PROPOSALS

By Simon CHEREL & Enguerrand DECLERCQ

Contents

Topics to tackle

1. Current issues
2. Improvement proposals

Current issues

UX drawbacks

- Usage-based obfuscation;
- Fixed deposit and withdrawal amounts;
- One-to-one relationship between sending and receiving wallets.

Issue #1

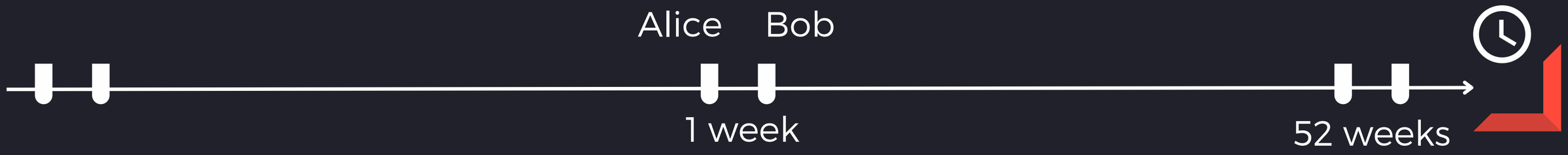
Usage-based obfuscation

- The protocol's guidelines encourage users to space deposits and withdrawals;
- Overall lack of usage of the protocol (especially in the high-amount pools);
- The fewer the transactions, the higher the risk of time correlations.

Issue #1

Example

- Let a pool that is used 3 times a year;
- Alice and Bob respectively deposit and withdraw funds in a 1-week time window;
- Because of the lack of usage, a time correlation is possible.



Issue #2

Fixed tx/rx amounts

- Great mechanism to enforce privacy;
- Expensive both in time and gas fees for "exotic" amounts;
- **Example:** let a protocol containing 3 token T pools (0.1 T, 1 T and 10 T) a user willing to mix 15.3 T has to use the protocol 9 nines in total.

Issue #3

One-to-one relationship between sending and receiving wallets

- Some users want to send their funds to differente wallet addresses;
- To do so, they need to split their deposit in separate transactions;
- This implies a previous agreement between the sender and the receiver to have one deposit/receiving wallet;
- Gas fees evolve linearly with the number of deposits.

