BCDEx Network

The Paradigm Shift of BTC-native DeFi

BCDEX

BITCOIN DECENTRALIZED EXCHANGE NETWORK

BCDEx.net

CONTENTS

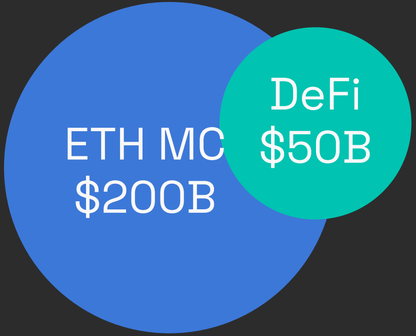
01 DeFi+BTC =
100x Potential

02 BCDEx Demo
Tech Fundamentals

03 BCDEx Network
Status quo

04 More dApps
built on BCDEx

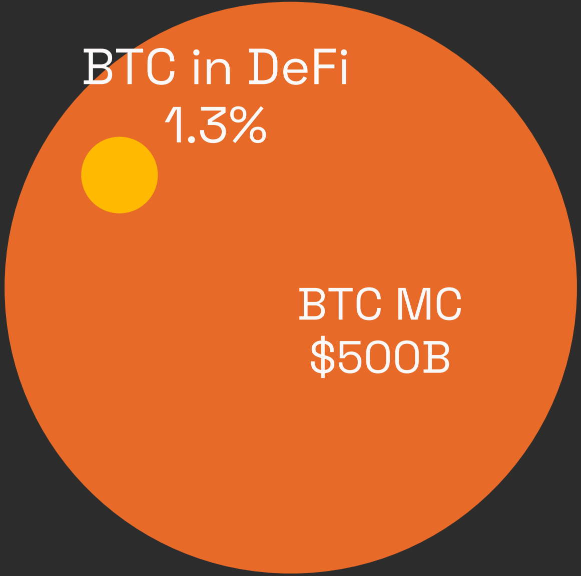
DeFi needs BTC, and soon



DeFi TVL
capped by L1 MC

Market Size
100x

To exchange native BTC
w/ assets on EVM



Most BTC is hibernating

Source: CMC
WBTC $4b, BTCB $1.4b, HBTC $1b, renBTC $100m, RBTC $100m

Native BTC DeFi benefits BTC

No reliable yield for BTC
BTC 5.2% APY on FTX is a scam

LSD makes ETH into interest bearing assets with 5% APY

WBTC or BTCB/HBTC are not reliable nor decentralized

What is BCDEx?

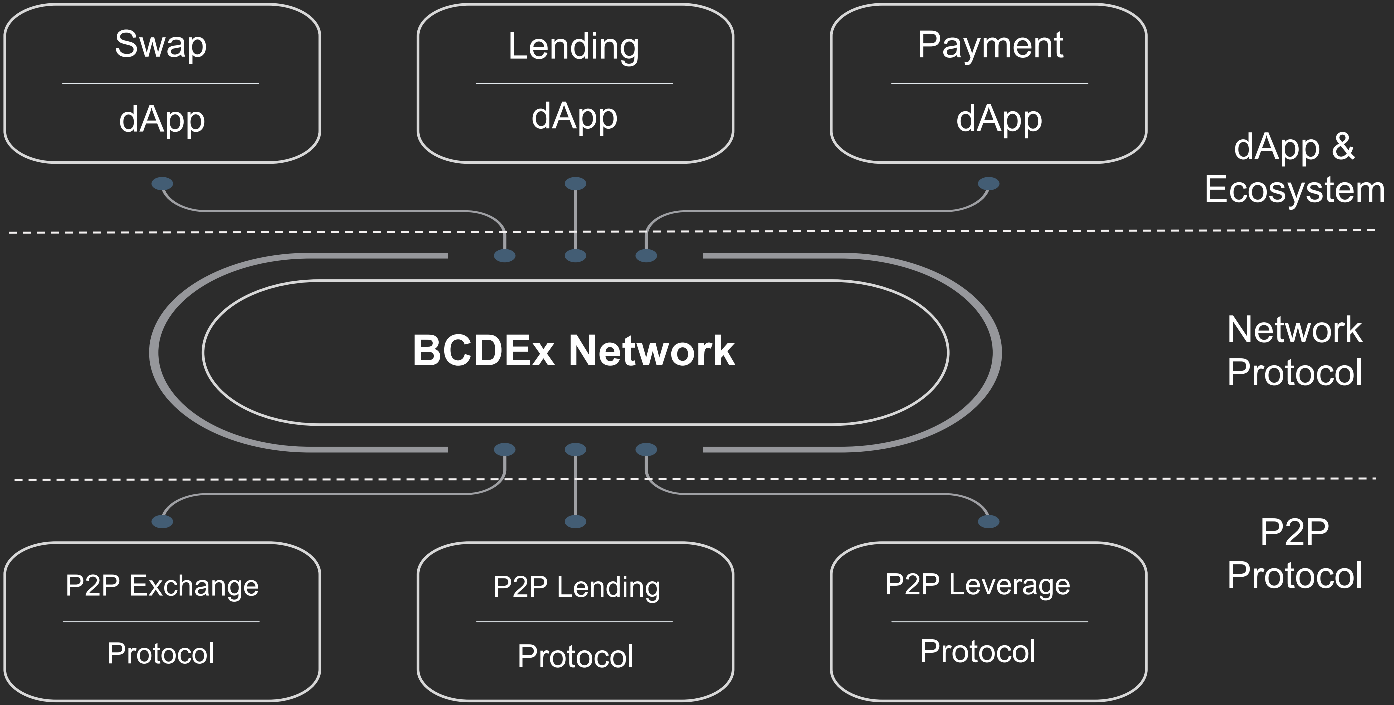
An exchange protocol which enables native BTC DeFi and NFT - allowing developers to construct dApps on top of it.

