leading to Weakest Link Contagion)
- Risk of bridge failure held by all users of the token
- No large amounts of custodied funds
- Closer to true “fungibility” of the token
- Addresses liquidity fragmentation

The Mint and Burn system has advantages and disadvantages. There are no “honeypot” creation of funds locked on the contracts, which pose as attractive target for hackers. The Mint and Burn system allows for an effectively fungible token interchange between chains. From a risk perspective however, the Burn and Mint system allows for price devaluations in both directions. An issue with unauthorised minting of tokens would have a direct price effect on the other chains. Even if centralised bridge providers were able to isolate the corrupt token on a specific chain, an attacker could swap the corrupt tokens for other unrelated tokens on that chain in order to preserve value. Furthermore, the Mint and Burn system does not put locked funds at risk, thus the attack vector is reduced to preventing unauthorised minting of tokens.

1) Burn and Mint Contagion:

a) Weakest Link Contagion: In the case of multiple interdependent chains, “51% attacking even one chain would create a systemic contagion that threatens the economy on that entire ecosystem” [44]. Given a set of connected chains C, with fungible token supply T across chains $C = \{C_1, C_2, ...C_n\}$, the security of the token is the security of the weakest chain C_w. Since every chain has a different security model, and has different bridge implementations, the weakest link in the network can act as a point of initial failure, followed by the spread of price risk across multiple chains. For example, DAI, a stablecoin, if fungible and to be utilised by multiple L2 chains as well as Ethereum L1, the stability of DAI could be impacted if one of the L2 rollups are insecure, which will have a contagious effect on the multiple chains which utilise DAI. This is exemplified by Diagram 13.

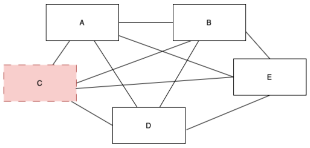

Fig. 13. Weakest Link Contagion in a network of connected chains

For example in Diagram 13, suppose chain C is the chain with the weakest security guarantees, and a fungible cross chain token exists on chains A to E. Should the token be “burned” on chain C, and minted to chain A, however, the burning of the tokens is reversed (not accepted as the longest chain), then the user has both the tokens on chain A and chain C effectively creating new tokens to the token supply and allowing the user to double spend. This could be the case for fungible DAI, if maliciously minted on an L2 rollup (chain C), and bridged back to Ethereum (chain A). The security of such token would fall to the level of security of the weakest chain.

Given the issues with honeypot hacks of lock and mint style tokens, there is an increasing push for standardised fungible burn and mint tokens across EVM based chains, such as new token standard with the burn and mint interface, ERC-7281 [58]. It is crucial to understand how risk spread will occur with the construction of networks of chains.

2) Mitigation of Weakest Link Contagion:

Interchain consensus protocols, which creates consensus on top of multiple chains, can be used to increase the security of crosschain network. Protocols such as Truboost, assume the existence of weaker security chains or maliciously attacked chains in the network [6], enabling boosted security.

Removing Weak Links Another method to mitigate weakest link contagion, is to only allow chains with a proven level of security into the network, effectively removing the “weakest link” in the network. However, the identification of weakest link chains is likely difficult in practice, as security of a chain takes time and users to prove robustness, especially with smaller, newer chains. Thus, the assumption of weaker chains in the network should be the standard to development of future protocols and mitigation methods.

Centralised Blacklisting An easily implementable approach is for coin issuers to monitor their tokens across all the chains issued, and in the event of an attack, freeze the assets created or stolen by the attacker via blacklisting function or something alike (in the case of USDT). This assumes the hacks will be monitored in real-time and alerted to project teams in due time, which has also been proven to be an issue in past hacks. In addition, despite being one of the most practical solutions, this approach also raises ethical concerns as a seizure of funds by a centralised decision effectively makes the protocol trusted rather than trustless.

E. Liquidity Networks

Liquidity networks enable fast crosschain liquidity transfer via swaps of native tokens existing on the source and destination chains.

LNs use Continous Liquidity Pools of assets which create an incentive for hacks. Risk in LNs is primarily taken on by the Liquidity Provider. The Liquidity Provider acts as the insurer receiving payment for covering for two risk types whilst the transaction is in progress; transaction reversal and the risk of cross-chain messaging infrastructure failure [18]. The cross-chain messaging infrastructure can also involve true bridges thus risk is true bridge failure also exists.

