

Iterative User Research

tBTC v2 - Bridge Usability
Testing

May-June 2023

Design Researcher: **Sasha Tanase**
Product Designer: **Sasha Tanase**



Agenda

- Methodology
- Usability Tests - Methodology
- Findings - Page by Page
- Appendix
 - Interview Script
 - Figma Prototype [here](#)

Design Research

Design Research helps teams build the right thing, the right way.

Explorative Design

helps building the *right thing*.

Iterative Design

helps building the *thing right*.

Design Research

Design Research helps teams build the right thing, the right way.

Iterative Research

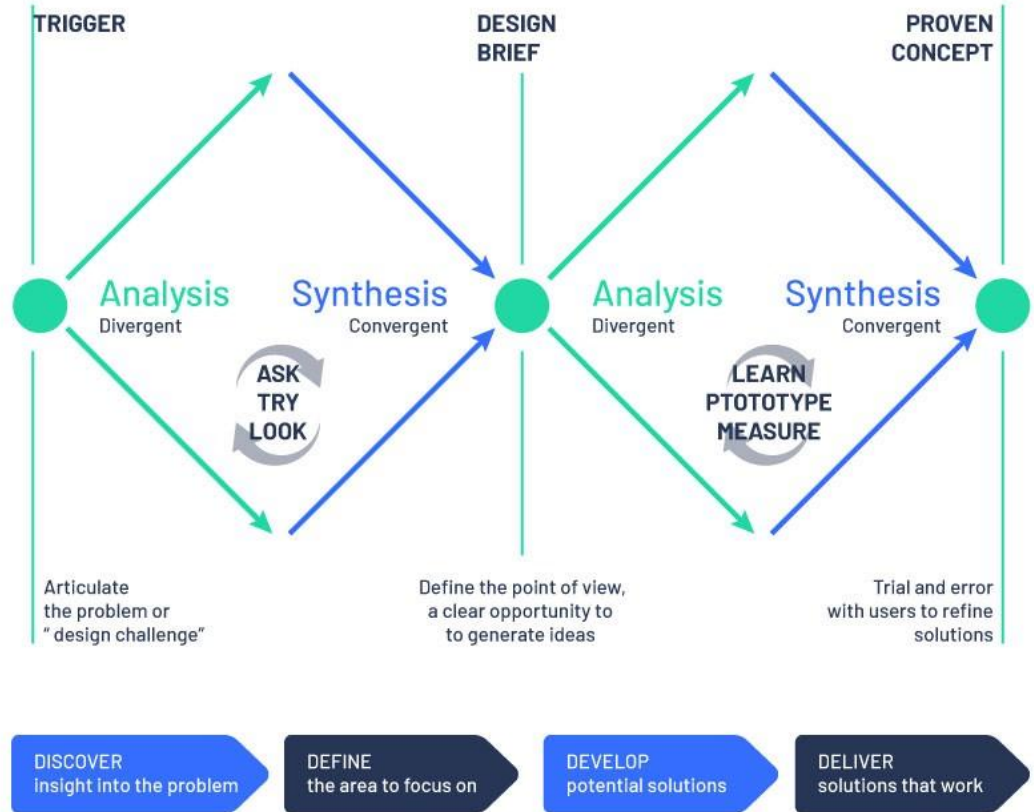
User testing to determine whether what we've built meets user needs, is understood, and is easy to use

Methodology

DOUBLE DIAMOND

In our Design Process, Coverage Pool is in the **Synthesis Step**. We have prototyped and tested our solutions to the users. We have gathered feedback and found what we need to change and what we need to add.

Next step - Go back to the drawing board, find solutions based on the findings and test again.



Study Goals

- learn more about BTC users
- learn more about potential tBTC users
- discover pain points and turn them into opportunities
- learn about the bridge anxiety
- test the minting/depositing flow
- test the unminting/withdrawing flow
- resuming a deposit **(needs a separate study)**
- test the Visibility of System Status designs
- check if our product offers what the market needs
- check if bridging BTC NFTs would be something interesting **(one insight, needs a separate study)**

Research Methods and Users

WHAT WE DID

- We interviewed **6 users**
- Qualified users were individuals who **used BTC to ETH bridges or who owned WBTC, tBTC, renBTC**
- **60 minutes** video calls
- Figma Clickable Prototype used for the test
 - [Minting flow](#)
 - [Unminting Flow](#)

Research Methods and Users

TOPICS COVERED IN THE INTERVIEW

Demographics

- are not extremely important only the tech background and tech profile

Bitcoin holders, bridges experience, motivation behind bridging assets

- we wanted to find what is the common behaviour, the fears, the needs, when bridging assets to any chain not only BTC to ETH

Prototype Walkthrough

- This exercise involved thinking out loud technique in which users had to go through both the minting and unminting flow and describe what they see, and also checked how well the How it works page performs. We used a clickable prototype made in [Figma](#)

- [Minting flow](#)
- [Unminting Flow](#)

100

Deep Learnings



Research Methods and Users

BITCOIN HOLDERS BEHAVIOUR

BEHAVIOURS NOTED

Most of the participants we've talked to are holding Bitcoin tokens and the majority of them bought Bitcoin in 2017 via Centralized Exchanges. Only one of them is mining Bitcoin since 2014.

Keeping and Swapping in CEXs

The majority of the participants said that they keep their funds in cold wallets or on CEXs. The ones who particularly use CEXs said that they like to keep their funds in exchanges because it is easier for them to see all of their tokens across multiple blockchains but also it's easier to just swap tokens if they need to do anything.

Using Bitcoin

Some of the participants mentioned that they are using Bitcoin in daily life errands. One of them mentioned that he is using BTC to pay for his rent because he is living in Asia and it's easier.

Research Methods and Users

BITCOIN HOLDERS BEHAVIOUR

Using Bitcoin

All of the ones who mentioned using BTC for daily usage actually mentioned they are doing this in order to avoid international banking transfers because they said “they are too complicated and take too long”.

Using Wrapped Bitcoin

Most of the participants mentioned they used wrapped BTC tokens for the following reasons:

- To experiment, out of curiosity
- To overpass the long duration of the BTC transactions
- To gain yield on DeFi protocols

Methods of getting wrapped Bitcoin. They use either CEXs or DEXs to swap for them, however most of the time they use ETH or other tokens to swap for wrapped BTC.

If by any chance they swap from BTC, they will swap back as soon as possible to the original.

Research Methods and Users

BITCOIN HOLDERS BEHAVIOUR

Bitcoin as a store of value

All the participants we've talked to consider their Bitcoin funds as a store of value, their grey pound, something that that store safely and they would not touch.

They are very cautious with these funds and nothing seems to be worthy of touching them. Only one of them considered maybe bridging their funds only and if only there would be a large yield.

Research Methods and Users

BITCOIN HOLDERS BEHAVIOUR

“-Have you ever used any other wrapped BTC Tokens other than WBTC?” (researcher)

“- What? Are there any others than WBTC?” (particiapnt 4)

Research Methods and Users

BITCOIN HOLDERS BEHAVIOUR

Bridge experience

Most of the participants that we talked to do not have a lot of experience with Bitcoin bridges and consider 2-3 hours a long time. They prefer to swap even though they know they will have bigger fees to pay, but they consider it the price of the the ease of use.

