Rollups are the most secure bridges

Bartek Kiepuszewski

L2Beat, MakerDAO

A Multichain Strategy and Roadmap for Maker

Governance ■ layer-2 ■ protocol-engineering ■ strategy

The aim of this forum post is to present a bird's eye view of the Layer 2 ecosystem and the various opportunities that exist. By presenting our interpretation of the multichain landscape we hope to be able to (1) Guide and engage with the broader community on this specific topic, (2) Gather feedback regarding the various opportunities, and (3) Align technical and development resources to agree on a strategy for how MakerDAO should embrace this new and complex landscape.

This approach will help to define our collective focus on the Layer2 priorities that exist - specifically, which ones offer the right balance of growth, exposure and security to protect the integrity of DAI as a stablecoin across multiple chains. We welcome community feedback and plan to host a series of AMA / discussions in the coming weeks as we solidify the strategy and roadmap for the coming months.

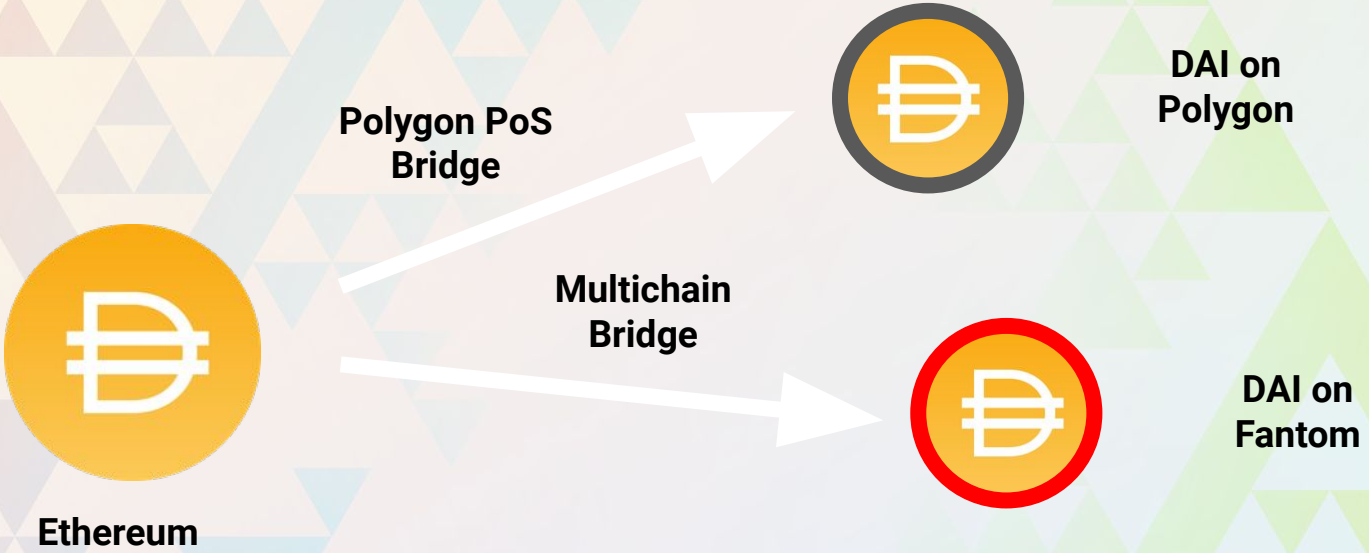
Today's Multichain Environment

We currently stand at the cross-roads of two questions:

"*How will DeFi grow?*" and "*Where will the liquidity go?*"

The rapid and evolving growth of DeFi makes these difficult questions to answer; Will it be one chain? One Layer2 implementation? Will liquidity concentrate in one or multiple places? It appears that at this nascent stage, concentration in any one particular place is unlikely due to the innovation and development happening in various ecosystems.

Ethereum is likely to become a global settlement layer (think of it as the Manhattan of crypto), in this context it is unreasonable to assume that everybody will fit into a single "city" where property prices skyrocket. Instead, people with growing DeFi needs will establish new, thriving communities by creating their own islands 31. Haseeb Qureshi also draws out this line of thinking in ETH2 Cities, Suburbs, Farms 69 where "blockchain urban planning" and sharding will be used to meet demand.



1. Is DAI on Polygon / Fantom “as secure” as DAI on Ethereum ?
2. Can you make all these DAI fungible ?
3. What is needed to be able to mint DAI on all these chains ?

#	NAME	TVL	BREAKDOWN	7D CHANGE	MARKET SHARE
1	Arbitrum One	$2.38B		+1.13%	50.72%
2	Optimism	$1.44B		+0.19%	30.74%
3	dYdX	$379M		-0.86%	8.08%
4	Loopring	$138M		-1.86%	2.95%
5	Metis Andromeda	$125M		+8.51%	2.67%
6	zkSync	$52.87M			
7	Immutable X	$41.08M			
8	ZKSpace	$38.36M			
9	Boba Network	$28.10M			
10	rhino.fi	$21.94M			
11	Sorare	$20.45M			
12	Aztec Connect	$7.31M			

