2022

Bitcoin DeFi: The Good, The Bad, The Ugly

Alexei Zamyatin
Bitcoin Austria Meetup, 23 August 2022

Disclaimer:
This talk is purely informative and does not constitute any form of financial advice.

Mentions of specific projects are not endorsements.

I am the co-founder of Interlay, a project that is building decentralized infrastructure to use BTC on other blockchains. Some of the projects mentioned in this talk are direct competitors to Interlay. While I do my best to be neutral and “wear” my academic researcher hat, please always DYOR.

Preliminaries

What is DeFi?

Short for decentralized finance, DeFi is an umbrella term for peer-to-peer financial services on public blockchains, primarily Ethereum. (from: Coinbase)

derivatives
interest
lend
trade
buy insurance
borrow

+

Global
Digital
Peer-to-peer
Open-to-all
Pseudonymous
Transparent

At the core of DeFi: Fair Exchange

A very very old problem.

Alice and Bob exchange goods, such that:

- Alice and Bob both get the goods
- Trade does not happen (Alice and Bob keep their goods)

→ **atomically!**

(In the digital world) someone **must make the first move**.

To ensure fairness in 100% of cases: **need a Trusted Third Party**

DeFi tries to use blockchain networks as “Trusted” Third Parties

Centralized exchange

Trading logic
enforced by
exchange operator

Organization of people.
Top-down decision-making.

Database
History can be changed by admin

Centralized exchange

Trading logic
enforced exchange

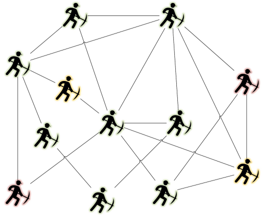
Organization of people.
Top-down decision-making.

Database
History can be changed by admin

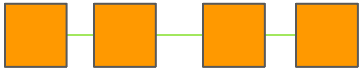
VS

Decentralized exchange

Trading logic
enforced by decentralized network.



Decentralized network of pseudonymous participants.
Majority-based decision.



Blockchain
Immutable. History can be changed but needs complete rewrite & 50%+ agreement.

What makes something “decentralized”?

There is always some form of trust & centralization when using crypto.

- Blockchain secure
- Your private keys not corrupted

→ We look into **additional trust assumptions**.

Decentralized and Trustless

Suggested (for this talk):

- **Decentralized** = **no single point of failure** & **anyone can participate** in operating the service (you don't need to ask permission!)
- **Trustless** = too broad and difficult to quantify. Better:
  - **Non-custodial**: no-one can access your funds, at all.
  - **Financially trustless**: your funds can be lost, but the system will (provably) try to reimburse you, e.g. in some other assets

DeFi Crash Course

And how DeFi products differ from traditional finance

Trading

= exchange BTC for some other (digital) asset

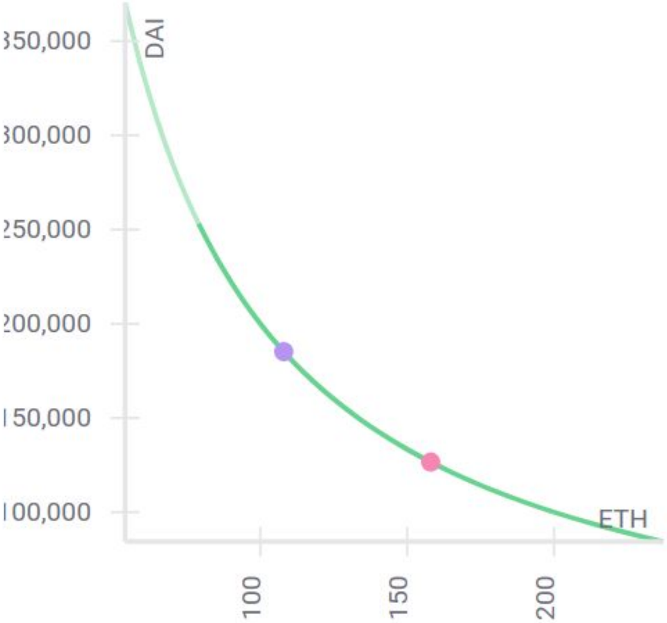
Already discussed: Fair exchange

- Needs some way to make sure trade is atomic

→ Use “smart contract” enforced by the decentralized network

Example: Uniswap

AMMs



Traditional exchanges = order books (buyer/seller)

DeFi → AMMs

- Trades happen along a “curve”
- Each buy / sell moves the current price

Most typical: “xyk” AMMs

→ exponential price increase as we get close to 0 supply of one asset

Liquidity providers “lend” capital to the pool → traders can use trading → LPs earn fees

Want to try it out? https://amm-playground.on.fleek.co/

Money Markets

E.g. Aave, Compound

= Borrowing and Lending

Traditional world: put down some mortage / collateral.

- Car, house. Vault not always more than credit → legal system

DeFi: No legal system, pseudonymous participants.

→ **Everything is over-collateralized** (because of price swings)

→ **Price oracles** to track price (off vs on-chain)

→ **Liquidations** if collateral drops to far

Stablecoins / Synthetics

= mint an token that tracks the price of another, existing asset.

Most prominent: USD stablecoins

1. Lock collateral (e.g. 150% ratio)
2. Get USD-tracking token
3. Use token
4. Return token & pay fees
5. Withdraw collateral

Risk: Liquidation is collateral price drops too far

Why? Long/short positions without selling your collateral

E.g. MakerDAO’s DAI

Derivatives

Complex set of products to bet on BTC price / hedge BTC price risk.

→ “Go long” vs “go short”

Options, futures, perpetual swaps, margin trading…

Mix of:

- **Fair exchange**
- **Price oracles** to track price (off vs on-chain)
- **Over-collateralization & liquidations**

Very new field → not many established yet (e.g. dydx, Opyn)

Bitcoin DeFi Landscape

Where can we use Bitcoin?

	On Bitcoin	On centralized platforms (incl. custodial wallets)	On other chains
What do I need?	Bitcoin wallet	Account on platform (may need KYC)	Wallet on other chain; a bridge
What do I trust?	Bitcoin network is secure; Wallet not corrupted;	Bitcoin network is secure; Wallet not corrupted; Provider is solvent & honest.	Bitcoin network is secure; Other network is secure; Wallets not corrupted; Bridge is not corrupted (might be centralized).
How can I check?	Open source code	Reputation of provider? (rare: open source code)	Open source code (but might not always be available); Reputation of provider if centralized.

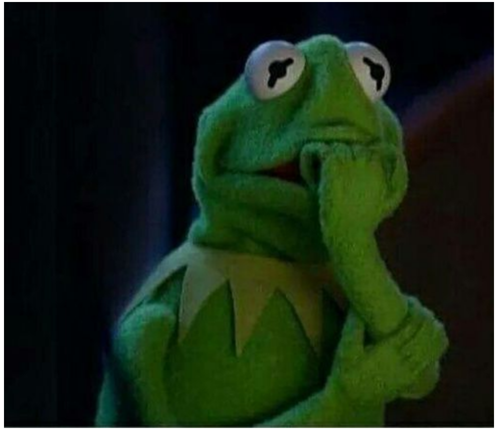
In this talk:

	On Bitcoin	~~On centralized platforms (incl. custodial wallets)~~	On other chains
What do I need?	Bitcoin wallet	~~Account on platform (may need KYC)~~	Wallet on other chain; a bridge
What do I trust?	Bitcoin network is secure; Wallet not corrupted;	~~Bitcoin network is secure;~~ ~~Wallet not corrupted;~~ ~~Provider is solvent & honest~~	Bitcoin network is secure; Other network is secure; Wallets not corrupted; Bridge is not corrupted (might be centralized).
How can I check?	Open source code	~~Reputation of provider? (rare: open source code)~~	Open source code (but might not always be available); Reputation of provider if centralized.

Bitcoin-native DeFi

Strictly on the Bitcoin blockchain

Not really much there... yet!



DeFi on Bitcoin - Requirements

1. **Some way to represent other assets**
   - Colored coins: used OP_RETURN to taint and track coins
   - Taro: uses special Merkle Trees to represent assets (enabled by the Taproot upgrade)
   - RGB?

2. **Some way to exchange assets without trusting a 3rd party**
   - Atomic swaps using HTLCs (or other constructions)

3. **Ways to react to price changes**
   - DLCs

Outlook: Stuff *is* happening

1. **Some way to represent other assets** ⏳
    - Colored coins: used OP_RETURN to taint and track coins
    - Taro: uses special Merkle Trees to represent assets (enabled by the Taproot upgrade)
    - RGB?

Question: who mints these assets? → **USDT-like or synthetics (e.g. stablesats)?**

2. **Some way to exchange assets without trusting a 3rd party** ✅
    - Atomic swaps using HTLCs (or other constructions)

3. **Ways to react to price changes** ⏳
    - DLCs ... **but still needs a centralized oracle**

Is BTC <> Fiat considered DeFi?

The involvement of fiat generally means that you need an “arbitration” service.

→ Resolve disputes if you sent USD but BTC withheld (or vice versa)

→ No way to check on Bitcoin programmatically

Always needs a 3rd party

→ Not really DeFi

P2P Bitcoin-Fiat Trading

- **Bisq**. Multisig between seller and buyer - with timelock spend to Bisq.

  → Bisq gets funds and resolves in case of dispute

- **Hodl hold**. Multisig with Hodl Hodl

  → Hodl hodl acts as mediator to clear trades

- **Localbitcoins**. Secrets released by buyer or arbitrator to execute transaction.

