Course IV:

DeFi Risks and Opportunities

3. Scaling Risk

(iii) Layer 2

Risks: Scaling risk

Layer 2

- *Layer 2* refers to a solution built on top of a blockchain that relies on cryptography and economic guarantees to maintain desired levels of security.
- Transactions can be signed and aggregated in a form resistant to malicious actors, but are not directly posted to the blockchain unless there is a discrepancy of some kind.
- This removes the constraints of a fixed block size and block rate, allowing for much higher throughput. Some layer-2 solutions are live today.

Risks: Scaling risk: Layer 2

- Take small transactions out of the main blockchain (off chain)
- The same intuition applies to Coinbase where it is fast and cheap to transfer among all of those whom have Coinbase wallets. Coinbase is not putting all of the small transactions on-chain.
- However, Coinbase is a centralized organization
- L2 is a much more general approach

Risks: Scaling risk: Layer 2

- Suppose Cam buys a coffee regularly at Starbucks
- It is inefficient to use the main blockchain for small transactions
- The solution is to set up a multi-signature address that is shared by Cam and Starbucks

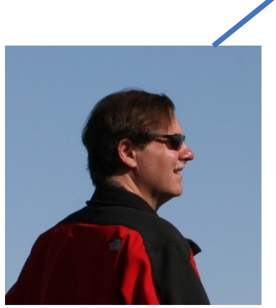
Risks: Scaling risk: Layer 2

Multi-signature address is like a vault that can only be opened when both parties agree. This is a "payment channel".

Multi-signature address

Payment Channel Ledger	
Cam	0.05
Starbucks	0.00

Cam deposits 0.05ETH



Starbucks deposits 0.00ETH

Risks: Scaling risk: Layer 2

- Payment Channel is established on main blockchain by two on-chain transactions
- Cam can see his 0.05 ETH
- Starbucks can see that Cam has 0.05 ETH of spending power
- Initial seeding of the channel is “on chain”

Risks: Scaling risk: Layer 2

- Cam goes to Starbucks and orders an expresso which costs 0.005 ETH
- Payment channel ledger is updated off chain

Payment Channel Ledger	
Cam	0.045
Starbucks	0.005

- Cam and Starbucks sign the updated balance sheet and each keep a copy of the ledger

Risks: Scaling risk: Layer 2

- Cam can continue to buy coffee until balance is exhausted
- There is no limit on the number of transactions per second because these transactions are happening off chain

Payment Channel Ledger	
Cam	0.015
Starbucks	0.035

Risks: Scaling risk: Layer 2

- Payment Channel can be closed at any time
- Either party simply needs to take the latest ledger which is signed by both parties and broadcast it to the network
- Miners verify the signatures on the ledger and then release the funds (single transaction to close). This is an on-chain transaction.

0.015 to Cam

Payment Channel Ledger	
Cam	0.015
Starbucks	0.035

0.035 to SB

Risks: Scaling risk: Layer 2

- Important 1: Any party can release the funds – even if one party does not want to release the funds. There is no way for Cam to hold Starbucks hostage for the funds.

