




The Private Exchange

Building a privacy-focused dapp

Takamichi Tsutsumi

Software Engineer – PSE, Ethereum Foundation

The background is a complex, abstract geometric pattern. It features a variety of triangles in different sizes and orientations, some pointing up and some down. The colors are warm and muted, including shades of orange, yellow, light blue, and pale green. These elements are layered and overlap, creating a sense of depth and movement. Some of the triangles are solid, while others are outlined or have internal patterns. The overall effect is a modern, artistic, and somewhat chaotic yet harmonious visual field.

I WANT TO SHOW YOU A

Privacy preserving decentralized exchange



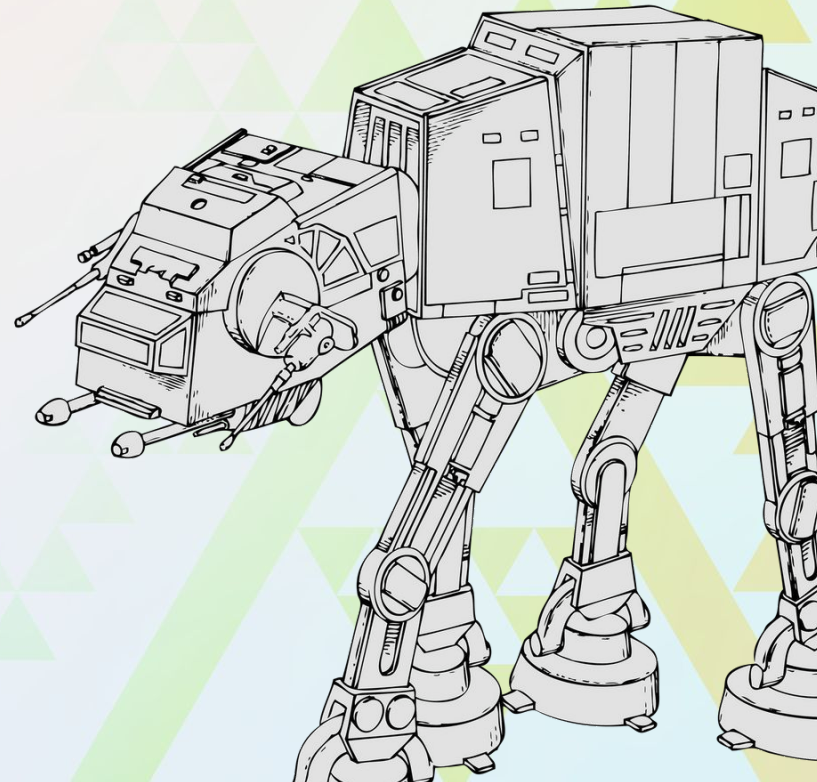
Why do we need privacy?

Why do we need privacy?

Censorship resistance

Anti-MEV and front-running

Human rights



No one shall be subjected to arbitrary interference with his **privacy**, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

-The Universal Declaration of Human Rights. Article 12



Section 2

What is Private Exchange?



Make exchange more **private**

What exchanges do



Automated Market Maker (AMM)