L2BEAT

Total Value Locked

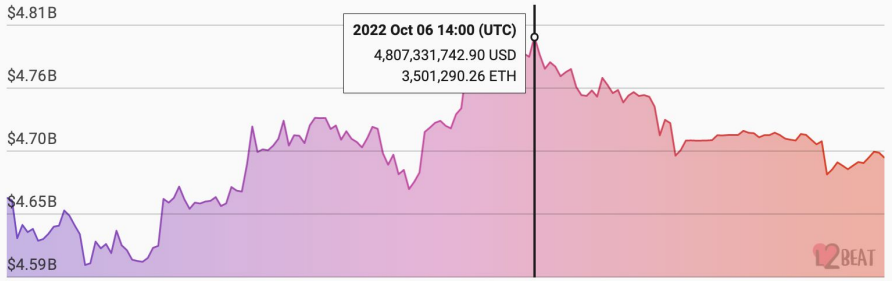
$4.70B

Sum of all funds locked on Ethereum converted to USD

+0.75% / 7 days

2022 Oct 02 – 09

7D 30D 90D 180D 1Y MAX



USD ETH*

Total Value Locked (USD equivalent)

LOG LIN

The state of Bridging 2022

2021 started to be bad for the bridges

CoinDesk

Bitcoin $19,300.70 -1.16% Ethereum

Markets

Cross-Chain DeFi … Hundreds of Millio…

DeFi platform Poly Network wa… hacker draining roughly $600 m…

By Eliza Gkritsi, Muyao Shen Aug…

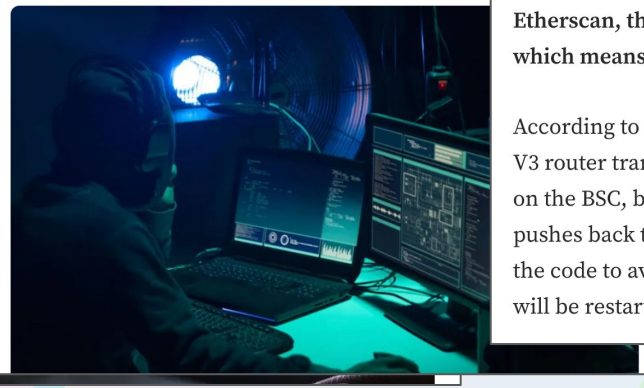
yahoo!finance Search for news, symbols or companies

COIN RIVET

ChainSwap hackers steal $8m…

Sam Cooling

July 12, 2021 · 3 min read



ChainCatcher

Jul 12, 2021 · 2 min read · Listen

After Chainswap, cross-chain bridge AnySwap was hacked and lost $7.87 million

Early morning today, cross chain bridge project Anyswap announced that the new V3 across chain liquidity pools was hacked in the morning yesterday, resulting a total loss of 5.5 million MIM and 2.39 million USDC. Hackers address is 0x0ae1554860e51844b61ae20823ef1268c3949f7c. **According to Etherscan, the hackers have sold all the MIMs and obtained 5.48 million DAI, which means that AnySwap's total loss is more than $7.87 million.**

According to AnySwp's announcement explaining the reason for the theft, two V3 router transactions have been detected under the V3 router MPC account on the BSC, both transactions have the same R-value signature, and the hacker pushes back to the private key of the MPC account. The team has now fixed the code to avoid using the same R signature and the multi-chain router V3 will be restarted in about 48 hours with no security risks for V1 and V2.

2022 is shaping up to be much worse

QANX Token Collapses 90% After $1 Million Bridge Hack

Author: Andrew Throuvalas • Last Updated Oct 11, 2022 @ 16:11

Nearly half of the token's entire supply was claimed by the hacker.

QANplatform – a quantum-resistant layer 1 blockchain – lost $1 million to a hacker who targeted the network's blockchain bridge.

Since the attack, its native QANX token has suffered a price collapse of over 90%.

The Latest Bridge Attack

At 05:01 EST on Tuesday, QANplatform tweeted that its smart contract bridge had been hacked and that the attacker had already withdrawn tokens. Etherscan data appears to reinforce this, displaying two bulk withdrawals from the bridge at 08:17 AM and 09:40 AM UTC.

With The $570
(BNB) Hack? And
ally Mean For
s?

nt Contributor
ansparent.