What is BCDEx

NATIVE on

BTC Mainnet &

Lightning Network

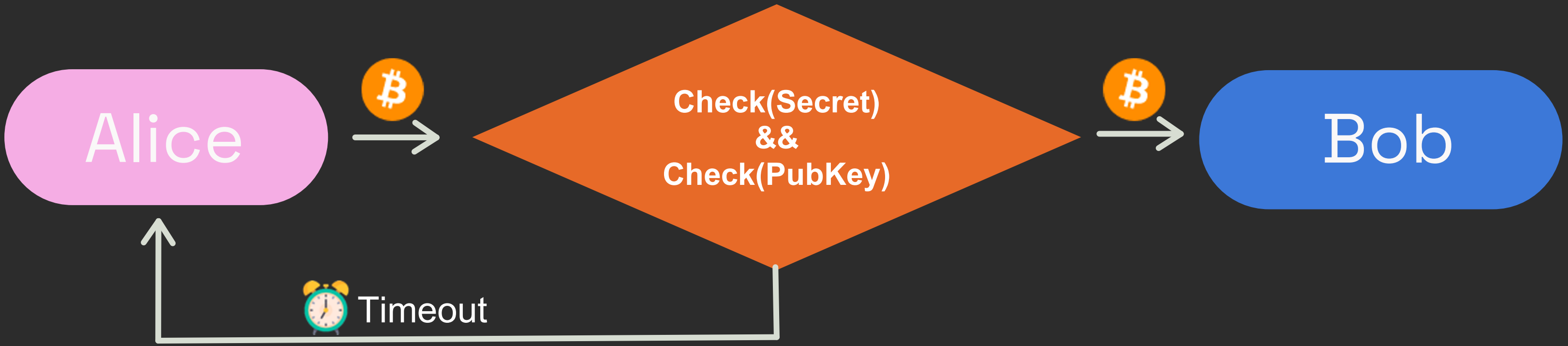


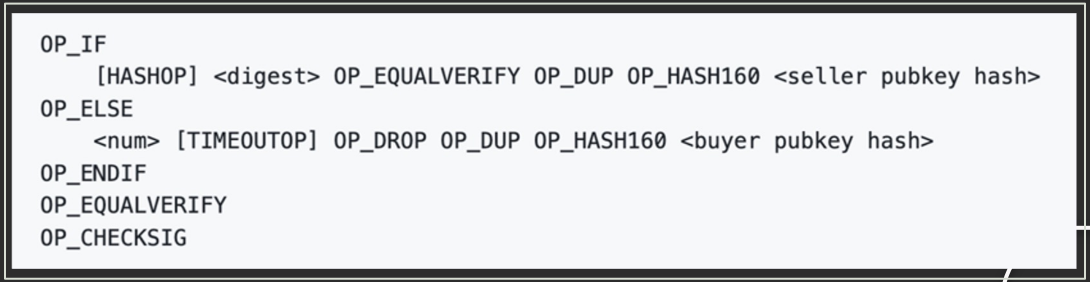
Tech Fundamentals

HTLC

Game Theory

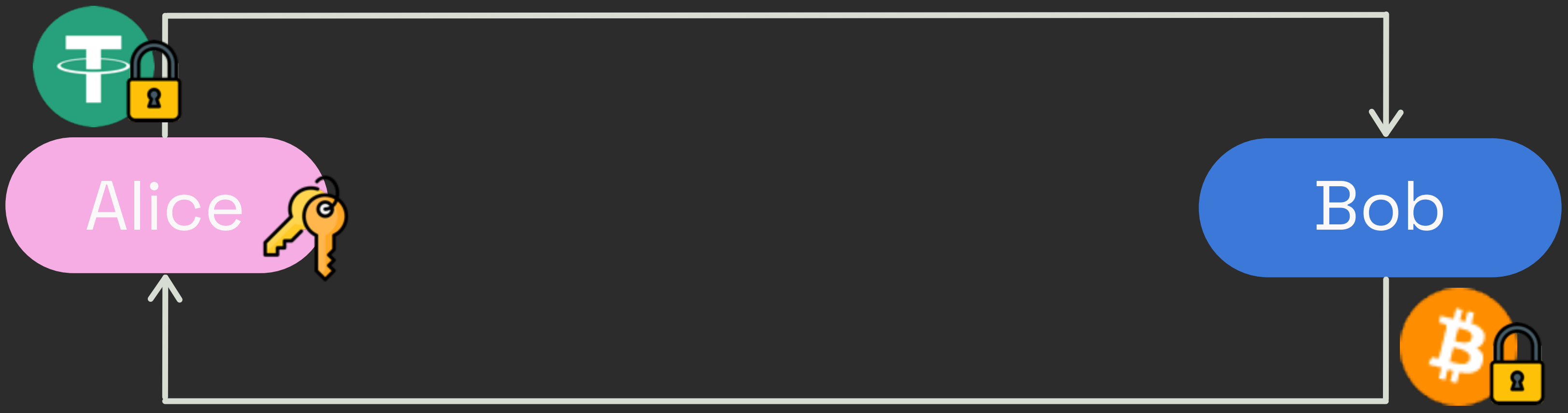
What is HTLC





```
OP_IF
    [HASHOP] <digest> OP_EQUALVERIFY OP_DUP OP_HASH160 <seller pubkey hash>
OP_ELSE
    <num> [TIMEOUTOP] OP_DROP OP_DUP OP_HASH160 <buyer pubkey hash>
OP_ENDIF
OP_EQUALVERIFY
OP_CHECKSIG
```