Alice



Public txn

Address: 0xasd..
Send : 1 ETH
Receive: 1500 DAI

SMART
CONTRACT



Orderbook



Alice



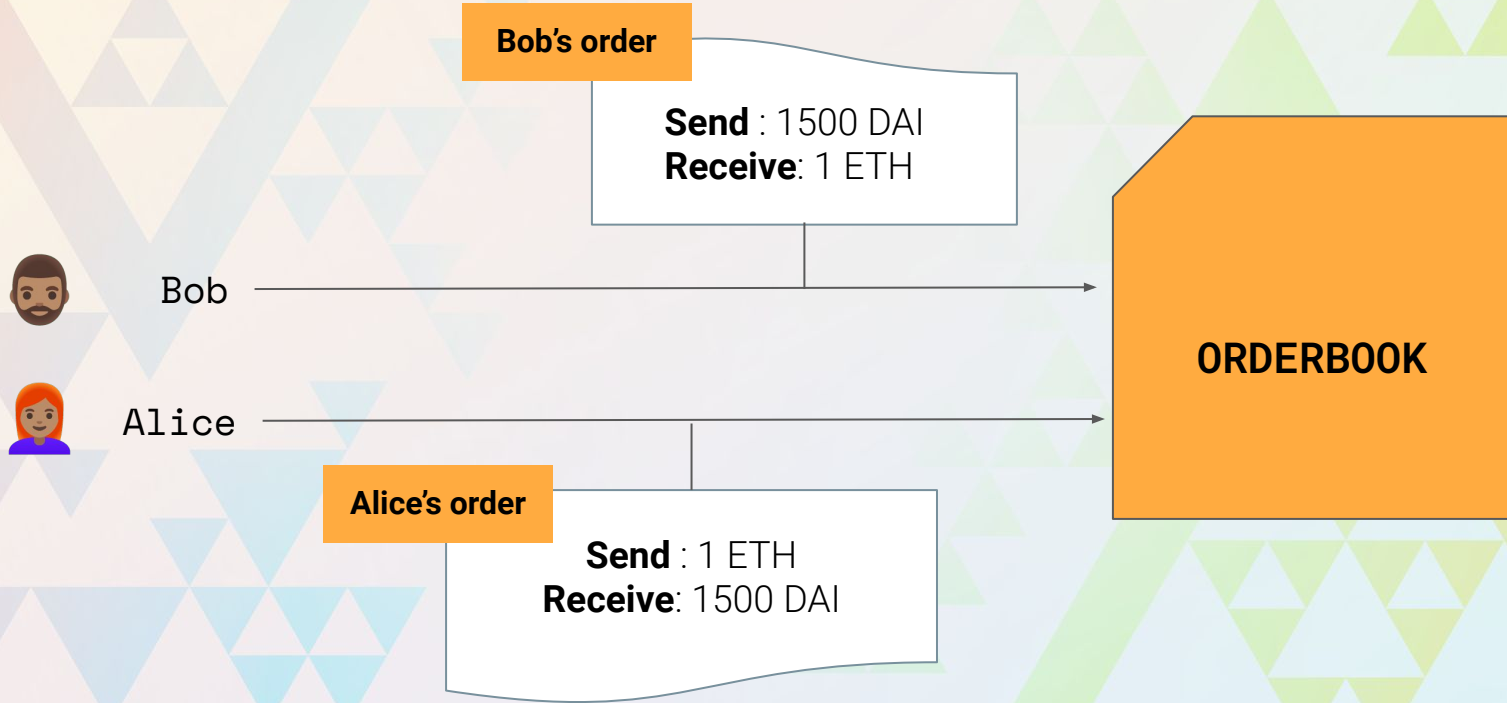
Order

Send: 1 ETH
Receive: 1500 DAI

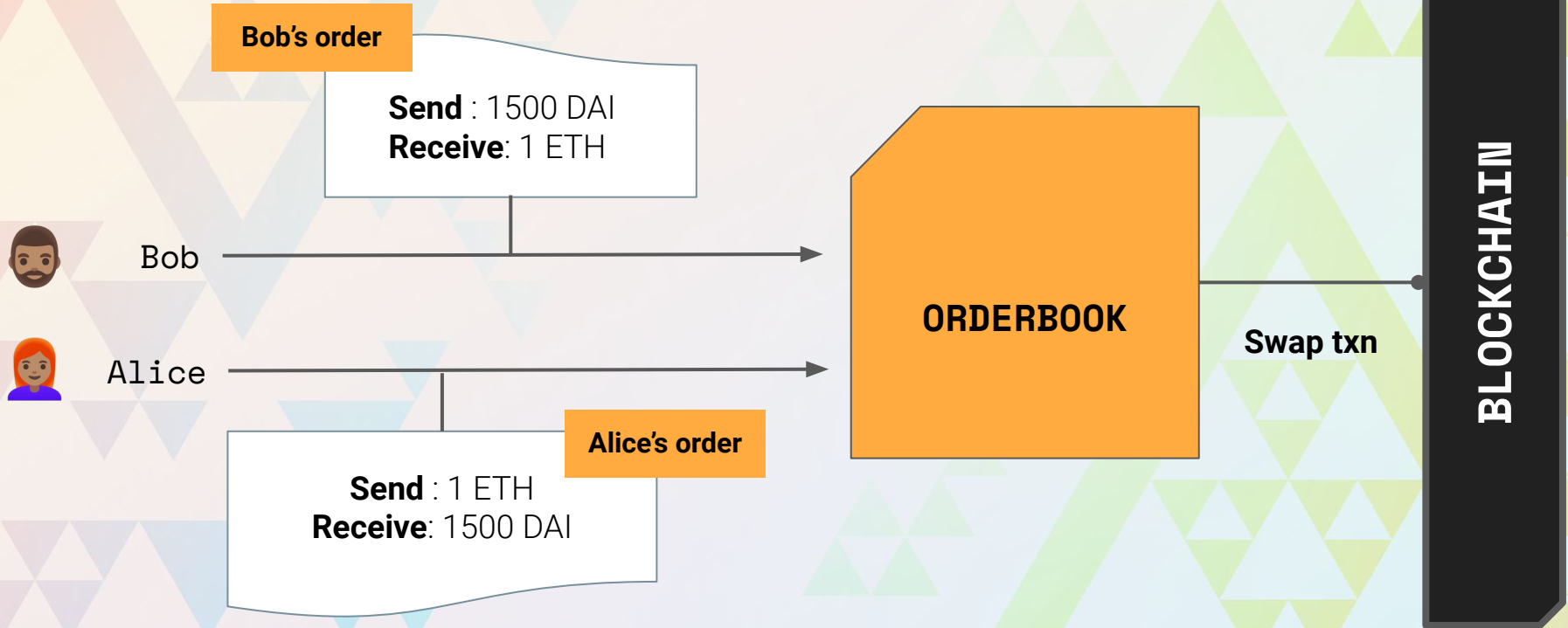
Price: 1500 DAI / ETH

