Sensible Fungible Token方案

陈诚

独立开发者

Bitcoin SV BOOTCAMP

概要

- token实现方案
- 基于token方案实现扩展：swap

特性

- 高并发
  - 基于utxo模型
- 零确认
  - 与bsv同级别的零确认速度
- 高安全性
  - 合约逻辑由矿工验证

设计原则

- 保证合约代码精简

代码少的好处

- 减少bug，提高合约安全性
  - 每个token的utxo都是一份完整的合约

代码少的好处

- bug少
- 交易手续费少

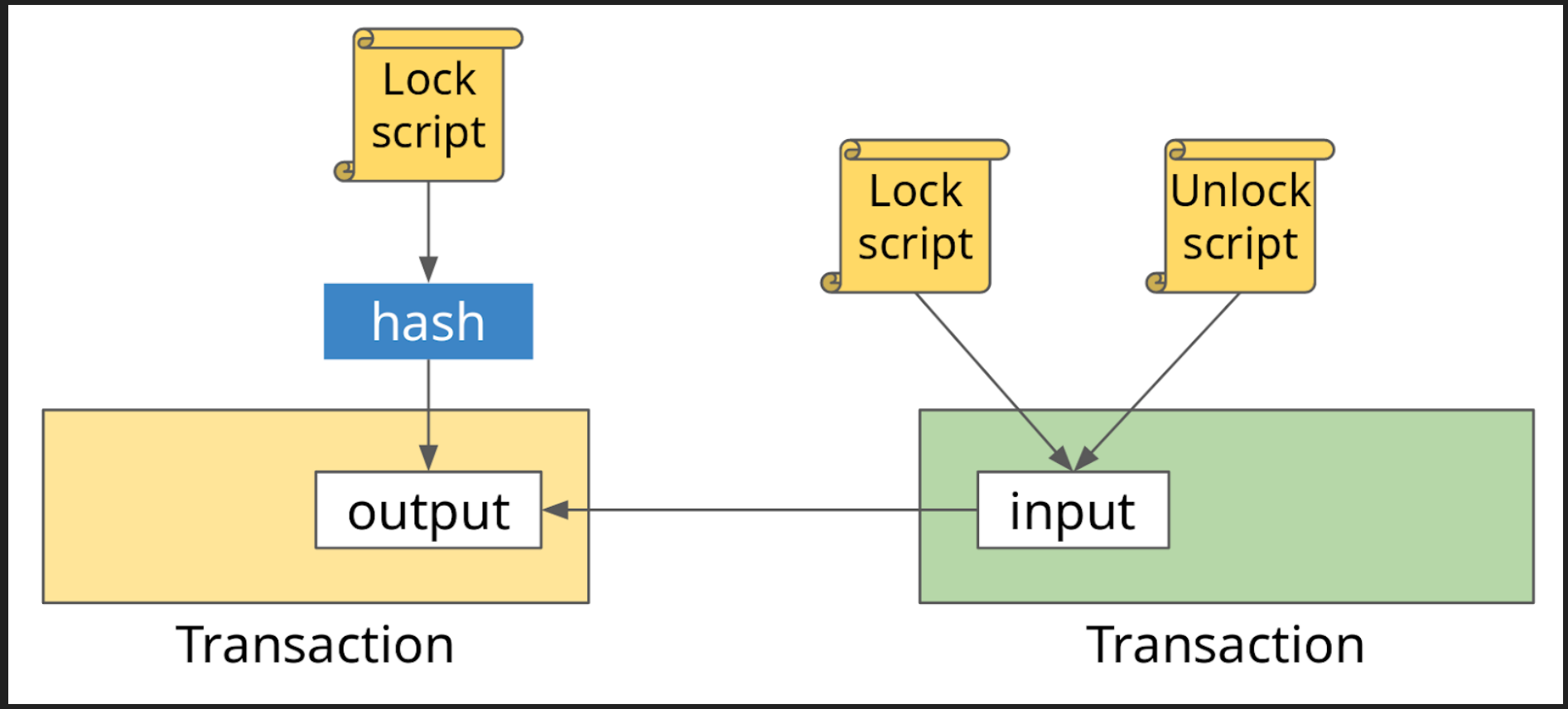
设计原则

- 保证合约代码精简
- 可扩展性
  - 支持第三方的开发者开发基于token合约的应用，比如多签，dex，借贷等等。

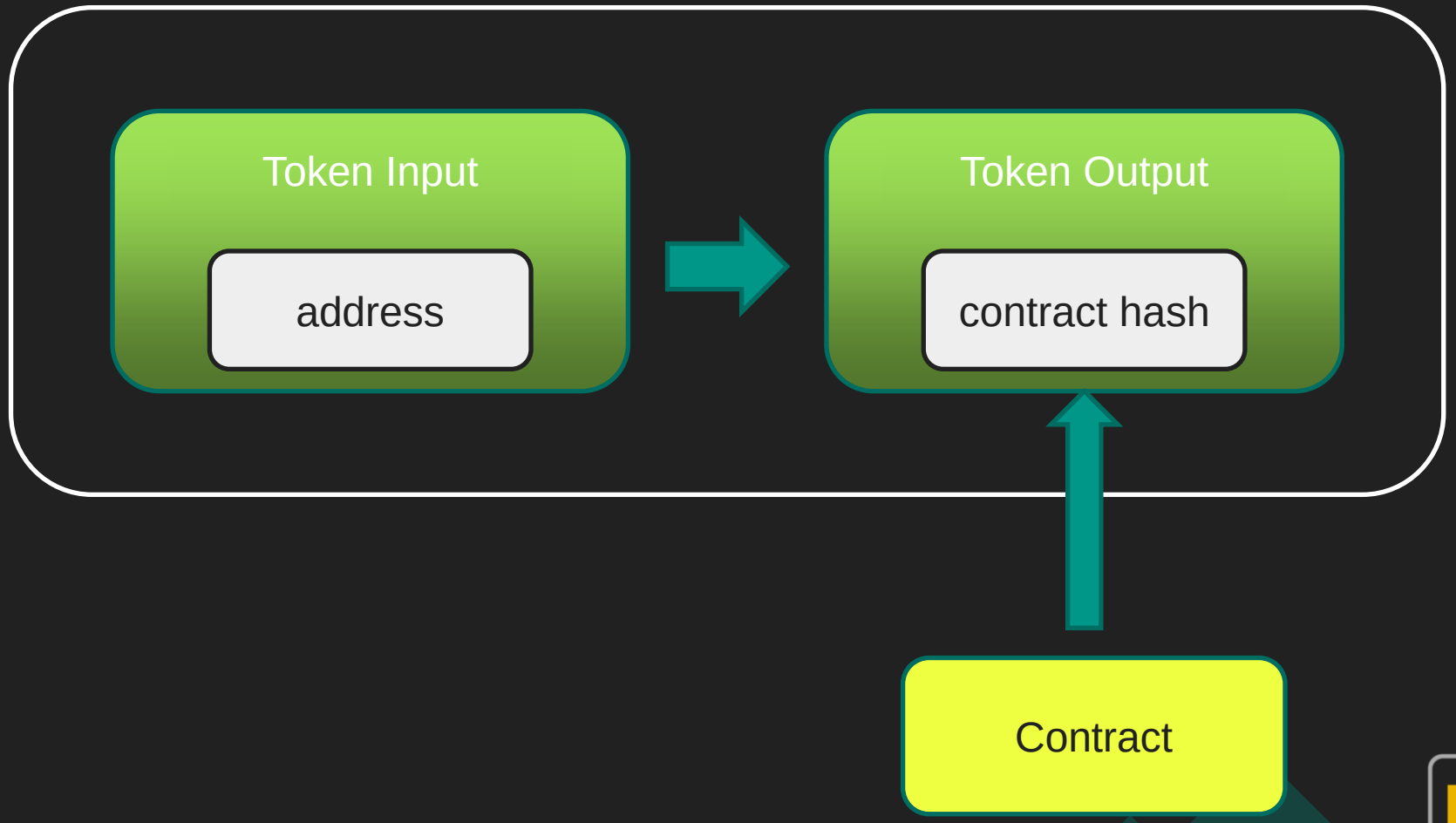
Pay To Contract Hash

把token的控制权交给合约。

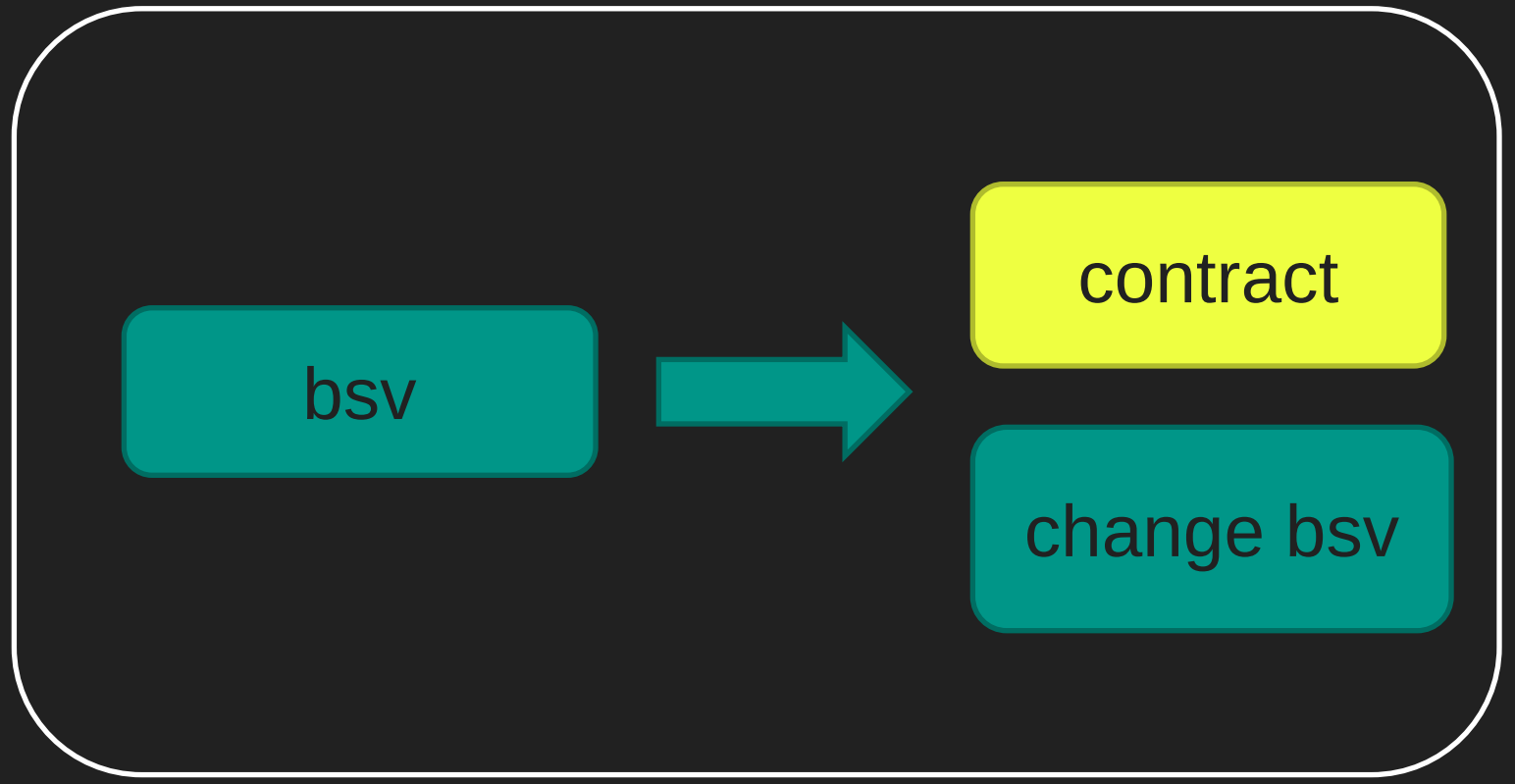
Pay To Script Hash



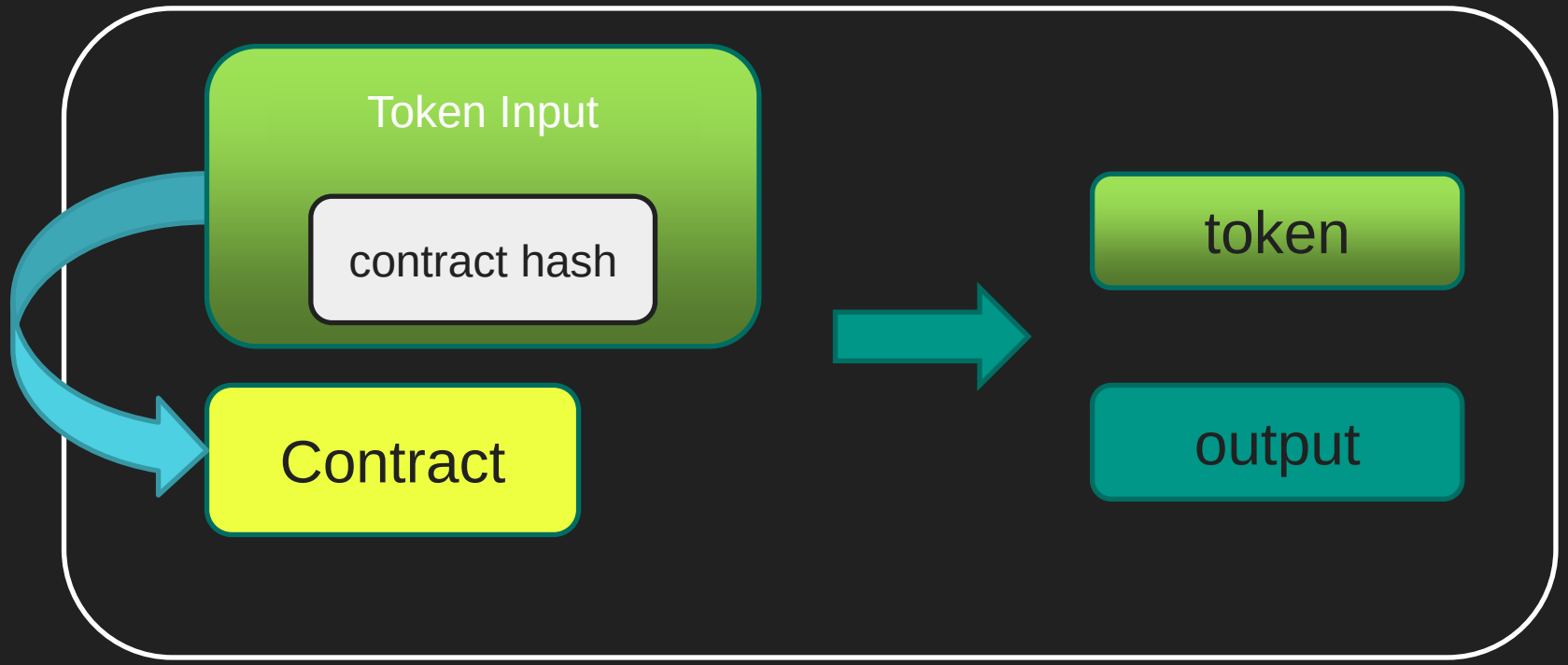
Pay To Contract Hash



Pay To Contract Hash



Pay To Contract Hash



Token合约

数据格式

Token基本功能

- 转账(route)
- 从其他合约解锁(unlockContract)

转账

- 检查输入输出的数量是否相等
- 遍历交易的输入和输出
  - loop展开导致合约代码扩大

合约大小

- routeAmountCheck
  - 3输入3输出，5858 bytte
  - 6输入6输出，9995 byte
  - 12输入12输出，18269 byte

合约拆分

- 把数量检查的功能拆分成一个独立合约
  - tokenRouteAmountCheck
- 提供多种输入输出组合的合约
- token合约在转账时中检测输入中是否存在数量检查的合约

```
return hash == contractCodeHashArray[0] ||
hash == contractCodeHashArray[1] || hash ==
contractCodeHashArray[2] || hash ==
contractCodeHashArray[3] || hash ==
contractCodeHashArray[4];
```