Most of them consider bridges experience too cumbersome so they default to swapping. Another thing is that they do not consider bridges safe, on the contrary they are afraid of bridge hacks more than anything.

When thinking about bridges it seems that once a bridge was hacked it can never be redeemed in their eyes.

Research Methods and Users

BITCOIN HOLDERS BEHAVIOUR

Safety factors

A lot of the user who are Bitcoin first consider that the Bitcoin Network is the safest and as long as they are not moving their funds there can be nothing wrong. The majority of them consider all of the other blockchains to have smart contract vulnerabilities.

When they are considering choosing a product they will check:

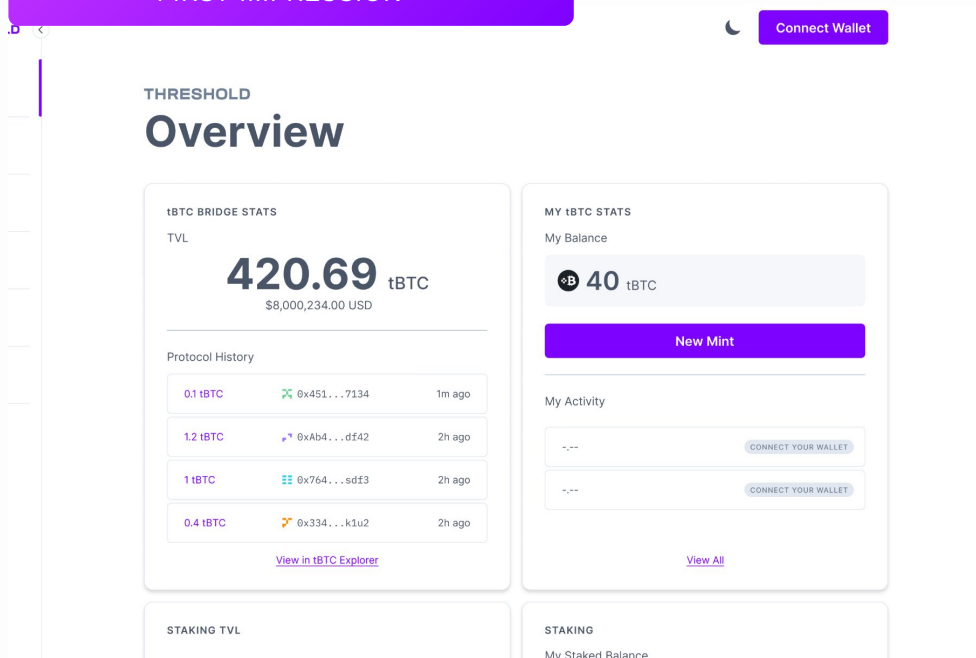
- Hack history
- the team who built it
- Audits (even though a lot of them say that the audit doesn't represent that much, a protocol can be hacked even though it has been audited)
- Protocol backers, big financial organizations associated with the protocol
- TVL to an extent - a lot of them say that security is not in numbers.

Screen by Screen Walkthrough



Findings and Recommendations

FIRST IMPRESSION



FINDING

4 out of 6 participants did not correlate the term “minting” with bridging.

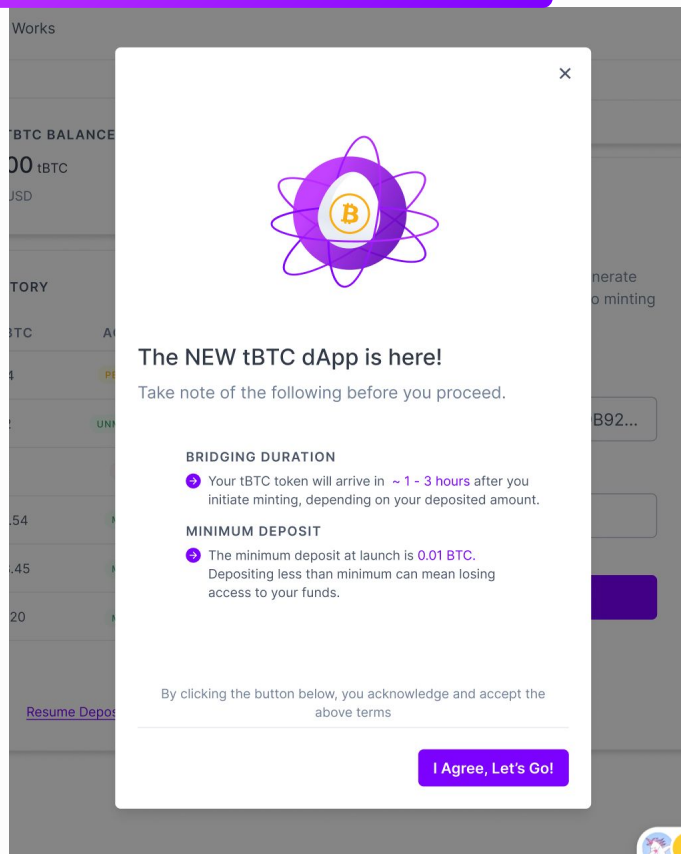
RECOMMENDATION

Consider changing the term “Mint” to “Deposit” or “Bridge”.

Most of the current bridges use the term “Deposit” for bridging and “Withdraw” for bridging back.

Findings and Recommendations

MODAL



FINDING

All participants read the modal and found the information useful. The information that seemed to have stuck out the most was the timing duration.

A lot of participants found useful the How it works page, however the page is hidden behind the modal, so if users do not agree they cannot see other pages.

RECOMMENDATION

Consider showing the modal only when the new users click on the bridge tab and not on How it works or tBTC Explorer.

Findings and Recommendations

HOW IT WORKS PAGE

FINDING

Only 3/6 participants noticed the How it works page. The ones that were able to see the page displayed an interesting behaviour. Before taking any action inside the bridge they patiently went through the How it works page. It appears that the timeline was quite helpful.

Unsurprisingly the section that was the most problematic was the one regarding the recovery of the funds. The term .JSON confused them.

Some of them mentioned that it's great that there are all the contracts and audits aggregated under this page however most of them said they wouldn't know how to read through the reports and they would prefer to have a section in which they are explained how the security model works.

IBTC BRIDGE

The second generation of IBTC is a truly decentralized bridge between Bitcoin and Ethereum.

It provides Bitcoin holders permissionless access to DeFi and the expanding web3 universe.



MINTING TIMELINE

STEP 1 OFF-CHAIN ACTION

PROVIDE DATA

- 1 Provide an ETH address and a BTC Recovery address to generate a unique BTC deposit address.



ETH Address:

- 1 This is where your IBTC (ERC20) will be sent after minting initiation.