Follow

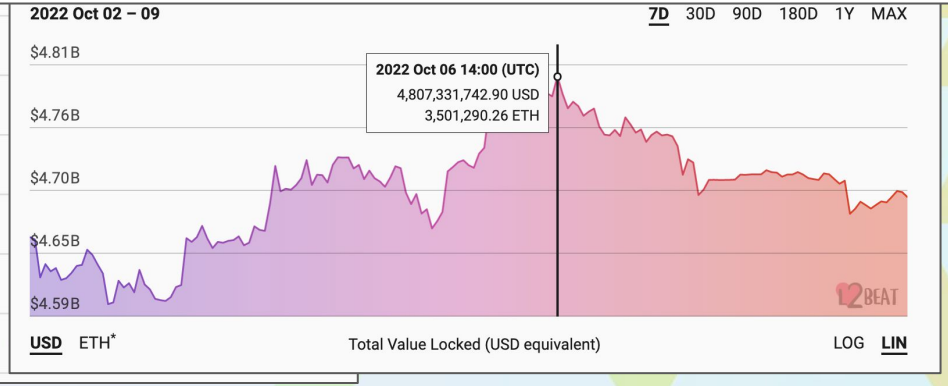
0

Photo: iStock

1 min read . Updated: 02 Aug 2022, 01:35 PM IST

At l2beat, we have been looking at L2s so far…

#	NAME	TVL	BREAKDOWN
1	Arbitrum One	$2.38B	
2	Optimism	$1.44B	
3	dYdX	$379M	
4	Loopring	$138M	
5	Metis Andromeda	$125M	
6	zkSync	$52.87M	
7	Immutable X	$41.08M	
8	ZKSpace	$38.36M	
9	Boba Network	$28.10M	
10	rhino.fi	$21.94M	
11	Sorare	$20.45M	
12	Aztec Connect	$7.31M	



Announcing 12beat for bridges

We track TVL (Locked in Bridges)

#	NAME	TVL	BREAKDOWN	7
1	Polygon PoS	$2.82B		
2	Multichain	$1.43B		
3	Rainbow Bridge	$1.31B		
4	Ronin V2	$840M		
5	Avalanche Bridge	$793M		
6	Polygon "Plasma"	$622M		
7	StarGate	$130M		
8	Wormhole V2	$115M		
9	xDai Omni	$101M		
10	Satellite Bridge	$94.99M		
11	Across V2	$35.91M		-5.50% 0.42%

Total Value Locked

$8.47B

Sum of all funds locked on Ethereum converted to USD

-0.76% / 7 days

L2BEAT Bridges is a work in progress. You might find incomplete research or inconsistent naming. Join our discord to suggest improvements!

2021 Oct 08 – 2022 Oct 07

7D 30D 90D 180D 1Y MAX

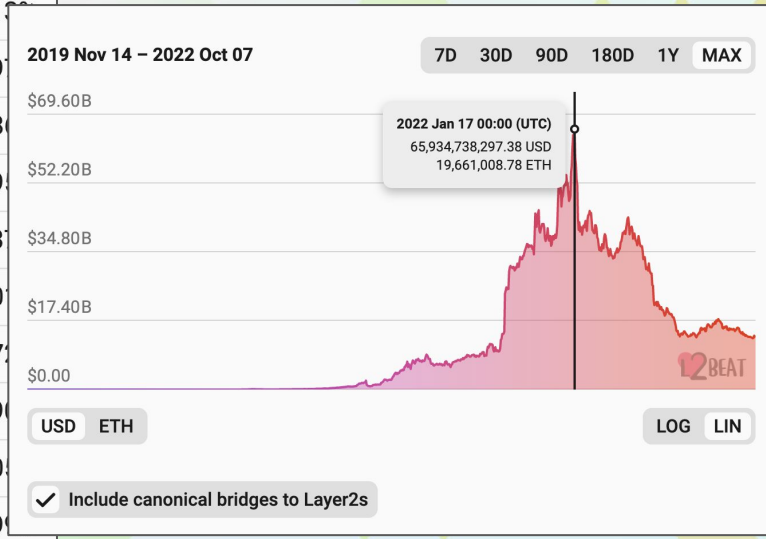
USD ETH

LOG LIN

Canonical bridges to L2s can be included

Include canonical bridges to Layer2s

#	NAME	TVL	BREAKDOWN	7D CHANGE	MARKET SHARE
1	Polygon PoS	$2.82B		+0.16%	21.45%
2	Arbitrum One	$2.39B		-0.52%	18.1
3	Optimism	$1.44B		-0.64%	10.9
4	Multichain	$1.43B		-1.46%	10.8
5	Rainbow Bridge	$1.31B		+1.41%	9.9
6	Ronin V2	$840M		-1.50%	6.3
7	Avalanche Bridge	$793M		-9.23%	6.0
8	Polygon "Plasma"	$622M		+6.44%	4.7
9	dYdX	$383M		-1.19%	2.9
10	Loopring	$138M		-3.15%	1.0
11	StarGate	$130M		-2.72%	0.9



L2beat is primarily about risk analysis

Risk Analysis

#	NAME	STATE VALIDATION	DATA AVAILABILITY	UPGRADEABILITY	SEQUENCER FAILURE	VALIDATOR FAILURE
1	Arbitrum One	Fraud proofs (INT)	On chain	Yes	Transact using L1	No mechanism
2	Optimism	In development	On chain	Yes	Transact using L1	No mechanism
3	dYdX		ain	Yes	Force trade/exit to L1	Escape hatch (MP)
4	Loopring		ain	Yes	Force exit to L1	Escape hatch (MP)
5	Metis Andromeda	In development	External (MEMO)	Yes	Transact using L1	No mechanism
6	zkSync	ZK proofs (SN)	On chain	21d or no delay	Force exit to L1	Escape hatch (ZK)
7	Immutable X	ZK proofs (ST)	External (DAC)	14 days delay	Force exit to L1	Escape hatch (MP)
8	ZKSpace	ZK proofs (SN)	On chain	8 days delay	Force exit to L1	Escape hatch (ZK)

Currently the system permits invalid state roots. More details in project overview.