  → Arbitrator can execute the trade or refund

P2P Bitcoin Lending

- **Hodl hold**. Multisig with Hodl Hodl

  → Hodl hodl acts as mediator to clear trades

Others?

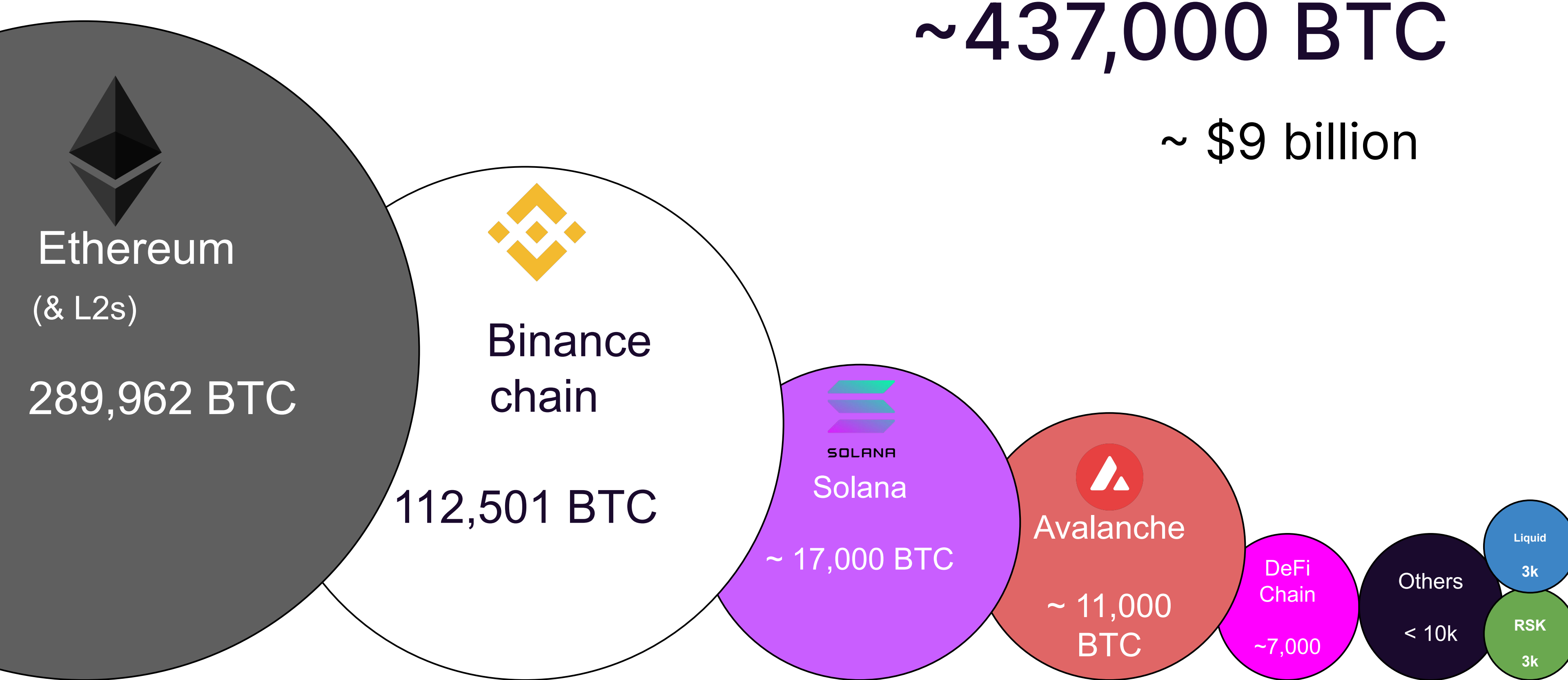
Bitcoin DeFi - On other Chains

Leveraging smart contracts and bridges

Bitcoin on other chains

~437,000 BTC

~ $9 billion



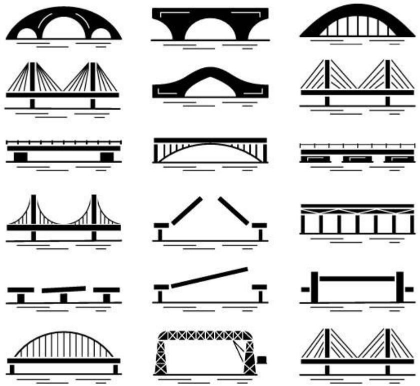
How do I use BTC on other chains?

BTC only exists on Bitcoin. To use it on other chains, BTC needs to be “wrapped”.

Wrapping = create a 1:1 representation of BTC on another network, i.e., as a native token.

Analogy: deposit BTC onto an exchange

→ Done via “**Bridges**”



How does wrapping work?

Mint

1. Lock BTC on Bitcoin
2. Issuer on target network verifies the lock
3. Issuer mints a native “wrapped BTC” token at a 1:1 rate (minus fees)

Redeem

1. Return wrapped BTC to issuer on the target network
2. Issuer sends BTC to your Bitcoin wallet at a 1:1 rate (minus fees)
3. Wrapped BTC is deleted (“burned”)

Important: The Issuer can be an individual, a group of people (multisig), or a smart contract (enforced by consensus)

That’s great!

But there’s a catch

Wrapping is dangerous

Why? Requirements:

- **Lock** BTC while wrapped BTC is being used
- **Unlock** BTC when wrapped BTC is returned

Challenge: Bitcoin cannot react to external events

→ **Someone** needs to do the locking and unlocking

Question to ask: How much do you need to trust this **someone**?

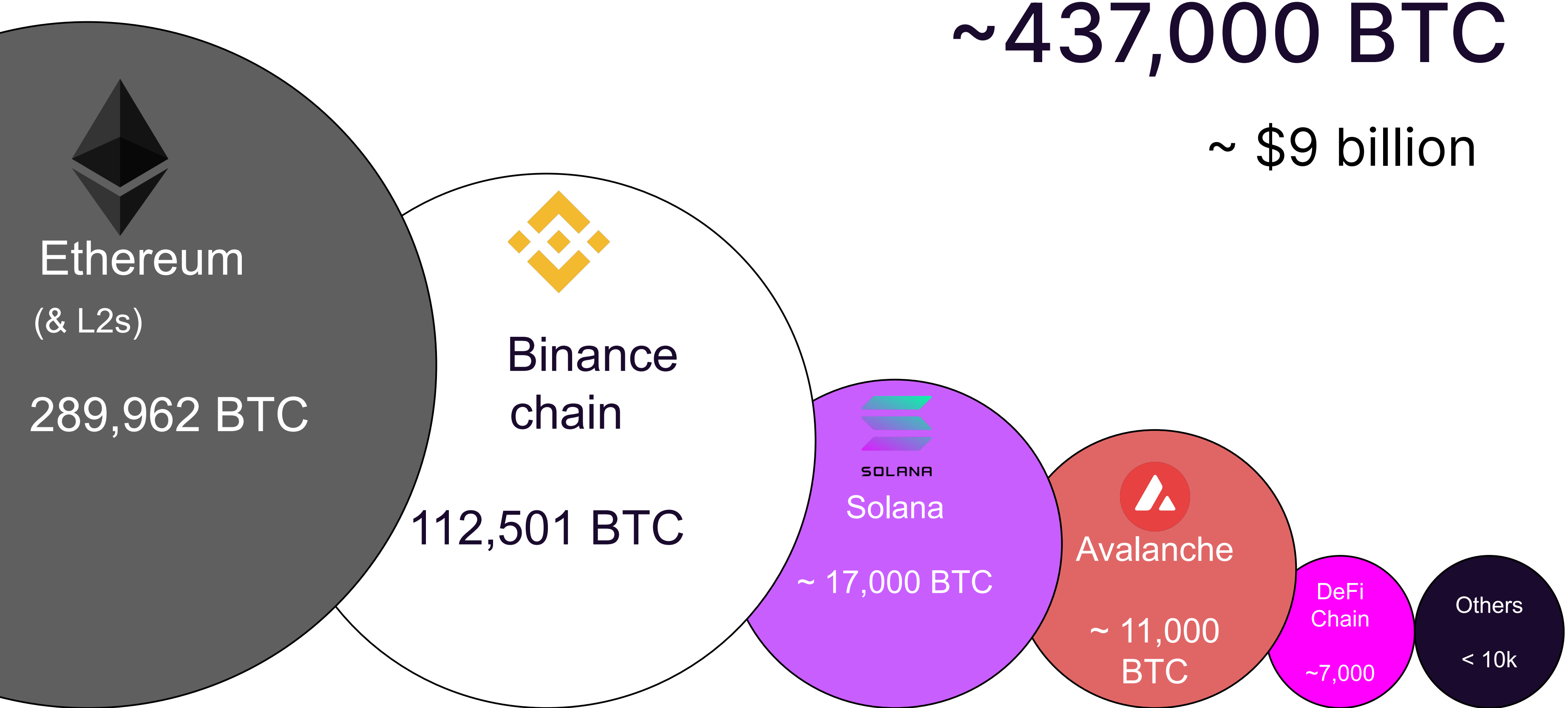
Reminder: Trust Models

	On Bitcoin	**On other chains**
What do I need?	Bitcoin wallet	Wallet on other chain; a bridge
What do I trust?	Bitcoin network is secure; Wallet not corrupted;	Bitcoin network is secure; Other network is secure; Wallets not corrupted; Bridge is not corrupted (might be centralized).
How can I check?	Open source code	Open source code (but might not always be available); Reputation of provider if centralized.