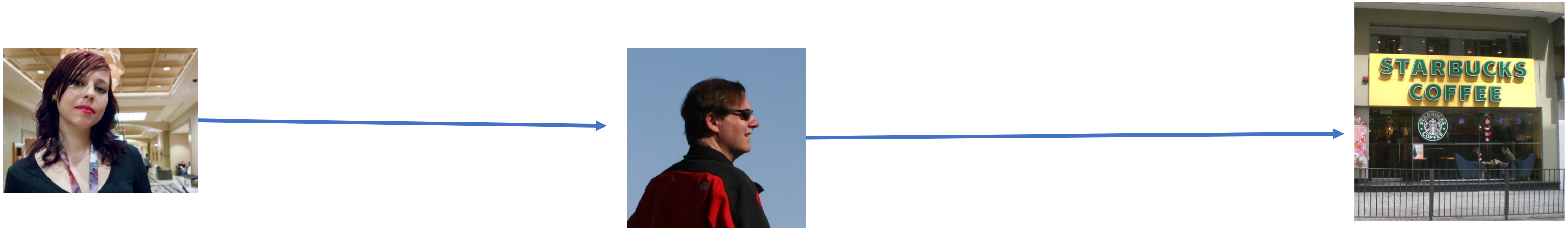
0.015 to Cam

Payment Channel Ledger	
Cam	0.015
Starbucks	0.035

0.035 to SB

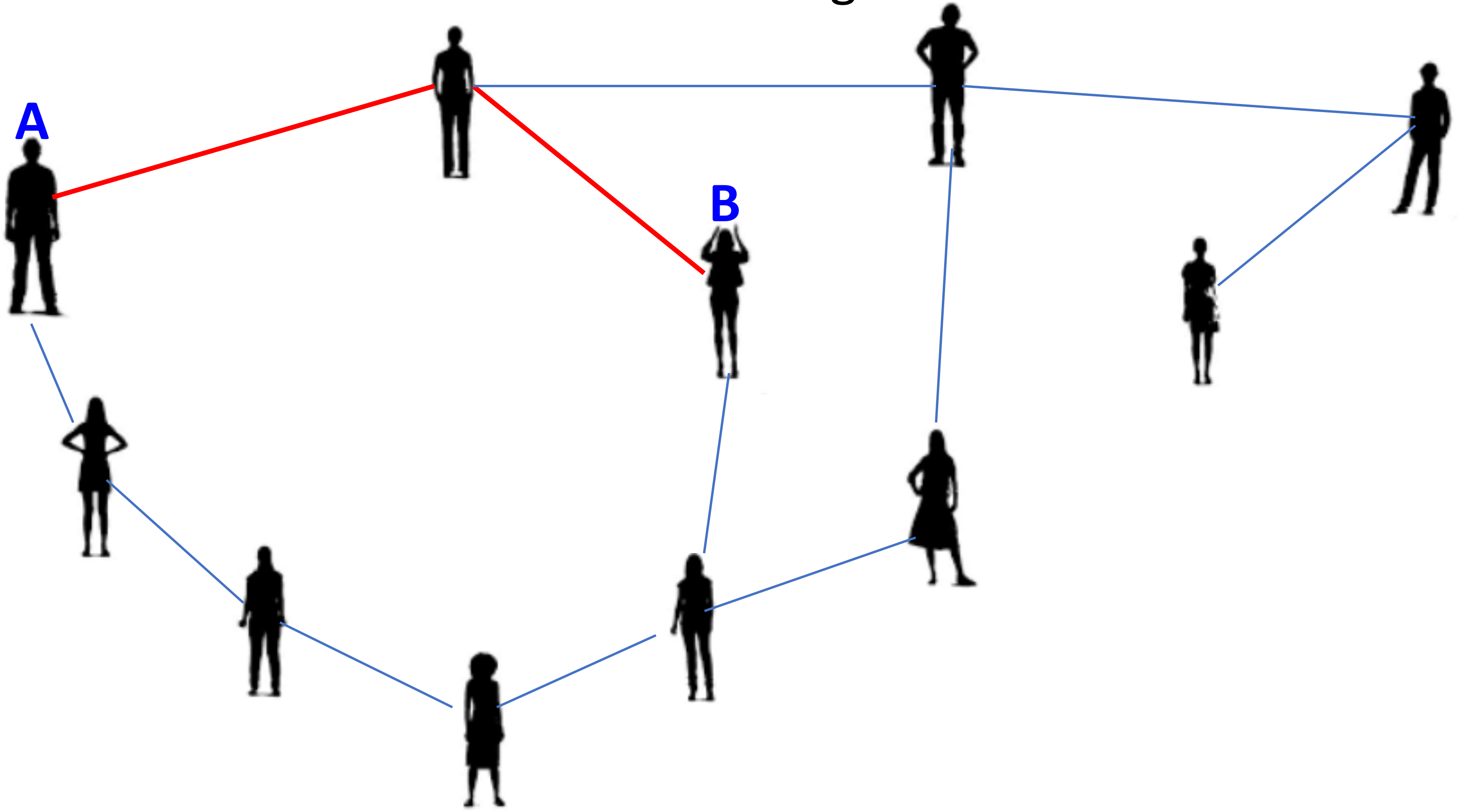
Risks: Scaling risk: Layer 2

- Important 2: You do not need to set up a separate payment channel for Starbucks – you can use the network.
- Suppose Amber and Cam have a payment channel. Suppose Amber wants a cup of coffee at Starbucks.
- Amber does not have a payment channel with Starbuck but she knows that Cam has a payment channel



Risks: Scaling risk: Layer 2

- Important 2: Network finds the fastest and cheapest way to connect A to B. It is also important that the channels have enough funds to do the transaction.



Risks: Scaling risk: Layer 2

False concerns

- I don’t want to prefund future payments
- I don’t want to lock-up funds so that I can’t use them elsewhere
- I’ll have to close and reopen the channel whenever I want to replenish funds
- I have no idea in advance how many coffees I’ll buy from Starbucks

Risks: Scaling risk: Layer 2

Allayed concerns

- Your regular L2 channel will be just like your hot/spending wallet (think of the difference between your “wallet” and your “savings account”)
- Establishing a channel is analogous to funding a hot wallet
- You don’t need to open a channel with every Starbucks

Risks: Scaling risk: Layer 2

Real concerns

- L2 depends on changes in blockchain protocol
- Some are concerned that the payment channels maybe become “centralized” with a few important players
- You need to hold crypto in the channel and crypto is a volatile store of value
- Is a second layer, L2, enough? Will there need to be a third level?