We need a proper risk framework for Bridges

- Risks should be disclosed
- We should make users aware of the underlying security assumptions
- We should constantly monitor infrastructure for upgrades and changes to important security parameters
- We will make multichain infrastructure more transparent and secure while keeping teams developing bridges honest

Did you know that ...

- Multichain can take funds from Escrow without burning corresponding tokens on the destination chain ?
- Omni bridge permissioned accounts can put users' bridge funds into Aave/Compound ?
- Polygon Plasma bridge does not have much Plasma in it as the implementation (available on testnet) was never deployed on mainnet ?
- Most bridges **can be upgraded** by MSigs, tokens that they mint on the destination chain **can be upgraded**, and some have **unverified** smart contract code so it is impossible to tell what exactly they are doing ?

Multichain - what is going on here ?

456 days 4 hrs ago	Multichain: Fantom Bridge	IN	0x5e583b6a1686f7bc09…	60,209,029	AtariToken (ATRI)
456 days 4 hrs ago	Multichain: Fantom Bridge	IN	0x5e583b6a1686f7bc09…	2,639.2955122612217	Wrapped Ethe... (WETH)
456 days 4 hrs ago	Multichain: Fantom Bridge	IN	0x5e583b6a1686f7bc09…	3,373,189.7735298405	IceToken (ICE)
456 days 5 hrs ago	Multichain: Fantom Bridge	IN	0x5e583b6a1686f7bc09…	9,557,974.271217	Tether USD (USDT)
456 days 5 hrs ago	Multichain: Fantom Bridge	IN	0x5e583b6a1686f7bc09…	302.78335046	Wrapped BTC (WBTC)
456 days 5 hrs ago	Multichain: Fantom Bridge	IN	0x5e583b6a1686f7bc09…	52,187,197.28316887	Dai Stableco... (DAI)
456 days 5 hrs ago	Multichain: Fantom Bridge	IN	0x5e583b6a1686f7bc09…	79,977,632.106981	USD Coin (USDC)
456 days 5 hrs ago	Multichain: Fantom Bridge	IN	0x5e583b6a1686f7bc09…	1	USD Coin (USDC)

These did not result in corresponding token burns on Fantom !

Plasma Bridge

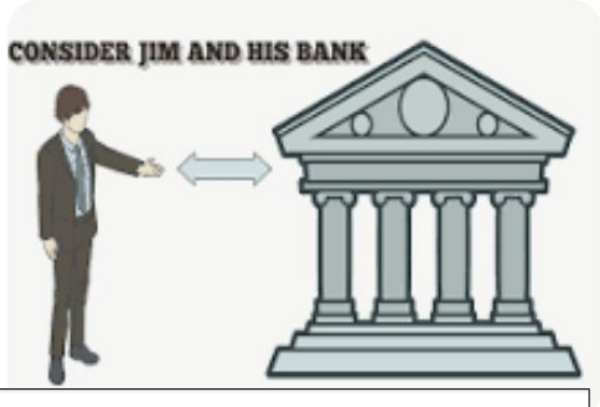
Please check the latest Matic.js documentation on Plasma to get started.

A bridge is basically a set of contracts that help in moving assets from the root chain to the child chain. There are primarily two bridges to move assets between Ethereum and Polygon. First one is the Plasma bridge and the second one is called the **PoS Bridge** or **Proof of Stake bridge**. **Plasma bridge** provides an increased security guarantees due to the Plasma exit mechanism.

However, there are certain restrictions on the child token and there is a 7-day withdrawal period associated with all exits/withdraws from Polygon to Ethereum on the Plasma bridge. The PoS Bridge is more flexible and features faster withdrawals.

There no Plasma exit mechanism deployed on mainnet

Rehypothecation is **a practice whereby banks and brokers use, for their own purposes, assets that have been posted as collateral by their clients**. Clients who permit rehypothecation of their collateral may be compensated either through a lower cost of borrowing or a rebate on fees.



Remove Funds from lending protocols AAVE and Compound and disable Interest Function on Omni Bridge and xDAI Bridge

📦 Justification: reduce risk and exposure during the uncertainty that came with the merge. After the merge, a new strategy must be developed in order to define how to approach this type of investment considering the implications related to transparency to the users and the risk involved.

✅ Implemented: September 14, 2022

L2Beat Bridge Risk Framework

Let's start with bridge types

- **Token Bridge** - mints token on a destination chain
- **Liquidity Network** - uses liquidity pools on a destination chain to deliver token minted previously by a Token Bridge to users
- Token Bridges typically have **Escrows** on a source chain
- Liqudity Networks have **Liquidity Pools** on both source and destination chains
- Bridges can be **Hybrid**, i.e. for some tokens act as a Token Bridge, for other tokens as a Liqudity Network. Best example: **Multichain**

Token Bridge vs Liquidity Network

Token Bridge

- Unlimited liquidity
- Tokens held on a destination still are at-risk of a Token Bridge Validators
- Can be slow and expensive