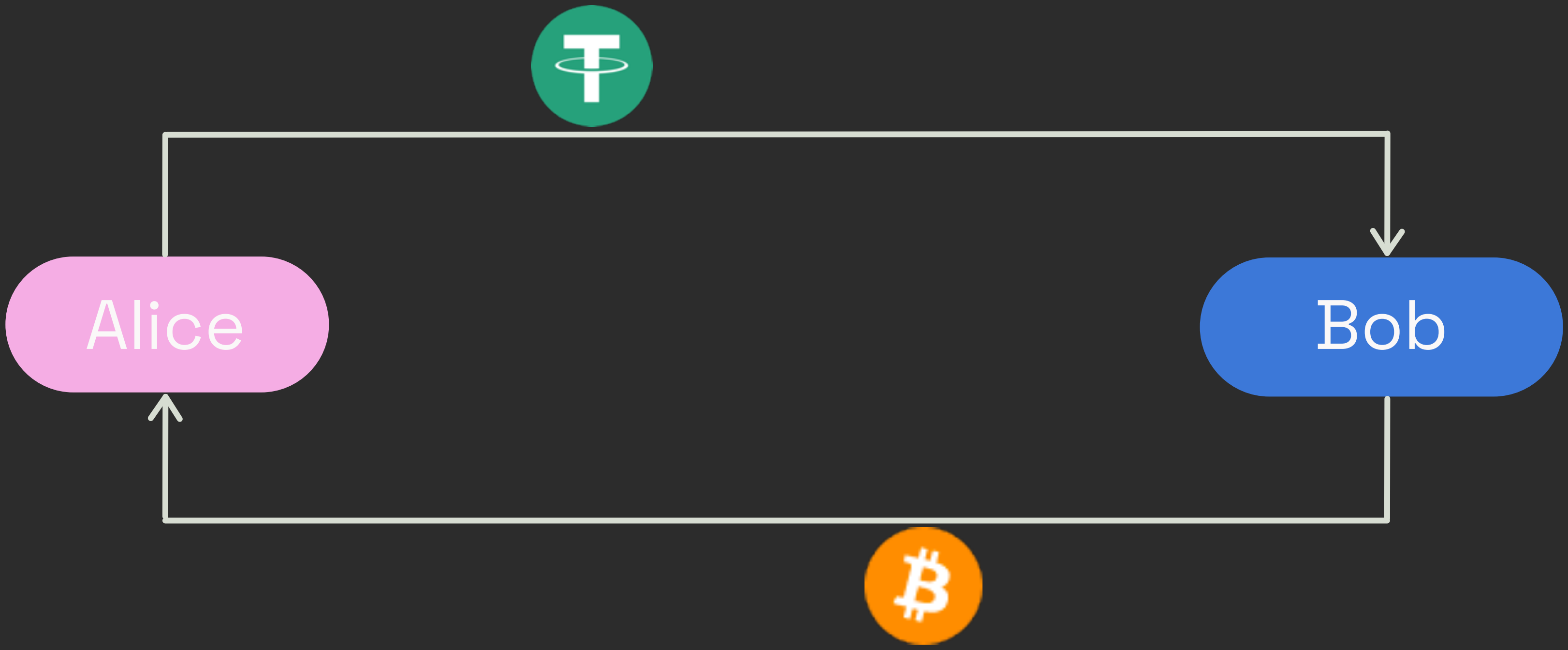
Atomic Swap



Alice

Bob

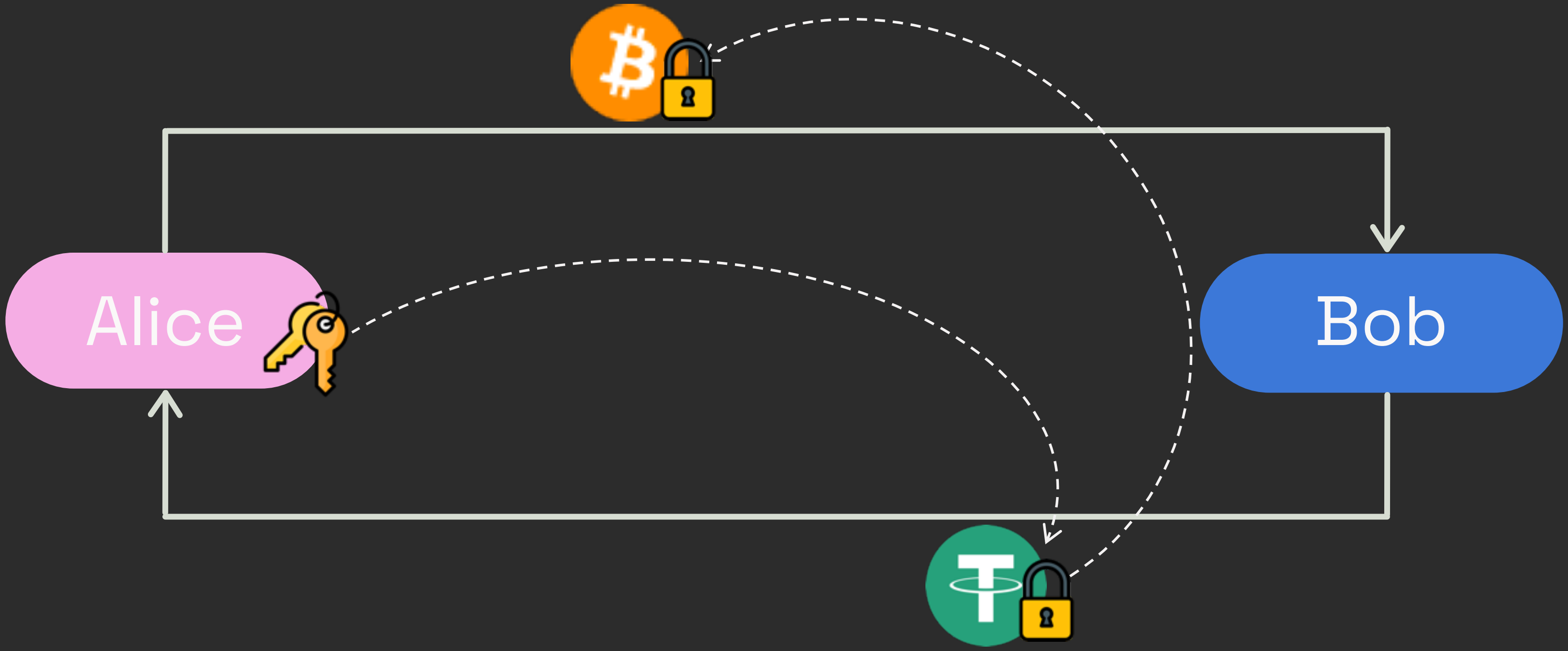
Atomic Swap



Alice

Bob

Atomic Swap



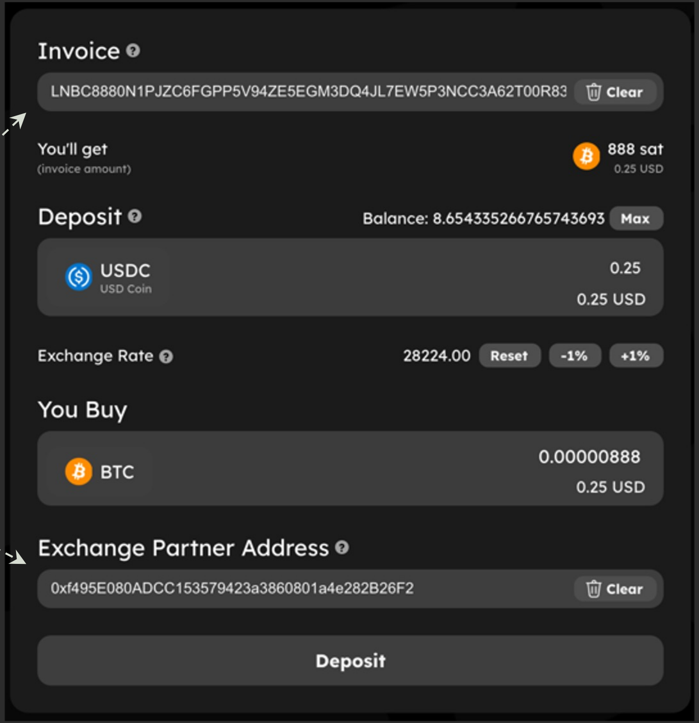
BCDEx Network

What have we built so far?