Proposals

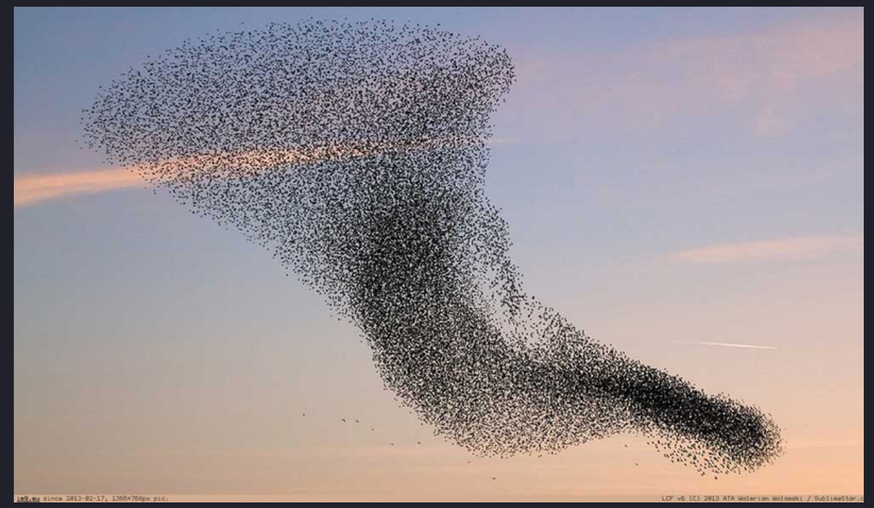
Privacy-enhancing design

- Transaction fuzzing;
- Batched withdrawals;
- Multiple recipient addresses

Proposal #1

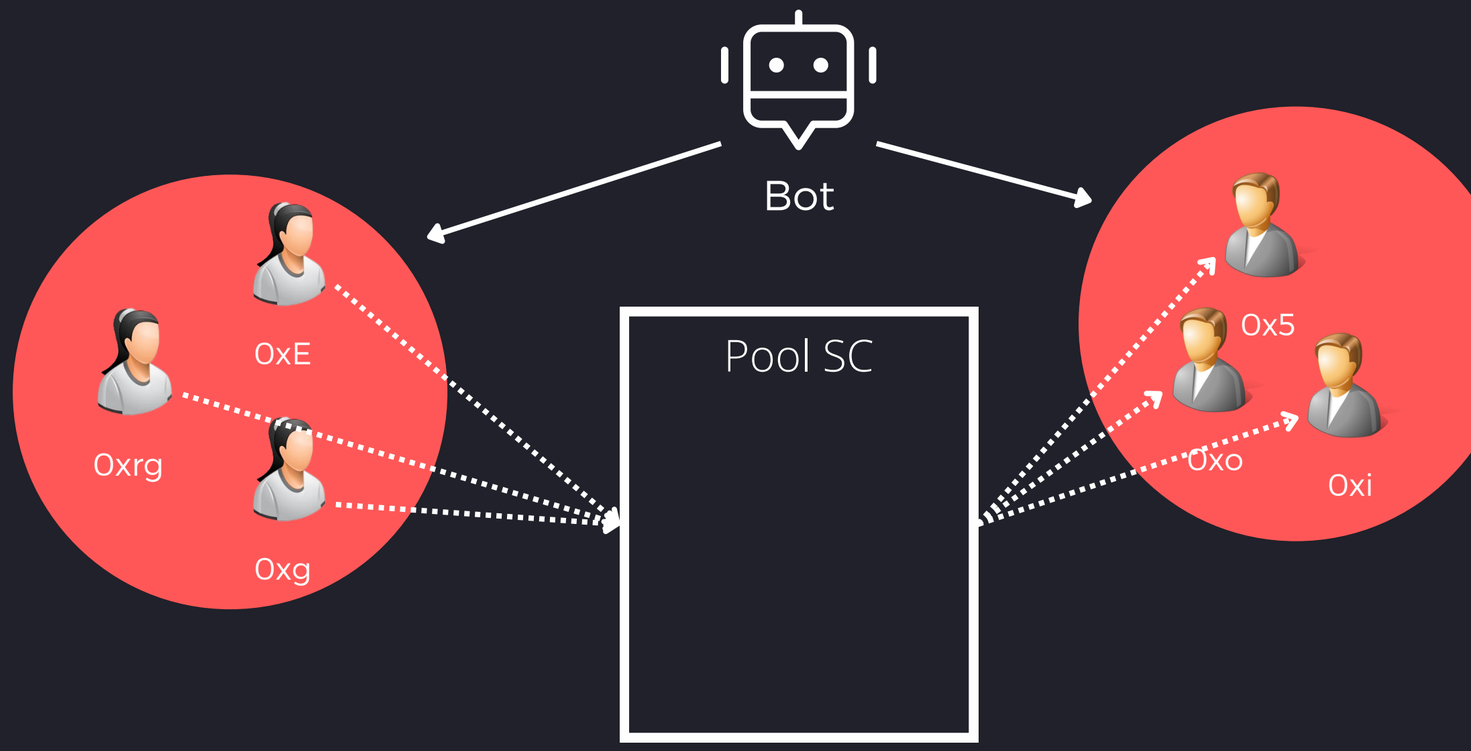
Transaction fuzzing

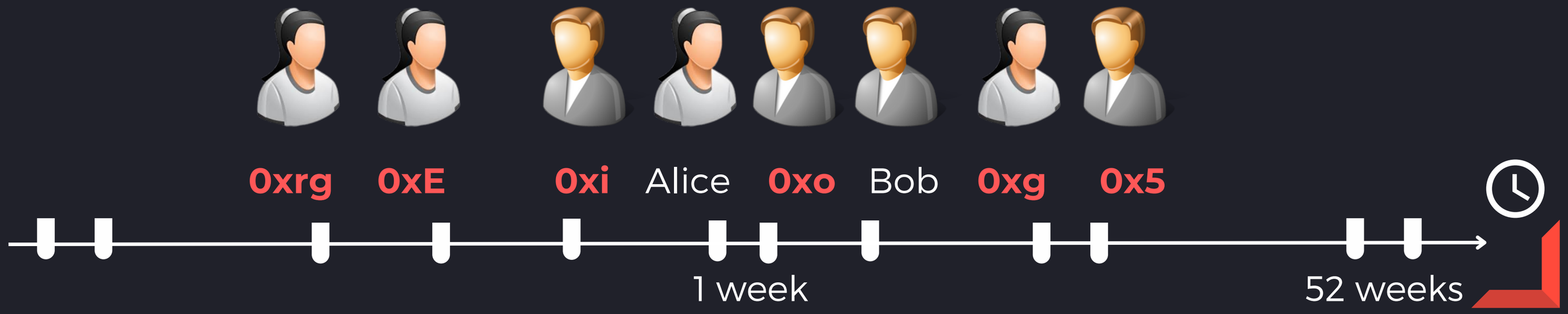
- Flooding the protocol with mixing transactions to artificially increase traffic;
- Bots swarm mixing funds back-and-forth;
- Liquidity providers are financially incentivized to lend funds to the bots;
- One-to-one relationship between a user and a bot;
- The list of LPs can be stored on-chain without threatening privacy;
- No predictible time-based patterns.