Bitcoin on other chains

~437,000 BTC

~ $9 billion



Ethereum

(& L2s)

289,962 BTC

Binance chain

112,501 BTC

SOLANA

Solana

~ 17,000 BTC

Avalanche

~ 11,000 BTC

DeFi Chain

~7,000

Others

< 10k

How much is decentralized?

How much is decentralized?

< 0.5 % (~2000 BTC)

~1,700 on Thorchain

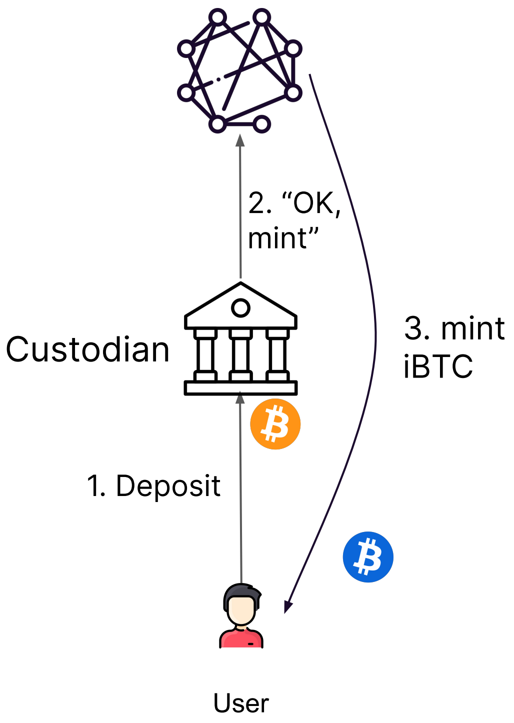
~ 300 on tBTC

~ 80 on Interlay & networks

What makes a bridge decentralized?

Most (centralized) bridges:

Mint:



2. “OK, mint”

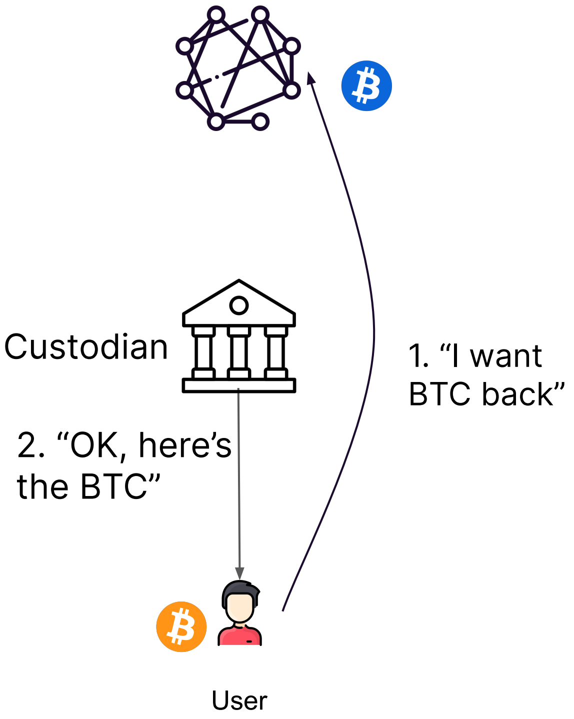
Custodian

3. mint iBTC

1. Deposit

User

Redeem (success):



Custodian

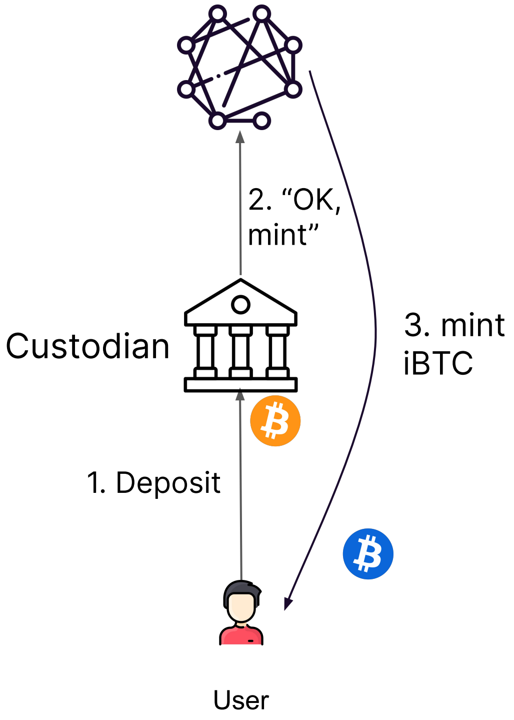
1. “I want BTC back”

2. “OK, here’s the BTC”

User

Most (centralized) bridges:

Mint:



Custodian

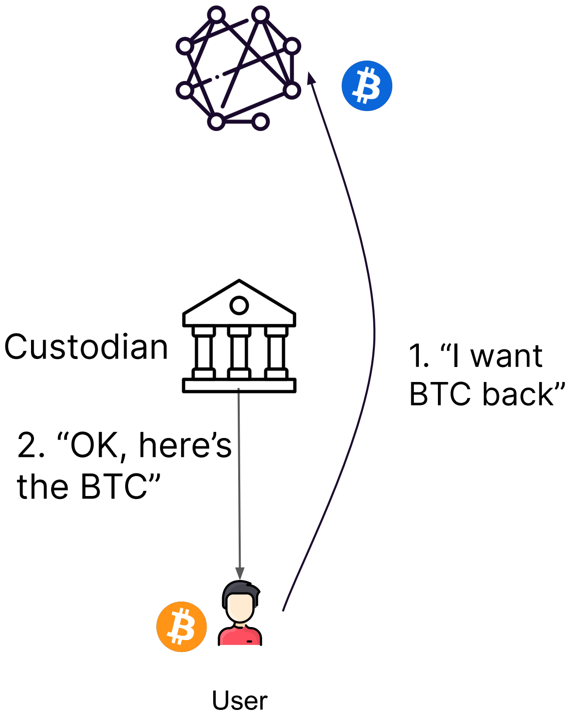
1. Deposit

2. “OK, mint”

3. mint iBTC

User

Redeem (success):



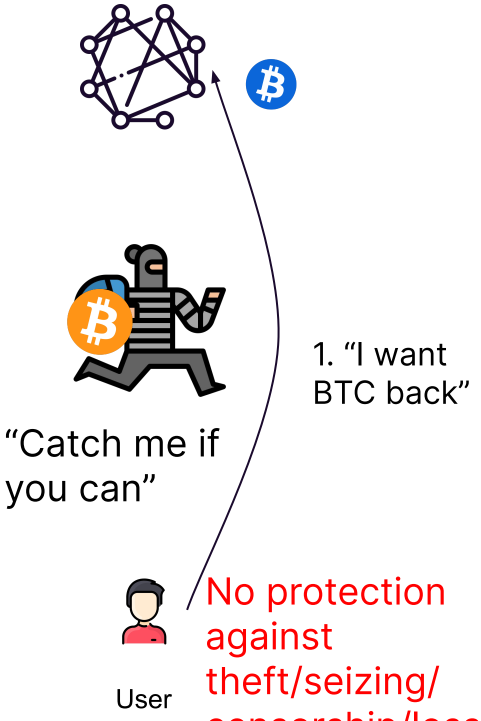
Custodian

1. “I want BTC back”

2. “OK, here’s the BTC”

User

Redeem (fail):



“Catch me if you can”

1. “I want BTC back”

User

No protection against theft/seizing/ censorship/loss.

Custodian types

A custodian can be a single entity or a group / “federation” (=multisig).

Often, bridges will use fancy terms, obfuscating the trust model:

- Multi-party computation **= multig**
- Threshold signatures **= multig**
- Trusted hardware **= trust that there is no new Intel SGX hack**

These are all nice “additions”, and may work in practice… until they don’t

→ In the end, you trust that group of people will not steal your BTC

How to build a decentralized bridge?

1) Allow **anyone** to become a operator/custodian

How to build a decentralized bridge?

1) Allow **anyone** to become a operator/custodian

2) Realize this is even worse... now we're **sending BTC to random people on the internet**

How to build a decentralized bridge?