Recovery BTC Address:

- 1 Providing a BTC Return address means your bitcoin will be safe, even in the unlikely case of an error minting. [Read more ^](#)
- 2 Make sure you provide a single BTC Return address that you control. Don't use a multi-sig or an exchange address. You can read more about the requirements and P2PKH. [Read more ^](#)
- 3 This address has to start with the letters "bc" for Bitcoin Mainnet and with the letter "1" for Testnet Bitcoin. This means that your addresses are P2PKH or P2WPKH compliant. [Read more ^](#)

Based on these two addresses, the protocol will create a unique BTC deposit address using a P2SHW for each user. [Read more ^](#)

STEP 2 ACTION ON BITCOIN NETWORK

MAKE A BTC DEPOSIT

- 1 Send any amount larger than 0.01 BTC to this unique BTC Deposit Address. The amount you send will be minted as IBTC.



STEP 3 ACTION ON ETHEREUM NETWORK

INITIATE MINTING

- 1 Minting IBTC does not require you to wait for the Bitcoin confirmations. Sign an Ethereum transaction in your wallet, and your IBTC will arrive in around 3 hours.



DEPOSIT RECEIPT FILE FOR FUND RECOVERIES

The Deposit Receipt under the form of a .JSON file is important to save in case you need to recover your funds.

It's important to keep this .JSON file until you have successfully initiated IBTC minting.

This file contains the BTC Return address, a wallet public key, a refund public key and a refund lock time. It reconstructs the deposit address in case a very unlikely incident were to happen.

Each new deposit will generate a new .JSON file. Take note: Recovery time lock is currently 9 months.

Recovery guide can be found [Here ^](#)



CONTRACTS

	Token Contract	Read More ^
	Bridge Contract	Read More ^

AUDIT REPORTS

	Least Authority Report IBTC Bridge v2 Security	Read More ^
	Certik Report Vending Machine Security	Read More ^
	ChainSecurity Report Staking Contract, T Token, Vending Machine Security	Read More ^

Findings and Recommendations

HOW IT WORKS PAGE

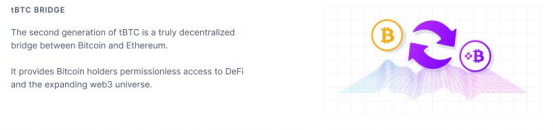
RECOMMENDATION

Bring the **How it works page** more in front and help the user see it. We could add it in the Bridge modal or in the bridge dApp. This will help the users understand how things are done in the dApp and what are the necessary steps for them.

Add a card about **Optimistic minting** and help users understand what that means and how is actually impacting their actions if any.

Explain in **plain language what is the security model** of the bridge and what measure we take in order for the bridge to be secure and safe for our users.

Deposit Receipt and Recovery - I propose to have a very simple explanation about the Receipt in the How it works page and display a more detailed explanation in the Deposit Resuming page.



MINTING TIMELINE

STEP 1

PROVIDE DATA

- Provide an ETH address and a BTC Recovery address to generate a unique BTC deposit address.



ETH Address:

- This is where your IBTC (ERC20) will be sent after minting initiation.

Recovery BTC Address:

- Providing a BTC Return address means your bitcoin will be safe, even in the unlikely case of an error minting. [Read more ^](#)
- Make sure you provide a single BTC Return address that you control. Don't use a multi-sig or an exchange address. You can read more about the requirements and P2PKH. [Read more ^](#)
- This address has to start with the letters "bc" for Bitcoin Mainnet and with the letter "t" for Testnet Bitcoin. This means that your addresses are P2PKH or P2WPKH compliant. [Read more ^](#)

Based on these two addresses, the protocol will create a unique BTC deposit address using a P2SHW for each user. [Read more ^](#)

STEP 2

MAKE A BTC DEPOSIT

- Send any amount larger than 0.01 BTC to this unique BTC Deposit Address. The amount you send will be minted as IBTC.



STEP 3

INITIATE MINTING

- Minting IBTC does not require you to wait for the Bitcoin confirmations. Sign an Ethereum transaction in your wallet, and your IBTC will arrive in around 3 hours.



DEPOSIT RECEIPT FILE FOR FUND RECOVERIES

The Deposit Receipt under the form of a .JSON file is important to save in case you need to recover your funds.

It's important to keep this .JSON file until you have successfully initiated IBTC minting.

This file contains the BTC Return address, a wallet public key, a refund public key and a refund lock time. It reconstructs the deposit address in case a very unlikely incident were to happen.

Each new deposit will generate a new .JSON file. Take note: Recovery time lock is currently 9 months.

Recovery guide can be found [Here ^](#)



CONTRACTS



Token Contract

[Read More ^](#)



Bridge Contract

[Read More ^](#)

AUDIT REPORTS



Least Authority Report
IBTC Bridge v2 Security

[Read More ^](#)



Certik Report
Vending Machine Security

[Read More ^](#)



ChainSecurity Report
Staking Contract, T Token,
Vending Machine Security

[Read More ^](#)

Findings and Recommendations

STEP 1

tBTC BALANCE

0.00 tBTC
\$0 USD

MY ACTIVITY

TBTC	STATE
---	---
---	---

You have no activity yet.

TBTC - MINTING PROCESS

Step 1 - Generate a Deposit Address

Based on these two addresses, the system will generate for you an unique BTC deposit address.

ETH Address ①

Address where you'll receive your tBTC

BTC Return Address ①

BTC Address should start with "bc"

Generate Deposit Address

[Bridge Contract](#)

DURATION

~ 1 Hour	< 0.10 BTC
~ 1.5 Hours	< 1.00 BTC
~ 2 Hours	> 1.00 BTC

TIMELINE

STEP 1
ACTION OFF-CHAIN
DEPOSIT ADDRESS
Provide an ETH address and a BTC Return address to generate an unique BTC deposit address.
[Read more](#)

STEP 2
ACTION ON BITCOIN
MAKE A BTC DEPOSIT

STEP 3
ACTION ON ETHEREUM
INITIATE MINTING

FINDING

It is great that we autocomplete the Ethereum address however a lot of participants had a difficulty with understand the process not because it is complicated but because it was not matching their mental model of how bridges work.

For now the information we give doesn't seem to make sense in their heads why they have to take this step that is so new to them.

RECOMMENDATION

I propose to explain how this Unique addresses increase the safety or helps the user. This way they will accept it easier.

Findings and Recommendations

STEP 1

tBTC BALANCE
0.00 tBTC
\$0 USD

MY ACTIVITY

TBTC	STATE
--	--
--	--



You have no activity yet.

TBTC - MINTING PROCESS

Step 1 - Generate a Deposit Address

Based on these two addresses, the system will generate for you an unique BTC deposit address.

ETH Address ⓘ

BTC Return Address ⓘ

Generate Deposit Address

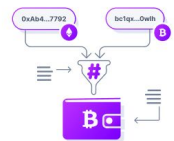
[Bridge Contract](#)

DURATION

~ 1 Hour	< 0.10 BTC
~ 1.5 Hours	< 1.00 BTC
~ 2 Hours	≥ 1.00 BTC

TIMELINE

STEP 1
ACTION OFF-CHAIN
DEPOSIT ADDRESS
Provide an ETH address and a BTC Return address to generate an unique BTC deposit address.
[Read more](#)



STEP 2
ACTION ON BITCOIN
MAKE A BTC DEPOSIT

STEP 3
ACTION ON ETHEREUM
INITIATE MINTING

FINDING

No user noticed the duration section. When asked if the information given in this section would influence their choice of the amount deposited they replied that “if I made it to here it means that I believe in this product and I would not fragment my deposit to pay a lot of gas”.