Bitcoin SV
BOOTCAMP

合约拆分

amountCheck
3:3

amountCheck
6:6

amountCheck
10:10

Token

合约拆分

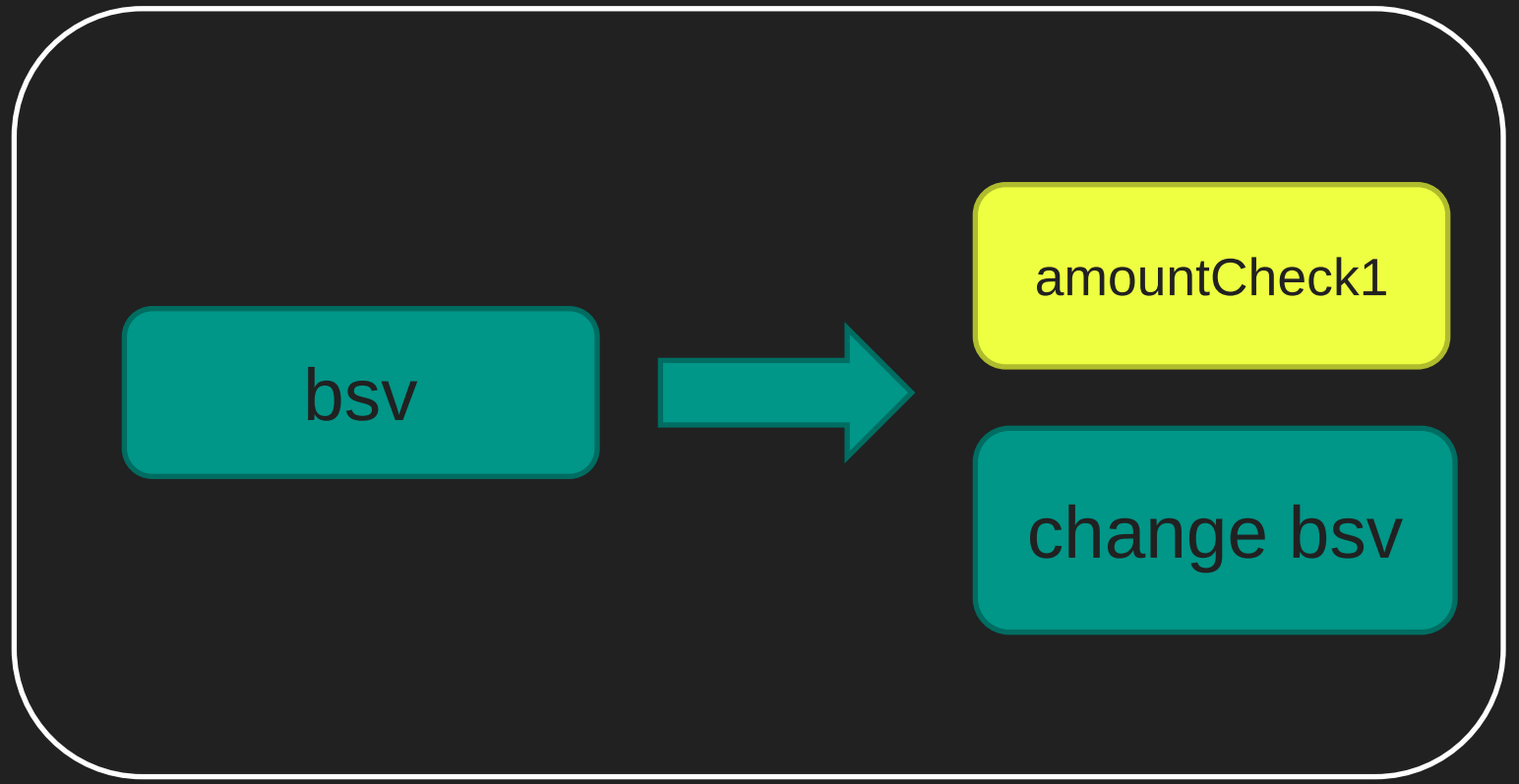
amountCheck
3:3

amountCheck
6:6

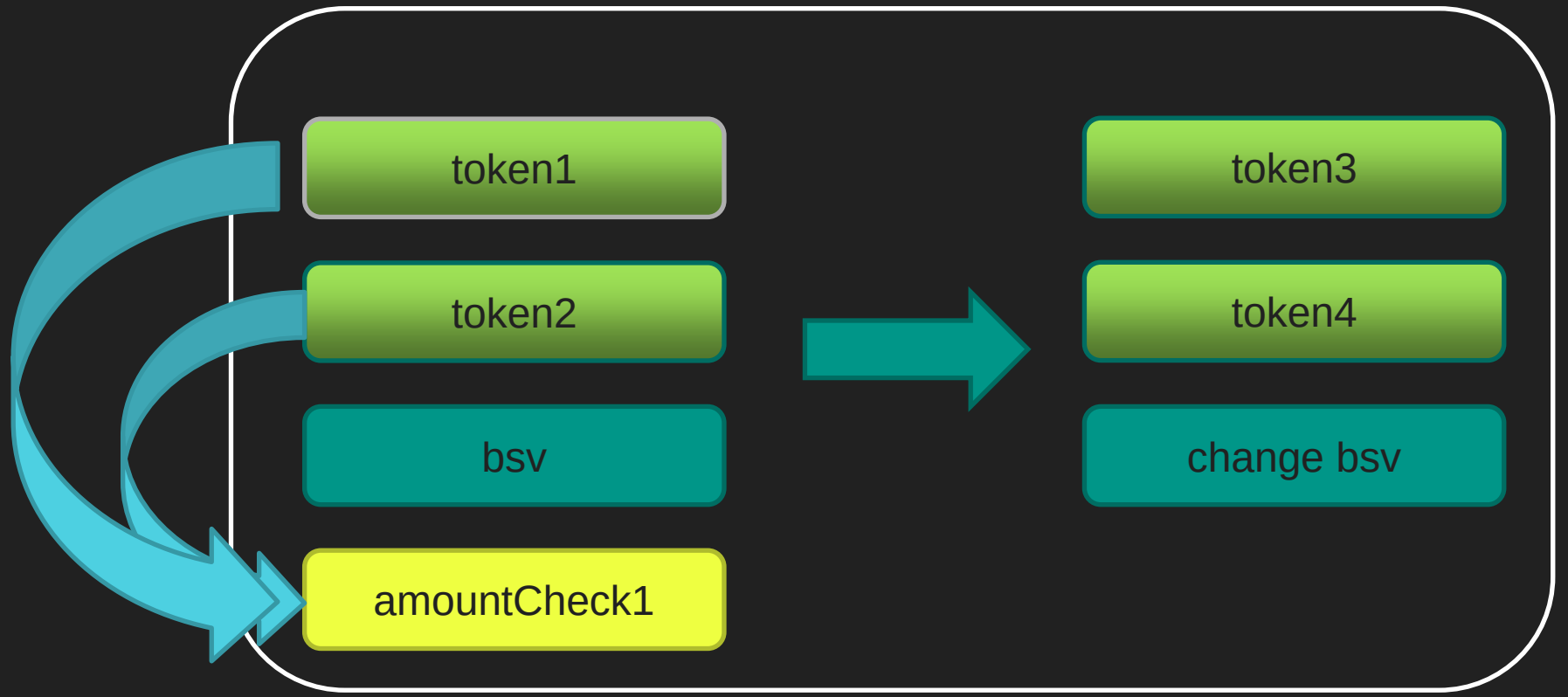
amountCheck
10:10

Token

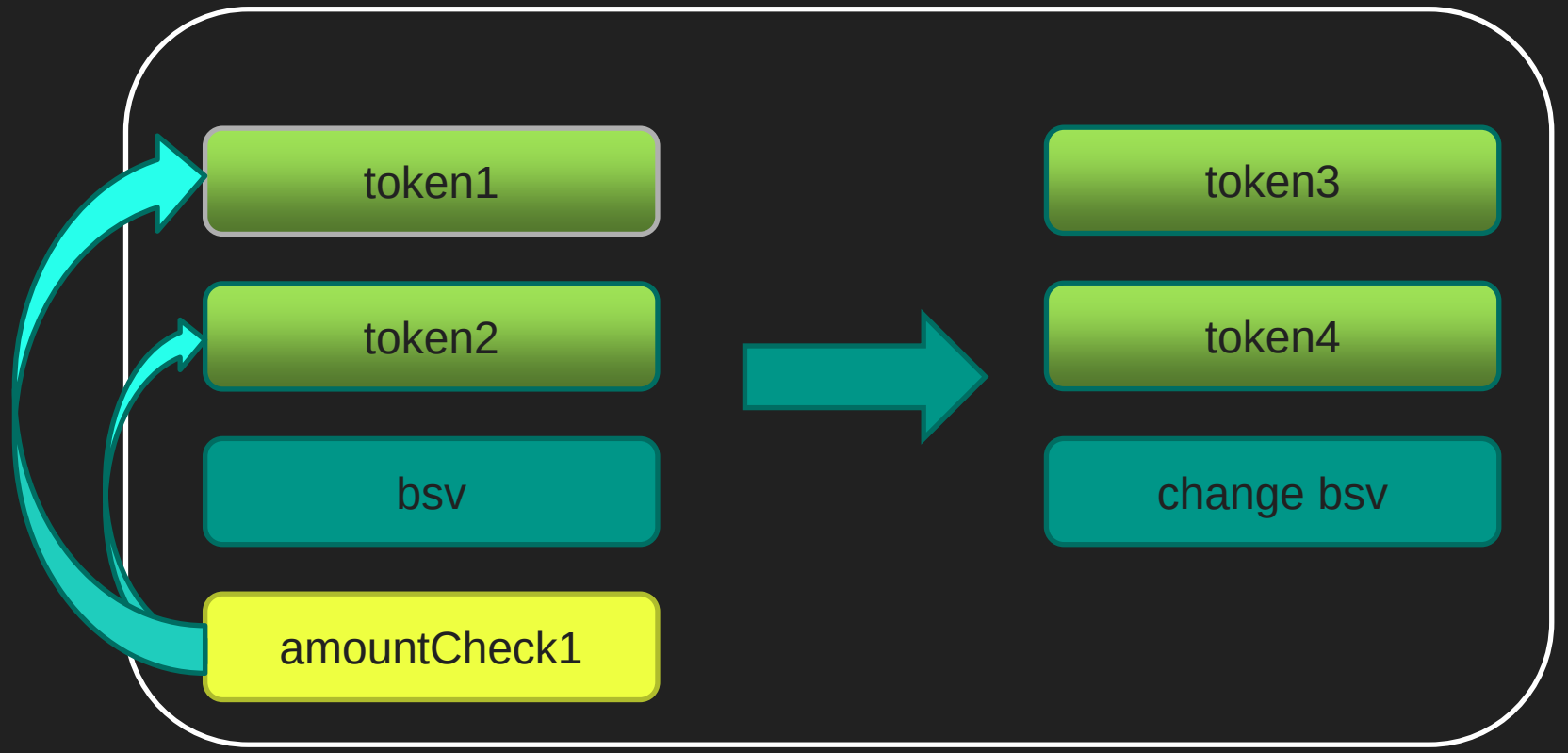
转账交易



转账交易



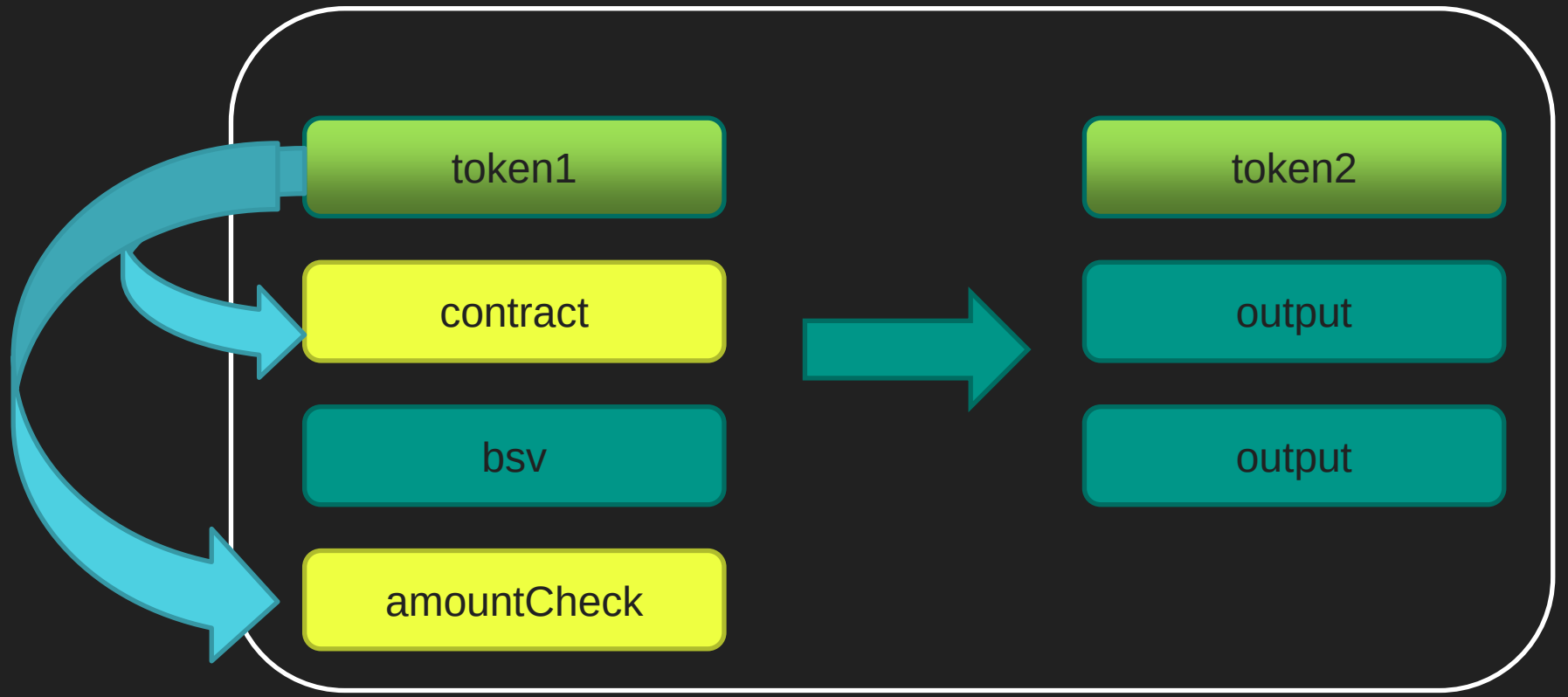
转账交易



从合约解锁

- 转账到合约hash
- 检查输入中是否有对应的合约
- 数量检查
  - unlockContractAmountCheck

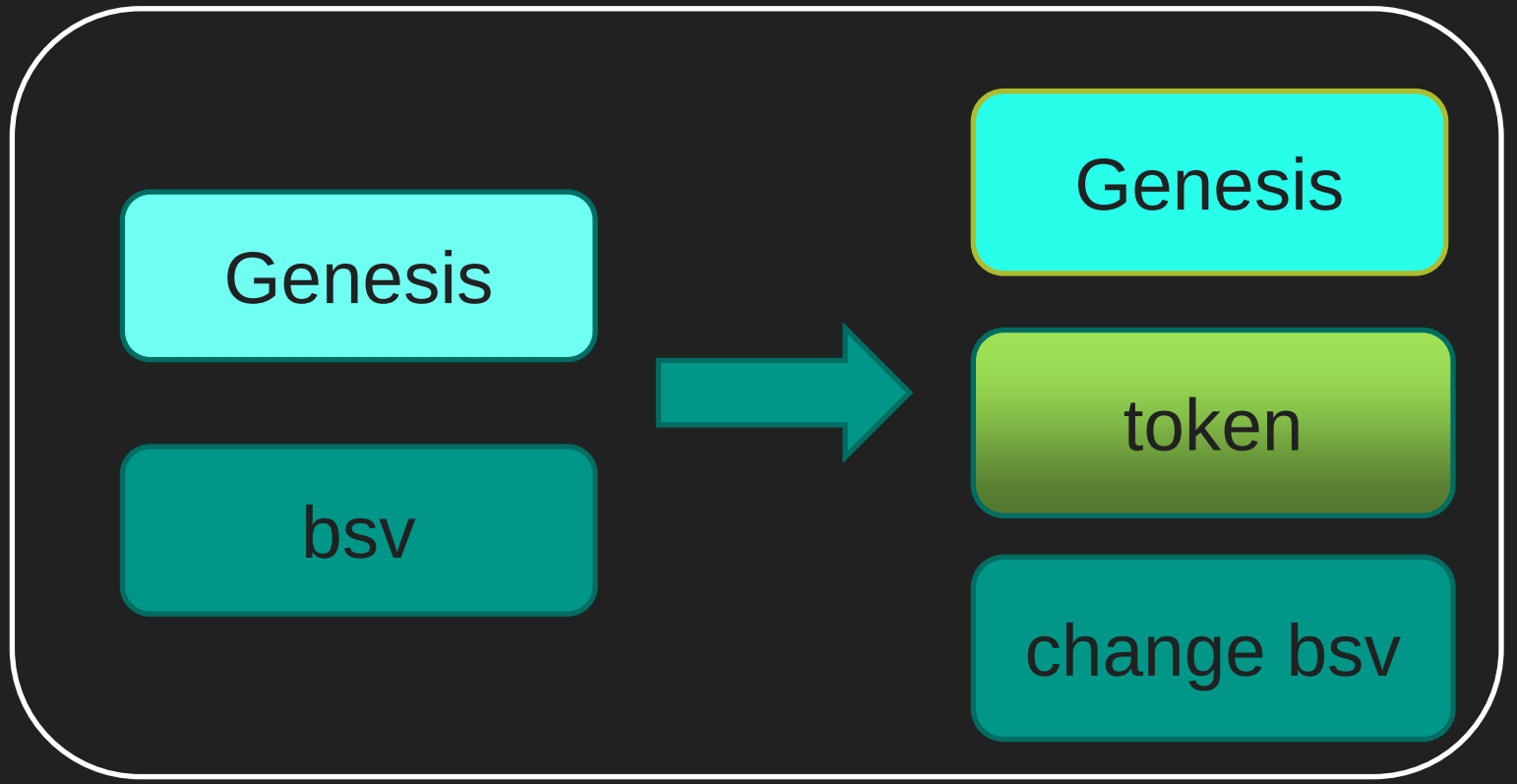
合约解锁交易



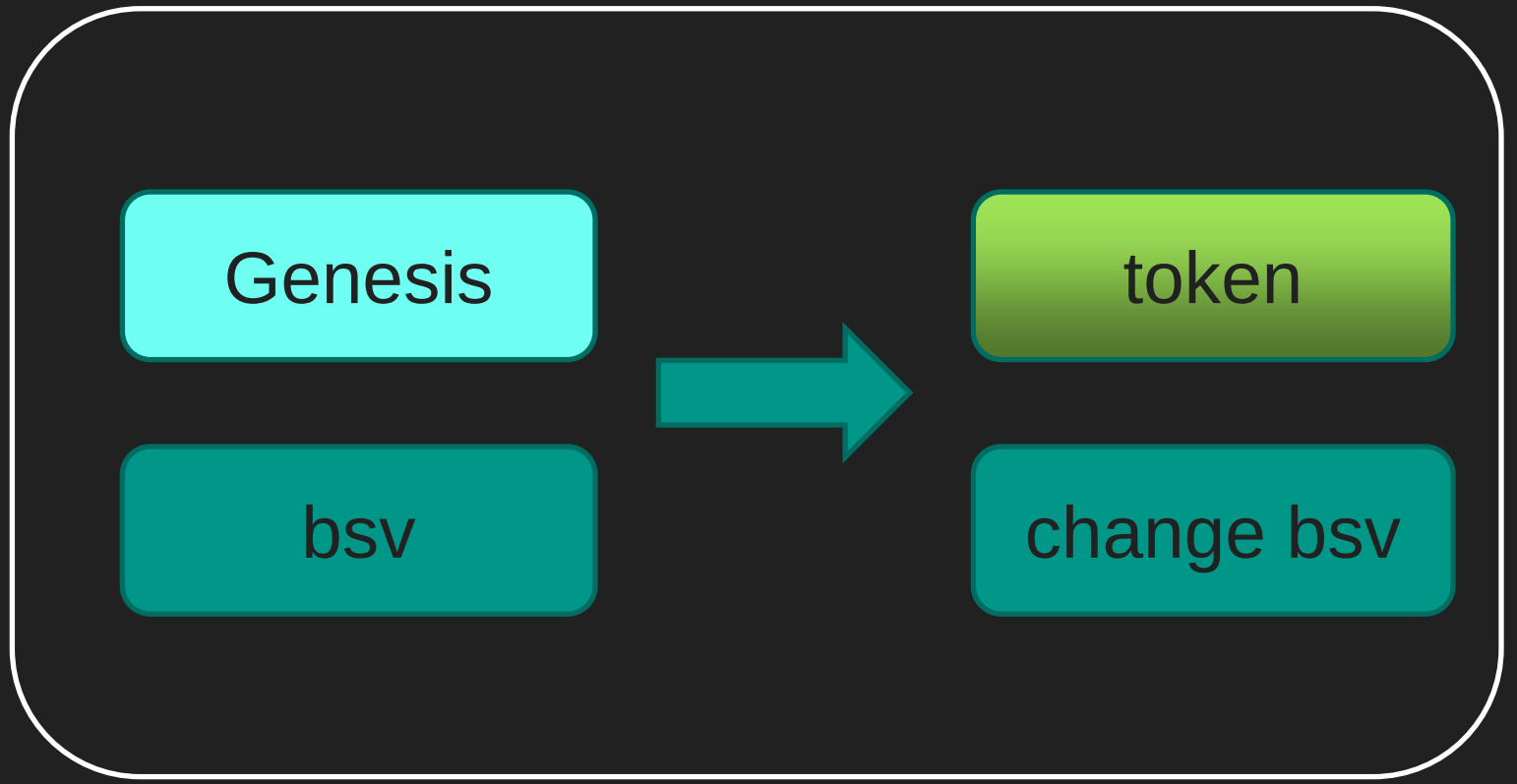
token增发

- 引入tokenGenesis，通过tokenGenesis生成token

增发交易



禁止增发