1) Allow **anyone** to become a operator/custodian

2) Realize this is even worse… now we're sending BTC to random people on the internet

3) Use same tools as Bitcoin to fix:

- **Incentives:** operators lock collateral
- **Punishment:** if operator misbehaves, slash collateral (& reimburse victims)

History of Decentralized BTC bridges

First design in 2018... by me :)

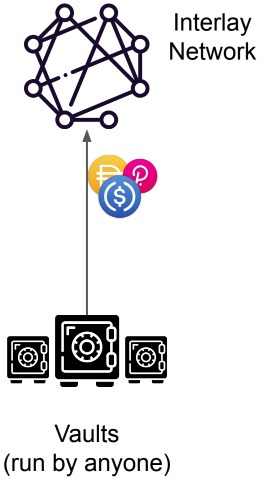
Presented at Scaling Bitcoin 2018

First deployment: tBTC on Ethereum in 2020 (*with some tweaks that broke it a bit :/*)

Example: interBTC

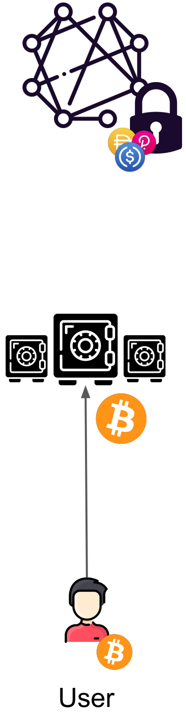
0. Vaults Register

Vaults deposit collateral



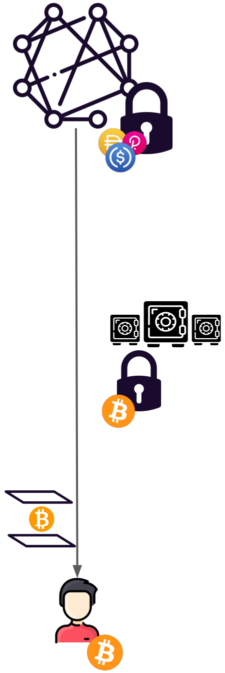
1. Lock BTC

User: Lock BTC



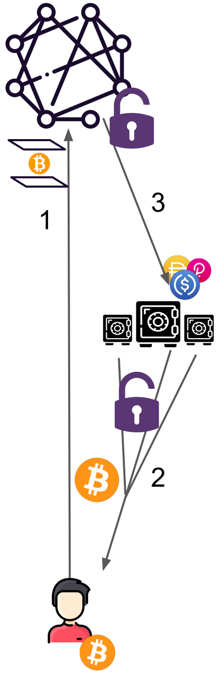
2. Mint iBTC

Chain: Mint iBTC to User



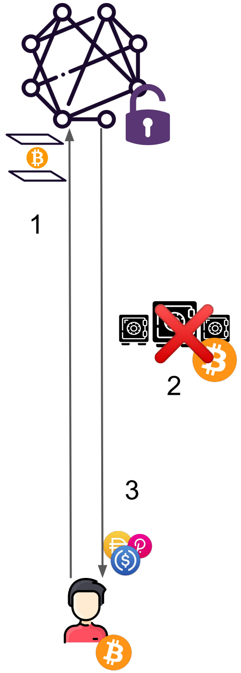
3a. Redeem (Good Vault)

1. User returns iBTC,
2. Vault returns BTC to user,
3. Vault collateral unlocked



3b. Reimburse (Bad Vault)

1. User returns iBTC,
2. Vault fails,
3. User is reimbursed (or tries different Vault)



How to verify BTC payments?

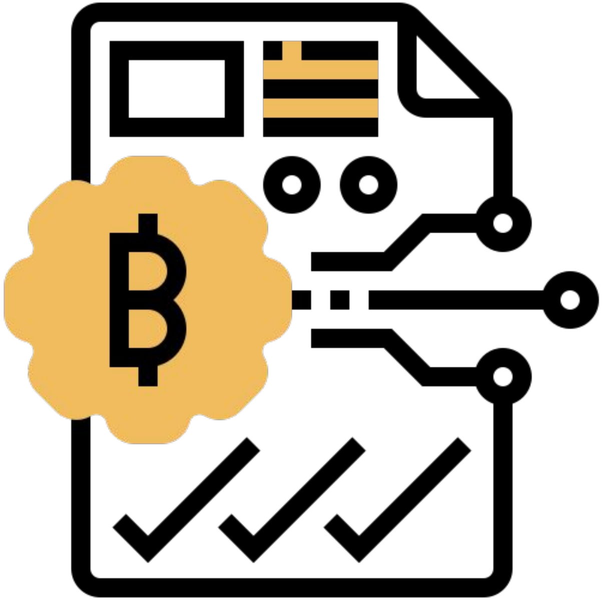
Bitcoin light client deployed as a smart contract

→ **Track** all Bitcoin block headers

→ **Verify** Bitcoin transactions

Concept: if in Bitcoin main chain → must be valid

(same as any mobile wallet)



Decentralized BTC Bridges

Thorchain: deposit BTC liquidity into Thorchain AMM

- **BTC secured:** stakers of native Rune token, arranged into 3-5 groups of 16 signers (threshold sig)
- **Verification:** Non-cryptographic; Thorchain nodes must vote
- **Indirect insurance:** if a group loses BTC, Rune is slashed and deployed into the trading pools for arbitrage against BTC → arb traders can profit.

tBTC: use BTC on Ethereum

- **BTC secured:** open-for-all network of overcollateralized signers; 3 signers per “Vault” (threshold sig)
- **Verification:** BTC light client
- **Direct insurance:** ETH, paid to user or liquidator

interBTC: use BTC on Polkadot (& soon Cosmos, Ethereum)

- **BTC secured:** open-for-all network of overcollateralized Vaults. Vault can be solo or group-managed.
- **Verification:** BTC light client
- **Direct insurance:** multi-collateral, paid to user or liquidator

Side note:
There are **no**
non-custodial bridges…

… yet

BTC Synthetics

= cannot be redeemed for BTC. Pegged to value of BTC, backed by some other collateral assets

How it works?

1. Deposit collateral, e.g. in USDC
2. You get *USDC * exchange rate * collateralization ratio* in BTC
   a. E.g. 40k USDC give you 1 BTC at current $21k/BTC price
3. Use BTC synthetic
4. Close position and pay **loan repayment fees** (“stability fee”)

→ Basically, you are borrowing a BTC-pegged asset from the protocol treasury.

Risk: if collateral drops too far, your position is liquidated (e.g. at 120%)

Where to people use BTC in DeFi?

Case study: Ethereum

Wrapped BTC on Ethereum

- wBTC (247k BTC): **centralized**, minted mainly by institutions or via exchanges

- hBTC (39k BTC): **centralized** minted via Huobi exchange. Most held by 1 account?
- renBTC (3k BTC): **centralized**, mint/redeem by anyone, BTC held in team multisig*
- imBTC (790 BTC): **centralized**, minted via Tokenlon (?)
- sBTC (599): **decentralized synthetic** , minted by locking SNX token
- tBTC (330): **decentralized, insured by ETH**, minted by locking BTC with Signers (but changing model for v2… → removing/reducing insurance)

Source: https://dune.com/eliasimos/btc-on-ethereum_1

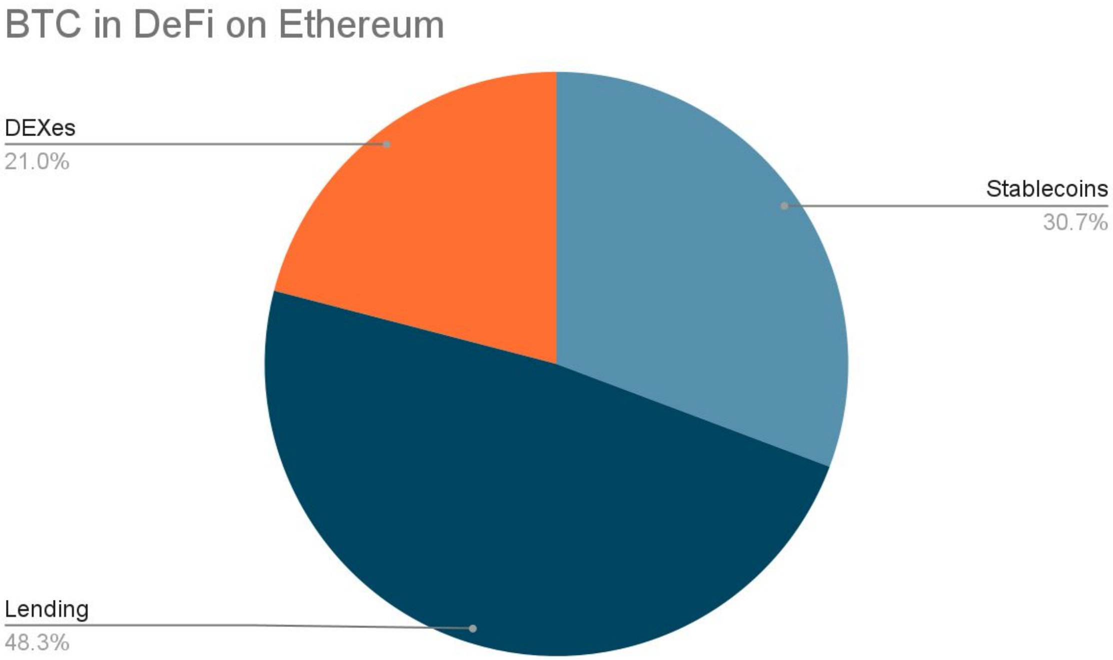
* claimed to be decentralized, then “path to decentralization” when multisig uncovered

Main use cases

1. **Lending** (Compound, Aave)

2. **Stablecoin collateral** (DAI)

3. **Trading / yield farming** (Uniswap, Curve, Balancer)