ORDERBOOK

Orderbook



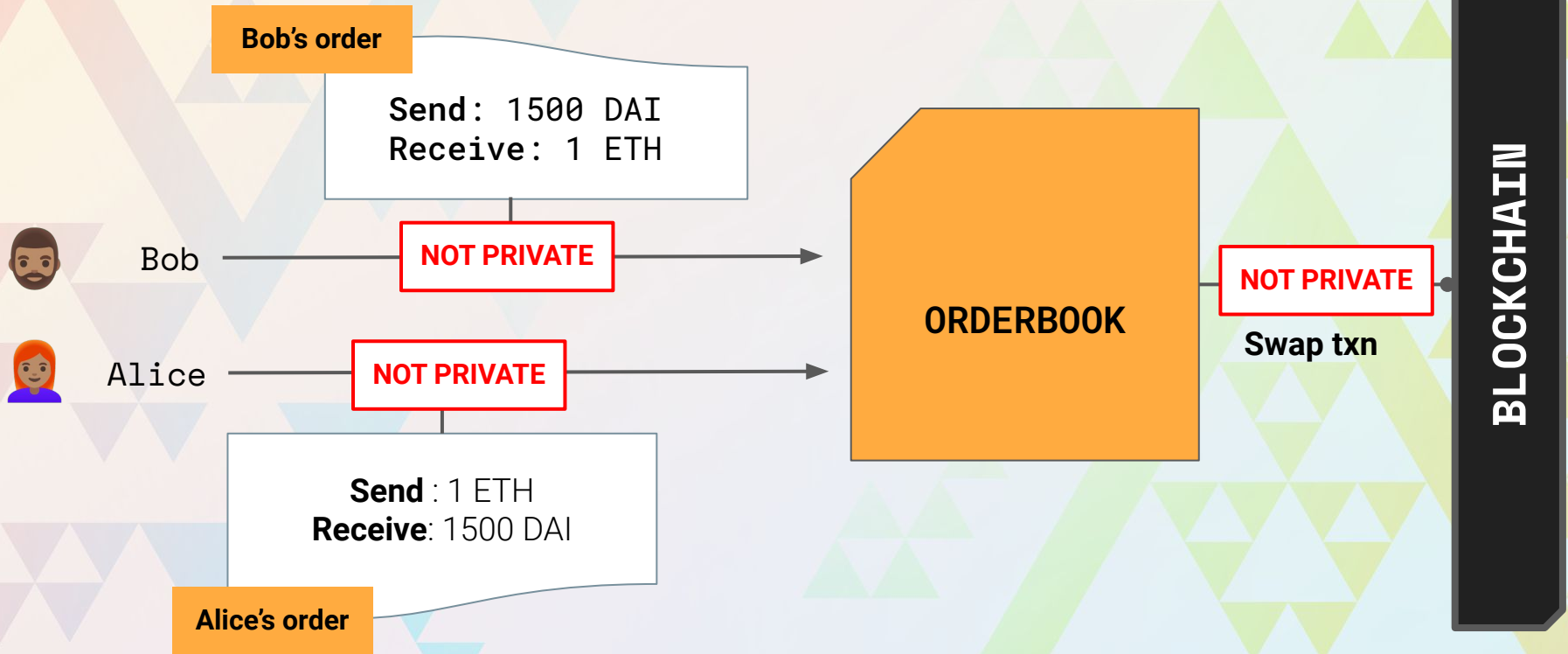
Orderbook



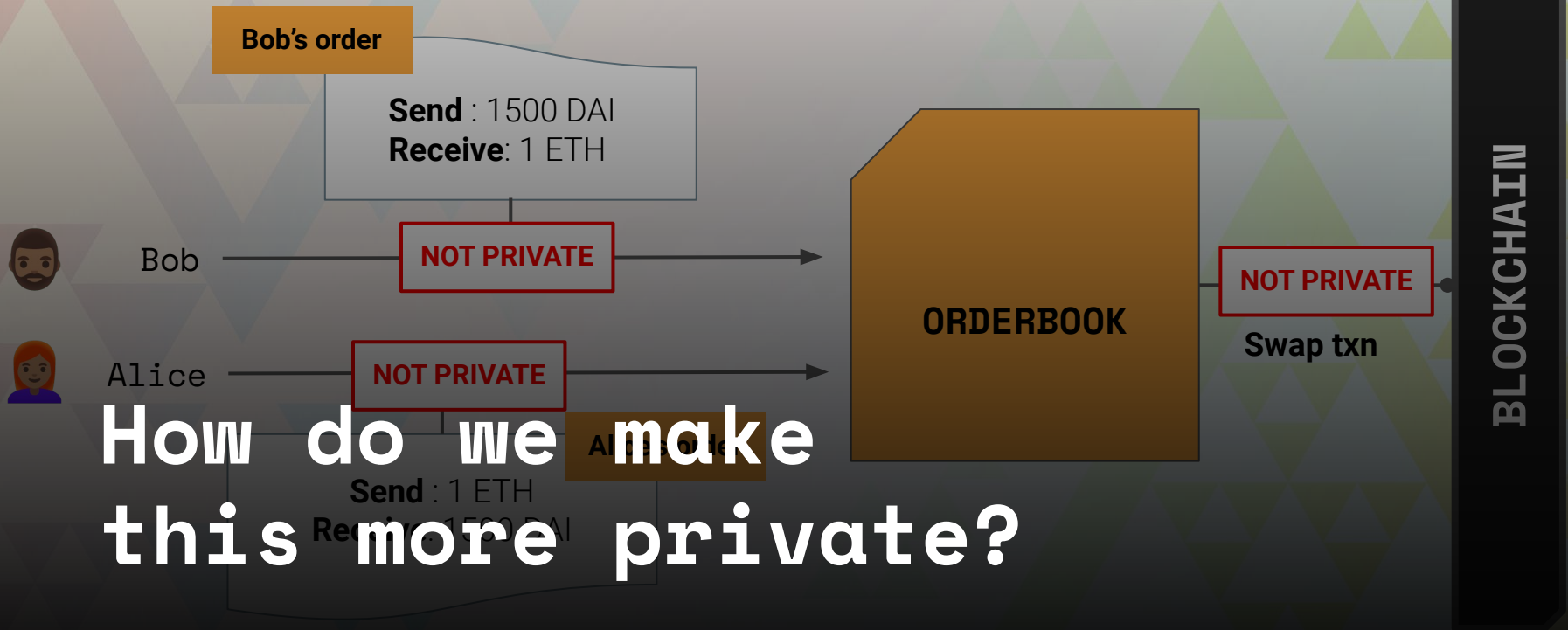


Let's make it more *private*

Orderbook



Orderbook





Three zk protocols

Our toolkit



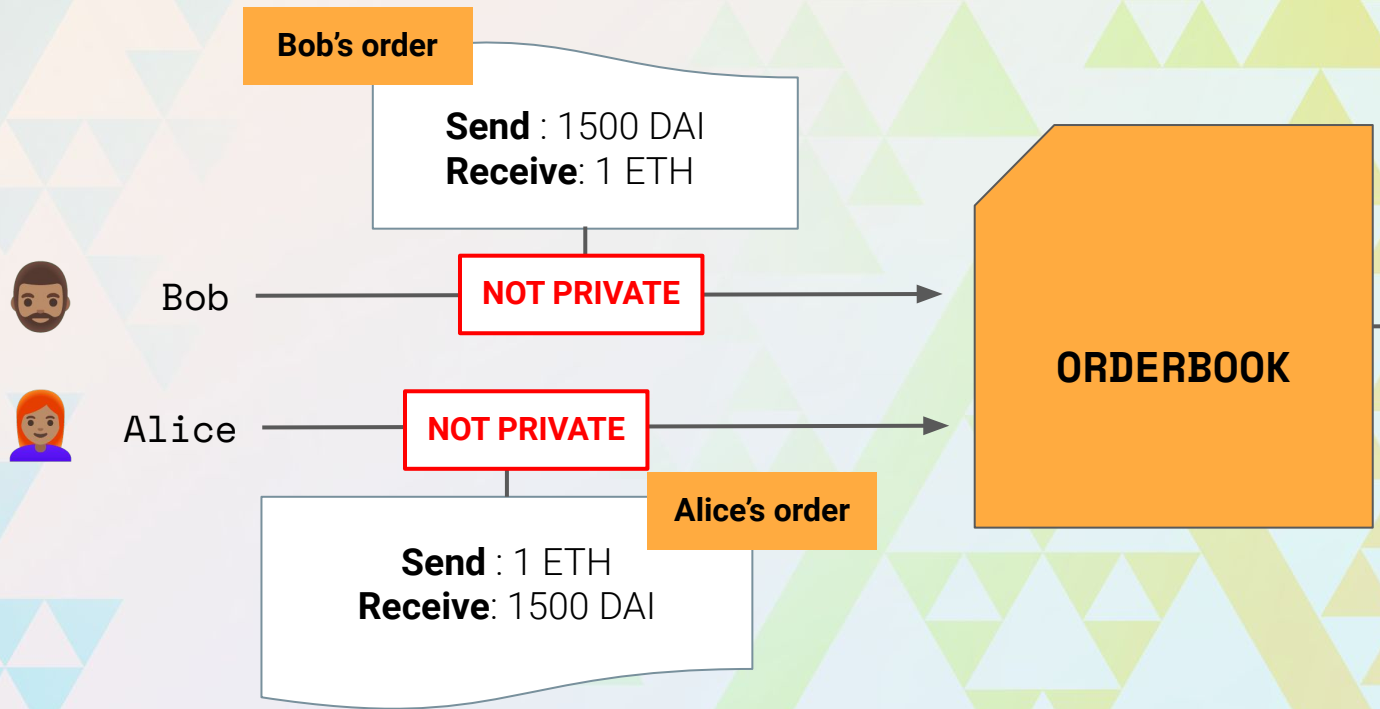