RECOMMENDATION

I propose removing this section from step 1 and add it in the proximity of the QR code where the user is actually needed to send their tokens.

Findings and Recommendations

STEP 1

tBTC BALANCE
0.00 tBTC
\$0 USD

MY ACTIVITY

TBTC	STATE
--	--
--	--



You have no activity yet.

TBTC - MINTING PROCESS

Step 1 - Generate a Deposit Address

Based on these two addresses, the system will generate for you an unique BTC deposit address.

ETH Address ⓘ

BTC Return Address ⓘ

Generate Deposit Address

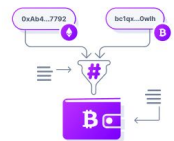
[Bridge Contract](#)

DURATION

~ 1 Hour	< 0.10 BTC
~ 1.5 Hours	< 1.00 BTC
~ 2 Hours	≥ 1.00 BTC

TIMELINE

STEP 1
ACTION OFF-CHAIN
DEPOSIT ADDRESS
Provide an ETH address and a BTC Return address to generate an unique BTC deposit address.
[Read more](#)



STEP 2
ACTION ON BITCOIN
MAKE A BTC DEPOSIT

STEP 3
ACTION ON ETHEREUM
INITIATE MINTING

FINDING

Most of the users do not actually notice the network labels in the timeline.

RECOMMENDATION

I propose removing the chain labels from the timeline and adding them in closer to the body text in the main dApp area.

Findings and Recommendations

BEHAVIOUR NOTED

FINDING

Just like in previous studies participants in this study told me that whenever they are considering using a new protocol, they will first use a very small amount of funds and then they will see what happens.

This behaviour is usually tied to the security of a bridge and to decrease the risk of being rugged or losing a big chunk of funds.

However, this behaviour happens also as a method of learning the way a dApp works. Based on this interaction with the product, the users will decide if they are going to stick with the product or look for something else.

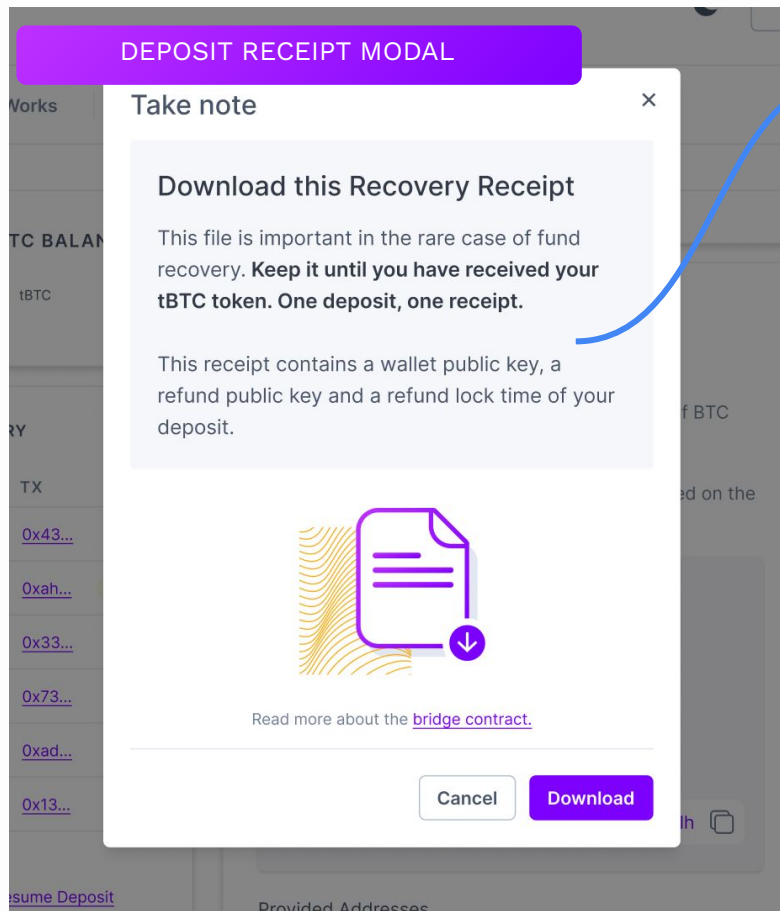
RECOMMENDATION

Since the tBTC Bridge dApp comes with some new patterns and challenges the usual bridge experience I propose to support a sandbox inside the dApp that doesn't require actual tokens, and is not on-chain.

This “**sandbox/demo**” will help the users learn the way they need to interact with the bridge without having the stress of fund loss.

I believe this will increase their trust in the actual product when they're going to take the actual actions of bridging.

Findings and Recommendations



FINDING

5% participants got frightened by this message. The participants became quite uncomfortable while reading this message. They were confused why they need to keep the receipt and why they are welcomed by this scary message.

RECOMMENDATION

We should remove this Recovery Receipt from the flow and start saving the receipt for the users. We should store and display the receipts on the Resume deposits page rather than scaring off the users.

Findings and Recommendations

STEP 2

tbtc balance
0.00 tbtc
\$0 USD

MY ACTIVITY

TBTC	STATE
---	---
---	---



You have no history yet.

Unmint

← **tbtc** - MINTING PROCESS

Step 2 - Make your BTC deposit

Use this generated address to send any amount larger than 0.01 BTC, to mint as tBTC.

BTC Deposit Address ⓘ



bc1qxy2kgdygjsqtzq2n0yrf2493p83bc1qxy2kgdygjsqtzq2n0yrf2493p83

📄

Provided Addresses Recap

ETH Address

0xAb4...7792

📄

BTC Recovery Address

bc1A4...7w1h

📄

Checking If The Funds Have Been Sent...

[Bridge Contract](#)

DURATION

~ 1 Hour

< 0.10 BTC

~ 1.5 Hours

< 1.00 BTC

~ 2 Hours

≥ 1.00 BTC

TIMELINE

STEP 1

ACTION OFF-CHAIN

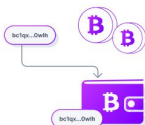
DEPOSIT ADDRESS

STEP 2

ACTION ON BITCOIN

MAKE A BTC DEPOSIT

Send any amount larger than 0.01 BTC to this unique BTC Deposit Address. The amount sent will be used to mint tBTC.



STEP 3

ACTION ON ETHEREUM

INITIATE MINTING

FINDING

Duration section is not noticed.

RECOMMENDATION

Move it closer to the QR code.

Findings and Recommendations

STEP 3

tBTC BALANCE

0.00 tBTC

\$0 USD

MY ACTIVITY

TBTC

STATE



You have no history yet.

Mint

Unmint

← tBTC - MINTING PROCESS

Step 3 - Initiate minting

This step requires you to sign one transaction in your Ethereum wallet.