swap

- 增加流动性（addLiquidity）
- 提取流动性（removeLiquidity）
- token换取bsv（swapTokenToBsv）
- bsv换取token（swapBsvToToken）

增加流动性

交易

b09adc8f688259937bf71b329af249efe18a17f89b691027beccdfac3485ea26

下载收据

详情 脚本 JSON

概览

区块	0000000000133816a9fbcb276c09bc1b4e4b1e835da3a0501aa6c26bfe05fd68 (#1419857)
时间戳	2021-04-10 08:49:43 utc
版本	1
大小	145,480 B
确认数	395
Fee Paid	0.0004 BSV ⇄ (0.09877862 BSV - 0.09837862 BSV)
交易费率	0.275 sat/B

6 Inputs, 5 Outputs

1 脚本哈希: ef0237831a1b3c714f82b000998e02f71b87357808f91e72e67d1739c2b15dc0 0.00000546 BSV ⇄

ASCII 脚本 sCrypt 十六进制

Q @ v © ¬X $sensible $X QQZ TX QyQy YyQy yZy yZy yZy y

1 0.00200546 BSV ⇄

脚本哈希: 5bf0e089ce6c2d482521f71e735e244278b13a48142a5a6ceea54e0d4f65ed55

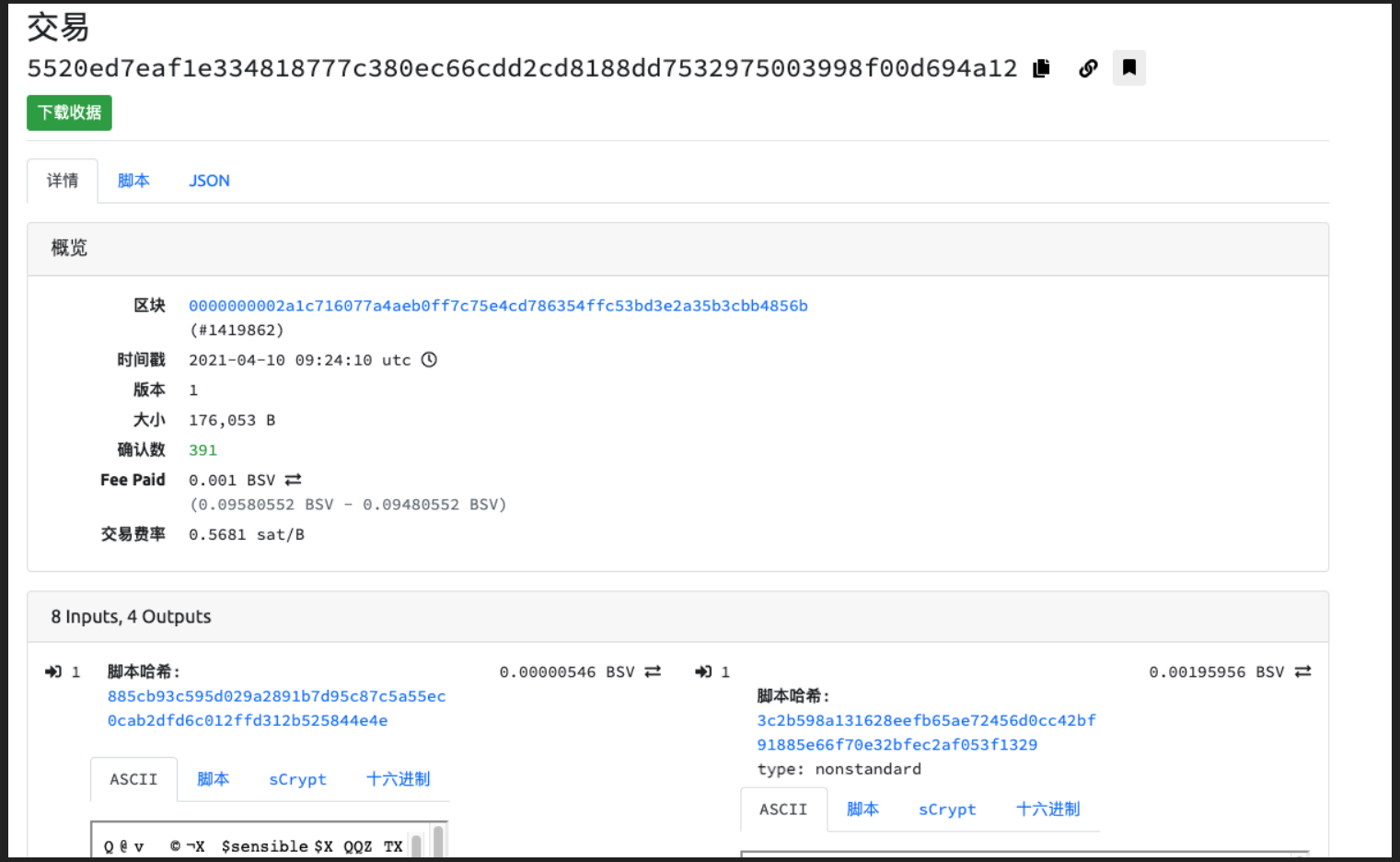
type: nonstandard

ASCII 脚本 sCrypt 十六进制

Q @ $

Bitcoin SV BOOTCAMP

提取流动性



Bitcoin SV BOOTCAMP

token交换bsv

交易

576a4aec28412f872b685146ee77b76204fe648b648a0ac0661464c008300c68

下载收据

详情 脚本 JSON

概览

区块 0000000002a1c716077a4aeb0ff7c75e4cd786354ffc53bd3e2a35b3cbb4856b
(#1419862)

时间戳 2021-04-10 09:24:10 utc

版本 1

大小 90,610 B

确认数 391

Fee Paid 0.0005 BSV ⇄
(0.00302184 BSV - 0.00252184 BSV)