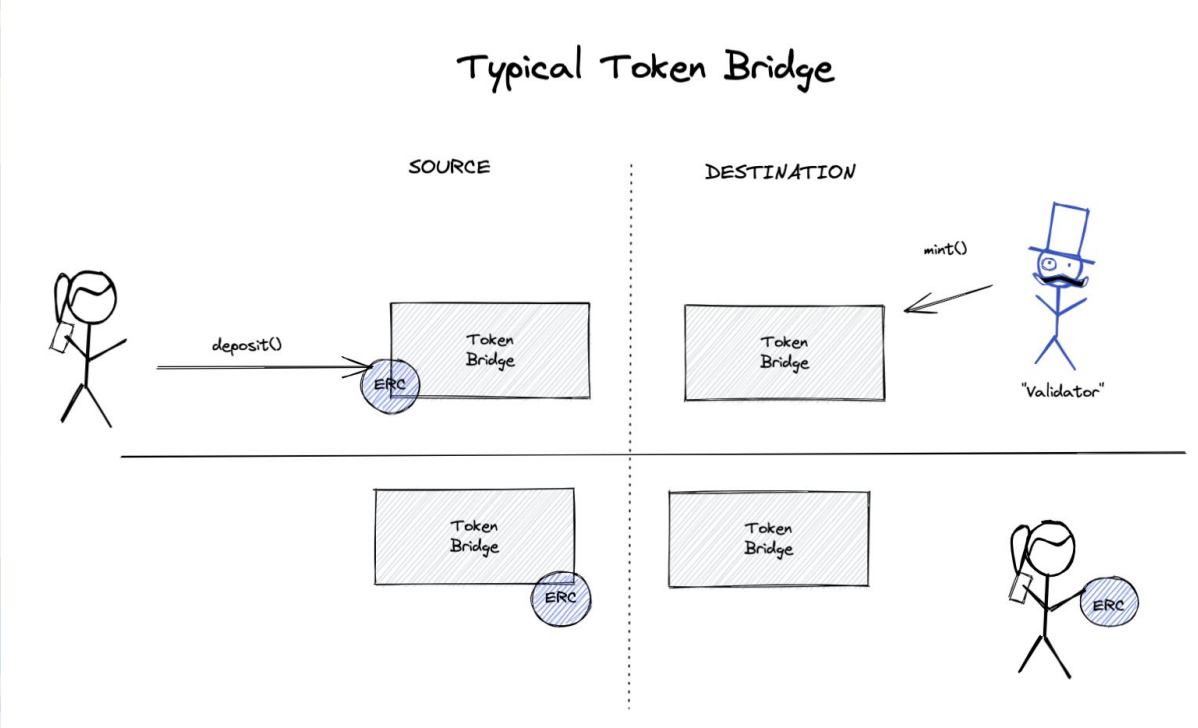
Liquidity Network

- Limited Liquidity
- Tokens held on a destination are not at risk of a Liquidity Network Validators, however they are at risk of a related Token Bridge
- Can be fast and cheap

Users should be aware if they are using Token Bridge or Liquidity Network. Today this is typically NOT the case

#	NAME	TVL	BREAKDOWN	7D CHANGE	MARKET SHARE	VALIDATED BY	TYPE
1	Polygon PoS	$2.82B		+0.16%	21.45%	Destination Chain	Token Bridge
2	Arbitrum One	$2.39B		-0.52%	18.13%	Ethereum	Optimistic Rollup
3	Optimism	$1.44B		-0.64%	10.97%	Ethereum	Optimistic Rollup
4	Multichain	$1.43B		-1.46%	10.86%	Third Party	Hybrid
5	Rainbow Bridge	$1.31B		+1.41%	9.95%	Destination Chain	Token Bridge
6	Ronin V2	$840M		-1.50%	6.37%	Third Party	Token Bridge
7	Avalanche Bridge	$793M		-9.23%	6.01%	Third Party	Token Bridge
8	Polygon "Plasma"	$622M		+6.44%	4.72%	Destination Chain	Token Bridge
9	dYdX	$383M		-1.19%	2.90%	Ethereum	ZK Rollup
10	Loopring	$138M		-3.15%	1.05%	Ethereum	ZK Rollup
11	StarGate	$130M		-2.72%	0.99%	Third Party	Liquidity Network
12	Metis Andromeda	$127M		+7.43%	0.96%	Ethereum	Optimistic Chain
13	Wormhole V2	$115M		-1.46%	0.88%	Third Party	Token Bridge
14	xDai Omni	$101M		-3.88%	0.77%	No info	Token Bridge
15	Satellite Bridge	$94.99M		+1.71%	0.72%	Third Party	Liquidity Network

To build a Token Bridge you need to relay cross-chain messages



How are these x-chain messages validated ?

- **Third Party** (EOA, MultiSig, MPC, intermediary blockchain with their own set of Validators)
- **Optimistically** (message considered valid until proven otherwise)
- **By originating chain Validators** (If Src Chain validators say msg are valid, they are considered valid on a Destination chain)
- **Trustlessly by Ethereum** (messages are validated by Ethereum smart contracts or possibly via the protocol itself). Examples - Optimistic Rollups, zkRollups, with some caveats regarding data availability other L2s such as Validiums and Optimistic Chains

What can go wrong ?