C2C Exchange

Alice

[Buy BTC Order]	
Invoice	# Receive 888 SATS Lnbc8880n1pjp3t...
Seller Address	# Bob’s Address: 0xABCDEX…
USDT	<**Deposit**> 0.25 USDT



Invoice

LNBC8880N1PJZC6FGPP5V94ZE5EGM3DQ4JL7EW5P3NCC3A62T00R83

You'll get (invoice amount): 888 sat, 0.25 USD

Deposit — Balance: 8.654335266765743693

USDC (USD Coin): 0.25, 0.25 USD

Exchange Rate: 28224.00

You Buy

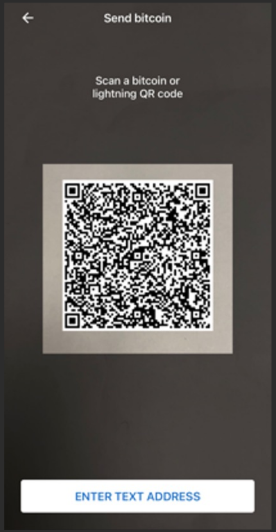
BTC: 0.00000888, 0.25 USD

Exchange Partner Address

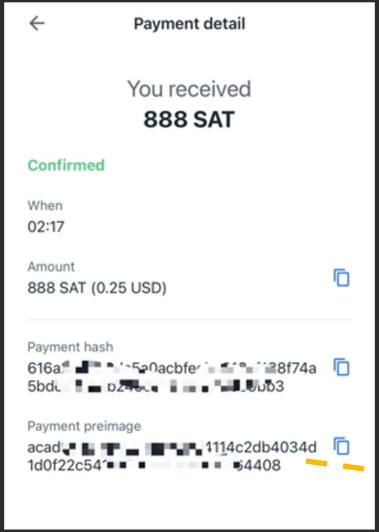
0xf495E080ADCC153579423a3860801a4e282B26F2

C2C Exchange

[Pay invoice]



[Get Secret]



Payment detail

You received
888 SAT

Confirmed

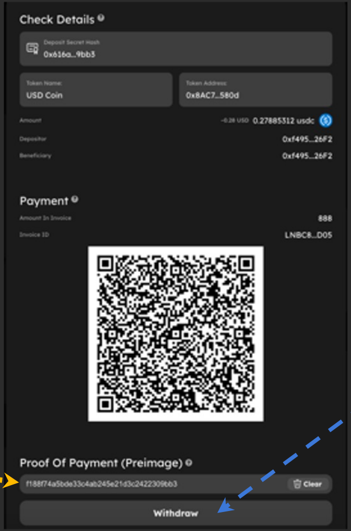
When
02:17

Amount
888 SAT (0.25 USD)

Payment hash
616a[redacted]5a0acbfe[redacted]28f74a
5bd[redacted]b3

Payment preimage
acad[redacted]1114c2db4034d
1d0f22c54[redacted]4408

[Withdraw]



Check Details

Deposit Secret Hash: 0x616a...9bb3

Token Name: USD Coin

Token Address: 0x8AC7...580d

Amount: ~0.28 USD 0.27885312 usdc

Depositor: 0xf495...26F2

Beneficiary: 0xf495...26F2

Payment

Amount In Invoice: 888

Invoice ID: LNBC8...D05

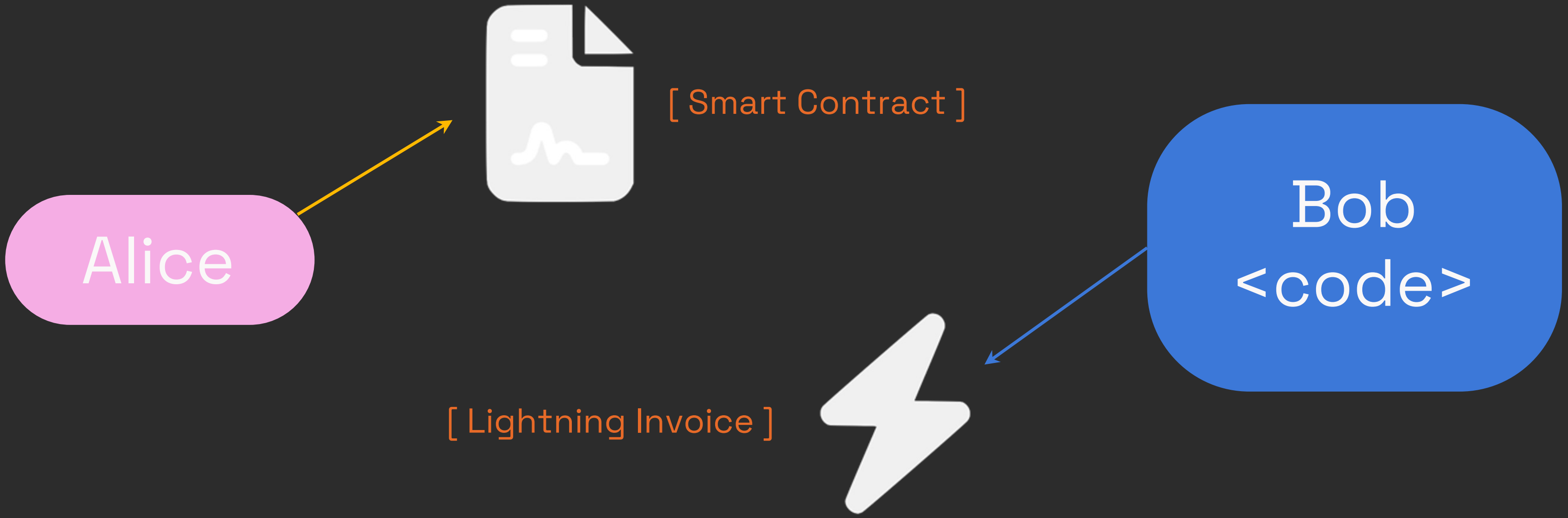
Proof Of Payment (Preimage)