The features of the LN can thus be summarised as follows:

1) Native token swap
    a) No risk held by users once swap is complete.
2) LP risk
    a) Risks taken on by Liquidity Providers (bonders or insurers) who front liquidity for user for a fee.

b) Larger the tx, larger the risk. Hence, larger the insurance fee.
c) LPs risk transaction reversal and cross-chain messaging infrastructure failure during the transaction and resttlement.
d) Exposure to price fluctuation before refund to LP completed.

3) AMM risks
   a) Liquidity Risk. Liquidity must be available for bridge to be operational. This also includes the need for liquidity bootstrapping for startup.
   b) Slippage depending on design of LN.

1) Continuous Liquidity Pool Risks: Similar to the Lock and Mint mechanism, Liquidity Networks attract attacks as they custody large amounts of funds in pools. Since Liquidity Networks use Automated Market Makers (AMMs) on origin and destination chain, Liquidity Networks are exposed to AMM risks. AMM risks can stem from protocol design and economic incentives, smart contract vulnerabilities or a combination. An example of this is price manipulation attacks leveraged by flash loans [1], [2].

Transaction reversal and risk of crosschain bridging infrastructure failure put the Liquidity Provider or Router at risk of bankruptcy while the transaction is in progress and the resettlement process has not fully completed. In such a case, all tokens previously swapped are unaffected. It will also likely lead to the halting of the bridging protocol, as in the case for the THORChain hack [15], [16], [23]. The pools of liquidity pose as a honey pot for hacks. The risk taken on by LPs still significant impact on further market depending on TVL in protocol. While robust bounty incentives, security auditing, and smart contract verification is a necessity to ensure funds are not hacked [23], liquidity pools continue to be an attractive target for hackers.

2) Liquidity Network Contagion Profile:

a) Bankruptcy of LPs: With large amounts of funds locked in LN protocols such as $331.04 million USD locked in Stargate, pools can be drained in the case of a hack.

b) Intermediary Token Risk Spread: If an intermediary bridge protocol token is used, as in the case of the Thorchain hack with RUNE, the intermediary token can suffer from price impact in response to a hacked bridge [23] or as a direct result of an attack. The price impact of an intermediary token spreads protocol wide, with all the swap pair pools affected.

3) Mitigating LN Risks: Since LN are application level protocols consisting of many parts, the most important way to mitigate LN risks is securing crosschain LN infrastructure and any bridges inside of it. As the Thorchain hacker has warned, robust bounty incentives, security auditing, and smart contract verification is essential when securing large amounts of custodied funds.

In addition, since multiple actors such as Liquidity Providers, arbitrageurs and bridge operators are involved, ensuring the cryptoeconomic incentives are aligned is another important aspect in securing the LN protocol.

Alternative approaches. such as liquidity on demand type LNs such as deSwap LN [17] remove the need to pool assets to provide on demand liquidity. Removing pools of assets reduces the incentive for hacks to occur. If these P2P trading LNs can meet liquidity as effectively as classical liquidity pool LNs, this may be a safer approach in mitigating potential damage.

F. Case Studies of Contagion

a) QANX Bridge: QANX, is a native token to the blockchain QAN Platform, a quantum resistant blockchain. The QANX token is also available on Ethereum and Binance Smart Chain (BSC). The QANX bridge, no longer in operation after the October 2022 hack, allowed users to swap their QANX from BSC to Ethereum and vice versa.

In October 2022, 3 withdrawal transactions occurred from the QANX Bridge contracts. First, over 1.44 billion QANX tokens were withdrawn from the QANX Bridge's BSC smart contract. Additionally on Ethereum QANX Bridge, two further transactions of 1.43 billion and 23 million QANX tokens occurred.

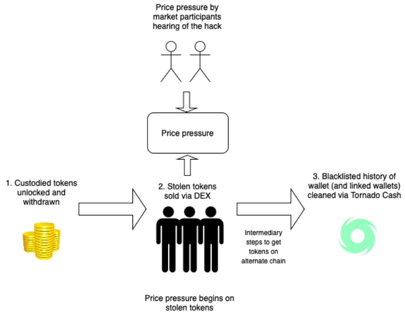

Fig. 14. Typical blueprint for stolen funds.

Following the withdrawals, the attacker swapped the stolen QANX on BSC for WBNB via PancakeSwap through a series of swaps. The total initially stolen QANX (approximately 3 billion) was worth $2 million USD.

