Homework 1

zuli

8. April 2022

1 Design and draw out a multi-stage Tx System

1.1 Goals and purpose

A multi-stage contract adds an additional layer of security to a transaction that can be implemented as a trustless proxy adress, for example as an automated release escrow service, or by use of a conditional smart contract that grants time or adress-sequence sensitive accessability. It facilitates the evasion of off-chain liabilities ranging from hot-wallet private key compromise to smart contract powered refundability of a transaction.

1.2 Parties involved

Third party reliability can be circumvented by using a multi-stage contract between two individuals. Depending on the number of participants mutliple non-dependant stages can be implemented. As an example:

A+B only pay when C+D or E pay in advance. E is only willing to participate, if A+D contribution is larger than B's. B on the other hand wishes to know how liquid A is before the transacting, but A only intends to show during the payment. Such a case can be simplified in a multi-stage smart contract without the parties relying on different mediators doing the work and verifying each other multiple times during different stages.

1.3 An overview of the transactions themselves

A time sensitive acessability of funds could require a second stage to „change the lock“ after a certain block height. Given that the block times stochastically even out after a while, the reliability of such a condition can vary depending on the scope of time. An example for a time conditioned contract could be the following example:

Let F have 10.000 Block times to pay G 100 Erg, but every 1000 Blocks, F has to lock at least 5 Erg in the contract as part of repayment. If the 100 Ergs are not paid in time, G is not granted acess to F's deposits, but instead receives the previously locked collateral and F is granted access to his deposits.

2 Specify the following information

2.1 Purpose of the box

The box poses the foundation of each user's fungibility during a transaction, be it P2P or multi-stage smart contract interaction. It carries or stores its content with immutability, yet still remains transparent and „spendable". Each box can be assigned data that can be drawn from by programmable validators and code that be used as means of conditions or verifications of a transaction.

2.2 Registers

There are four predefined registers: monetary value (R0), protecting script (R1), token (R2) and identifier of a transaction which created the box, output index of the transaction and the block height during its creation (R4). A box may have up to six additional registers with typed data. The script is able to access its registers and registers of input and output boxes of the spending transaction.

2.3 Guard Script

Ergoscript is the language used to guard the contents of a box from malicious takeovers. During every transaction the guard script checks the validity of the key for the box's lock and wether it is allowed to create new boxes under preset conditions. If a transaction is invalid, the guard script prevents the box from being converted to being classified as „spent" and since Turing-completeness is given, a rejection of a transaction is only determined by the code's logic.