Intro

There has been a lot of interest lately in private smart contracts. The thinking that we have the EVM which is good. So it would also be good if we have a private version of the EVM. Where no one knows what anyone else is doing.

The EVM has two components the execution which takes a mix of input from users and the global state. Global state is any variable that a user is able to update during their transactions. For example the contracts balance this.balance

can be updated by sending 1 eth to the contract. Or the contracts internal variables such as that contracts balance of an erc20 token.

ZKPs allow you to prove the state of some data that you know. They do not let you prove about things that you do not know.

So ZKPs solve the first part they let you have a private execution. But they don't let you have private global state.

Here we discuss an example smart contract that is impossible. We hope that this will help others reason about what is and is not possible with zkp based private smart contracts.

Lack of global state

Uniswap is a constant product exchange. It is a very simple ethereum smart contract that allows people to trade. The contract holds balance of two tokens, token a and token b. It lets you deposit token a and withdraw some amount of token b defined by the ratio in the pools between bal(token_a)

and bal(token_b)

Find more info on constant product exchanges in the original post byAlen Lu.

In order to build a private uniswap users need to deposit tokens A and withdraw token B. In order to prove that they have correctly withdrawn they need to know what the current balance of token A and token B are.

If you tell users what the current state they will be able to observe other users interactions see the state before and the state after someone else has used the contract. Using this they can infer what these users have done.

For example say the pool has 1 eth and 1 dai. I know the state but I don't see users actions. Lets say a user does something. I don't know what but the new state of the system is 2 eth and 0.5 dai. I know that they deposited 1 eth and removed 0.5 dai.

Conclusion

So anyone who is able to update the system must have this state info in order to create the zkp that they updated correctly. If they have the state info they can monitor as the state changes. If they can monitor as the state changes they can see what others are doing.

So with ZKPs you end up building private things using only user specific state. So everything is like an atomic swap. If there is global state then this breaks privacy as it needs to be shared for others to make proofs about this state.

https://en.wikipedia.org/wiki/Indistinguishability_obfuscation can allow us to make global private state but that tech is a long way from production IMO.