Initiate Mint

[Bridge Contract](#)

DURATION

~ 1.5 Hours < 1.00 BTC

TIMELINE

STEP 1

ACTION OFF-CHAIN

DEPOSIT ADDRESS

STEP 2

ACTION ON BITCOIN

MAKE A BTC DEPOSIT

STEP 3

ACTION ON ETHEREUM

INITIATE MINTING

Minting tBTC does not require you to wait for the Bitcoin confirmations.
Sign an Ethereum transaction in your wallet and your tBTC will arrive in around 1 to 2 hours.



FINDING

The text here is not offering enough information to the users. Most of the participants would actually wait for their BTC deposit to be confirmed before actually reveal on Ethereum.

This finding is corroborated by the analytics, all the users who are using the tBTC bridge will wait their deposit to be confirmed before hitting “Initiate minting”

RECOMMENDATION

We should help the users understand that they can reveal before their deposit confirmation. We should also help them understand that the Bitcoin Network confirmations are going to happen after the reveal.

Findings and Recommendations

REVEAL TRANSACTION

Initiate minting tBTC

You will initiate the minting of

☒ tBTC

Minting tBTC requires a single transaction on Ethereum and takes approximately 2 hours.

Minted Amount	☒ tBTC
Estimated Ethereum Gas Cost	☒ gWEI
Bitcoin Miner Fee	0.0002 BTC
Threshold Network Fee	0.01 BTC
ETH Address	0xAb4...3789

View [bridge contract](#).

Cancel

Start Minting

FINDING

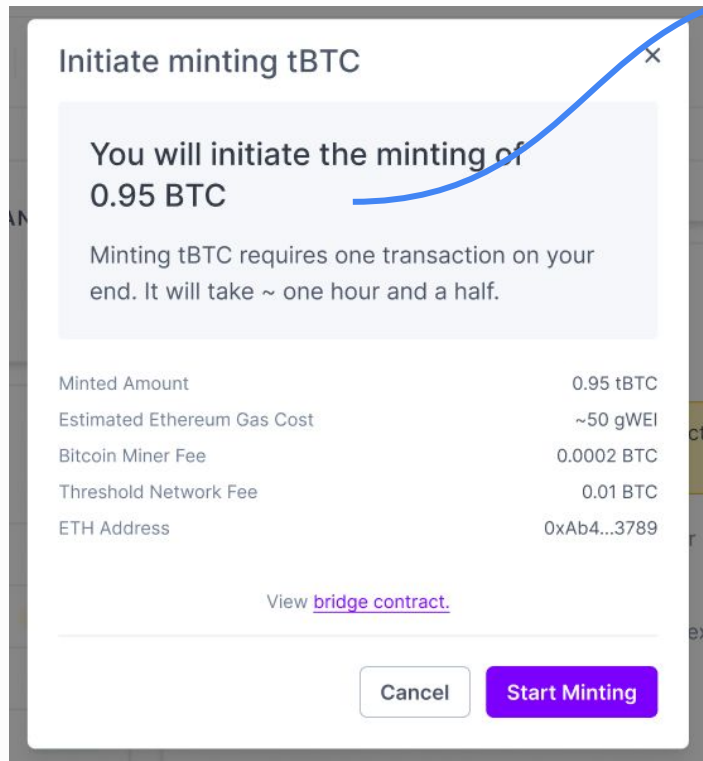
If the Bitcoin miner fee is referring to the fee the user has paid for their own deposit, we can actually remove it since users got a bit confused by it.

RECOMMENDATION

Remove the Bitcoin miner fee in this modal, if the fee refers to the Bitcoin deposit the user has just made.

Findings and Recommendations

REVEAL TRANSACTION



Initiate minting tBTC

You will initiate the minting of
0.95 BTC

Minting tBTC requires one transaction on your end. It will take ~ one hour and a half.

Minted Amount	0.95 tBTC
Estimated Ethereum Gas Cost	~50 gWEI
Bitcoin Miner Fee	0.0002 BTC
Threshold Network Fee	0.01 BTC
ETH Address	0xAb4...3789

View [bridge contract](#).

FINDING

We need to make sure we are displaying here the actual minted amount and not the deposited amount.

RECOMMENDATION

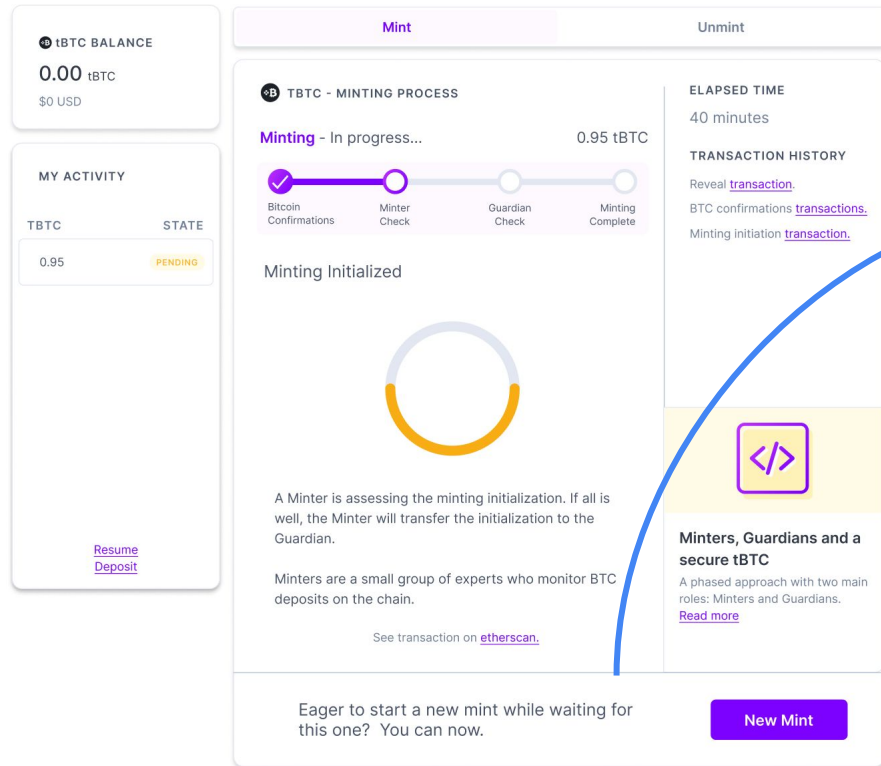
Depending on what actual data we use to display this amount I propose we either:

- display the deposited amount but change the wording
- display the minted amount with the subtracted fees.

Either way we can consider removing this modal and add this information on Step 3.

Findings and Recommendations

VISIBILITY OF SYSTEM



FINDING

"I don't know who these people are but I don't really care about them"

A lot of the participants weren't extremely interested in what the Minters and Guardians are, however some of them thought that minters are actual people who are manually transferring tokens.