Blind-find



Socialist Millionaire
Problem (SMP)

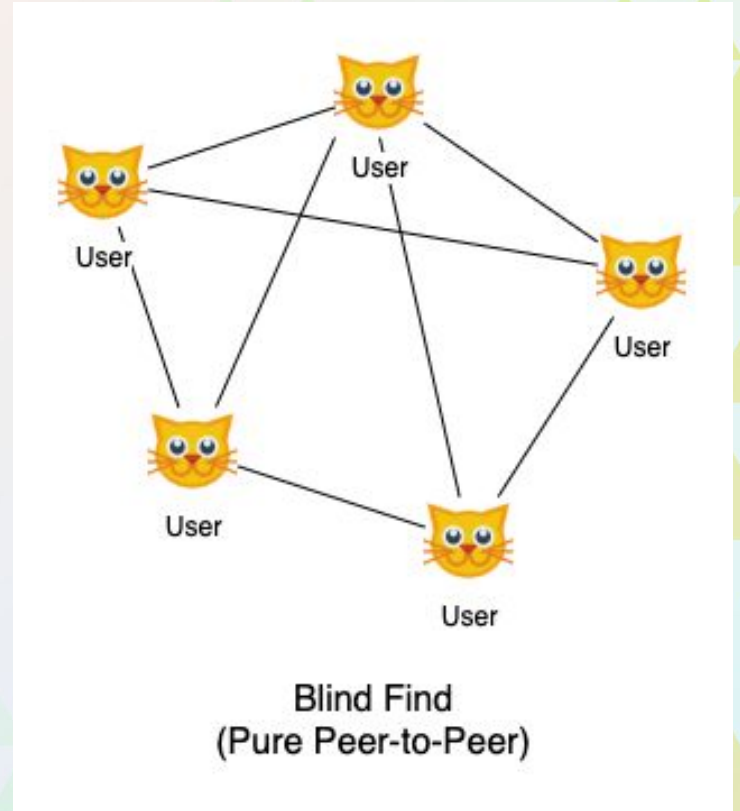


ZKOPRU
(*zk optimistic rollup*)



Blind-find

Find peers in a network without revealing that you are searching for Alice.



Socialist Millionaire Problem (SMP)