交易费率 0.5519 sat/B

4 Inputs, 3 Outputs

1 脚本哈希:
56de09104fa2c99e9b6f9d41799cdccc141
68379680569f6cc0cfc87e2e8bd5f

0.00000546 BSV ⇄

ASCII 脚本 sCrypt 十六进制

1

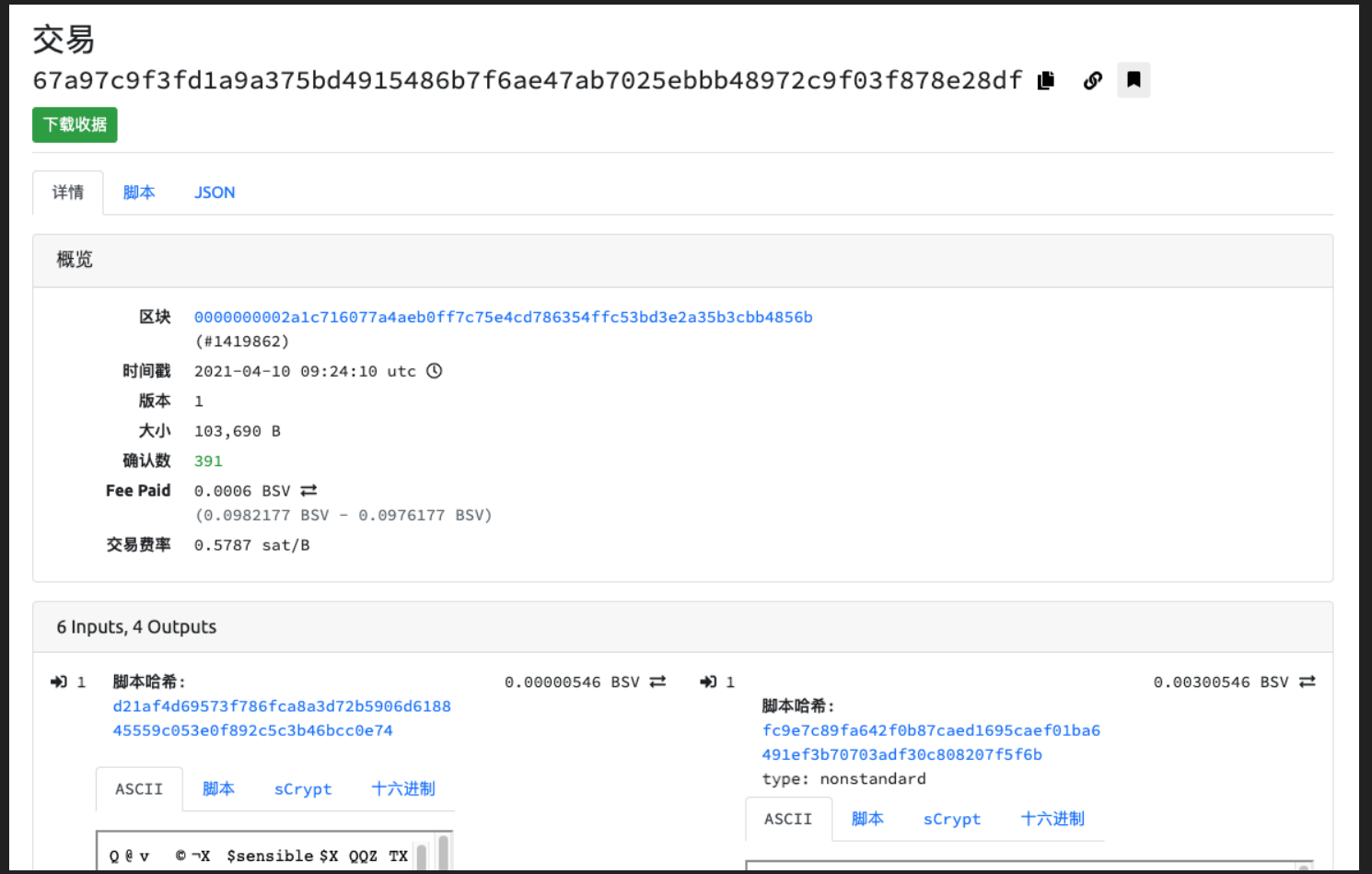
0.00200966 BSV ⇄

脚本哈希:
8e298d448d583eae37a2950d56a50284567
d0c3b57eaa5b6071b7c6c9e50e8fc
type: nonstandard

ASCII 脚本 sCrypt 十六进制

Bitcoin SV BOOTCAMP

bsv交换token



Bitcoin SV BOOTCAMP

合约拆分

addLiq

removeLiq

bsvToToken

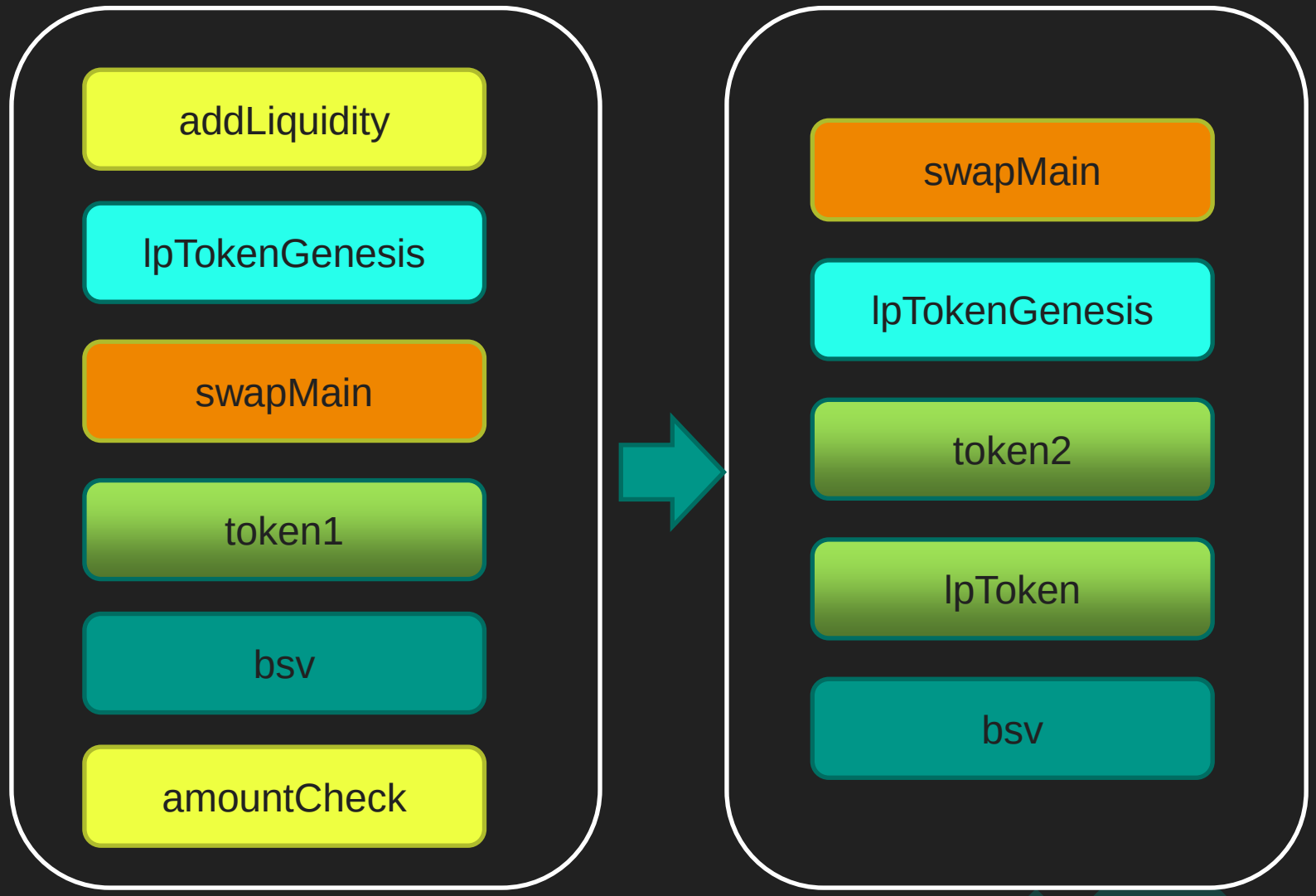
TokenToBsv

swapMain

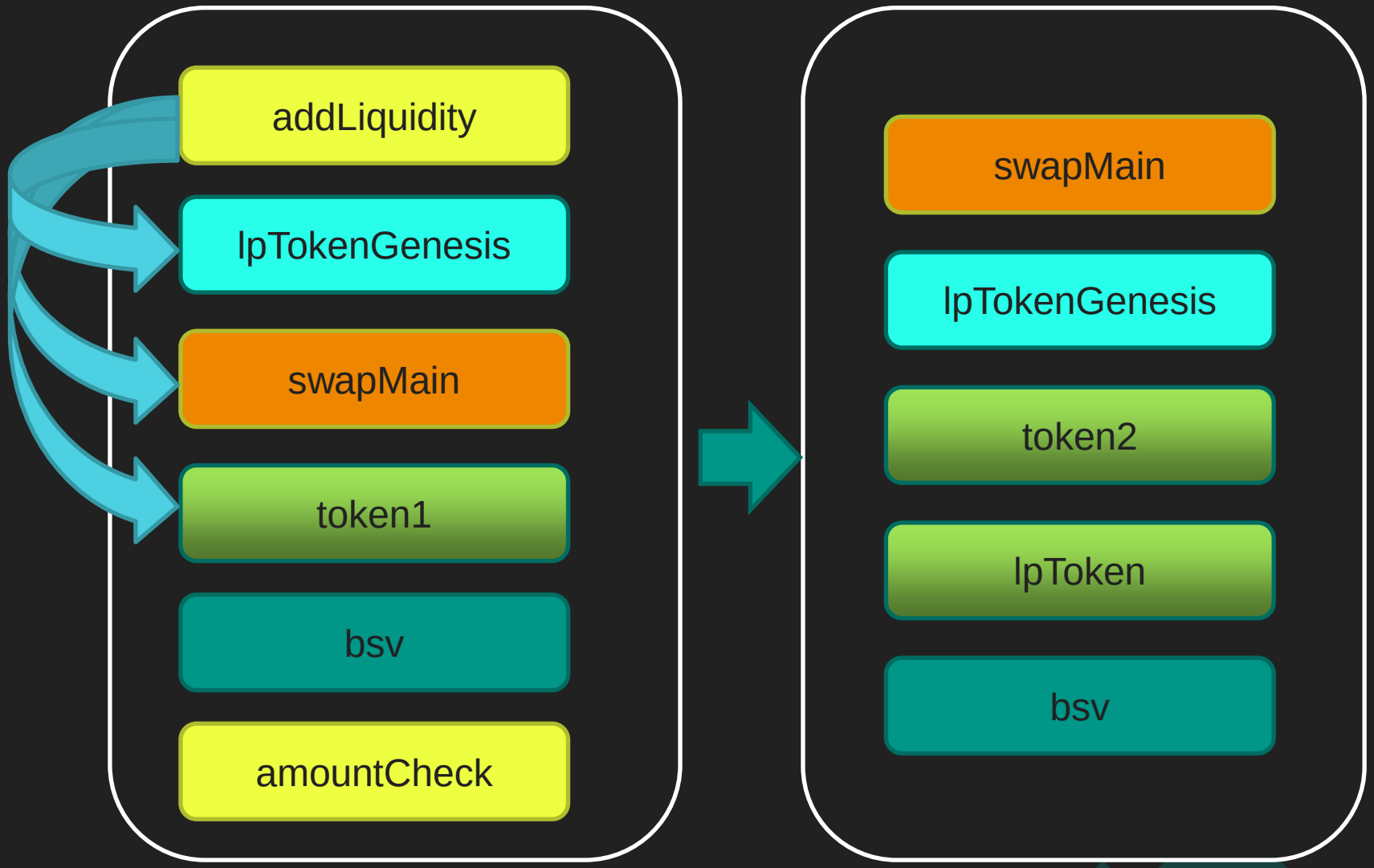
增加流动性

- token转账到addLiquidity contract hash
- 生成addLiqudity合约tx
- 生成unlockContractAmountCheck合约tx