Proposal #1

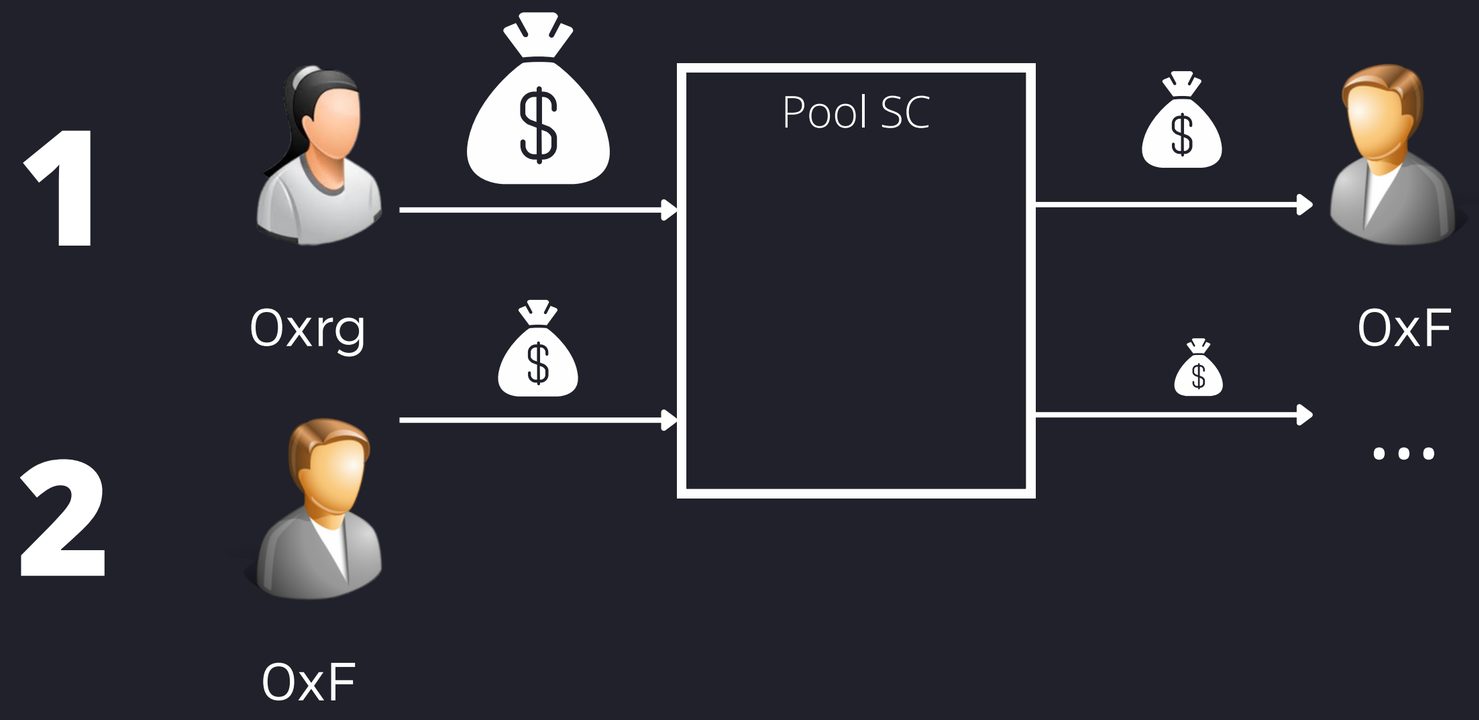
Diagram





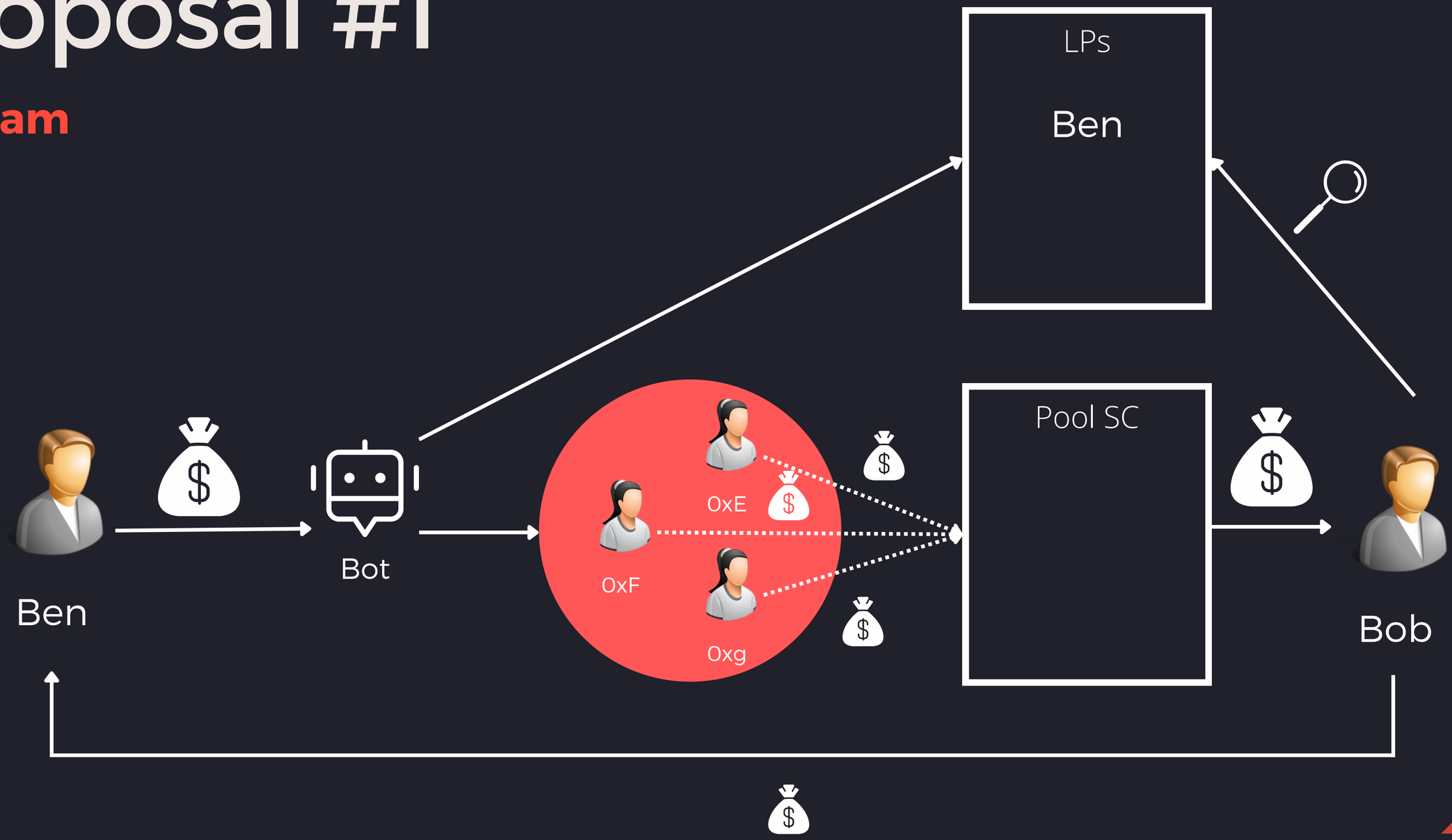
Proposal #1

Diagram



Proposal #1

Diagram



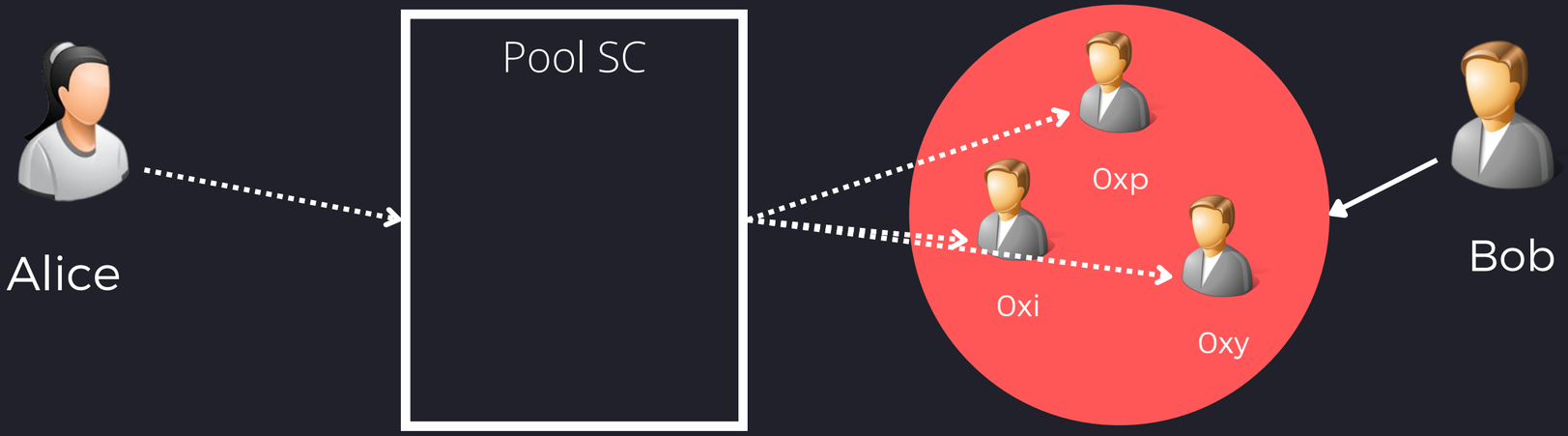
Proposal #2

Batched withdrawals

- In current implementations, users redeem their funds whenever they want;
- Human behaviour can harm privacy;
- Instead, withdrawals should be sent altogether;
- Fixed-size withdrawal batches;
- Mitigates time-correlation risks;
- Compliant with the previous improvement proposal;
- Users are financially incentivized to release transactions;
- No relayer-network.