Check equality of two values without revealing the actual values

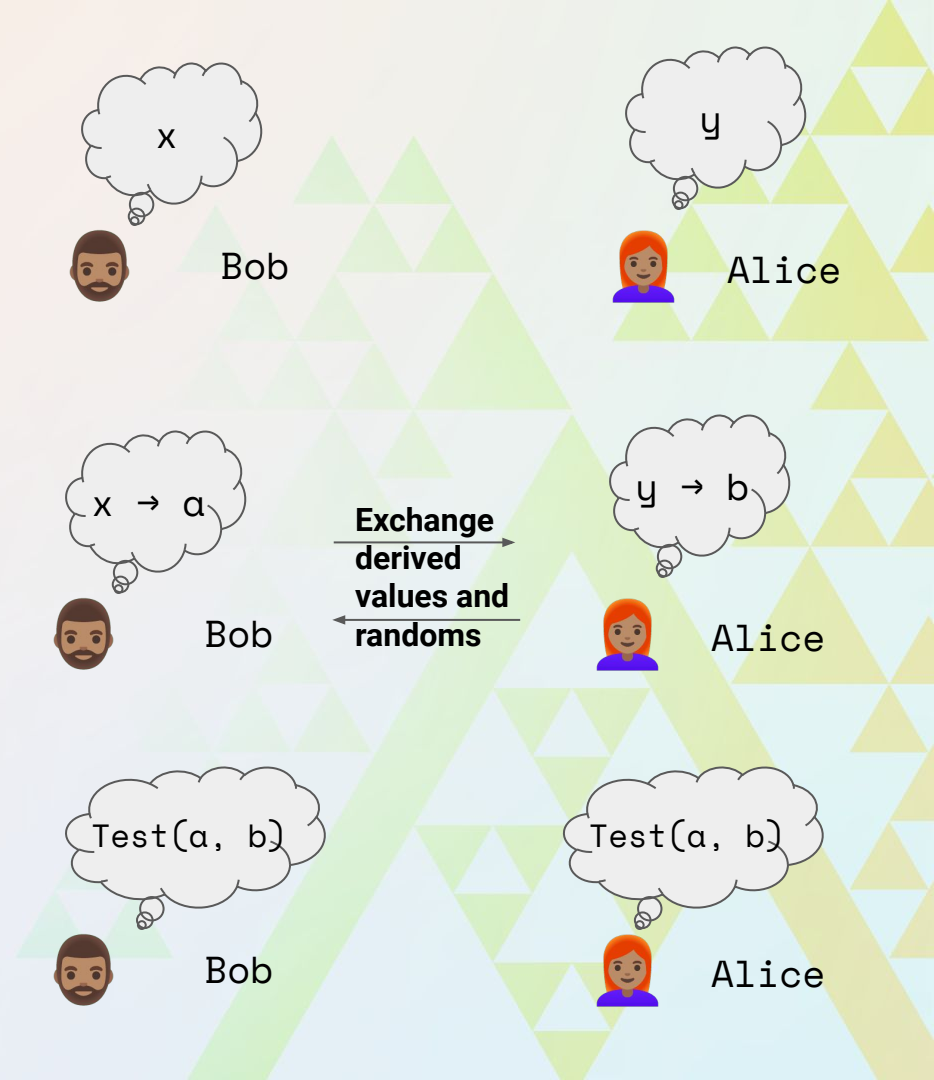
	Alice	Multiparty	Bob
1	Message x Random a, α, r	Public p, h	Message y Random b, β, s
2		Secure $g = \langle h a, b \rangle$	
3		Secure $\gamma = \langle h \alpha, \beta \rangle$	
4	Test $h^b \neq 1, h^\beta \neq 1$		Test $h^a \neq 1, h^\alpha \neq 1$
5	$P_a = \gamma^r$ $Q_a = h^r g^x$		$P_b = \gamma^s$ $Q_b = h^s g^y$
6		Insecure exchange P_a, Q_a, P_b, Q_b	
7		Secure $c = \langle Q_a Q_b^{-1} \alpha, \beta \rangle$	
8	Test $P_a \neq P_b, Q_a \neq Q_b$		Test $P_a \neq P_b, Q_a \neq Q_b$
9	Test $c = P_a P_b^{-1}$		Test $c = P_a P_b^{-1}$

$\langle h|a, b \rangle$: Diffie-Hellman key exchange



Socialist Millionaire Problem (SMP)

Check equality of two values without revealing the actual values



Socialist Millionaire Problem (SMP)

SMP process

1. Alice creates an ad
2. Bob find it
3. Bob reaches out to Alice in P2P network (Blind-find)
4. They execute order matching (SMP)
5. If price matches, they do swap transaction



