The Private Exchange
Building a privacy-focused dapp

Takamichi Tsutsumi
Software Engineer – PSE, Ethereum Foundation
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
What is Private Exchange?
Make exchange more private
What exchanges do

Alice sends
1.0 ETH

Alice receives
1500 DAI
Automated Market Maker (AMM)

Alice

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

Public txn

SMART CONTRACT
Orderbook

Alice

Order

Send: 1 ETH
Receive: 1500 DAI

Price: 1500 DAI / ETH
Orderbook

Alice

Send: 1 ETH
Receive: 1500 DAI

Bob

Send: 1500 DAI
Receive: 1 ETH

ORDERBOOK
Orderbook

Bob's order

Send: 1500 DAI
Receive: 1 ETH

Alice's order

Send: 1 ETH
Receive: 1500 DAI
Let’s make it more *private*
Orderbook

Bob's order

Send: 1500 DAI
Receive: 1 ETH

NOT PRIVATE

Bob

Alice's order

Send: 1 ETH
Receive: 1500 DAI

NOT PRIVATE

Alice

ORDERBOOK

NOT PRIVATE

Blockchain

Swap txn
Orderbook

Bob's order

Send: 1500 DAI
Receive: 1 ETH

Alice

Send: 1 ETH
Receive: 1500 DAI

Bob

How do we make this more private?
Three zk protocols
Our toolkit

Blind-find

Socialist Millionaire Problem (SMP)

ZKOPRU
(zk optimistic rollup)
Alice

Send: 1 ETH
Receive: 1500 DAI

Bob

Send: 1500 DAI
Receive: 1 ETH

NOT PRIVATE

Alice's order

Send: 1 ETH
Receive: 1500 DAI

NOT PRIVATE

Bob's order

ORDERBOOK
**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

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

$\langle h | a, b \rangle$ : 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 finds 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
Send: 1500 DAI
Receive: 1 ETH

PARTIALLY PRIVATE (SMP)
Alice

Send: 1 ETH
Receive: 1500 DAI

Bob

Send: 1500 DAI
Receive: 1 ETH

PARTIALLY PRIVATE (SMP)

Alice's Ad

Bob's Ad

Ad board

Blockchain

NOT PRIVATE

Swap txn
ZKOPRU

Secret transfer with cheap gas
ZKOPRU

Secret
Atomic Swap

One ZKOPRU Block

Agreement

SWAP TX

SWAP TX
...Ad

Ad board

PRIVATE (ZKOPRU)

Swap txn

ZKOPRU
Private Exchange

Alice

Send: 1 ETH
Receive: 1500 DAI

Bob

Send: 1500 DAI
Receive: 1 ETH

PARTIALLY PRIVATE (SMP)

Alice's Ad

Bob's Ad

Ad board

ZKOPRU

PRIVATE Swap txn
Ad is partially private (price)
Price matching is done privately
Peer finding is done privately
Tx content is private
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
[Blind-find] https://github.com/zkopru-network/blind-find
[PSE homepage] https://appliedzkp.org/