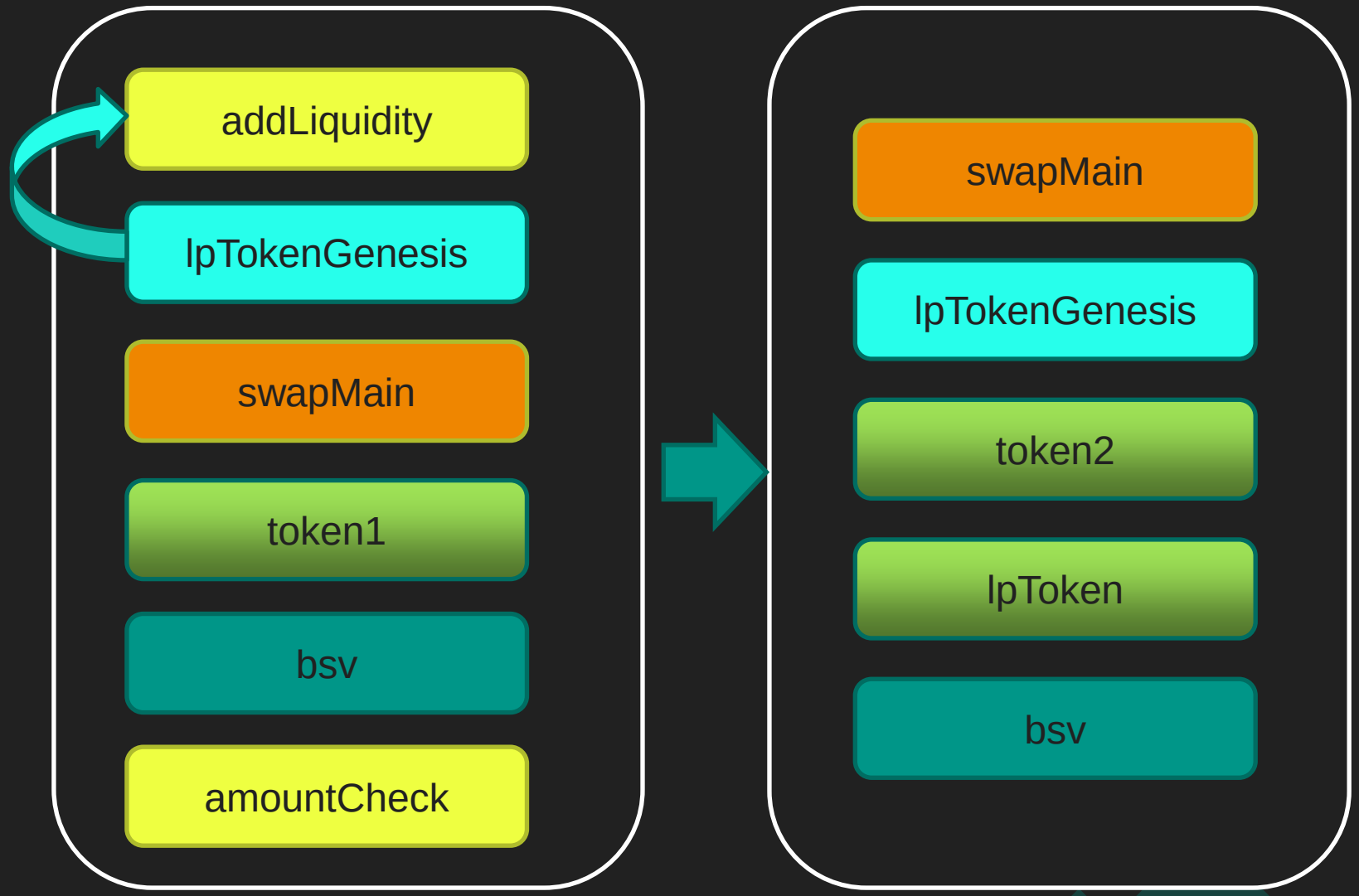
增加流动性



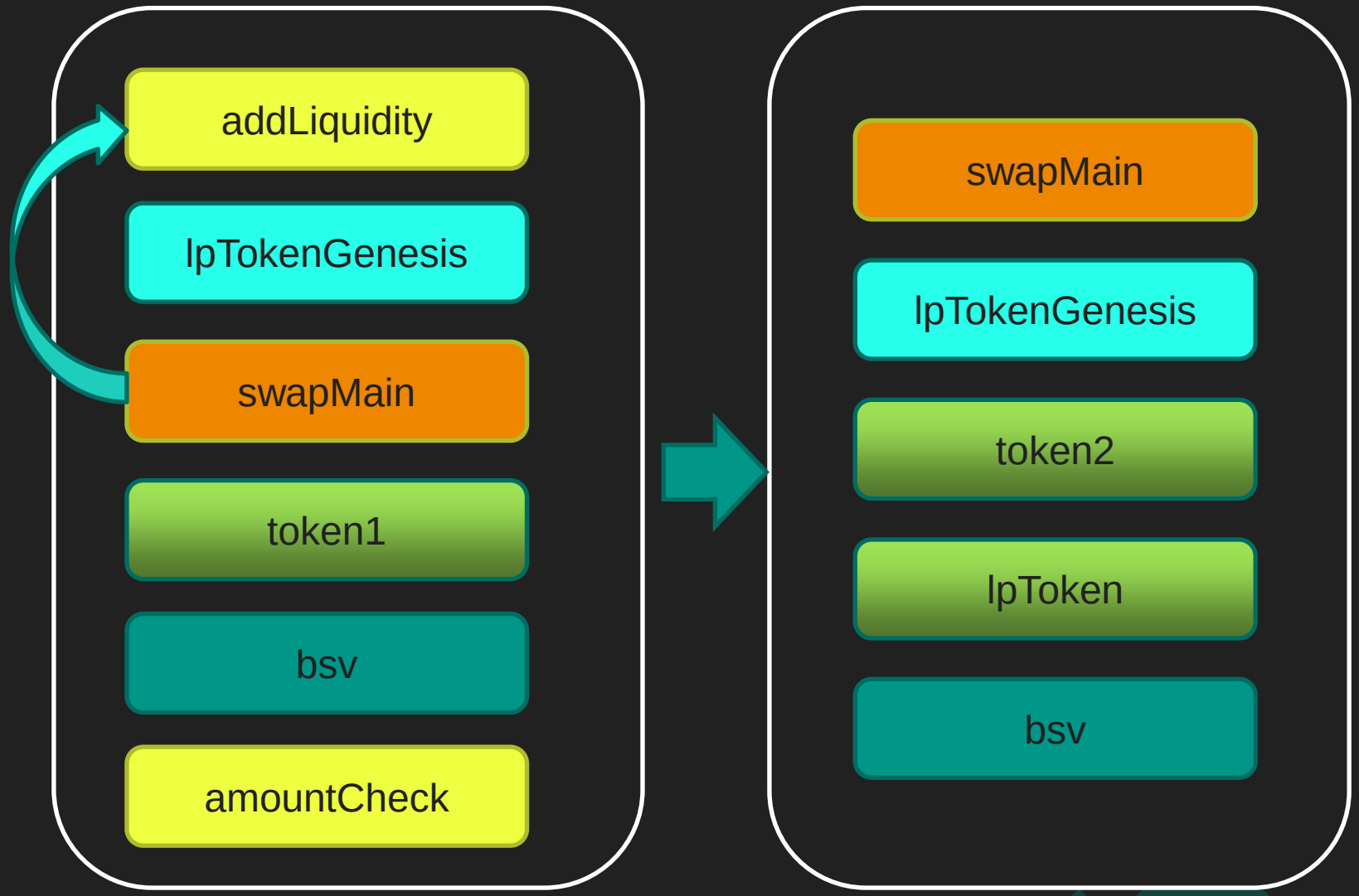
增加流动性



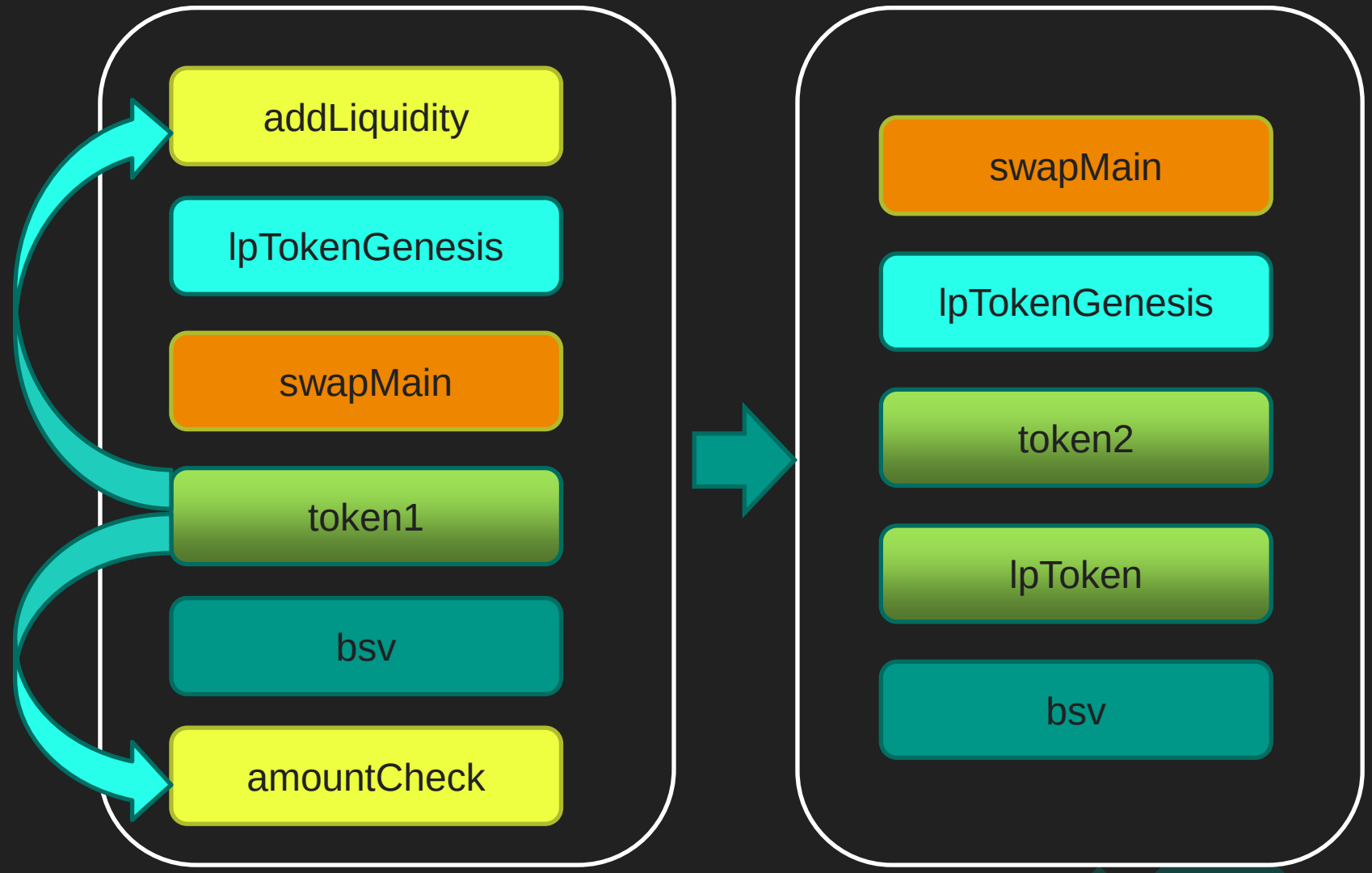
增加流动性



增加流动性



增加流动性



增加流动性

- 在增加流动性的地址上生成新的lp token
- token从addLiquidity hash转入到fetchToken hash
- fetchToken是swapMain合约用来控制token的合约