External Validators	Validators can **censor, steal, freeze funds**. Validator's keys **can be compromised**
Optimistic Validation	If Watchers are not active, messages can be **forged and funds can be stolen**
Light Client Validation	If Dst Chain is 51% (⅔) attacked, msgs can be censored and funds can be stolen. ⅓ of Validators can freeze funds. **Fork on a destination chain can lead to fund imbalance**
Full client Ethereum Validation	**Nothing ?** (if Ethereum forks, dst chain will fork with Ethereum)

Include canonical bridges to Layer2s

#	NAME	DESTINATION	VALIDATED BY	TYPE	UPGRADEABILITY
1	**Polygon PoS**	Polygon	Destination Chain	Token Bridge	48 hours delay
2	**Arbitrum One**	Arbitrum One	Ethereum	Optimistic Rollup	Yes
3	**Optimism**	Optimism	Ethereum	Optimistic Rollup	Yes
4	**Multichain**	Various	Third Party	Hybrid	No / EOA
5	**Rainbow Bridge**	Near, Aurora	Destination Chain	Token Bridge	Yes
6	**Ronin V2**	Axie Infinity Chain	Third Party	Token Bridge	Yes
7	**Avalanche Bridge**	Avalanche	Third Party	Token Bridge	EOA
8	**Polygon "Plasma"**	Polygon	Destination Chain	Token Bridge	48 hours delay
9	**dYdX**	dYdX	Ethereum	ZK Rollup	Yes
10	**Loopring**	Loopring	Ethereum	ZK Rollup	Yes
11	**StarGate**	Various	Third Party	Liquidity Network	No
12	**Metis Andromeda**	Metis Andromeda	Ethereum	Optimistic Chain	Yes
13	**Wormhole V2**	Various	Third Party	Token Bridge	Yes

Upgradability

- All is irrelevant if the bridge can be upgraded, especially with no notice
- Upgrades can lead to disastrous bugs → Nomad hack
- How do we protect ourselves from potentially catastrophic bugs and - at the same time - create uncensorable, immutable infrastructure ?
  - long upgrade delays for new feature upgrades
  - security councils with circuit breaker powers to react to critical bugs and distributed governance with power to restart bridges
  - semi-automatic circuit-breakers with permissionless, distributed keepers working, storage proofs, cryptoeconomic schemes
  - dark patches
  - **problem is very hard**