This led to a 99% reduction in token price. This was a natural response, given the advertised max supply of the token was 3.33 billion, thus the stolen funds represented around 93% of the total supply of the token.

The QAN Platform team resolved the situation by taking a snapshot of the token distribution, creating new QANX tokens on both BSC and Ethereum, and redistributing the new tokens to anyone who made a claim. The new QANX token price, trading around $0.02 per token, has recovered to the QANX token prices before the October 2022 hack but significantly below the peak trading prices, of around 18 cents in November 2021.

In addition to the October 2022 hack, in May 2022, a less publicised exploitation of the bridge occured, where attacker was able to deposit 1 QANX on BSC for arbitrarily greater amount of QANX on Ethereum. A series of deposits of 1 QANX on the BSC smart contract occured, followed by millions of QANX tokens withdrawn from the Ethereum QANX Bridge. The QANX team published a video of a plan to mitigate the effects; to contact relevant exchanges to blacklist the involved address to stop transactions from occurring. Price of QANX "tanked" on many DEXes. However, this was ineffective, and the hacker was able to swap their QANX for ETH, and funnelled the ETH through Tornado Cash.

G. Isolating Contagion

With the exception of contagion mitigation methods addressed in the previous sections, methods of isolating contagion based on historical hacks and system failures are outlined in the following.

a) Centralised Chains & Tokens: In the case of infinitely minted tokens or stablecoins on a chain, the question remains whether damage done can be isolated. For many existing bridges, transactions can be censored. In theory, it should be possible to censor minted tokens to be bridged out of a chain. There must be regular and perhaps incentivised *state consistency checks* across all chains the token is used on, to be able to detect hacked, minted tokens which has previously been an issue with existing bridges. However, being able to censor a transaction to prevent hacks means transactions can also be censored for political or other motivations which is a serious downside. Chains which are sufficiently centralised such as Binance Smart Chain (BSC), were able to stop transactions from occuring initiated by the hacker by validators stopping processing the transactions [53]. Tether, with blacklisting feature available, can effectively render any USDT useless by setting it as blacklisted.

Price Damage Centralised chains and tokens have advantages to be able to have some level of control when hacks occur and if the public has faith that the lost funds on the bridge will be restored, there are minimal serious long term effects on the health of the related tokens and chains (as in the case for Binance Smart Chain's bridge hack). This also depends on the proportion of the size of the hack versus the size of reserves. If a bridge or token's organisation clearly has more than enough funds to cover for the losses of the hack, the impact is, again, minimal.

If the minted tokens can be isolated to that chain (all outbridges for that token is blocked), the hacker will prioritise transferring the assets out to a more reliable, established chains such as Ethereum, where liquidity and privacy services such as Tornado Cash are easily available. If the bridges are out of use, the hacker will seek to exchange the token via DEX to an unaffected token, to transfer them out of chain and to safety.

Even if bridging is an available option, the hacker risks their own tokens being devalued if they choose to bridge first, and swap the assets. Thus, this will only likely occur if there is not enough liquidity available on the chain for the tokens to be exchanged.

DAOs could also coordinate to choose to censor hacked funds. However, this would require near instantaneous descision making and response, likely leading to only a small subset of participants voting to censor the hacked funds.

b) Community based Blacklisting: A bottom up approach of manually alerting other protocols and exchanges of the hacker's address, some protocols are able to blacklist the wallet or the tokens which have been stolen. An example of this includes Tether's blacklisting of stolen USDT in the Binance Smart Chain bridge hack. Blacklisting is a manual process controlled by the protocol or exchanges and must take place in real time (almost immediately) for them to be effective.

The ability to blacklist is an incredibly useful given the frequency of hacks which happen. They give an opportunity to curb the damage done by stolen funds. However, the ability to censor for good also comes with the ability to censor for personal or political gain. The inability to move one's tokens means that tokens are effectively seizable.

H. Secondary Impacts

a) Undercollateralised Loans: Loans with oracles tracking the price of the original asset instead of the wrapped version will suffer from undercollateralization without liquidation. The loans would still be considered as safe, even if the the wrapped token has been devalued. Examples include the WBTC.e lending pool on Aave, a derivation of Wrapped Bitcoin, with 965.50 WBTC.e worth $32.68M USD [2]. Since the pool tracks the value of BTC/USD, should a failure occur to WBTC bridge or the Avalanche bridge from Ethereum to Avalanche, the loans would be undercollaterlised without triggering liquidations.