fetchToken Contract

- removeLiquidity
- swapBsvToToken
- mergeToken

合约拆分

addLiq

removeLiq

bsvToToken

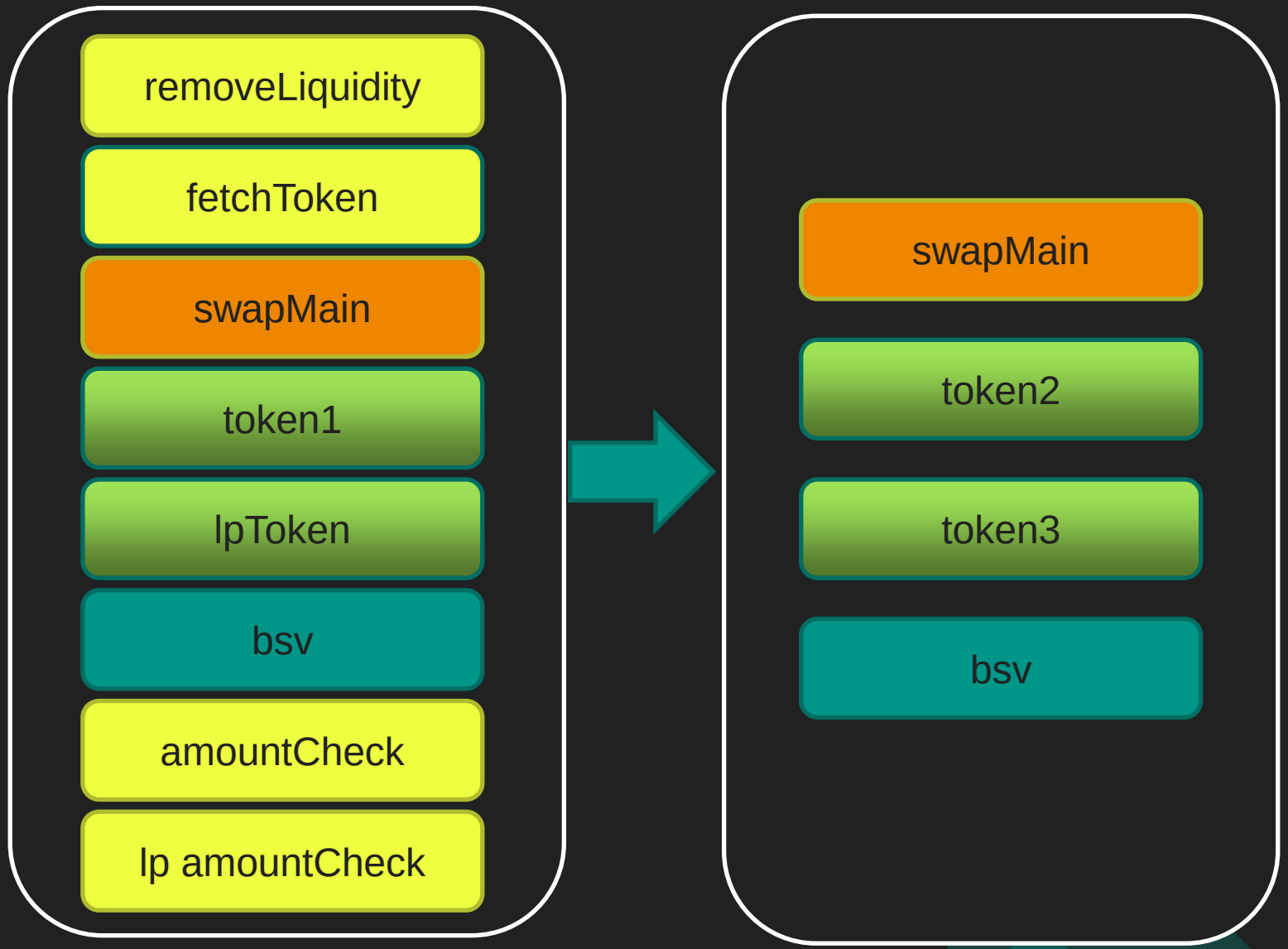
TokenToBsv

swapMain

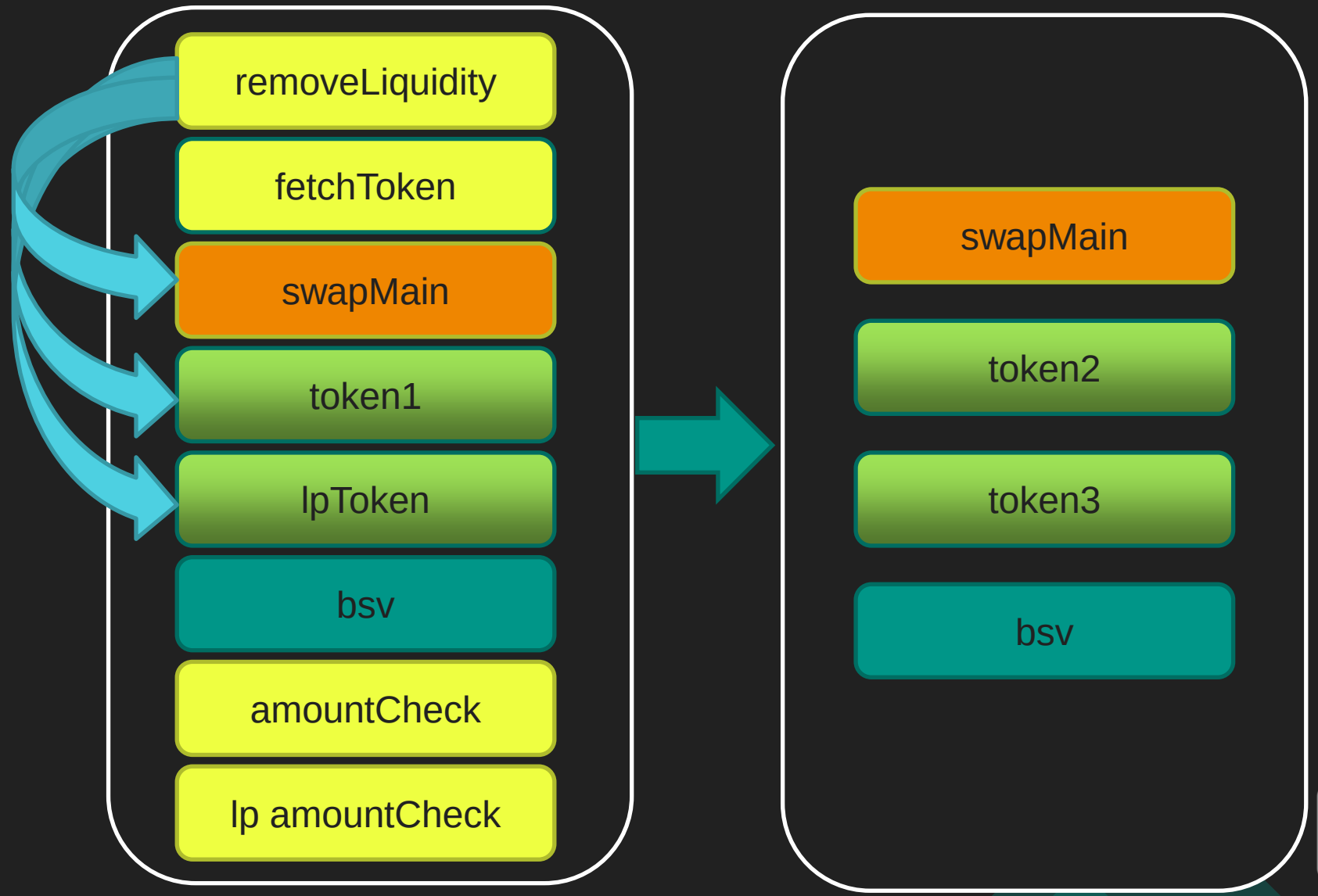
提取流动性

- lp token从用户转账到removeLiquidity contract hash
- 生成removeLiquidity合约tx
- 生成fetchToken合约tx
- 生成token unlokcContractAmountCheck合约tx
- 生成lp token unlokcContractAmountCheck合约tx

