sCrypt Smart Contract

TIMECHAIN LABS

PROGRAMMING VALUE

Task #1: Create a Wallet

Understanding ECDSA Key Pairs and Addresses

Task #2: Create a transaction

Understanding inputs and outputs and broadcasting to nodes and viewing on explorer

Standard Payment

Locking Script (ScryptPubKey):

Pay to PubKey Hash

```
OP_DUP OP_HASH160 <pubKeyHash>
OP_EQUALVERIFY OP_CHECKSIG
```

Unlocking Script (ScryptSig):

```
<sig> <pubKey>
```

Task #3:
Create a conditional output

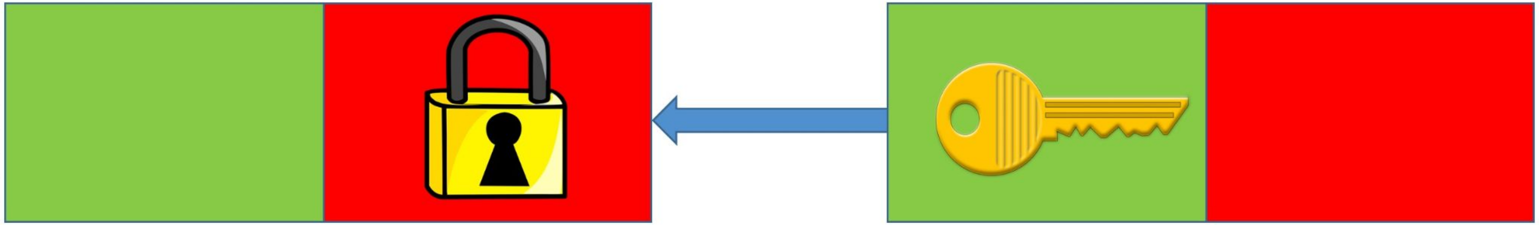
(Smart Contract)

UTXO

An Unspent Transaction Output (UTXO) is an output not consumed in any transaction yet.

The low-level bytecode/opcode is called Bitcoin Script, which is interpreted by the Bitcoin Virtual Machine (BVM).

UTXO Model



$$f() \qquad\qquad\qquad x$$

$$f(x) = \begin{cases} true & \checkmark \\ false & \times \end{cases}$$

UTXO

An **output** contains:

The amount of bitcoins (satoshis) it contains.
bytecodes (**the locking script**).

While an **input** contains:

A reference to the previous transaction output.
bytecodes (**the unlocking script**).

Typescript Smart Contracts

sCrypt is an embedded Domain Specific Language (eDSL) based on TypeScript for writing smart contracts on Bitcoin SV.

Embedded means that it is a language inside another language. sCrypt is strictly a subset of TypeScript, so all sCrypt code is valid TypeScript, but not vice versa.

Custom Information Locks

sCrypt is a high-level language to be compiled into Bitcoin Script. The resulting assembly-like scripts could be used as **locking scripts** when building transactions.

Prerequisites

1. Install Node.js (require version >=16) and NPM
2. Install Git.
3. Install VS Code or any other code editor supporting Typescript

Clone template repository:

`git clone https://github.com/timechainlabs/smart-contract-demo`

Clone template repository:

`git clone https://github.com/timechainlabs/smart-contract-demo`

Install all packages

`npm i`

Compile

`npm run compile`

Deploy

`npm run deploy`

How to write a smart contract

https://docs.scrypt.io/how-to-write-a-contract

Workshop Attendance

SCAN the QR Code below to mark your attendance

BSV Association Discord

Go to #tsoc-2024 and post your Bitcoin Script certificates

Thank you

TIMECHAIN LABS

PROGRAMMING VALUE