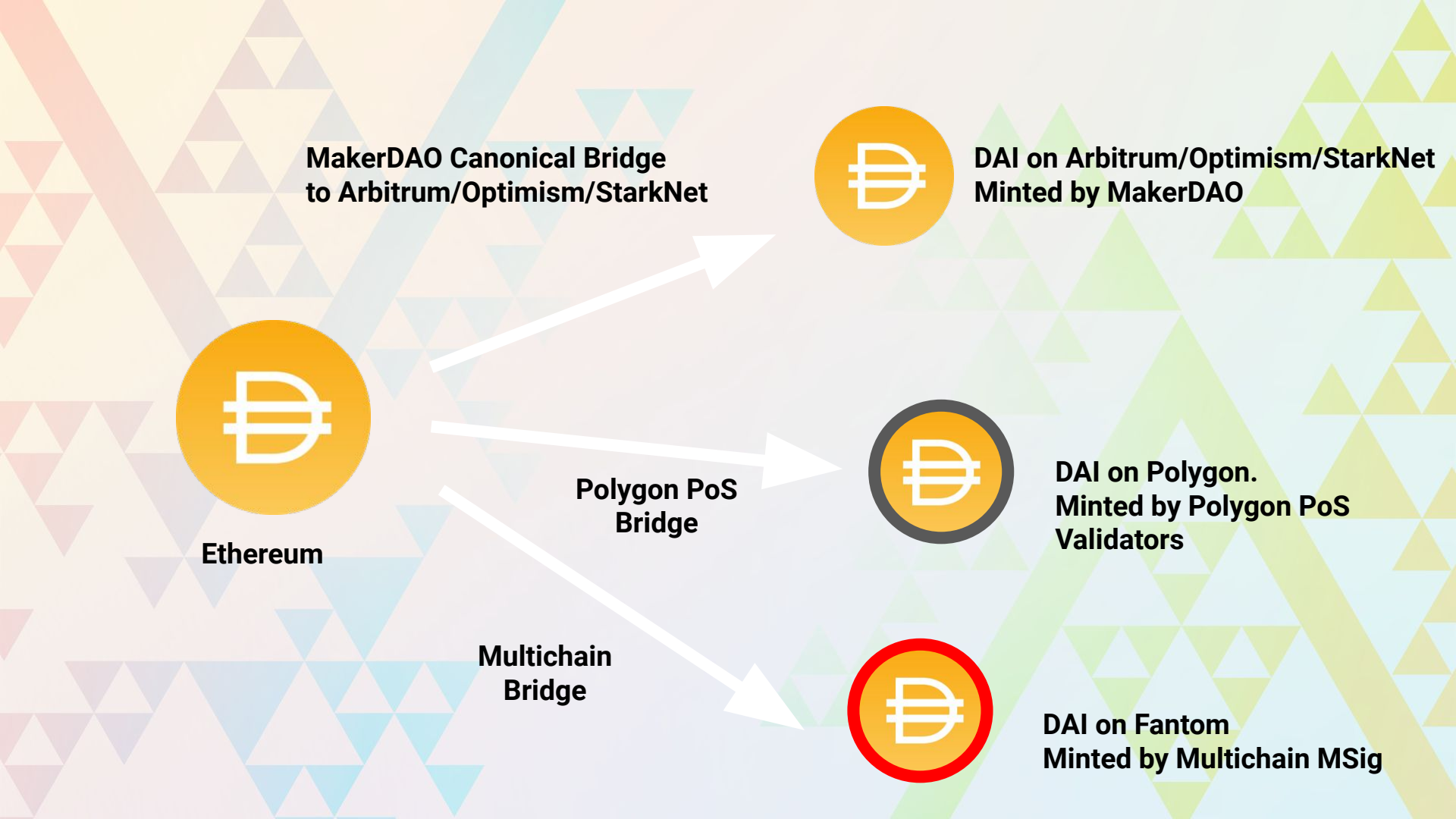
☑ Include canonical bridges to Layer2s

#	NAME	DESTINATION	VALIDATED BY	TYPE	UPGRADEABILITY	DESTINATION TOKEN
1	**Polygon PoS**	Polygon	Destination Chain	Token Bridge	48 hours delay	Wrapped
2	**Arbitrum One**	Arbitrum One	Ethereum	Optimist		& Canonical
3	**Optimism**	Optimism	Ethereum	Optimistic Rollup	Yes	Native & Canonical
4	**Multichain**	Various	Third Party	Hybrid	No / EOA	Canonical or Wrapped
5	**Rainbow Bridge**	Near, Aurora	Destination Chain	Token Bridge	Yes	Canonical or Wrapped
6	**Ronin V2**	Axie Infinity Chain	Third Party	Token Bridge	Yes	Canonical
7	**Avalanche Bridge**	Avalanche	Third Party	Token Bridge	EOA	Wrapped
8	**Polygon "Plasma"**	Polygon	Destination Chain	Token Bridge	48 hours delay	Native & Canonical
9	**dYdX**	dYdX	Ethereum	ZK Rollup	Yes	Canonical
10	**Loopring**	Loopring	Ethereum	ZK Rollup	Yes	Native & Canonical
11	**StarGate**	Various	Third Party	Liquidity Network	No	Canonical
12	**Metis Andromeda**	Metis Andromeda	Ethereum	Optimistic Chain	Yes	Native & Canonical

The bridge can be upgraded by 5/9 MSig after 48 hour delay.

Destination Token - what is really being minted ?

- Native token ? (i.e. token used to pay for gas)
- Wrapped token (“representation token”, “synthetic token”)
  - May be upgradable (by who ???)
  - May have very different characteristic than original token. E.g. DAI on Ethereum is permissionless and censorship resistant
    - “DAI” on Polygon ? - token minted by Polygon PoS bridge
    - “DAI” on Fantom ? - token minted by Multichain bridge
    - “DAI” on Solana ? - token minted by Wormhole bridge
- Canonical token → Canonical Token Bridge is the bridge with the ability to mint canonical token. It is always a wrapped token with socially agreed “special” status
    - USDC on Arbitrum → Arbitrum ERC20 token bridge
    - MIM on Arbitrum → Multichain bridge
    - DAI on Arbitrum → MakerDAO canonical bridge
    - FRAX on Arbitrum → any bridge and then swapped to “canonical” FRAX