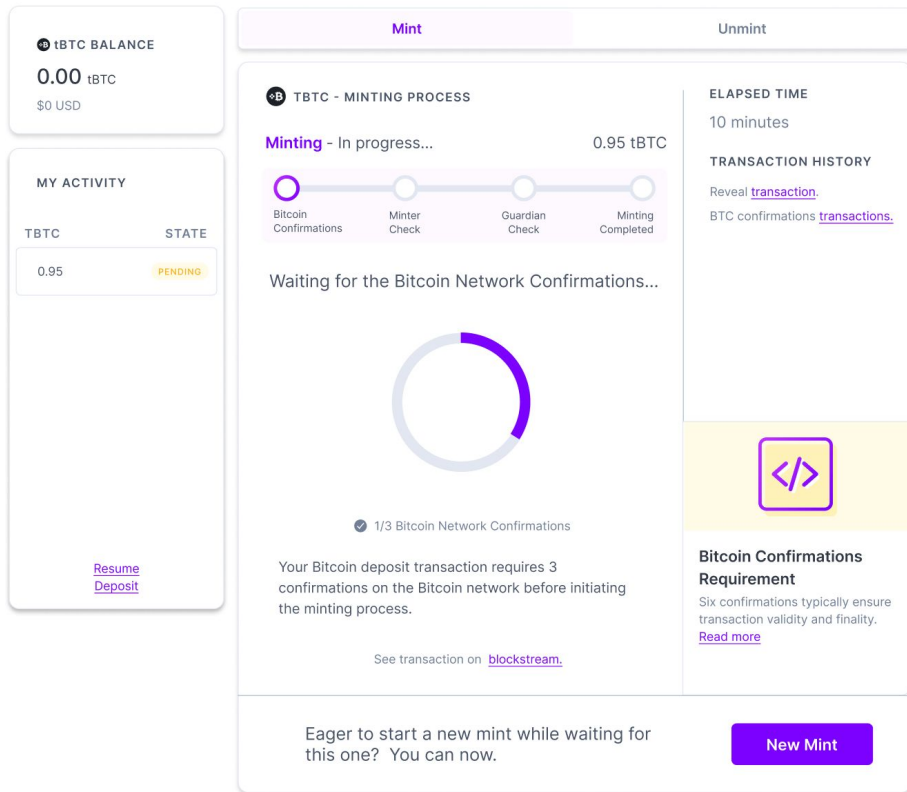
This perception kind of ruins our decentralized narrative.

RECOMMENDATION

Rewrite the body texts from the Minters and Guardians and make sure people understand this is an automated action and Minters and Guardians are software and not real people.

Findings and Recommendations

VISIBILITY OF SYSTEM



FINDING

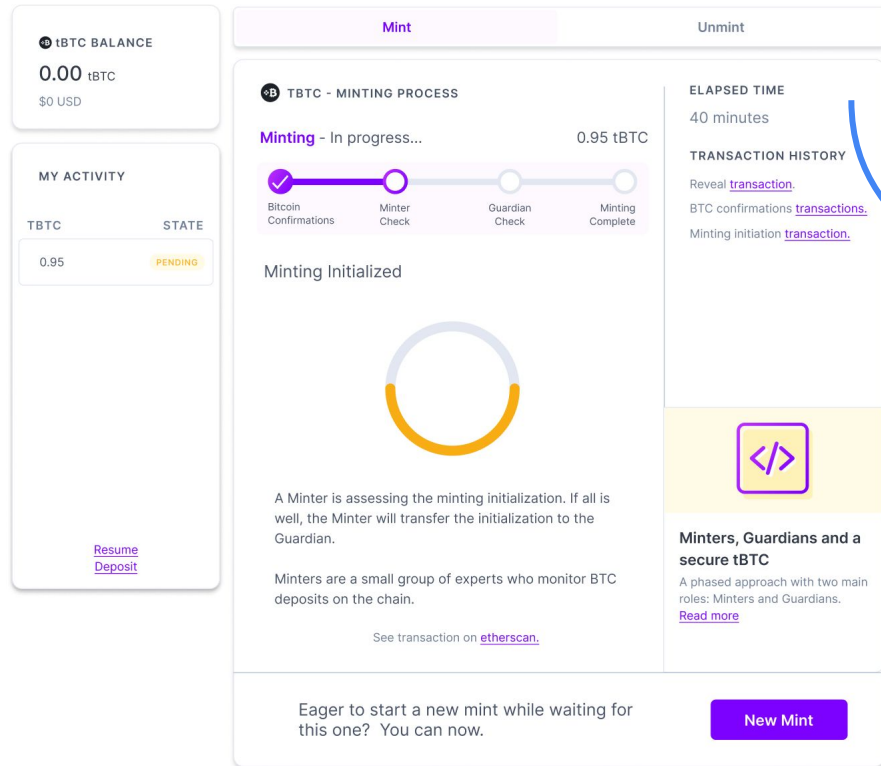
Same with the slide before.

RECOMMENDATION

Same with the slide before.

Findings and Recommendations

VISIBILITY OF SYSTEM



RECOMMENDATION

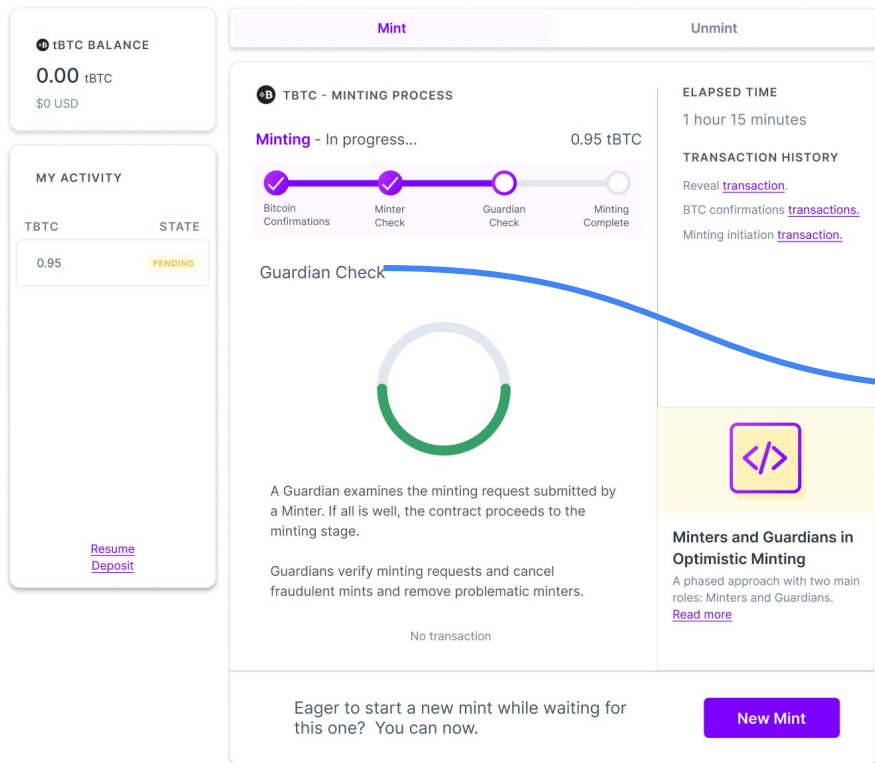
One potential way would be to show here the diagrams of the Optimistic minting so the users can follow the flow under the hood in an easier way rather than in plain text.