Bob

Bob's Ad

Send : 1500 DAI
Receive: 1 ETH



**PARTIALLY PRIVATE
(SMP)**

Ad board



Bob



Alice

Bob's Ad

Send : 1500 DAI
Receive: 1 ETH



**PARTIALLY PRIVATE
(SMP)**

Alice's Ad

Send : 1 ETH
Receive: 1500 DAI

Ad board

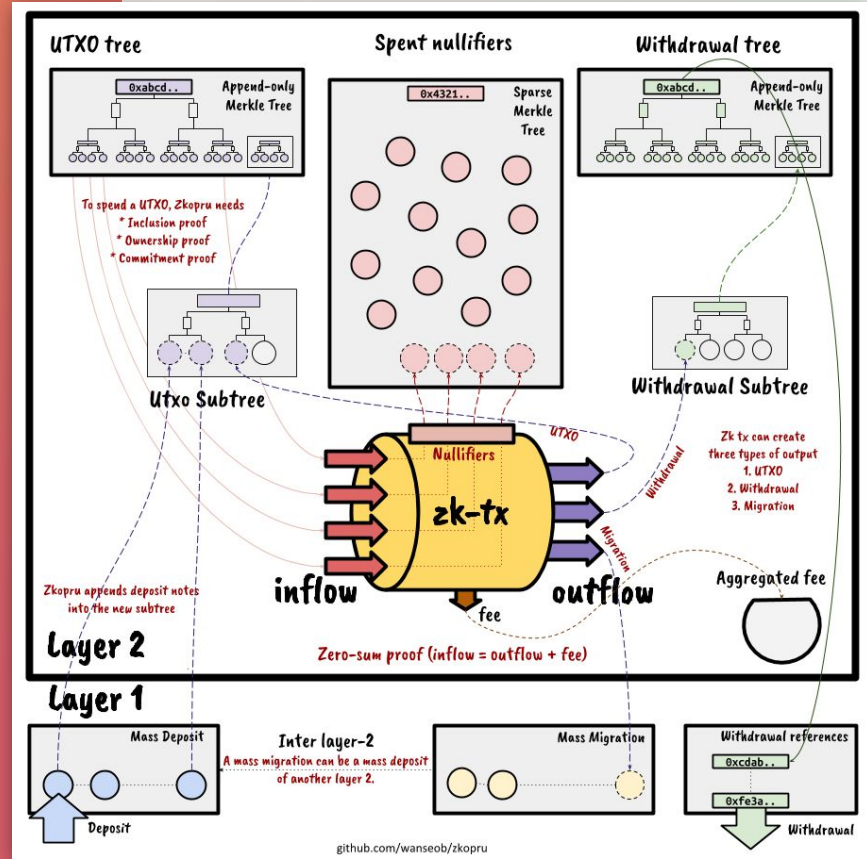
NOT PRIVATE

Swap txn

Blockchain

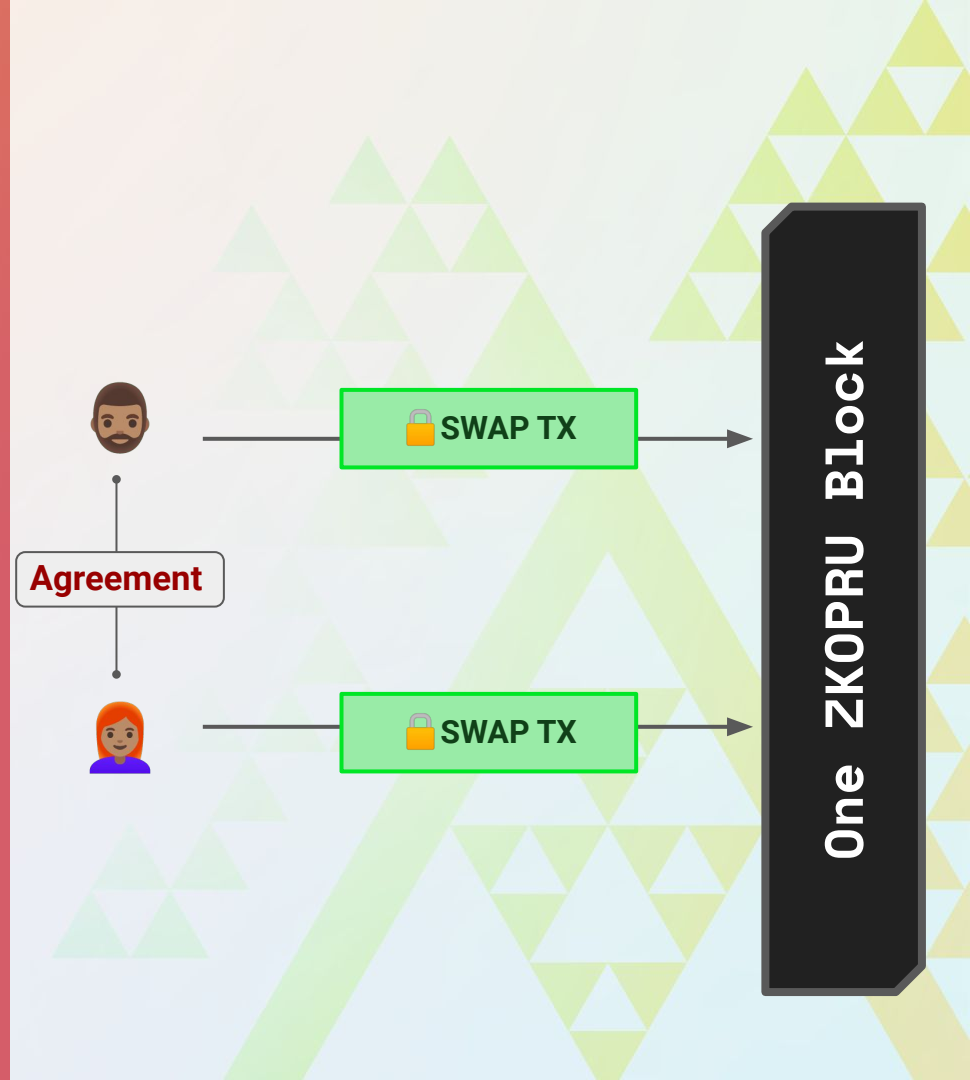
ZKOPRU

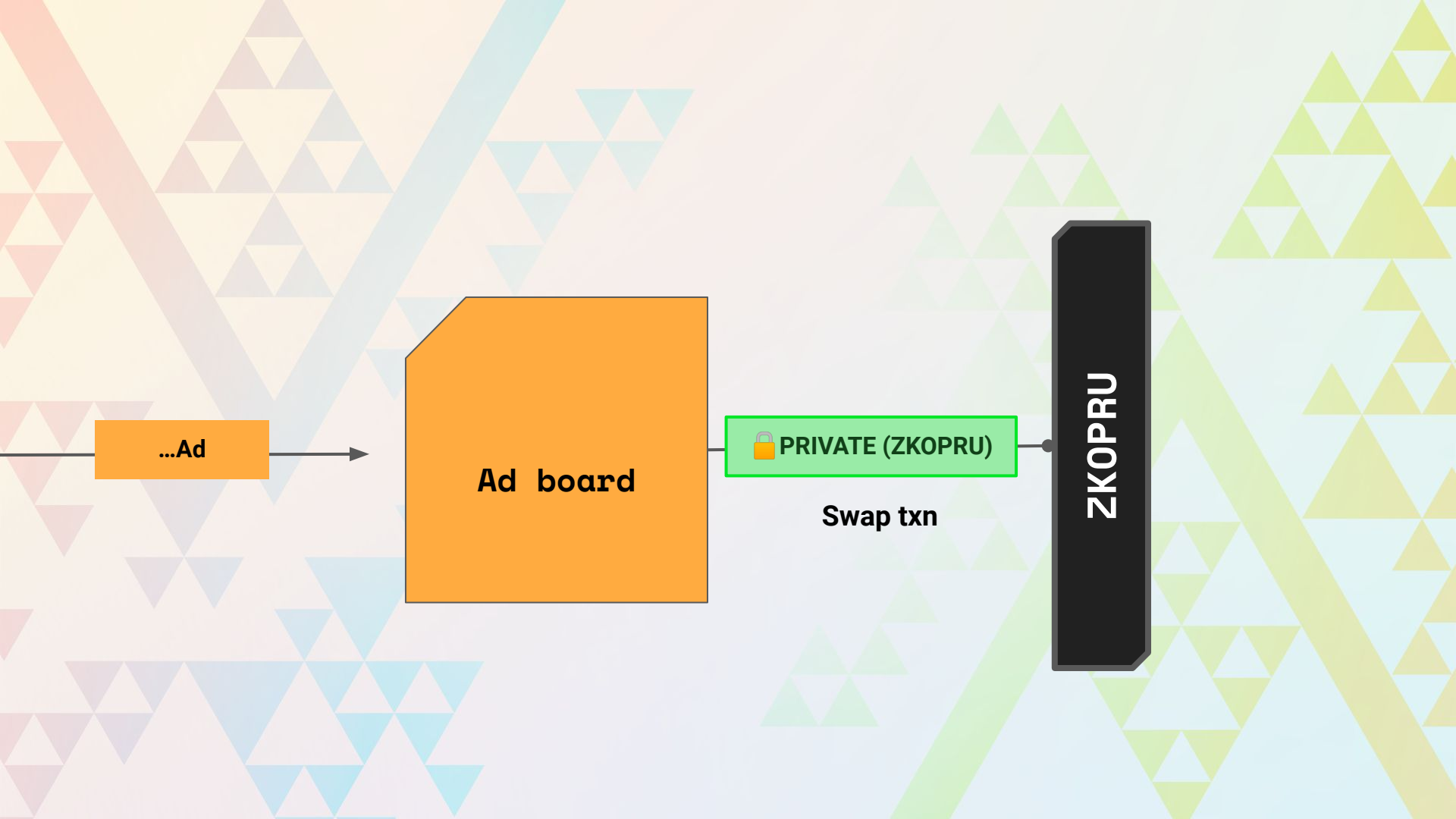
Secret transfer
with cheap gas



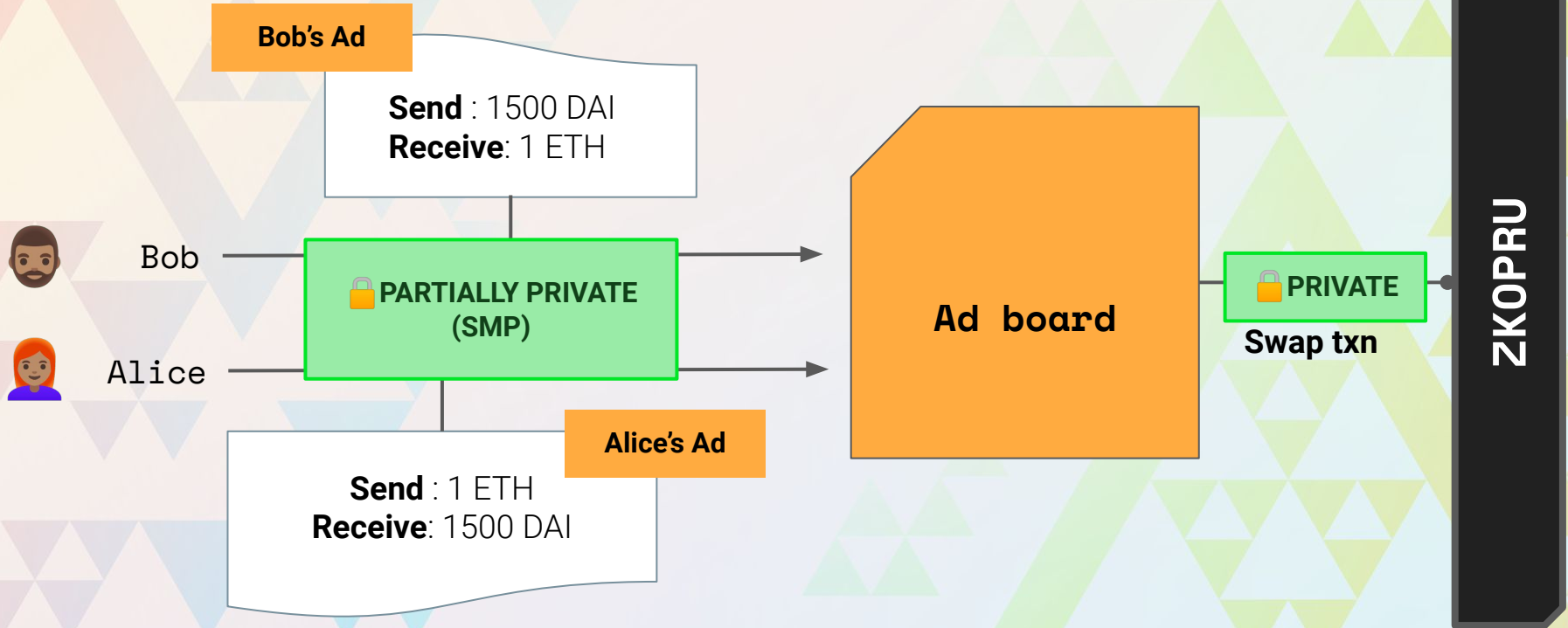
ZKOPRU

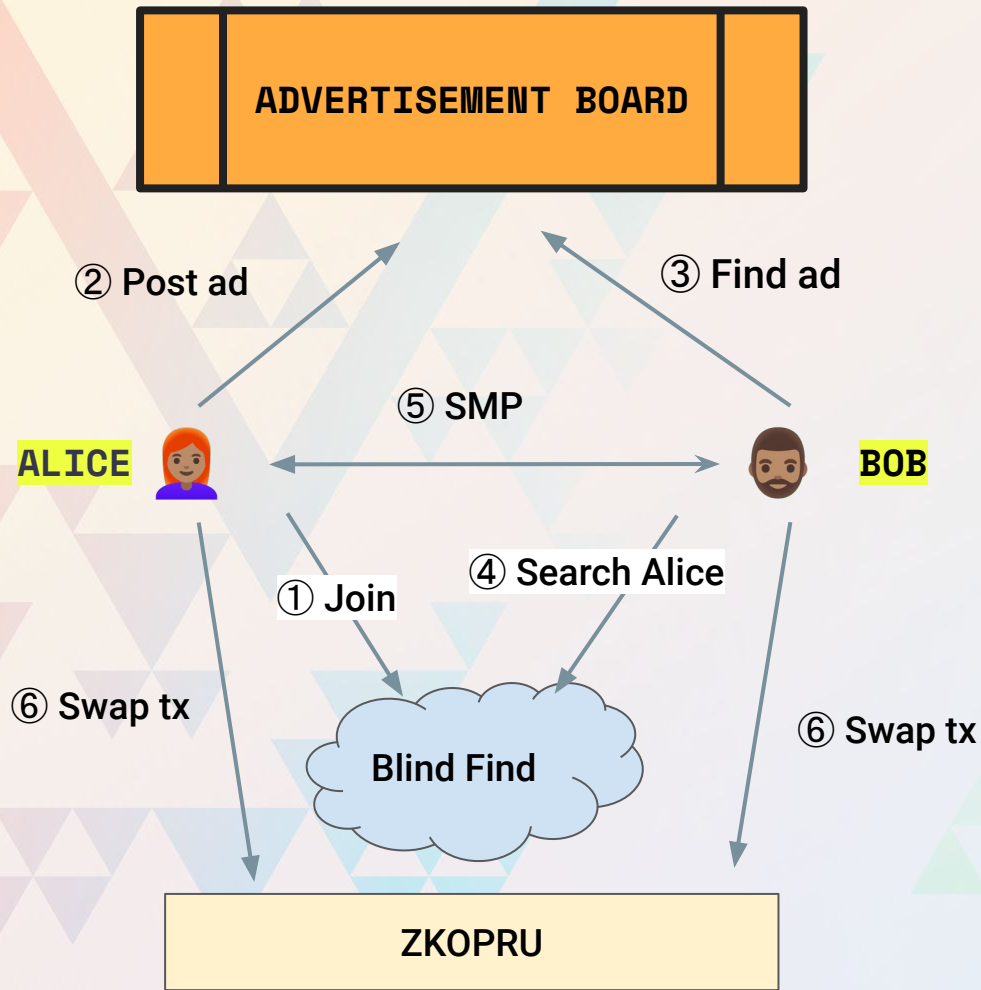