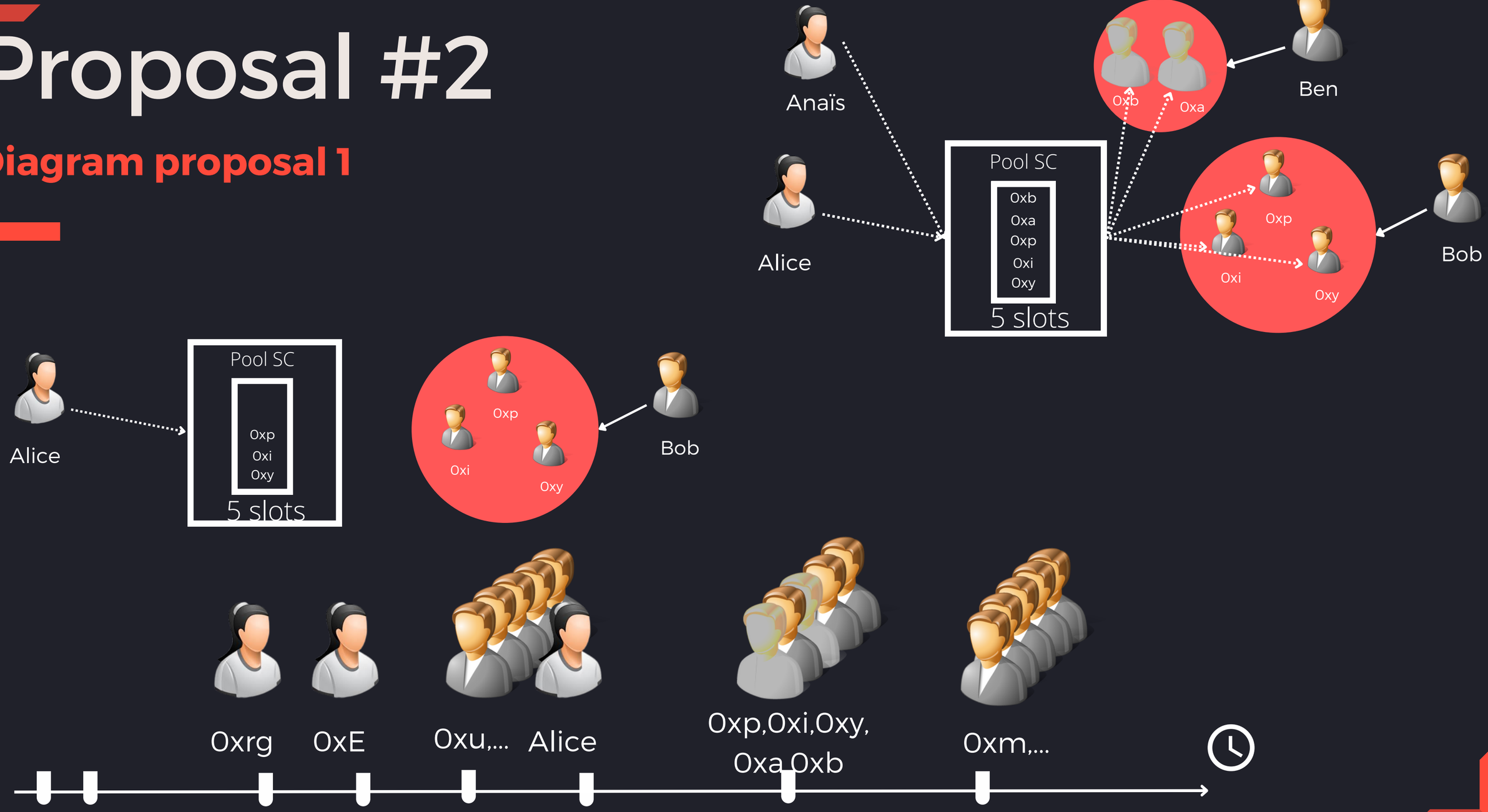
Proposal #2

Diagram issue



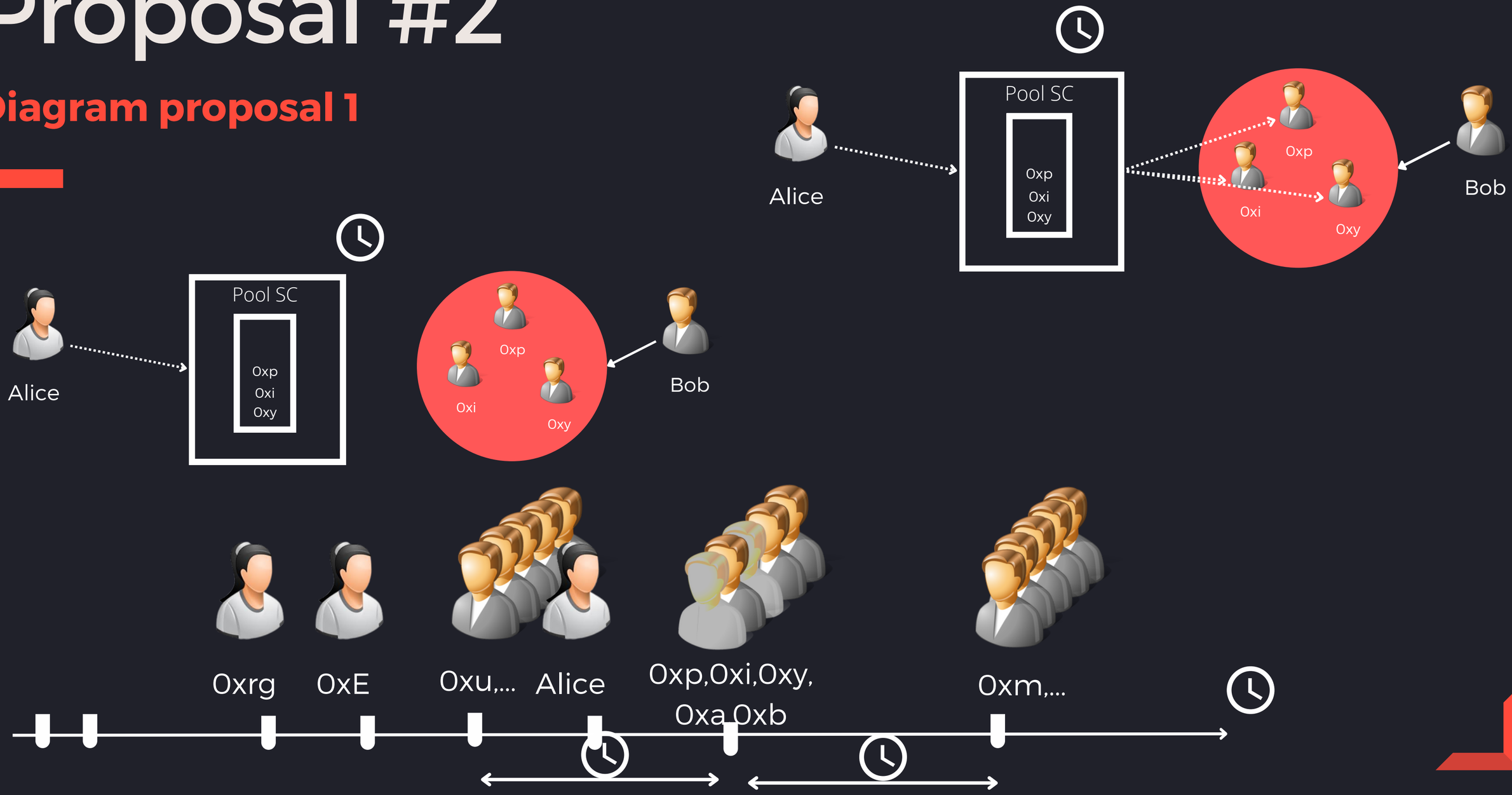
Proposal #2

Diagram proposal 1



Proposal #2

Diagram proposal 1



Proposal #2

Issues

- Storing the queued publicly the queued receiving addresses would make no sense;
- Storing them off-chain would raise trust issues.

Proposal #3

Multiple recipient addresses

- Storing the queued publicly the queued receiving addresses would make no sense;
- Storing them off-chain would raise trust issues.