Atomic swaps

Lorenzo Tucci

March 12, 2024

Parties U_0 and U_1 hold assets a on blockchain $\mathbb{A}$ and assets b on chain $\mathbb{B}$ respectively.
We define with $\mathsf{swp}(a)$ and $\mathsf{swp}(b)$ the amount of the assets the parties agreed to swap before starting the protocol.

We define the following oracles to interact with the blockchains.

- $\mathsf{PubTx}(\sigma_{tx}, tx, \mathbb{A})$ publish the transaction tx with signature σ_{tx} on chain $\mathbb{A}$
- $\mathsf{InitTx}(pk_{tx}, pk_{rx}, amnt, \mathbb{A})$ create an unsigned transaction paying $amnt$ from pk_{tx} to pk_{rx} on chain $\mathbb{A}$
- $\mathsf{WatchTx}(tx, \mathbb{A})$ wait for the transaction tx to be confirmed on chain $\mathbb{A}$
- $\mathsf{GetBal}(pk, \mathbb{A})$ get the balance of assets held by pk
- $\mathsf{GetSig}(pk, \mathbb{A})$ get the signature σ_{tx} of the latest transaction in pk's record on chain $\mathbb{A}$

U_1 starts counting the timeout from the moment they send the VTD commitment to U_0, and respectively U_0 starts counting down from the moment they receive it.

If the timeout expires before the protocol is completed:

- U_1 will transfer the coins from $pk(1)$ to another wallet on $\mathbb{B}$. From this moment on, if U_0 tries to $\mathsf{PubTx}(\sigma_{\mathsf{swp}(10)}, tx_{\mathsf{swp}}, \mathbb{A})$, the transaction will get rejected.

- U_0 will wait until $\Pi_{\mathsf{VTD}}.\mathsf{ForceOp}(C)$ is completed to get the other secret key share $sk_1(01)$ of $pk(10)$ to retrieve $sk(10)$ and transfer back assets a to $pk(0)$.

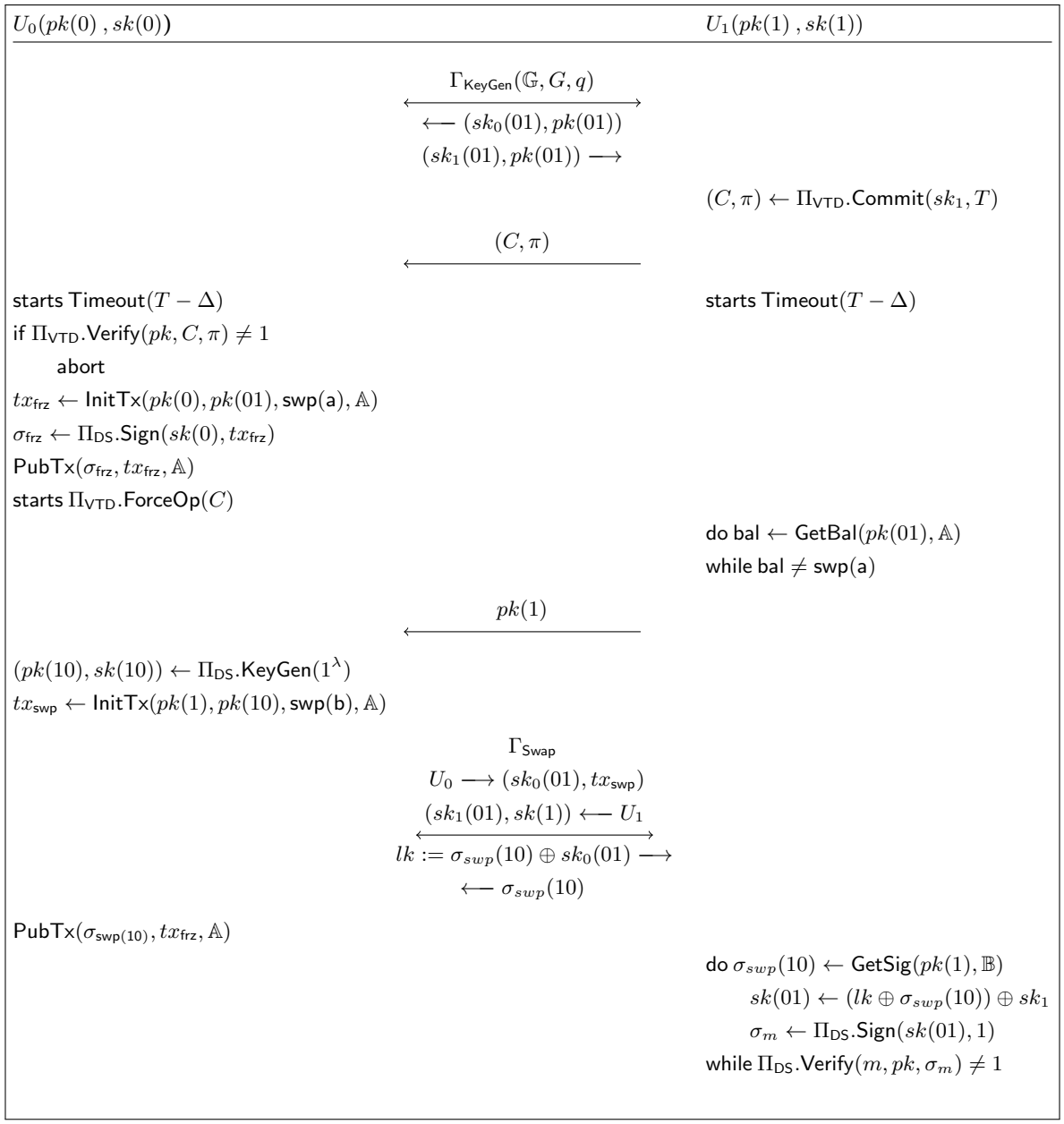

Figure 1: Protocol execution for a successful swap

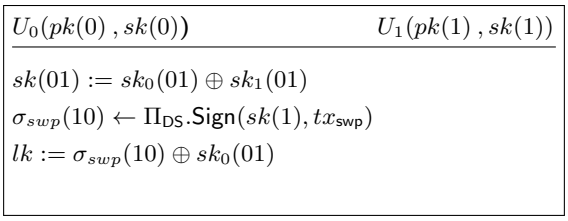

Figure 2: Protocol definition of 2PC Γ_{Swap}