Source: https://etherscan.io/

Lending

- Low-risk, passive income, while going long BTC

→ But: low utilization

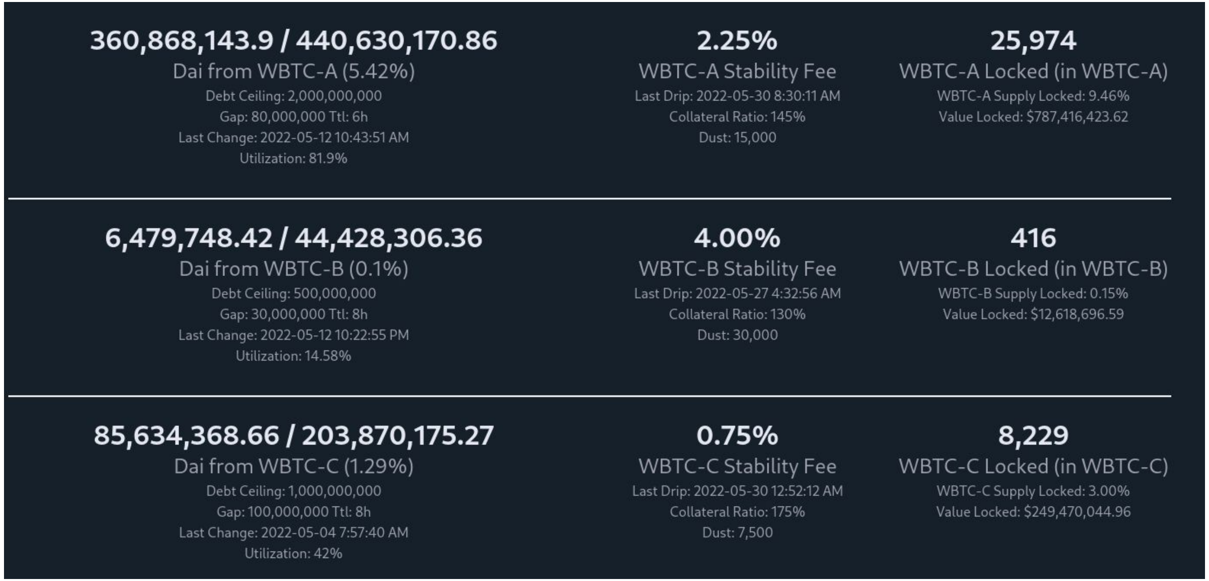
Protocol	Supplied	Borrowed	Utilization	Supply APY	Borrow APR
Aave	39.34k wBTC	1.3k wBTC	3.3%	0.01%	Variable 0.53% Stable 3.72%
Compound	35.03k wBTC	954 wBTC	2.7%	0.06% (for comparison: DAI 1.49% USDT 2.07%)	2.98% (for comparison: DAI 3.20% USDT 3.62%)

Stablecoin collateral

Mint DAI and use in DeFi (e.g. again lending/borrowing), while going long BTC

Mainly: Compound (lending) and LPs into Uniswap and Curve pools

→ Revenue made from using DAI must exceed stability fees



360,868,143.9 / 440,630,170.86
Dai from WBTC-A (5.42%)
Debt Ceiling: 2,000,000,000
Gap: 80,000,000 Ttl: 6h
Last Change: 2022-05-12 10:43:51 AM
Utilization: 81.9%

2.25%
WBTC-A Stability Fee
Last Drip: 2022-05-30 8:30:11 AM
Collateral Ratio: 145%
Dust: 15,000

25,974
WBTC-A Locked (in WBTC-A)
WBTC-A Supply Locked: 9.46%
Value Locked: $787,416,423.62

6,479,748.42 / 44,428,306.36
Dai from WBTC-B (0.1%)
Debt Ceiling: 500,000,000
Gap: 30,000,000 Ttl: 8h
Last Change: 2022-05-12 10:22:55 PM
Utilization: 14.58%

4.00%
WBTC-B Stability Fee
Last Drip: 2022-05-27 4:32:56 AM
Collateral Ratio: 130%
Dust: 30,000

416
WBTC-B Locked (in WBTC-B)
WBTC-B Supply Locked: 0.15%
Value Locked: $12,618,696.59

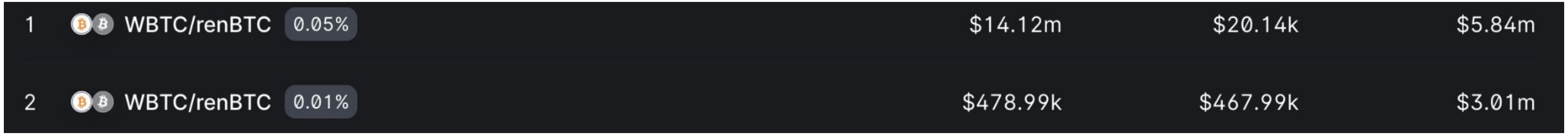
85,634,368.66 / 203,870,175.27
Dai from WBTC-C (1.29%)
Debt Ceiling: 1,000,000,000
Gap: 100,000,000 Ttl: 8h
Last Change: 2022-05-04 7:57:40 AM
Utilization: 42%

0.75%
WBTC-C Stability Fee
Last Drip: 2022-05-30 12:52:12 AM
Collateral Ratio: 175%
Dust: 7,500

8,229
WBTC-C Locked (in WBTC-C)
WBTC-C Supply Locked: 3.00%
Value Locked: $249,470,044.96