f188f74a5bde33c4ab245e21d3c2422309bb3

Bob

DEMO: https://dev.bcdex.net/

B2C and Maker



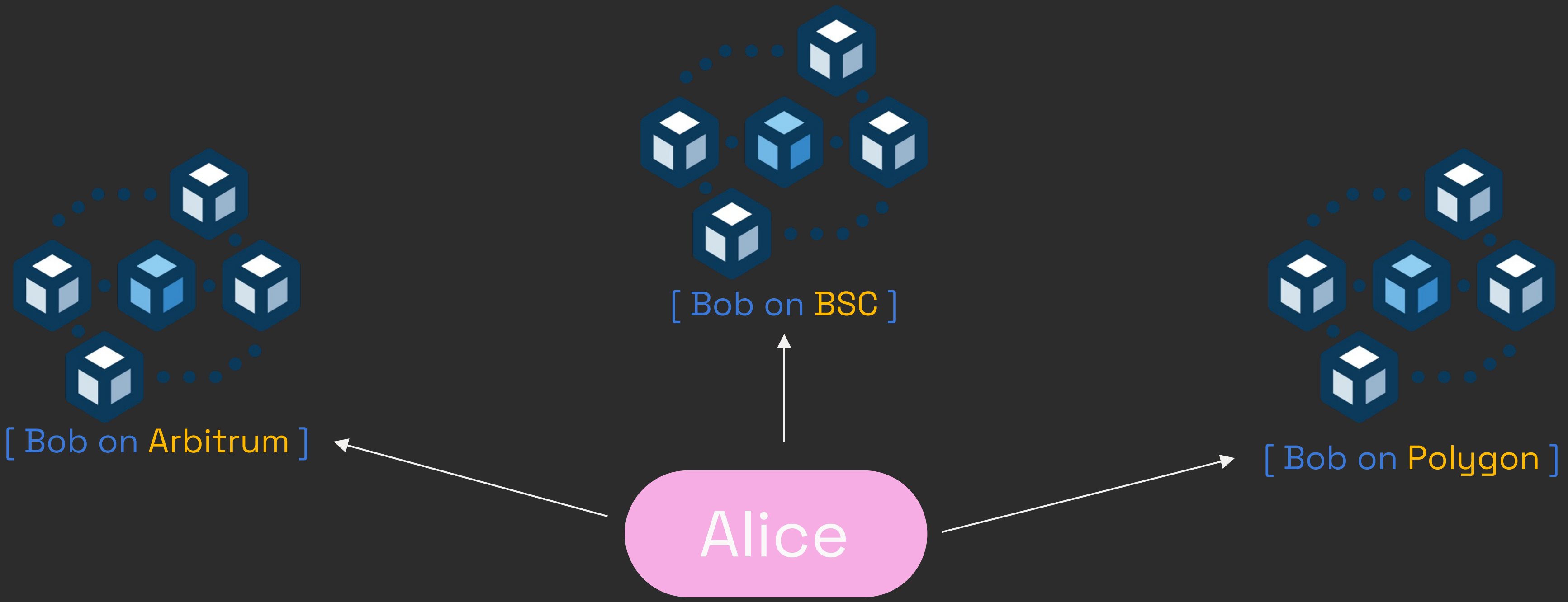
Alice

[Smart Contract]

Bob
<code>

[Lightning Invoice]

B2C and Maker



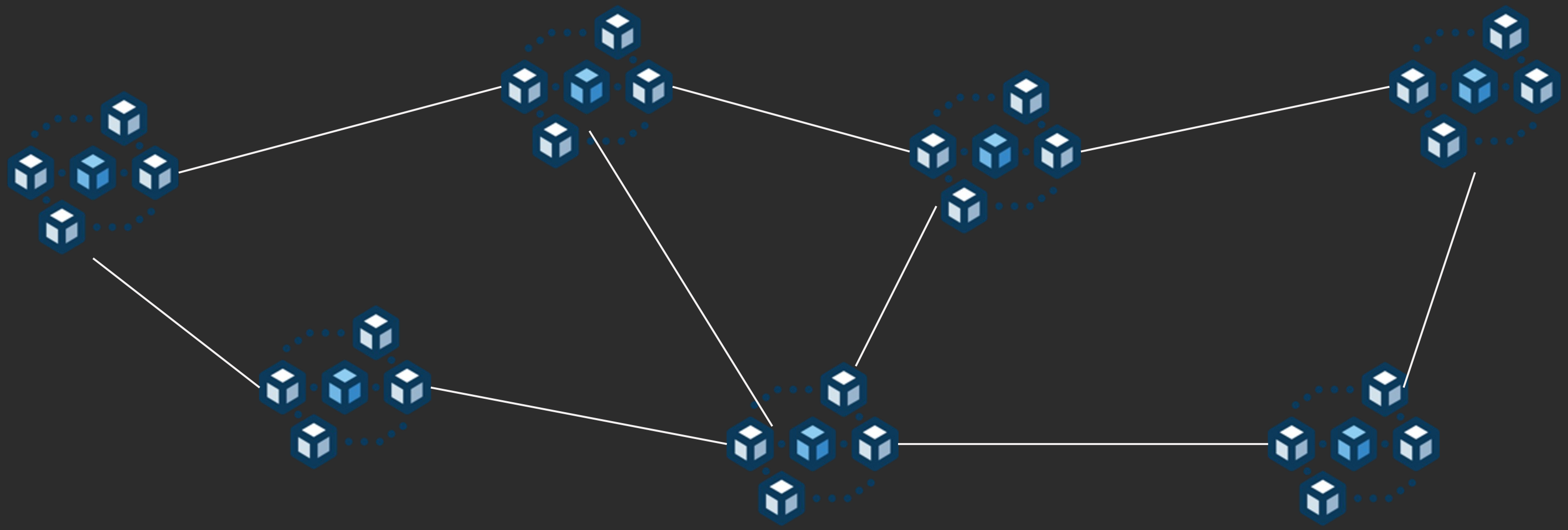
[Bob on BSC]

[Bob on Arbitrum]

[Bob on Polygon]

Alice

Exchange Network



BCDEx Network

/imagine more BTC-native opportunities…

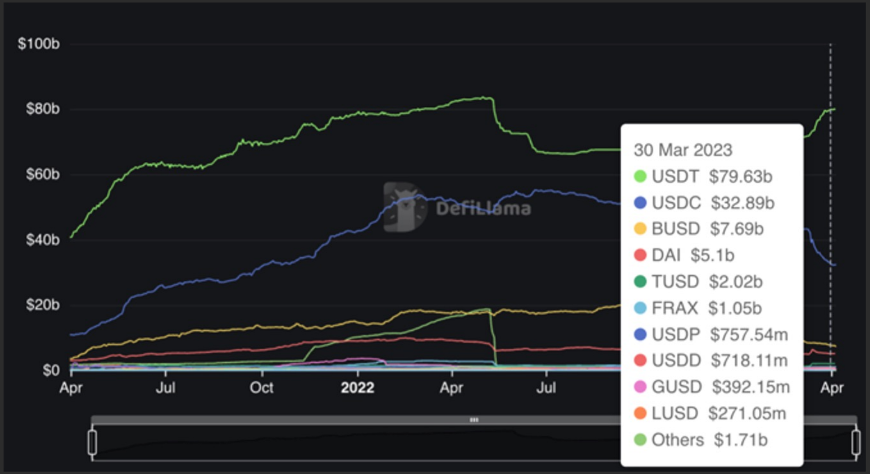
"Give people the right tools, and they will create wonderful things."
— Tim Berners-Lee (inventor of the World Wide Web)

Base On the Exchange Network

Stablecoin	$	Decentralized, 0% interest, BTC-native stablecoin
Swap NFT	⇄	NOT just FT, it can also be NFT, including inscriptions based on Ordinals protocol, sats name, and ”BRC-20"
Swap Route	📍	A pays B, B pays C, and C pays A, thus achieving interchain routing without direct channels
Proxy Payment	👛	BTC believers use Lightning wallets to pay for coffee. Merchants prefer stablecoins. AMM can help convert BTC to stablecoins for payment.
Payment & Call	🔀	Encoded payment or meaning triggers contract call. Automarket makers enable payment-on-call between Lightning Network and smart contracts.