FINDING

The elapsed time counter was extremely appreciated and loved.

Findings and Recommendations

VISIBILITY OF SYSTEM



FINDING

The previous finding on Minters applies for Guardians as well.

RECOMMENDATION

The previous recommendation on Minters applies for Guardians as well.

Findings and Recommendations

SUCCESS

tBTC BALANCE

0.95 tBTC

\$39,003.04 USD

MY ACTIVITY

TBTC

STATE

0.95

MINTED

tBTC - MINTING PROCESS

Minted

0.95 tBTC



Bitcoin Confirmations



Minter Check



Guardian Check



Minting Complete

Success!

Add the tBTC [token address](#) to your Ethereum wallet.

Ethereum Gas Cost

~50 gWEI

Bitcoin Miner Fee

0.0002 BTC

Threshold Network Fee

0.01 BTC

New Mint

TOTAL TIME

2 hours 15 minutes

TRANSACTION HISTORY

Reveal [transaction](#).

BTC confirmations [transactions](#).

Minting initiation [transaction](#).

Minting completion [transaction](#).



TBTC CURVE POOL

Deposit In Pool

POOL

APY

TVL

CONTRACT



tBTC/WBTC/sBTC

2.5-> 5.2% CRV

8,200,000.00

0xab4...7792

FINDING

- It was observed that at this stage the timeline is not adding value anymore and it might actually move the focus away from the minted amount and the state of success.
- All of the users mentioned that it would truly be helpful if they were able to have a total of fees denominated in USD.
- Most of the participants were excited by the fact that they had pools right close to the success state, however they weren't sure if Curve is there because Threshold has a preferential relationship with them.
- Total time was extremely appreciated.

Findings and Recommendations

SUCCESS

tBTC BALANCE

0.95 tBTC

\$39,003.04 USD

MY ACTIVITY

TBTC

STATE

0.95

MINTED

tBTC - MINTING PROCESS

Minted

0.95 tBTC



Bitcoin
Confirmations



Minter
Check



Guardian
Check



Minting
Complete

Success!

Add the tBTC [token address](#) to your Ethereum wallet.

Ethereum Gas Cost

~50 gWEI

Bitcoin Miner Fee

0.0002 BTC

Threshold Network Fee

0.01 BTC

New Mint

TOTAL TIME

2 hours 15 minutes

TRANSACTION HISTORY

Reveal [transaction](#).

BTC confirmations [transactions](#).

Minting initiation [transaction](#).

Minting completion [transaction](#).



TBTC CURVE POOL

Deposit In Pool

POOL

APY

TVL

CONTRACT



tBTC/WBTC/sBTC

2.5-> 5.2% CRV

8,200,000.00

0xab4...7792

RECOMMENDATION

- Remove the timeline
- Make the Success and minted amount main focus on this page.
- Add Total for fees denominated in USD.

Findings and Recommendations

UNMINTING

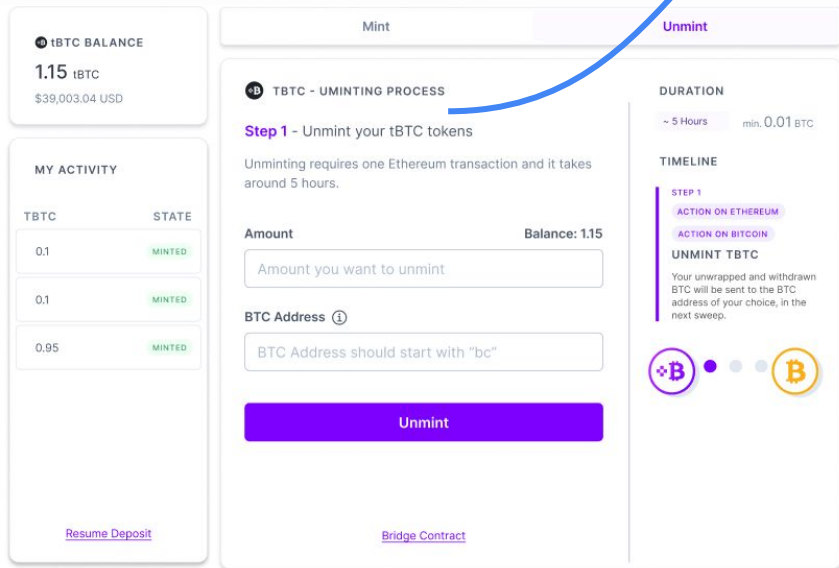
FINDING

Unminting is perceived by the participants as a much much easier process.

The thing that they mostly do not like is that it will take around 5 hours, and they consider this a long time.

RECOMMENDATION

Unless we can do optimistic unminting I do not have a lot of recommendations in this case.



The screenshot displays a web interface for the 'Unmint' process. At the top, there are two tabs: 'Mint' and 'Unmint', with 'Unmint' being the active tab. On the left side, there is a sidebar with two sections: 'tBTC BALANCE' showing '1.15 tBTC' and '\$39,003.04 USD', and 'MY ACTIVITY' which is a table of transactions. The main content area is titled 'tBTC - UNMINTING PROCESS' and includes a 'Step 1 - Unmint your tBTC tokens' section. This section contains a text box for 'Amount' (with a 'Balance: 1.15' label), a 'BTC Address' field with a warning icon and text 'BTC Address should start with "bc"', and a large orange 'Unmint' button. To the right of the main form, there is a 'DURATION' section indicating '~ 5 Hours' and 'min. 0.01 tBTC', and a 'TIMELINE' section showing 'STEP 1' with 'ACTION ON ETHEREUM' and 'ACTION ON BITCOIN' steps, followed by 'UNMINT tBTC' and a description: 'Your unwrapped and withdrawn BTC will be sent to the BTC address of your choice, in the next sweep.' At the bottom of the interface, there is a 'Bridge Contract' link.

TBTC	STATE
0.1	MINTED
0.1	MINTED
0.95	MINTED

[Resume Deposit](#)

[Bridge Contract](#)

Minting experience rating

Average Rating - 4.75

AVERAGE RATING 4.75

Why it didn't score 7? Reasons stated by the participants:

- They do not have access to the How It Works page before accepting the terms.
- It's a steep learning curve.
- The Recovery Receipt is scary and hard to understand.
- Our bridging flow is challenging the average bridge pattern that users are familiar with. (providing data and generating the deposit address)
- Users do not understand which actions are on Bitcoin and which actions are on Ethereum.
- They are confused by the mint term, they do not associate it with the bridge.
- Most of the participants believe that 2-3 hours is too long to bridge.
- They expect their tBTC to land in their wallets right after the deposit.
- Doesn't explain in plain language what is the safety mechanism.
- Some of the participants think that this is "manual" bridge.

Unminting experience rating

Average Rating - 6

AVERAGE RATING 6

I believe this rating is a reaction towards the Minting flow which was perceived super easy. However that being said we need to also be objective and accept that this flow is much much easier.