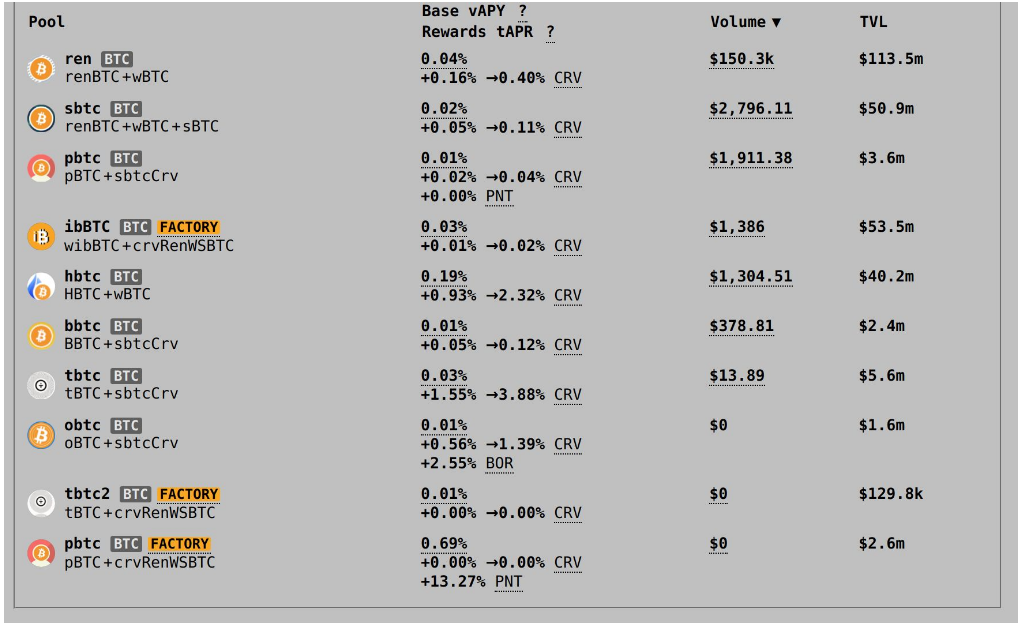
Trading

Mostly arbitrage trading between different wrapped BTC assets



1	WBTC/renBTC	0.05%	$14.12m	$20.14k	$5.84m
2	WBTC/renBTC	0.01%	$478.99k	$467.99k	$3.01m

Uniswap

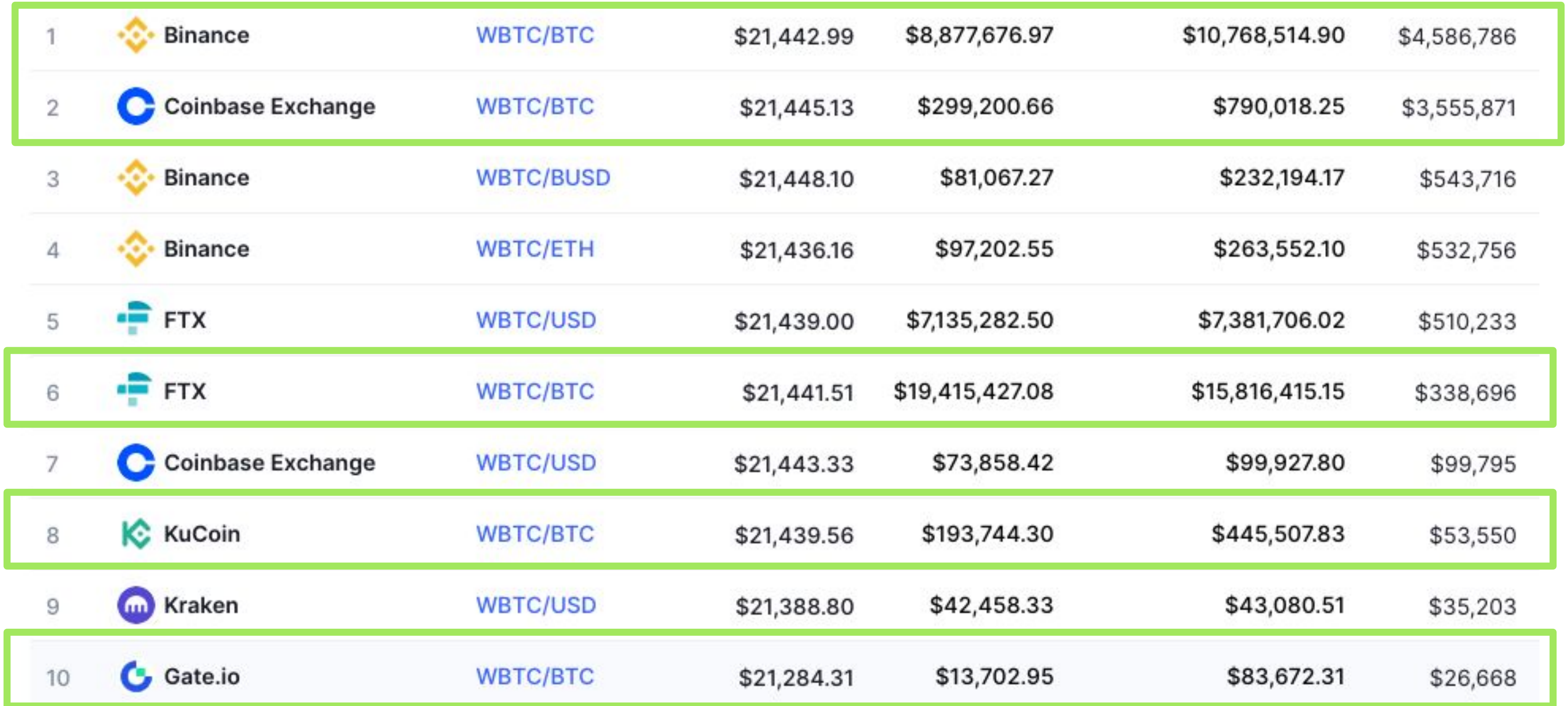


Pool	Base vAPY ? Rewards tAPR ?	Volume ▼	TVL
ren BTC renBTC+wBTC	0.04% +0.16% →0.40% CRV	$150.3k	$113.5m
sbtc BTC renBTC+wBTC+sBTC	0.02% +0.05% →0.11% CRV	$2,796.11	$50.9m
pbtc BTC pBTC+sbtcCrv	0.01% +0.02% →0.04% CRV +0.00% PNT	$1,911.38	$3.6m
ibBTC BTC FACTORY wibBTC+crvRenWSBTC	0.03% +0.01% →0.02% CRV	$1,386	$53.5m
hbtc BTC HBTC+wBTC	0.19% +0.93% →2.32% CRV	$1,304.51	$40.2m
bbtc BTC BBTC+sbtcCrv	0.01% +0.05% →0.12% CRV	$378.81	$2.4m
tbtc BTC tBTC+sbtcCrv	0.03% +1.55% →3.88% CRV	$13.89	$5.6m
obtc BTC oBTC+sbtcCrv	0.01% +0.56% →1.39% CRV +2.55% BOR	$0	$1.6m
tbtc2 BTC FACTORY tBTC+crvRenWSBTC	0.01% +0.00% →0.00% CRV	$0	$129.8k
pbtc BTC FACTORY pBTC+crvRenWSBTC	0.69% +0.00% →0.00% CRV +13.27% PNT	$0	$2.6m

Curve

Interesting: also on CEX

Highest volume = wBTC/BTC arb



1	Binance	WBTC/BTC	$21,442.99	$8,877,676.97	$10,768,514.90	$4,586,786
2	Coinbase Exchange	WBTC/BTC	$21,445.13	$299,200.66	$790,018.25	$3,555,871
3	Binance	WBTC/BUSD	$21,448.10	$81,067.27	$232,194.17	$543,716
4	Binance	WBTC/ETH	$21,436.16	$97,202.55	$263,552.10	$532,756
5	FTX	WBTC/USD	$21,439.00	$7,135,282.50	$7,381,706.02	$510,233
6	FTX	WBTC/BTC	$21,441.51	$19,415,427.08	$15,816,415.15	$338,696
7	Coinbase Exchange	WBTC/USD	$21,443.33	$73,858.42	$99,927.80	$99,795
8	KuCoin	WBTC/BTC	$21,439.56	$193,744.30	$445,507.83	$53,550
9	Kraken	WBTC/USD	$21,388.80	$42,458.33	$43,080.51	$35,203
10	Gate.io	WBTC/BTC	$21,284.31	$13,702.95	$83,672.31	$26,668

Derivatives & co

Not covered in detail because this is highly risky and protocols are mostly new

→ need to know what you are doing.

Most use synthetics → purely betting on price.

Settlement in stablecoins.

For those interested: https://defiprime.com/derivatives

RSK

What is RSK?

- L1 chain with Ethereum-style smart contracts
- Merged mined with Bitcoin
- BTC bridge:
  - **BTC secured**: Federation multisig
  - **Verification**: Centralized
  - **Insurance**: None

RSK hopes to achieve a Bitcoin soft fork since 2015 to launch Drivechains
→ Miners would control the BTC bridge. Unlikely to happen at this point

DeFi ecosystem: https://defillama.com/chain/RSK

- Money on chain: USD stablecoin and BTC investment products
- Sovryn: DEX with derivative products

What about Atomic Swaps?

If we have time

Conclusion

Conclusion

The Good:

- Lots of development on Bitcoin itself
- High demand for BTC across all other chains
- Easy to access DeFi on other chains as alternative to centralized platforms

The Bad:

- Bitcoin tooling still early and very complex
- 99% of BTC bridges are centralized → not true DeFi

The Ugly:

- Many BTC bridges wrongly market themselves as “DeFi” or non-custodial

Thanks!

Feel to reach out at:

Twitter: @alexeiZamyatin
Email: alexei+btcdefi@interlay.io
Website: alexeizamyatin.me

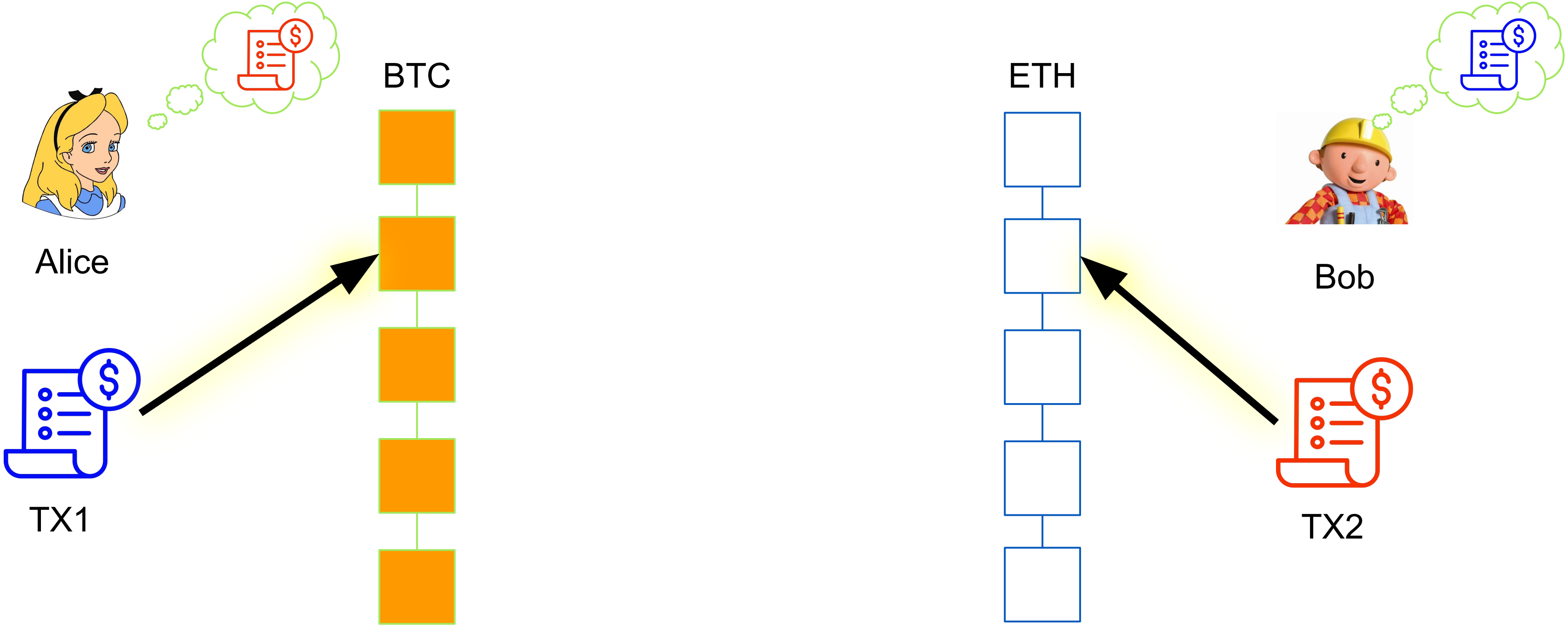
Check out what we are doing at Interlay:

Twitter: @interlayHQ
Website: Interlay.io
Community: linktr.ee/interlay

Atomic Swaps

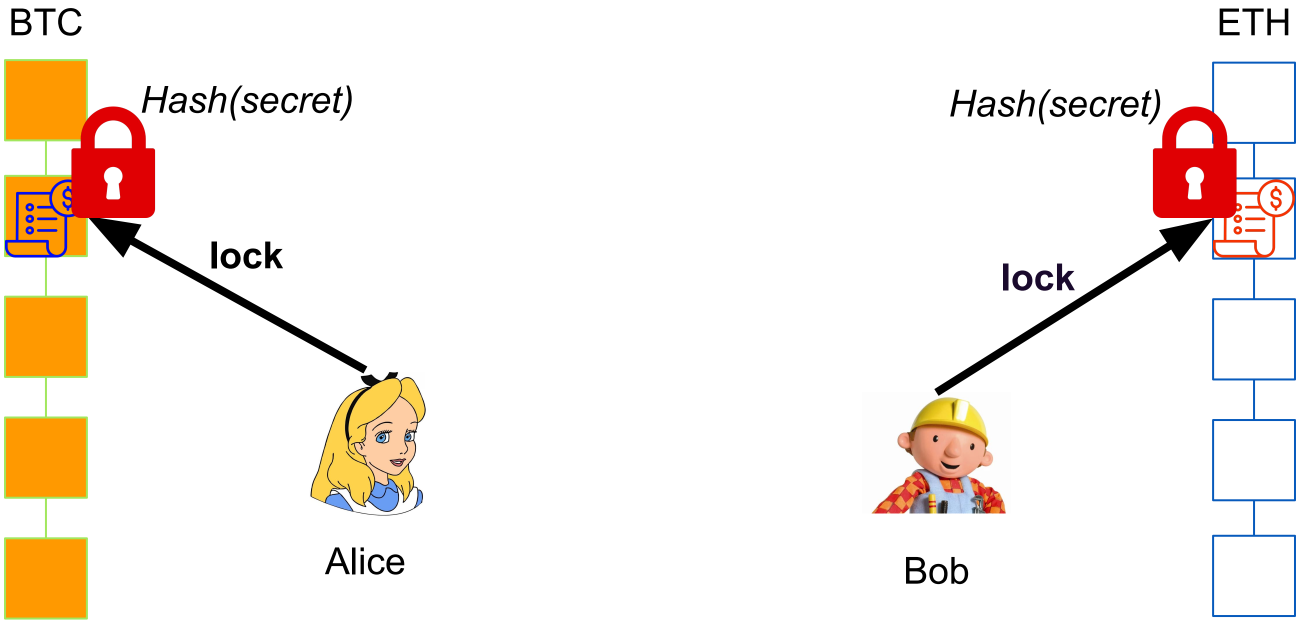
Fair Exchange

TX1 gives BTC to Bob
TX2 gives ETH to Alice ➡ Fair Exchange of assets



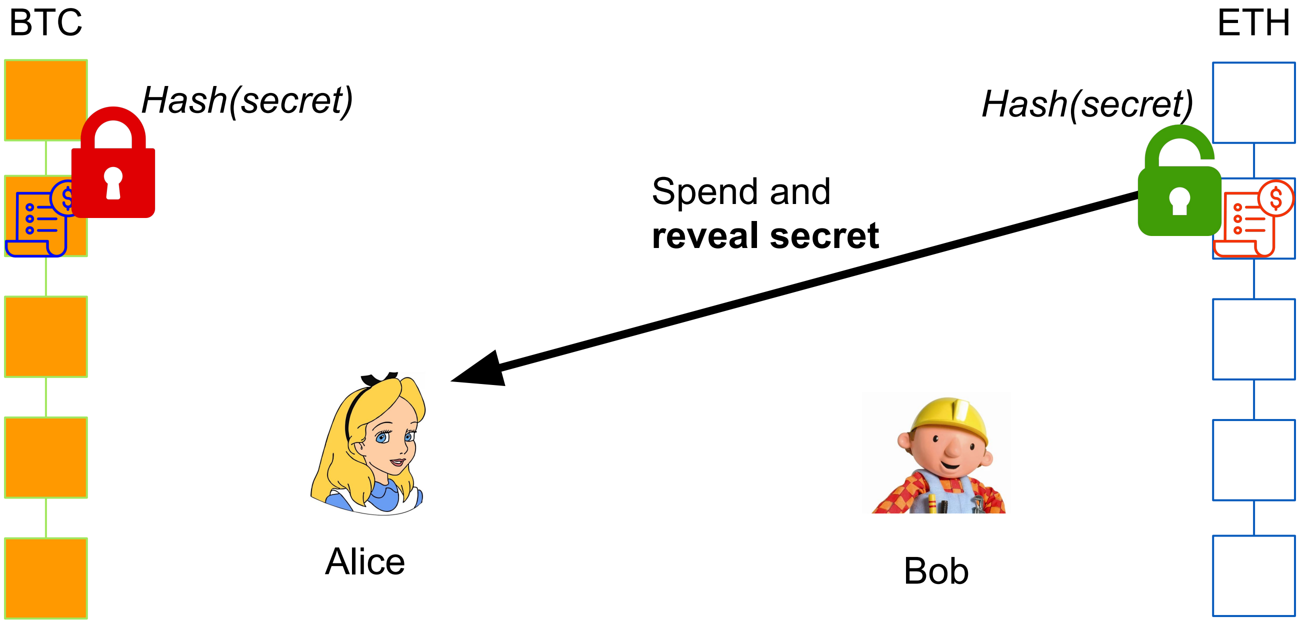
Atomic Swaps via HTLCs

Alice and Bob lock coins with the **same** lock on both chains.
HTLCs: hash lock (coins can be spent if pre-image/secret is revealed)



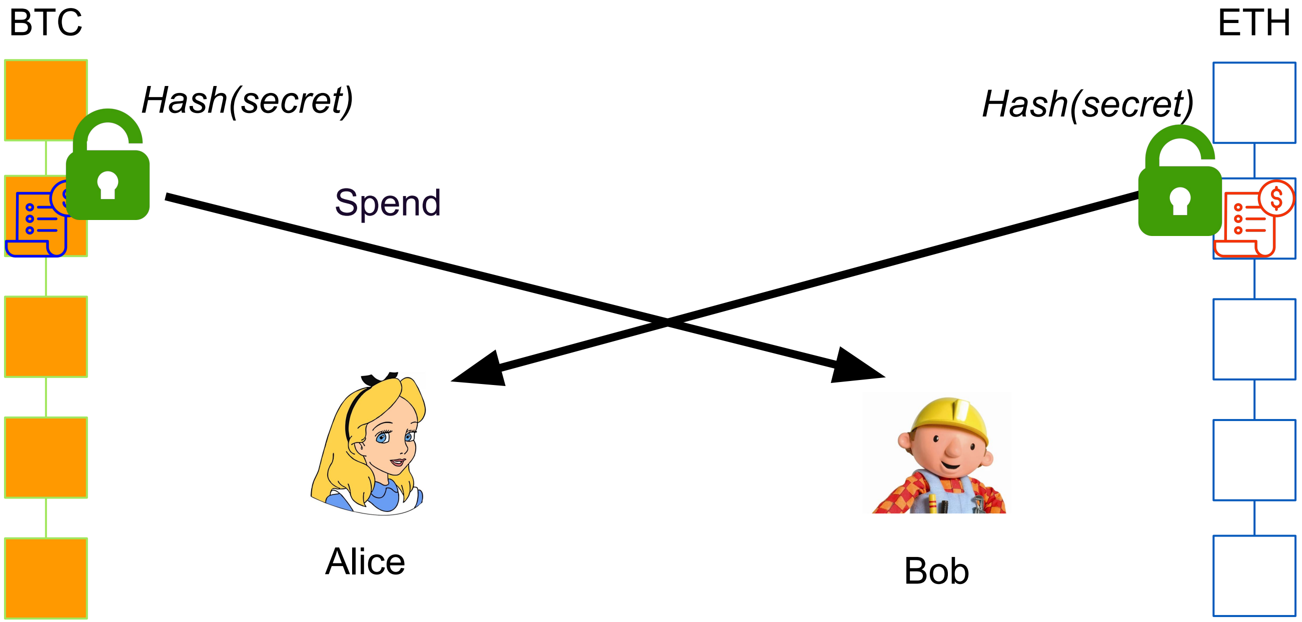
Atomic Swaps via HTLCs

If Alice spends Bob's coins, Bob can spend Alice's coins.



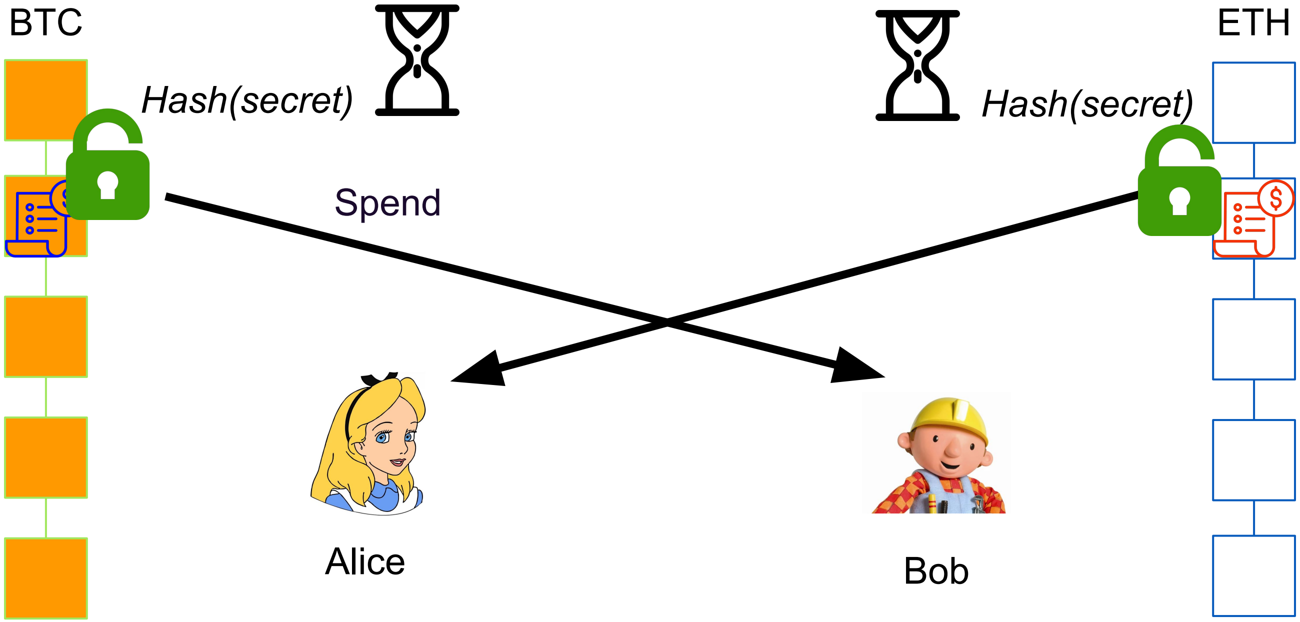
Atomic Swaps via HTLCs

If Alice spends Bob’s coins, Bob can spend Alice’s coins.