Stablecoin

Stablecoins are the Holy Grail of the crypto world



🟦

Fiat-Collateralized

USDC/USDT/BUSD

Centralization risk. On-chain and off-chain asynchronous.

🟧

Crypto-Collateralized

DAI/LUSD

Limited scalability. High opportunity cost for ETH

🟨

Algorithmic

UST/BAS/AMPL

Not sustainable nor scalable

Stablecoin

BTC-Native Stablecoin Using CDPs

A

Decentralization

BTC PoW guarantees no dependency on any entity

B

Large Scale

Underlying assets are robust, liquid, and with the largest market cap

C

Strong Demand

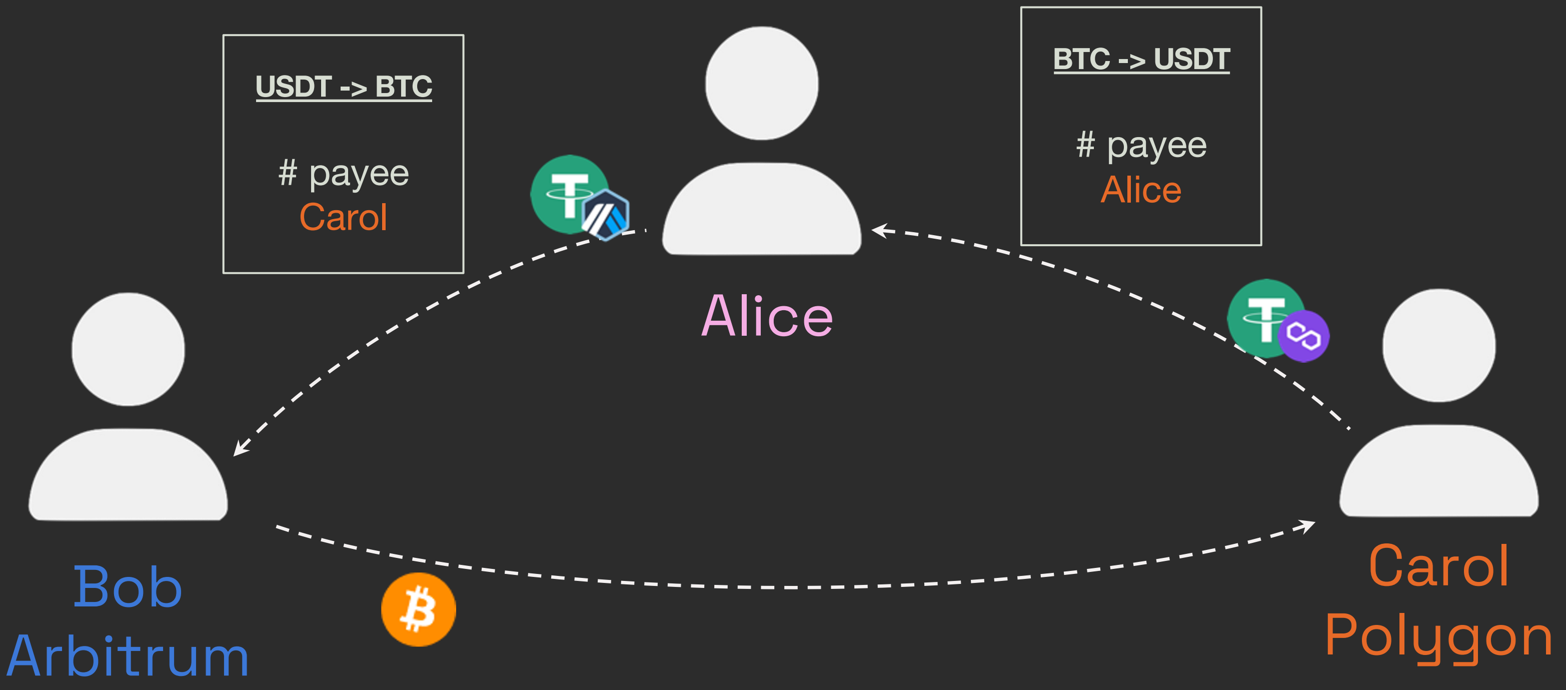
No yield-generating opportunities for BTC holders