As mentioned in Section III-B1., the pricing of wrapped, crosschain tokens should be different to pricing of the original token. However, wrapped token pricing are treated often as the original token's price even if the token has been bridged with multiple bridges compounding the risk of bridge failure.

b) Undercollaterlised Stablecoins: For crosschain burn and mint stablecoins, once news spread that the stablecoin has been arbitrarily minted on a chain, the pricing on exchanges will begin to reflect to the sudden inflation of stablecoins which has happened. Regardless of whether the stablecoin is generated endogenously or exogenously, the price of the stablecoin would likely reflect the changes, leading to an underbacked stablecoin.

V. Discussions for Future Design

As suggested by [5], [44], crosschain interoperability should be thought of "based on the idea of clusters of chains" with tight, trust minimized intracluster communication and trusted intercluster communication. This is in line with established literature in traditional finance suggests the best design for minimizing the impact of bankruptcies between a network of banks, is to design the network in the following manner; loosely connected intercluster connections, closely connected intracluster connections. This will likely result in "zones of interdependency are likely to align closely to zones of sovereignty" with "lots of Ethereum-universe applications interfacing closely with each other, lots of Avax-universe applications interfacing with each other but NOT Ethereum-universe and Avax-universe applications interfacing closely

[2] At time of writing in October 2023 taken from app.aave.com [4]

with each other)" [44]. For example, Lock and Mint can be used for Ethereum to rollups, native swaps via LNs for cross L1s and the use synths if value exposure to original assets is desired. Furthermore, bridging out of Ethereum and L2s, could be done via an L2 to minimize heavy gas fees on L1. All L2s interconnected to Ethereum cluster should near preserve security guarantees of the L1 when tokens are bridged. Users should only hold and use 1st order wrapped variants if possible (or in best case scenario native tokens).

Proposal of an extension to the ERC20 standard, called xERC20 [74], [76], aims to address the liquidity and token fragmentation. This is done through a Burn and Mint token mechanism with the token issuer able to whitelist bridges and place minting limits on bridges based on the security level. This allow tokens minted by different bridges to be fungibly exchanged including native bridges, bringing the token closer to true fungibility. A token would still have a "home" chain but then be able to be bridged across multiple chains in a fungible manner. Similarly, Omnichain Fungible Token (OFT) created by LayerZero and Anytoken on Multichain seek to address the same issue.

Another key aspect is the design of crosschain stablecoins. Stablecoins are the cornerstone of DeFi applications and play a crucial role by providing a token which holds consistent value. Stablecoin issuers are in a uniquely advantageous position to provide bridging and LN solutions to address the issues of fragmentation, security and usability.

The greatest advantages which stablecoin issuer based LNs and bridges can offer is the ability to unify liquidity and standardise the stablecoin across multiple heterogenous chains. This is not possible for third party bridges and LNs, unless they are using a token issuer based bridge as a part of their protocol. In addition, the Burn and Mint mechanism allows for no liquidity to be locked up which has proven to act as a significant incentive for hackers in Lock and Mint style bridges.

A robust crosschain stablecoin is crucial as large parts of the ecosystem depend on stablecoins as a crux of their day to day operations. The potential impact of a devaluation of a crosschain Burn and Mint style stablecoin is significant - as all stablecoins on all chains will be affected - serving as a point of systemic risk.

References

[1] "Flash Loan Attack Causes DeFi Token Bunny to Crash Over 95%." *CoinDesk*, https://www.coindesk.com/markets/2021/05/20/flash-loan-attack-causes-defi-token-bunny-to-crash-over-95/#:~:text=Register%20Now.%20Yield,borrow%20a%20huge%20supply.

[2] "DeFi Hack Analysis: Project PancakeBunny Attacked Via Major $200 Million Flash Loan Vulnerability." *Crowdfund Insider*, https://www.crowdfundinsider.com/2021/05/175611-defi-hack-analysis-project-pancakebunny-attacked-via-major-200-million-flash-loan-vulnerability/#:~:text=,with%20around%201%2C000.

[3] "RhinoLearn: How Do Blockchain Bridges Really Work and Can You Trust Them?" *Rhino.fi Blog*, https://rhino.fi/blog/rhinolearn-how-do-blockchain-bridges-really-work-and-can-you-trust-them/.