Why it didn't score 7? Reasons stated by the participants:

- Takes longer than minting.

Final thoughts and takeaways

Things that should be kept in mind

Keeping and Swapping in CEXs

The majority of the participants said that they keep their funds in cold wallets or on CEXs. The ones who particularly use CEXs said that they like to keep their funds in exchanges because it is easier for them to see all of their tokens across multiple blockchains but also it's easier to just swap tokens if they need to do anything.

Bitcoin as a store of value

All the participants we've talked to consider their Bitcoin funds as a store of value, their grey pound, something that that store safely and they would not touch.

They are very cautious with these funds and nothing seems to be worthy of touching them. Only one of them considered maybe bridging their funds only and if only there would be a large yield.

Final thoughts and takeaways

Things that should be kept in mind

Deposit Address Generation - Challenging the web3 bridge pattern

This is a step that no other bridge has and it kind of breaks the seamlessness of the interaction with the bridge. I am not sure if we can do anything about it but I would love to explore and listen to any ideas about how could we address this. Due to the fact that we have a different manner of bridging => a steeper learning curve I believe we should provide a sandbox or a "Demo" where the user can interact and go through the entire flow without having any funds inside. This proposal is based on the finding that all of the users are sending small amounts at first to see how things are working and then based on this experience they will decide to go all in or not.

Lack of Abstraction

Bridges have a horrible experience due to the fact that they require you to have the output native token for gas fees. I have proposed long ago some sort of account abstraction where either the DAO would pay for the gas fees and they would work just like a gas tank. After the bridging they would get their funds back directly from the deposited BTC. Other options can be from different other Account Abstraction protocols. Either way I am a STRONG believer and champion for account abstraction for our bridge.

Final thoughts and takeaways

Recovery Receipts that need to be downloaded by the user

I believe this matter can be handled much better than the current implementation. I believe that we could save for the users the deposit receipts in the dashboard

My thinking here is that we could make use of a gradual reveal of information. This means we should display the Deposit Receipt and drive the user to the Deposit Resuming only and if only necessary. The recovery tutorial and the steps a user needs to take in case of recovery could be displayed under the Resume Deposit category.

The way things are now handled are doing the dApp a disservice in terms of trust and restfulness. We need to keep in mind that bridges as product are already bearing a dark cloud over them and users commonly fear them.

Given this background, when our dApp talks about possible issues we are setting the user into a fight or flight mode instead of a calming and trusting state of mind.

Final thoughts and takeaways

Just like in previous studies participants in this study told me that whenever they are considering using a new protocol, they will first use a very small amount of funds and then they will see what happens.

This behaviour is usually tied to the security of a bridge and to decrease the risk of being rugged or losing a big chunk of funds.

However, this behaviour happens also as a method of learning the way a dApp works. Based on this interaction with the product, the users will decide if they are going to stick with the product or look for something else.

Since the tBTC Bridge dApp comes with some new patterns and challenges the usual bridge experience I propose to support a sandbox inside the dApp that doesn't require actual tokens, and is not on-chain.

This “**sandbox/demo**” will help the users learn the way they need to interact with the bridge without having the stress of fund loss.

I believe this will increase their trust in the actual product when they're going to take the actual actions of bridging.

Takeaways

- Users can't access the How It Works page before accepting the terms.
- The learning curve is steep.
- The Recovery Receipt is complex and intimidating.
- Our bridging flow challenges the average bridge pattern that users are used to.
- Users are unclear about actions on Bitcoin versus actions on Ethereum.
- There's confusion around the term "mint" and its association with the bridge.
- Most participants think 2-3 hours is too long to bridge.
- Users expect tBTC to appear in their wallets immediately after deposit.
- There's a lack of simple language explaining the safety mechanism.
- Some participants perceive the bridge as "manual."

Keeping and Swapping in CEXs

- Majority of participants store funds in cold wallets or CEXs.
- Users prefer CEXs for easier overview of tokens across multiple blockchains and ease of token swapping.

Takeaways

Bitcoin as a store of value

- Participants consider Bitcoin as a store of value.
- There's a high degree of caution with Bitcoin funds, and only high yields might persuade them to bridge these funds.

Deposit Address Generation

- The additional step of deposit address generation breaks the seamlessness of bridge interaction.
- Suggestions include creating a sandbox or "Demo" for users to practice the flow without risking funds.

Lack of Abstraction

- Bridges are criticized for requiring the output native token for gas fees.
- There's a strong advocacy for account abstraction where gas fees could be covered by the DAO or other Account Abstraction protocols.

Takeaways

Recovery Receipts

- The current requirement for users to download recovery receipts could be improved.
- Proposals include storing deposit receipts in the dashboard and only revealing information as necessary.

Overall

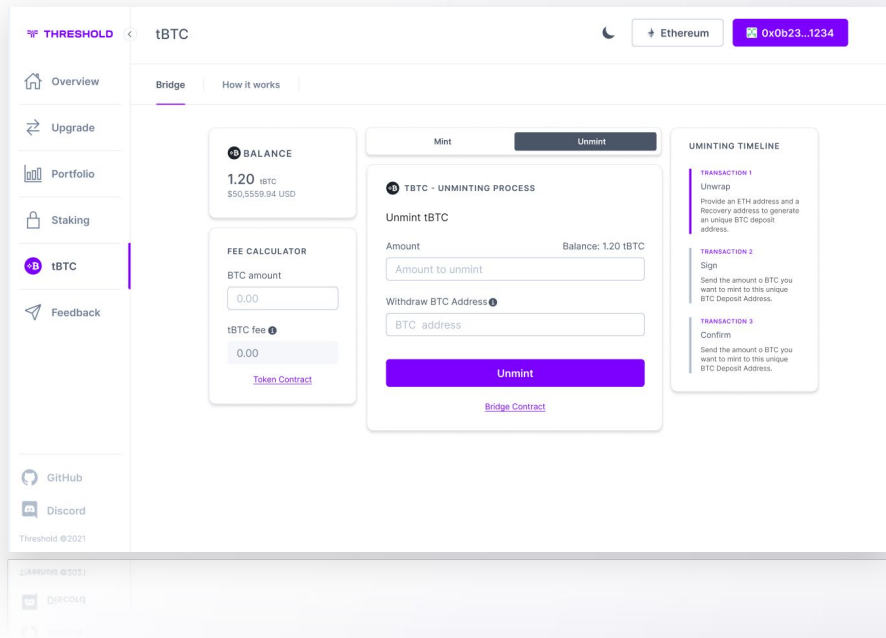
- The app may cause fear and uncertainty, as bridges are generally feared.
- Users test new protocols with small amounts to reduce risk and understand the platform.
- A sandbox inside the dApp that doesn't require actual tokens and is not on-chain to increase trust and comfort with the process.

What's Next

NEXT STEPS

Following this iterative user study the next action will be taken:

- Include the findings in the new design iteration of the tBTC dApp
- Run a new set of Usability Tests with at least 5 people



**Love your
users!**