D

Low Cost

Lightning network is fast, cheap and secure

Swap Route



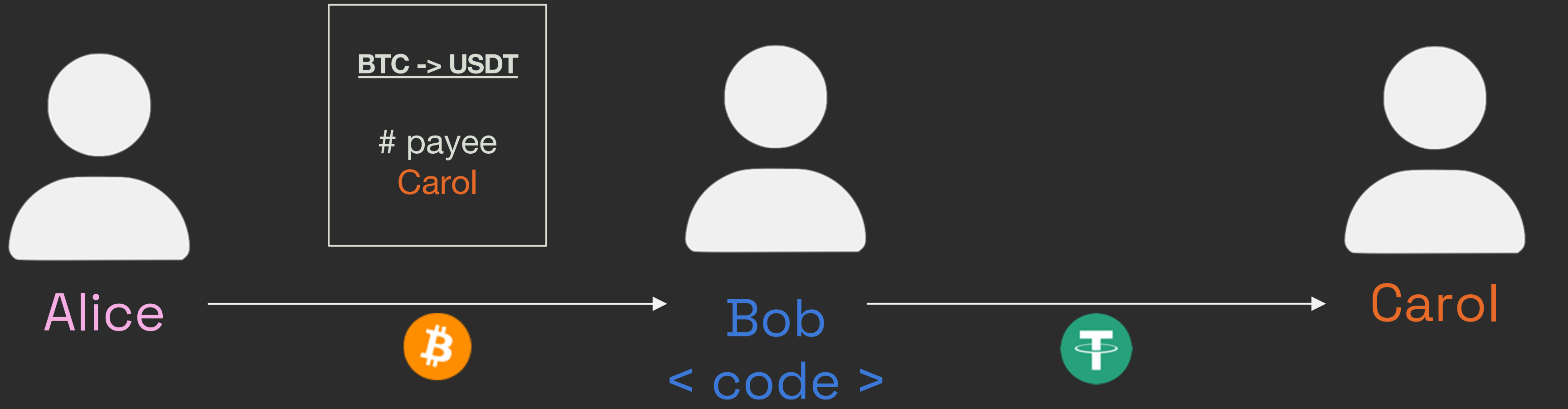
USDT -> BTC

# payee
Carol

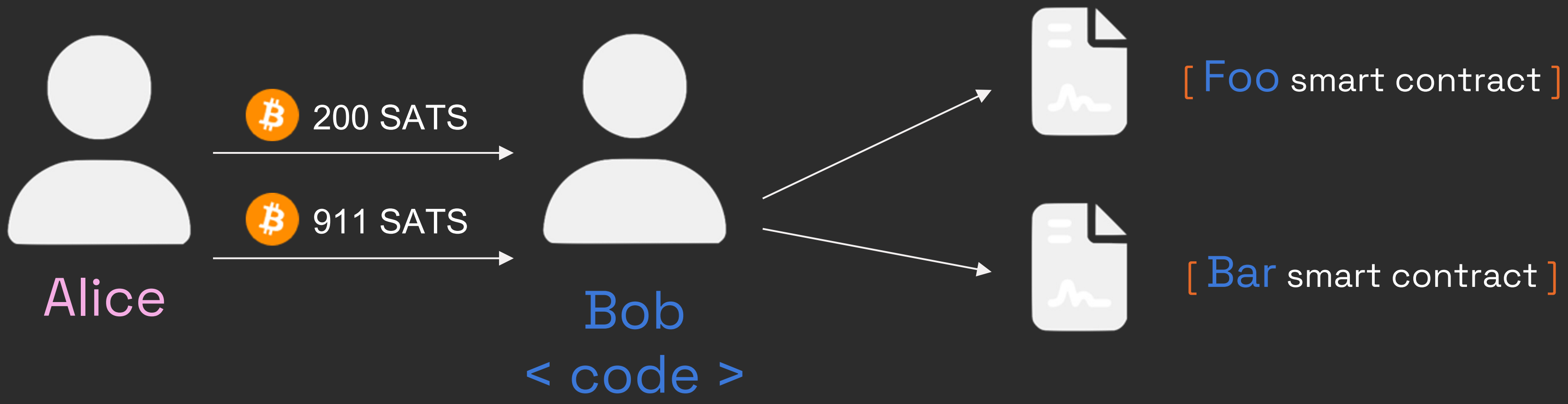
BTC -> USDT

# payee
Alice

Proxy Payment

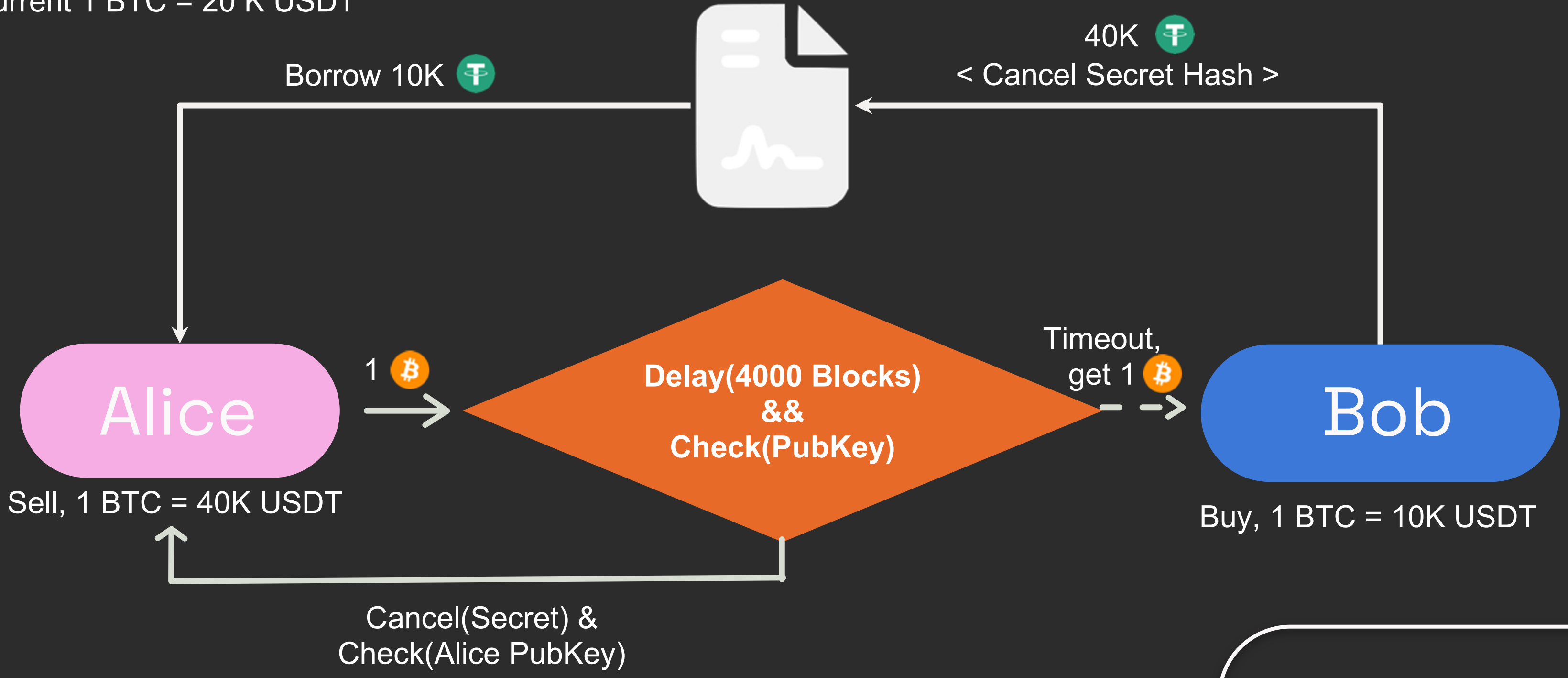


Payment and Call



Lending Protocol

Current 1 BTC = 20 K USDT



Borrow 10K

40K

< Cancel Secret Hash >

Alice

1

Delay(4000 Blocks)
&&
Check(PubKey)