[4] Aave. "Open Source Liquidity Protocol." *AAVE*, https://app.aave.com/reserve-overview/?underlyingAsset=0x50b7545627a5162f82a992c33b87adc75187b218&marketName=proto_avalanche_v3.

[5] Al-Bassam, Mustafa. "Clusters: How Trusted & Trust-Minimized Bridges Shape the Multi-Chain Landscape." *Celestia Blog*, Oct. 2022, https://blog.celestia.org/clusters/.

[6] Wang, Xuechao, et al. "Trustboost: Boosting Trust Among Interoperable Blockchains." *arXiv preprint arXiv:2210.11571*, 2022.

[7] Karakostas, Dimitris, and Aggelos Kiayias. "Securing Proof-of-Work Ledgers via Checkpointing." *2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. IEEE, 2021.

[8] Tas, Ertem Nusret, et al. "Interchain Timestamping for Mesh Security." *arXiv preprint arXiv:2305.07830*, 2023.

[9] "Polygon's Block Reorg Problem: Daily 10 Depth Reorgs." *Reddit*, r/0xPolygon, https://www.reddit.com/r/0xPolygon/comments/10bvruq/polygons_block_reorg_problem_daily_10_depth_reorgs/.

[10] "Bridges: Designs, Trade-offs, and Opportunities." *Medium*, Amber Group, https://medium.com/amber-group/bridges-designs-trade-offs-and-opportunities-2196b8754e70.

[11] "Hack Analysis: Beanstalk Governance Attack, April 2022." *Medium*, Immunefi, https://medium.com/immunefi/hack-analysis-beanstalk-governance-attack-april-2022-f42788fc821e.

[12] "[ARC] Aave V3 Fantom - Freeze Reserves." *Aave*, https://snapshot.org/#/aave.eth/proposal/0xeefcd76e523391a14cfd0a79b531ea0a3faf0eb4a058e255fac13a2d224cc647.

[13] "Cross-Chain Swaps & Liquidity." *DeBridge Finance Documentation*, https://docs.debridge.finance/cross-chain-trading/cross-chain-swaps-liquidity.

[14] Teutsch, Jason, Michael Straka, and Dan Boneh. "Retrofitting a Two-Way Peg between Blockchains." *arXiv preprint arXiv:1908.03999*, 2019.

[15] "Thorchain Rekt." *Rekt News*, https://rekt.news/thorchain-rekt/.

[16] "Thorchain Rekt2." *Rekt News*, https://rekt.news/thorchain-rekt2/.

[17] "Introduction - The Core Protocol." *DLN Trade Documentation*, https://docs.dln.trade/the-core-protocol/introduction.

[18] "Risk Distribution - DLN Overview." *DLN Trade Documentation*, https://docs.dln.trade/the-core-protocol/dln-overview#risk-distribution.

[19] "Architecture - Liquidity Model." *Squid Router Documentation*, https://docs.squidrouter.com/architecture/liquidity-model.

[20] "Providing Liquidity on Connext." *Medium*, Connext, https://medium.com/connext/providing-liquidity-on-connext-f7aa3f2bc7b8.

[21] "FAQ." *cBridge Documentation*, Celer Network, https://cbridge-docs.celer.network/reference/faq.

[22] "Understanding THORChain." *THORChain Documentation*, https://docs.thorchain.org/understanding-thorchain.

[23] "Thorchain Trolled by Hacker After Two Successful Seven-Figure Exploits." *Bitcoin.com*, https://news.bitcoin.com/thorchain-trolled-by-hacker-after-two-successful-seven-figure-exploits/.

[24] "For L1 - L2 Transactions." *Optimism Community Documentation*, https://community.optimism.io/docs/developers/bridge/messaging/#for-l1--l2-transactions.

[25] "How Long Does It Take Before I Receive My Funds When I Initiate Withdrawal from Arbitrum Chains One and Nova." *Arbitrum Documentation*, https://docs.arbitrum.io/for-users/troubleshooting-users#how-long-does-it-take-before-i-receive-my-funds-when-i-initiate-withdrawal-from-arbitrum-chains-one-and-nova.

[26] "Hop Protocol Whitepaper." *Hop Exchange*, https://hop.exchange/whitepaper.pdf.

[27] "A Short Explainer." *Hop Exchange Documentation*, https://docs.hop.exchange/basics/a-short-explainer.