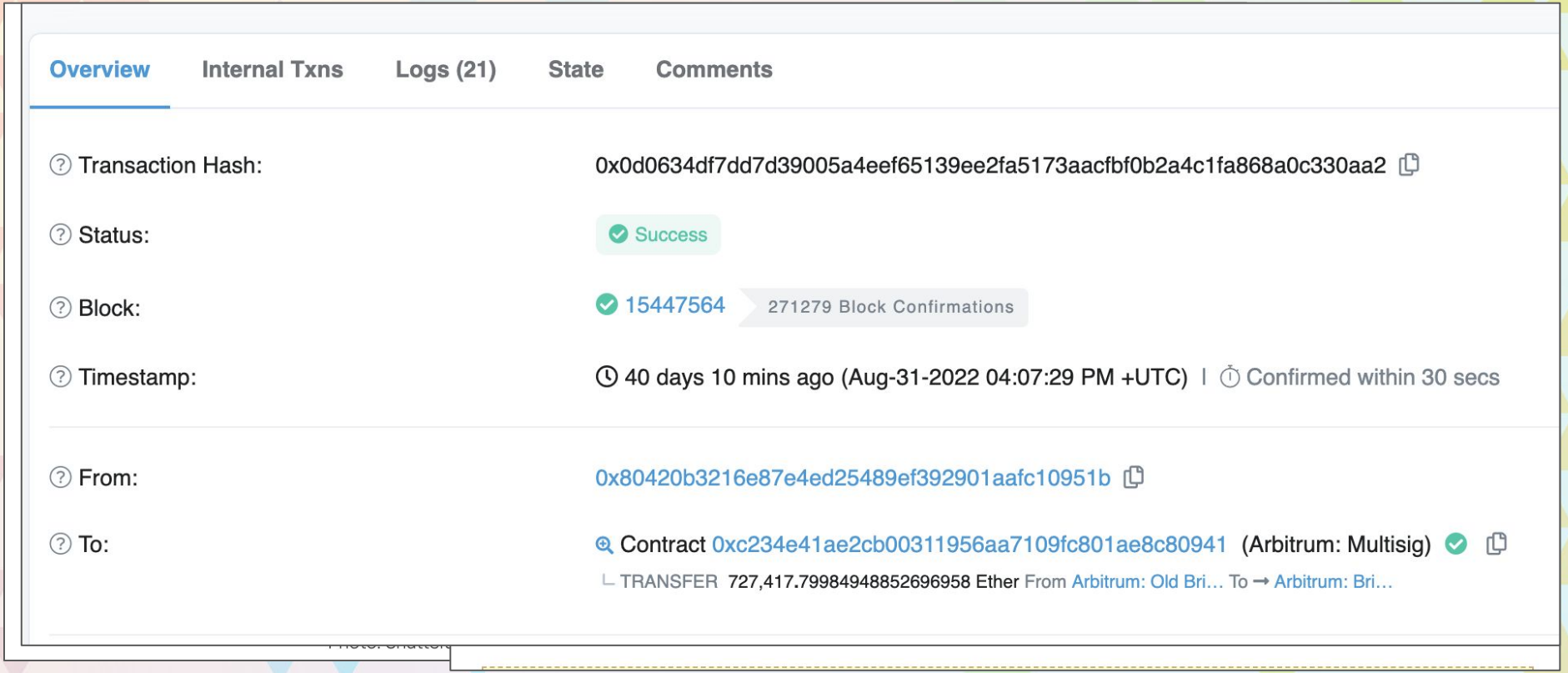

MakerDAO Canonical Bridge
to Arbitrum/Optimism/StarkNet
DAI on Arbitrum/Optimism/StarkNet
Minted by MakerDAO
Ethereum
Polygon PoS
Bridge
DAI on Polygon.
Minted by Polygon PoS
Validators
Multichain
Bridge
DAI on Fantom
Minted by Multichain MSig

Include canonical bridges to Layer2s

#	NAME	DESTINATION	VALIDATED BY	TYPE	UPGRADEABILITY	DESTINATION TOKEN
1	**Polygon PoS**	Polygon	Destination Chain	Token Bridge	48 hours delay	Wrapped
2	**Arbitrum One**	Arbitrum One	Ethereum	Optimistic Rollup	Yes	Native & Canonical
3	**Optimism**	Optimism	Ethereum	Optimistic Rollup	Yes	Native & Canonical
4	**Multichain**	Various	Third Party	Hybrid	No / EOA	Canonical or Wrapped
5	**Rainbow Bridge**	Near, Aurora	Destination Chain	Token Bridge	Yes	
6	**Ronin V2**	Axie Infinity Chain	Third Party	Token Bridge	Yes	
7	**Avalanche Bridge**	Avalanche	Third Party	Token Bridge	EOA	
8	**Polygon "Plasma"**	Polygon	Destination Chain	Token Bridge	48 hours	
9	**dYdX**	dYdX	Ethereum	ZK Rollup	Yes	Canonical

Some tokens transferred are considered canonical but some tokens are not. Users who wish to obtain the canonical counterparts need to do so by trading. Depending on the router configuration either Multichain tokens or Any tokens are minted.

So are trusted rollup bridges so good ?



Overview | Internal Txns | Logs (21) | State | Comments

Transaction Hash: 0x0d0634df7dd7d39005a4eef65139ee2fa5173aacfbf0b2a4c1fa868a0c330aa2

Status: Success

Block: 15447564 271279 Block Confirmations

Timestamp: 40 days 10 mins ago (Aug-31-2022 04:07:29 PM +UTC) | Confirmed within 30 secs

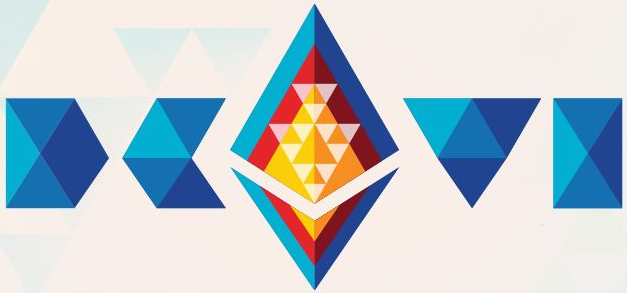
From: 0x80420b3216e87e4ed25489ef392901aafc10951b

To: Contract 0xc234e41ae2cb00311956aa7109fc801ae8c80941 (Arbitrum: Multisig)

TRANSFER 727,417.79984948852696958 Ether From Arbitrum: Old Bri… To → Arbitrum: Bri…

Yes, rollup bridges are the most secure, but

- They are immensely complex and the bug surface is huge
- None (except experimental Fuel 1.0) of them shed their “training wheels”
- We need way more time for the code to be ossified, battle-tested and considered to be secure
- **We still don’t seem to have a solution for dealing with discovery of potentially critical bugs w/out leaving upgrade keys to the protocol admins**



Thank you!

Bartek Kiepuszewski
(bartek.eth)

@bkiepuszewski