Timeout,
get 1

Bob

Sell, 1 BTC = 40K USDT

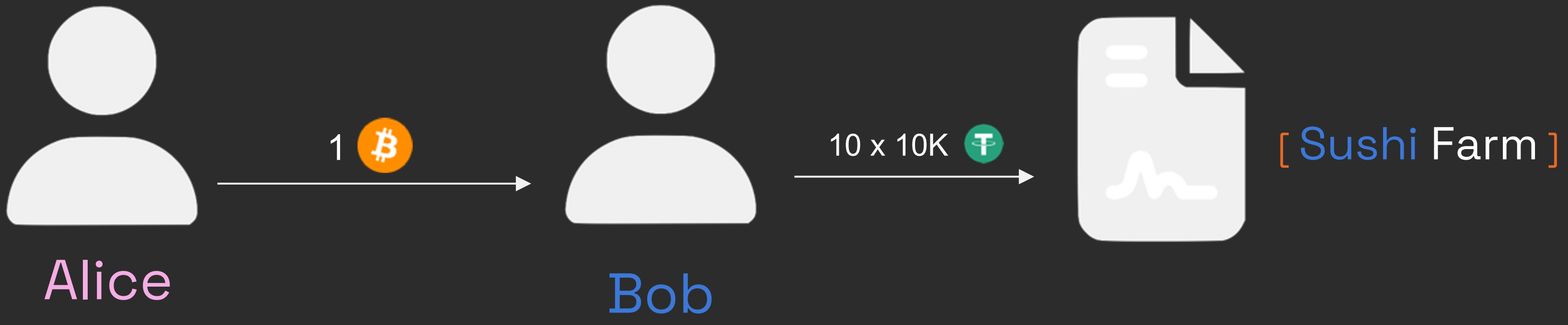
Buy, 1 BTC = 10K USDT

Cancel(Secret) &
Check(Alice PubKey)

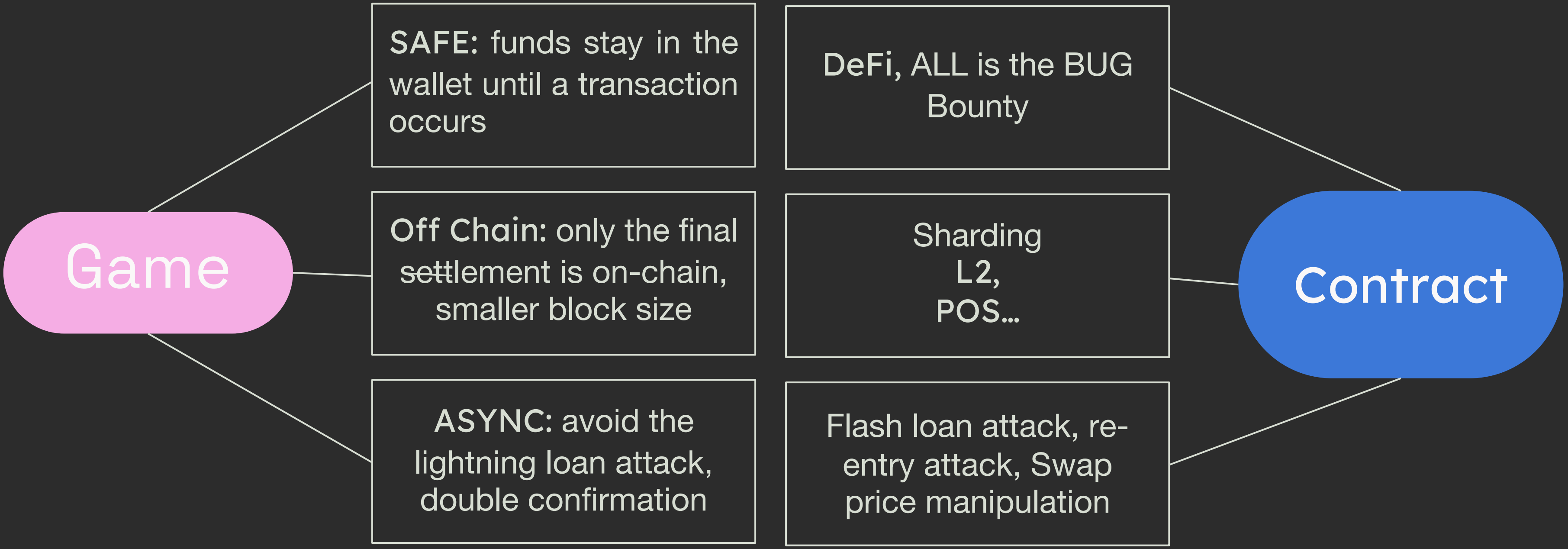
Lending Protocol

		Alice	Bob	Price
Alice	**Defaulted**	+10K USDT, -1 BTC	-10K USDT, +1 BTC	1 BTC < 10K USDT
	Repaid	No change	No change	
Bob	**Confirmed**	No change	No change	
	Defaulted	+40K USDT, -1 BTC	-40K USDT, +1BTC	1 BTC > 40K USDT

Leverage Protocol



GAME vs CONTRACT



Game

SAFE: funds stay in the wallet until a transaction occurs

Off Chain: only the final settlement is on-chain, smaller block size

ASYNC: avoid the lightning loan attack, double confirmation

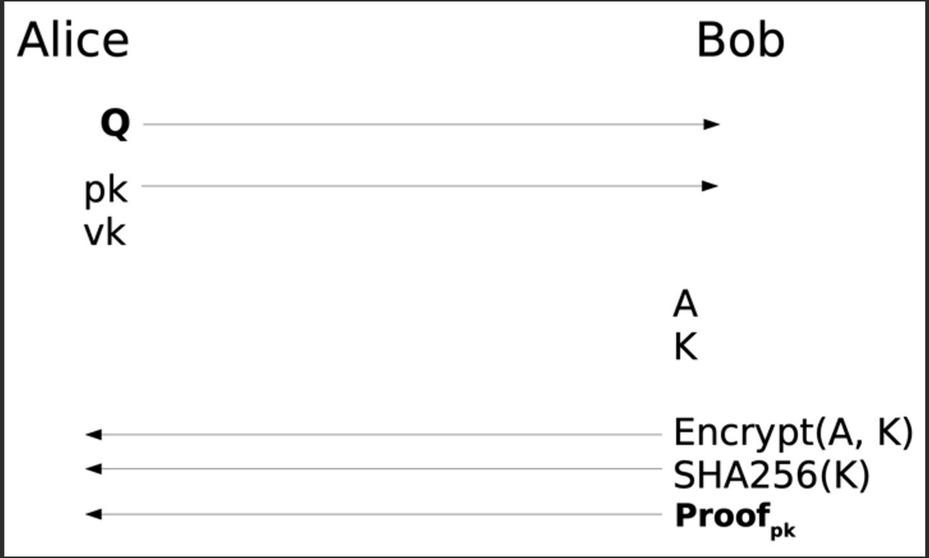
Contract

DeFi, ALL is the BUG Bounty

Sharding
L2,
POS...

Flash loan attack, re-entry attack, Swap price manipulation

/Imagine ZK+HTLC



Given a question Q, a hash H, and an encrypted answer E, Bob know answer A and key K

Step 1, Verify Proof and E(A,K)

Step 2, Swap K via HTLC

Thanks!

sjun.song@gmail.com

BCDEx.net

HAVE A TRY