[28] Martin, Kupka. "Analýza blockchainových bridge sítí v prostředí decentralizovaných financí." Master's thesis, České vysoké učení technické v Praze. Vypočetní a informační centrum, 2022.

[29] Xu, Jiahua, et al. "SoK: Decentralized Exchanges (DEX) with Automated Market Maker (AMM) Protocols." *ACM Computing Surveys*, vol. 55, no. 11, 2023, pp. 1-50.

[30] Freeman, Jay. "Attacking an Ethereum L2 with Unbridled Optimism." *Attacking an Ethereum L2 with Unbridled Optimism*, https://www.saurik.com/optimism.html.

[31] Li, Wenkai, et al. "A Survey of DeFi Security: Challenges and Opportunities." *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 10, 2022, pp. 10378-10404.

[32] Buterin, Vitalik. "How Does L2 Learn the Recent Ethereum State Root." *Vitalik's Website*, 20 June 2023, https://vitalik.ca/general/2023/06/20/deeperdive.html#how-does-l2-learn-the-recent-ethereum-state-root.

[33] Buterin, Vitalik. "Chain Interoperability." *R3 Research Paper*, vol. 9, 2016, pp. 1-25.

[34] "About." *Crypto51*, https://www.crypto51.app/about.html.

[35] "Crypto51." https://www.crypto51.app.

[36] Stone, Drew. "Trustless, Privacy-Preserving Blockchain Bridges." *CoRR*, vol. abs/2102.04660, 2021, https://arxiv.org/abs/2102.04660.

[37] Lee, Sung-Shine, et al. "SoK: Not Quite Water Under the Bridge: Review of Cross-Chain Bridge Hacks." *2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. IEEE, 2023.

[38] Zhao, Qianrui, et al. "A Comprehensive Overview of Security Vulnerability Penetration Methods in Blockchain Cross-Chain Bridges." 2023.

[39] "Why Li.Fi." *Li.Fi Documentation*, https://docs.li.fi/overview/why-li.fi.

[40] "Socket Liquidity Layer Overview." *Socket Tech Documentation*, https://docs.socket.tech/socket-liquidity-layer/socketll-overview.

[41] Muhammad, Ajmal, and Jesper Kristensen. "On Cross-chain Pathfinding and Bridge Selection for Decentralized Finance." 2023.

[42] "Understanding BUSD and Binance-Peg BUSD." *Binance Blog*, https://www.binance.com/en/blog/ecosystem/understanding-busd-and-binancepeg-busd-5526464425033159282.

[43] "BUSD." *Paxos*, https://paxos.com/busd/.

[44] Buterin, Vitalik. "[AMA] We Are the EF's Research Team (Pt. 7: 07 January, 2022)." *Reddit*, https://old.reddit.com/r/ethereum/comments/rwojtk/ama_we_are_the_efs_research_team_pt_7_07_january/hrngyk8/.

[45] Vilá Brualla, Marta. "Blockchain Layer 2 Scalability Solutions: A Framework for Comparison." MS thesis. Universitat Politècnica de Catalunya, 2023.

[46] "Evaluating Ethereum L2 Scaling Solutions: A Comparison Framework." *Matter Labs Blog*, https://blog.matter-labs.io/evaluating-ethereum-l2-scaling-solutions-a-comparison-framework-b6b2f410f955.

[47] Zheng, Jincheng, David Kuo Chuen Lee, and Dejun Qian. "An In-depth Guide to Cross-Chain Protocols under Multi-Chain World." 2023.

[48] "Transfer." *Portal Bridge*, https://www.portalbridge.com/#/transfer.

[49] "Wormhole Token List." *GitHub*, Wormhole Foundation, https://raw.githubusercontent.com/wormhole-foundation/wormhole-token-list/main/content/by_dest.csv.

[50] "Wormhole SDK" *npm*, https://www.npmjs.com/package/@certusone/wormhole-sdk.

[51] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[52] M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[53] Browne, Ryan. "$570 Million Worth of Binance's BNB Token Stolen in Another Major Crypto Hack." CNBC, CNBC, 7 Oct. 2022, www.cnbc.com/2022/10/07/more-than-100-million-worth-of-binances-bnb-token-stolen-in-another-major-crypto-hack.html.