Secret
Atomic Swap





Private Exchange





Ad is partially private (price)

Price matching is done privately

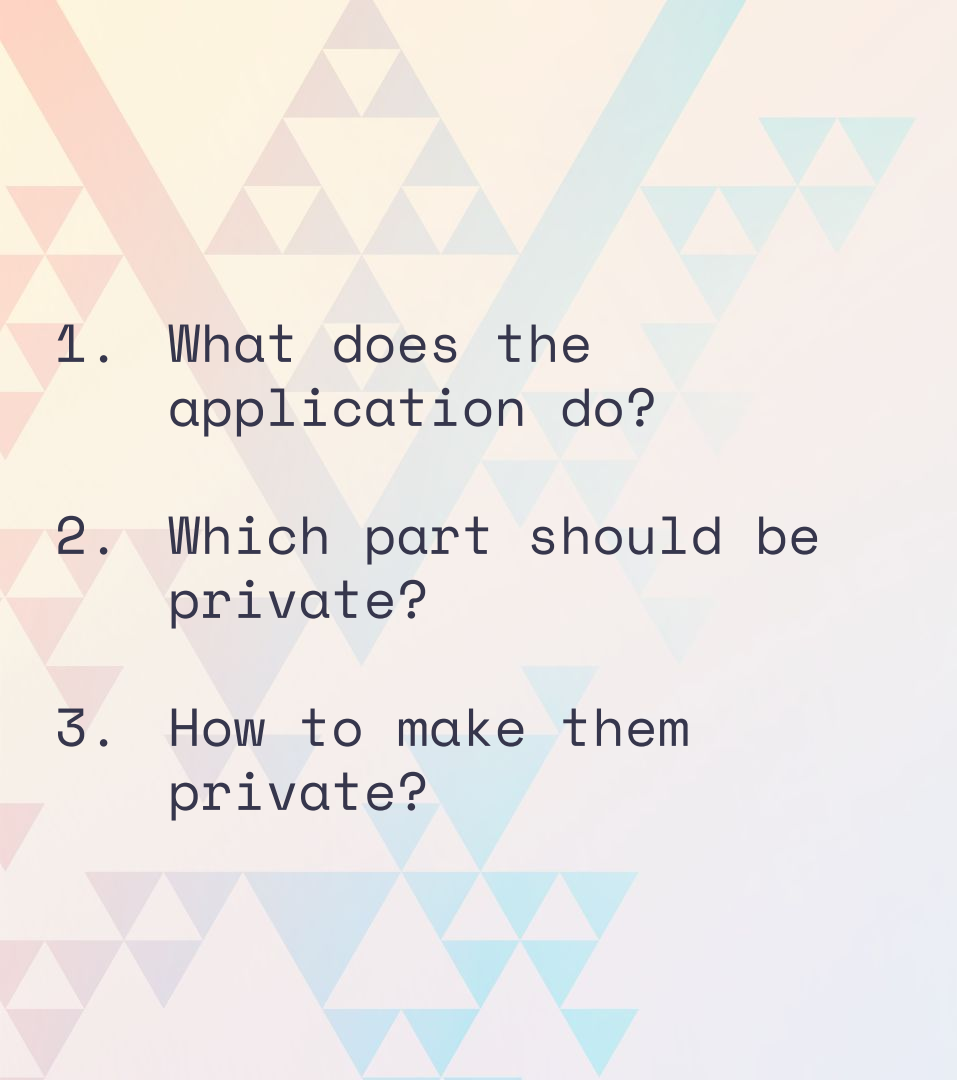
Peer finding is done privately

Tx content is private



Section 4

Summary

- 
1. What does the application do?
 2. Which part should be private?
 3. How to make them private?

Designing Privacy Application




Doesn't reveal
transactions content
(zkopru)

Doesn't reveal price of
orders to public (smp)

Doesn't reveal p2p routing
in network (blind-find)

**Private
Exchange
protects
privacy**



SMP can only check the
equality of exact values

Advertiser have to stay
online

Users need to join
blind-find before
starting the process

Challenges/ UX Compromisation

Privacy and Scaling Explorations



Links

[ZKOPRU] <https://docs.zkopru.network>

[SMP] https://en.wikipedia.org/wiki/Socialist_millionaire_problem

[Blind-find] <https://github.com/zkopru-network/blind-find>

[Private Exchange] <https://github.com/zkopru-network/private-exchange>

[PSE homepage] <https://appliedzkp.org/>