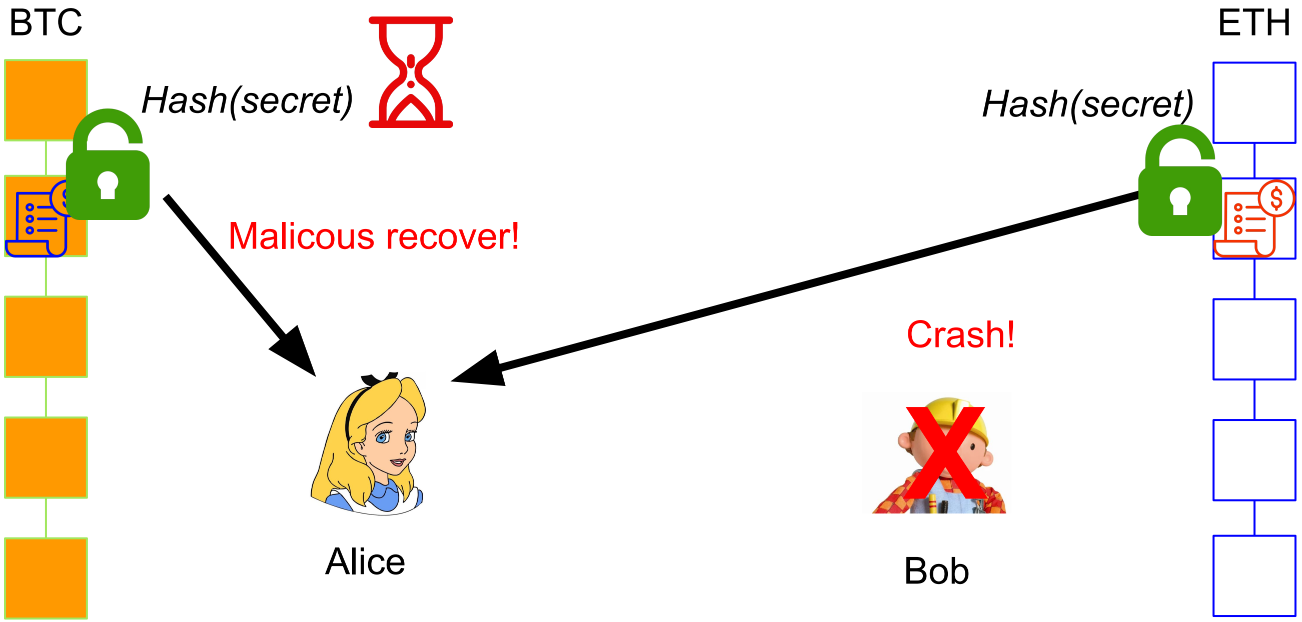
Atomic Swaps via HTLCs

Timelocks used to prevent indefinite lockup of funds
Alice and Bob can restore coins if nothing happens



Atomic Swaps via HTLCs

Problem: Alice spends and reveals …. but Bob crashes.
Alice can maliciously recover her coins, “stealing” from Bob

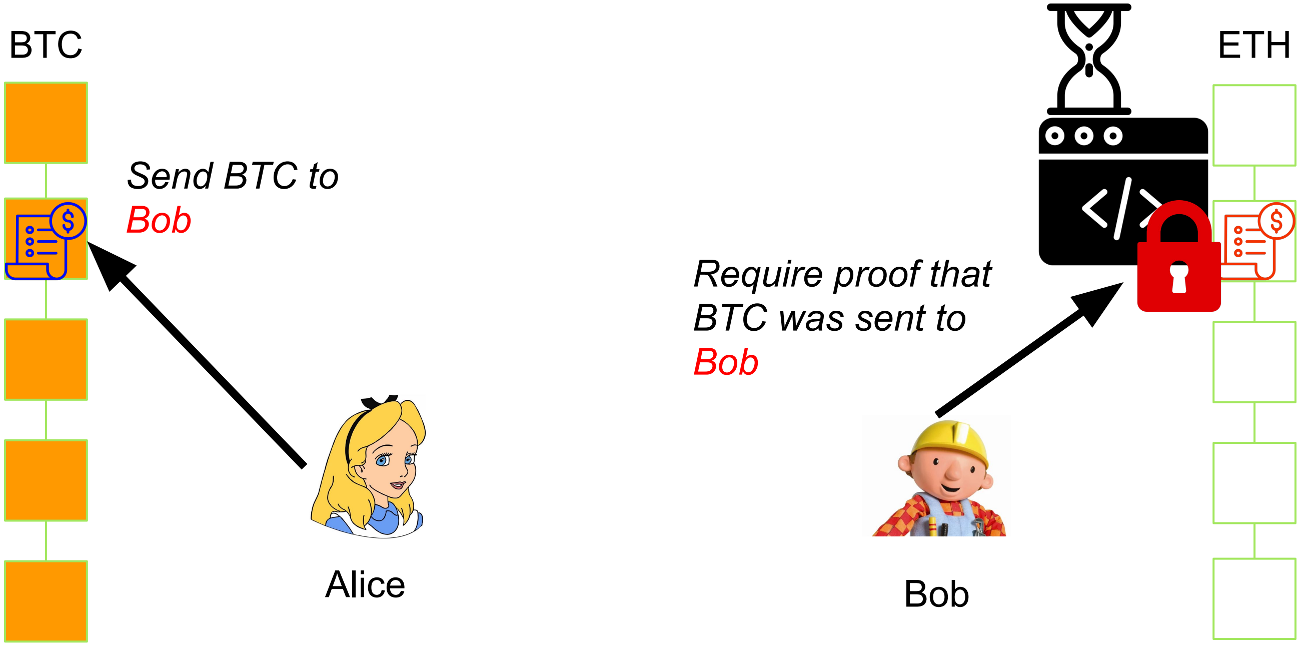


Atomic Swaps via SPV Proofs

Bob locks ETH in smart contract.

Unlock condition: someone sends him BTC on Bitcoin.

Alice sends BTC to Bob.

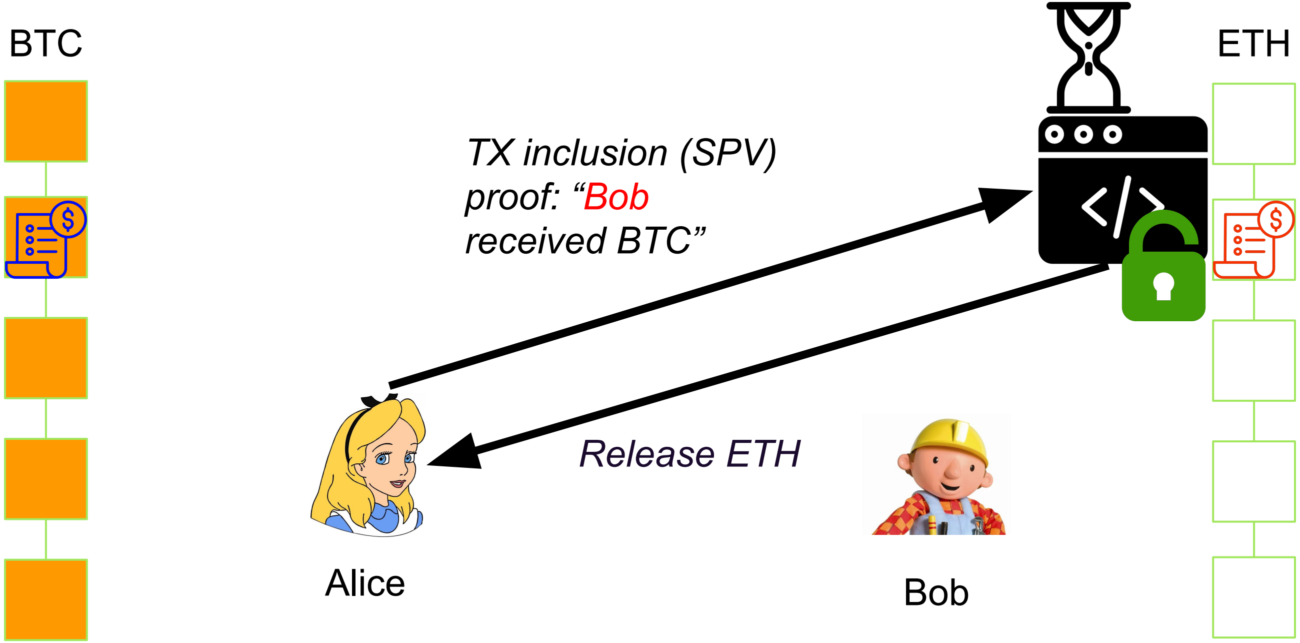


Atomic Swaps via SPV Proofs

Alice proves to contract that she sent BTC to Bob

Contract releases ETH to Alice.

Bob **can be offline** the entire time. Alice bears risk!



Atomic Swaps in Practice

Not very user friendly: mostly desktop applications

HTLC swaps:

- Komodo’s AtomicDEX

Adaptor signatures (enabled by Taproot):

- BTC <> Monero Atomic swaps: https://unstoppableswap.net/

Light clients:

- None active? Wrapping more efficient