[54] Aave, Open source liquidity protocol, https://app.aave.com/reserve-overview/?underlyingAsset=0x50b7545627a5162f82a992c33b87adc75187b218\&amp;marketName=proto_avalanche_v3

[55] McCorry, Patrick, et al. "Sok: Validating bridges as a scaling solution for blockchains." Cryptology ePrint Archive (2021).

[56] Circle, Cross-chain transfer protocol. [Online]. Available: https://developers.circle.com/stablecoin/docs.

[57] The DeFi Saint. "A Deep Dive to Bridges and Bridge Aggregators." *Medium*, https://medium.com/@TheDeFISaint/a-deep-dive-to-bridges-and-bridge-aggregators-861fc6863f8f.

[58] A. Bhuptani, Erc-7281: Sovereign bridged tokens, Jul. 2023. [Online]. Available: https://ethereum-magicians.org/t/erc-7281-sovereign-bridged-tokens/14979

[59] Aave, Open source liquidity protocol. [Online]. Available: https://app.aave.com/reserve-overview/?underlyingAsset=0x50b7545627a5162f82a992c33b87adc75187b218\&marketName=proto_avalanche_v3

[60] Across, How Across Works - Overview. Available: https://docs.across.to/how-across-works/overview

[61] Hop.exchange, What is special about Hop?, Available: https://docs.hop.exchange/basics/what-is-special-about-hop

[62] Kiepuszewski, Bartek and Chellani, Vaibhav, L2Bridge risk framework, L2BEAT, Jul. 2022 [Online]. Available: https://gov.l2beat.com/t/l2bridge-risk-framework/31

[63] Al-Bassam, Mustafa. "Clusters: How Trusted & Trust-Minimized Bridges Shape the Multi-Chain Landscape." *Celestia Blog*, Oct. 2022, https://blog.celestia.org/clusters/.

[64] McCorry, Patrick, Chris Buckland, Bennet Yee, and Dawn Song. "Sok: Validating Bridges as a Scaling Solution for Blockchains." *Cryptology ePrint Archive*, 2021.

[65] "Gnosis Chain." *Gnosis Chain*, https://www.gnosis.io/.

[66] "Chainlink Cross-Chain Interoperability Protocol (CCIP)." *Chainlink White Paper*, 2023, https://chain.link/CCIP.

[67] "Inter-Blockchain Communication Protocol (IBC)." *Cosmos Network Documentation*, 2023, https://docs.cosmos.network/master/ibc/.

[68] "Polkadot: Vision for a Heterogeneous Multi-Chain Framework." *Polkadot White Paper*, 2023, https://polkadot.network/Polkadot-whitepaper.pdf.

[69] Zarick, Ryan, Bryan Pellegrino, and Caleb Banister. "Layerzero: Trustless omnichain interoperability protocol." arXiv preprint arXiv:2110.13871 (2021).

[70] Zarick, Ryan, Bryan Pellegrino, and Caleb Banister. "Delta: Solving The Bridging Trilemma." 2023. Dropbox, https://www.dropbox.com/s/gf3606jedromp61/Delta-Solving.The.Bridging-Trilemma.pdf?dl=0.

[71] "QANPlatform Announces QANX Bridge Launch." *Medium*, QANPlatform, 2 Dec. 2021, https://medium.com/qanplatform/qanplatform-announces-qanx-bridge-launch-270dd15b4daa.

[72] "Cross-Chain Transfer Protocol." *Circle*, https://www.circle.com/en/cross-chain-transfer-protocol.

[73] "Cross-Chain Token Transfers." *Chainlink Blog*, https://blog.chain.link/cross-chain-token-transfers/.

[74] "Bridging the Gap: Better Token Standards for Cross-Chain Functionality." *DZone*, https://dzone.com/articles/bridging-the-gap-better-token-standards-for-cross.

[75] "Cross-Chain Bridge Hacks: A 2022 Review." *Chainalysis Blog*, https://www.chainalysis.com/blog/cross-chain-bridge-hacks-2022/.

[76] Bhuptani, Arjun. "ERC-7281: Sovereign Bridged Tokens." *Fellowship of Ethereum Magicians*, Jul. 2023, https://ethereum-magicians.org/t/erc-7281-sovereign-bridged-tokens/14979.

[77] "Bridged USDC Standard." *Circle Blog*, https://www.circle.com/blog/bridged-usdc-standard.

[78] "USDC Bridge." *Portal Bridge*, https://www.portalbridge.com/usdc-bridge/.