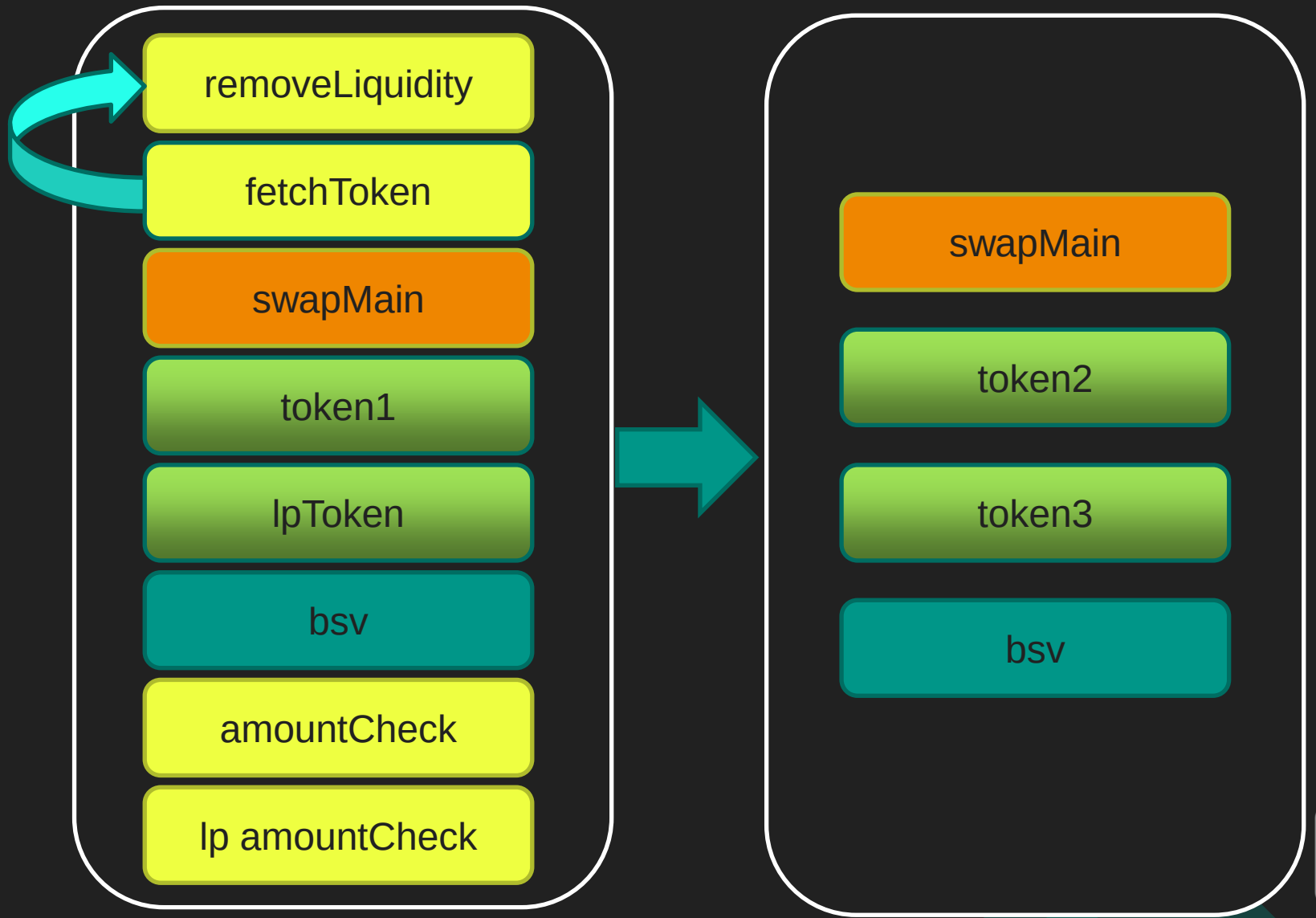
提取流动性



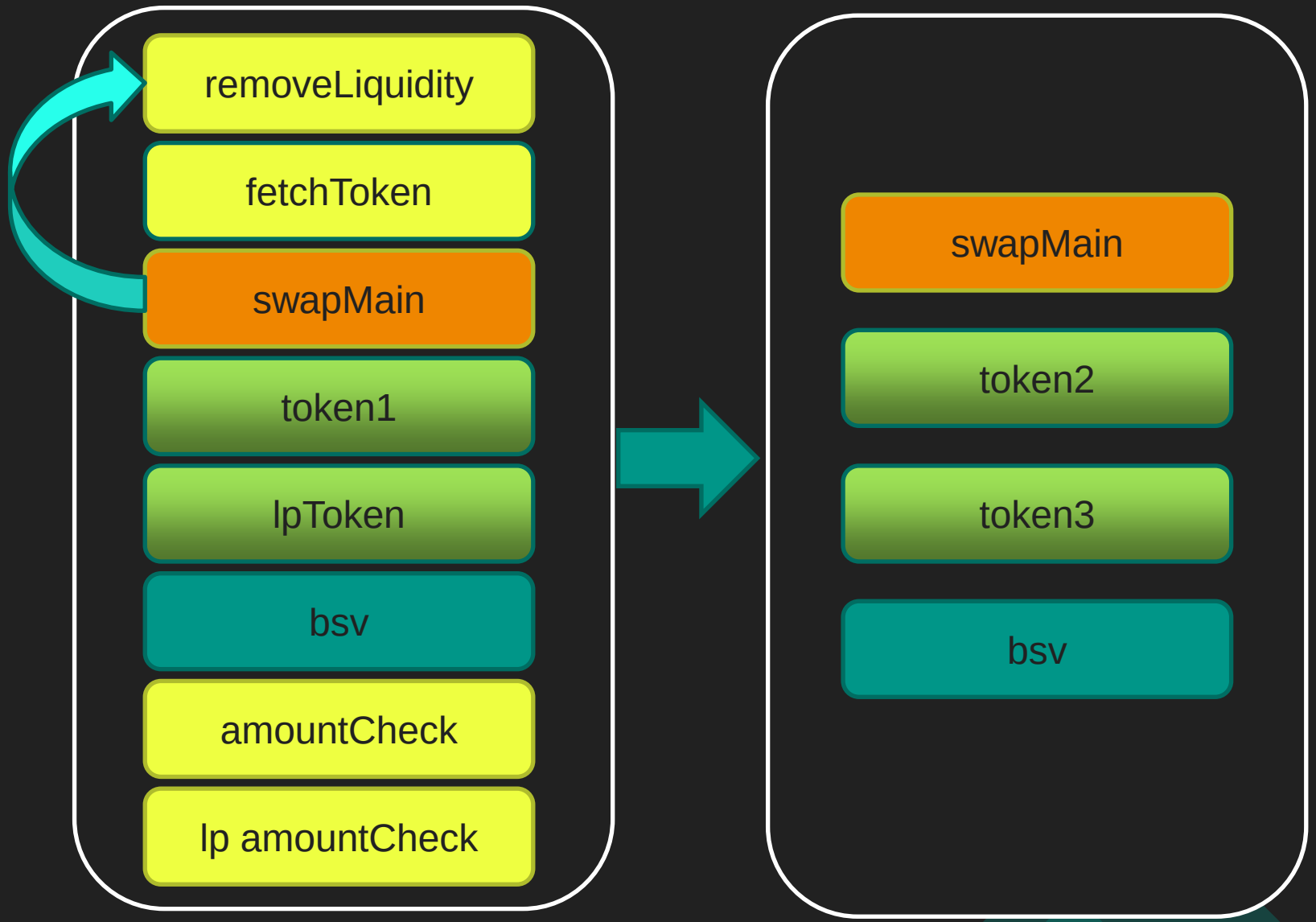
提取流动性



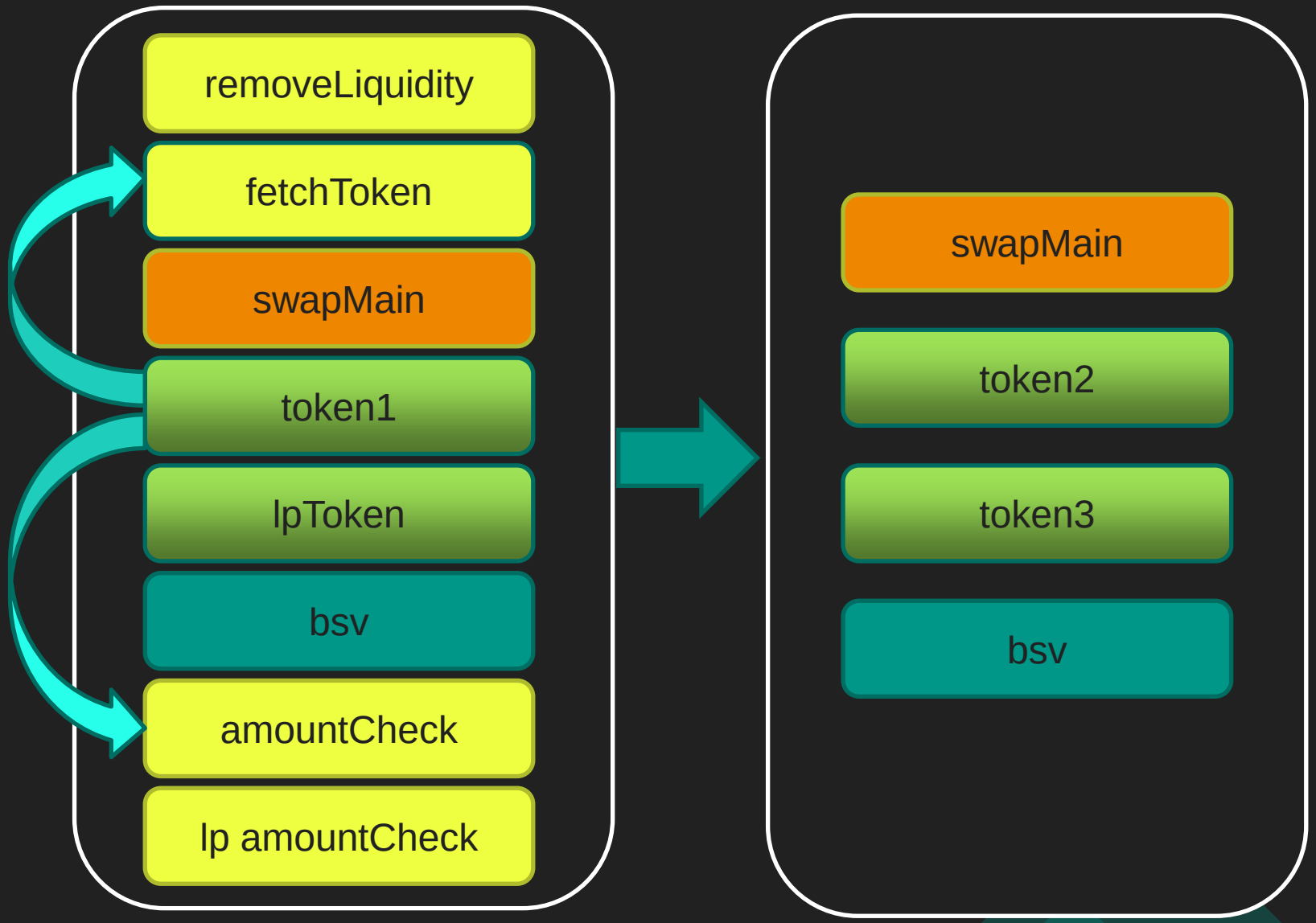
提取流动性



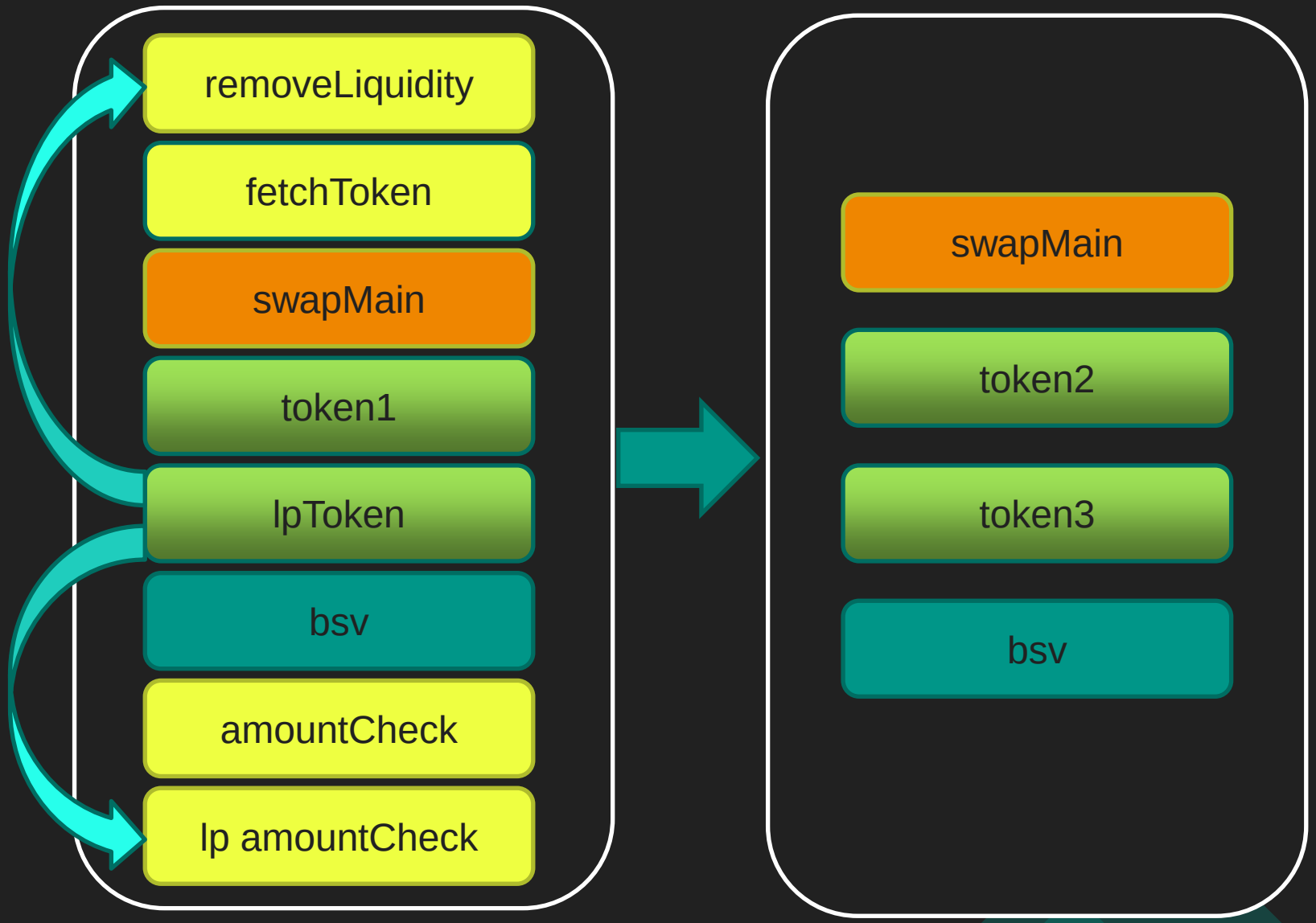
提取流动性



提取流动性



提取流动性



提取流动性

- lp token销毁
- token从fetchToken hash转账到用户
- 如果输入token数量大于用户提取的token，则找零到fetchToken hash

合约拆分

addLiq

removeLiq

bsvToToken

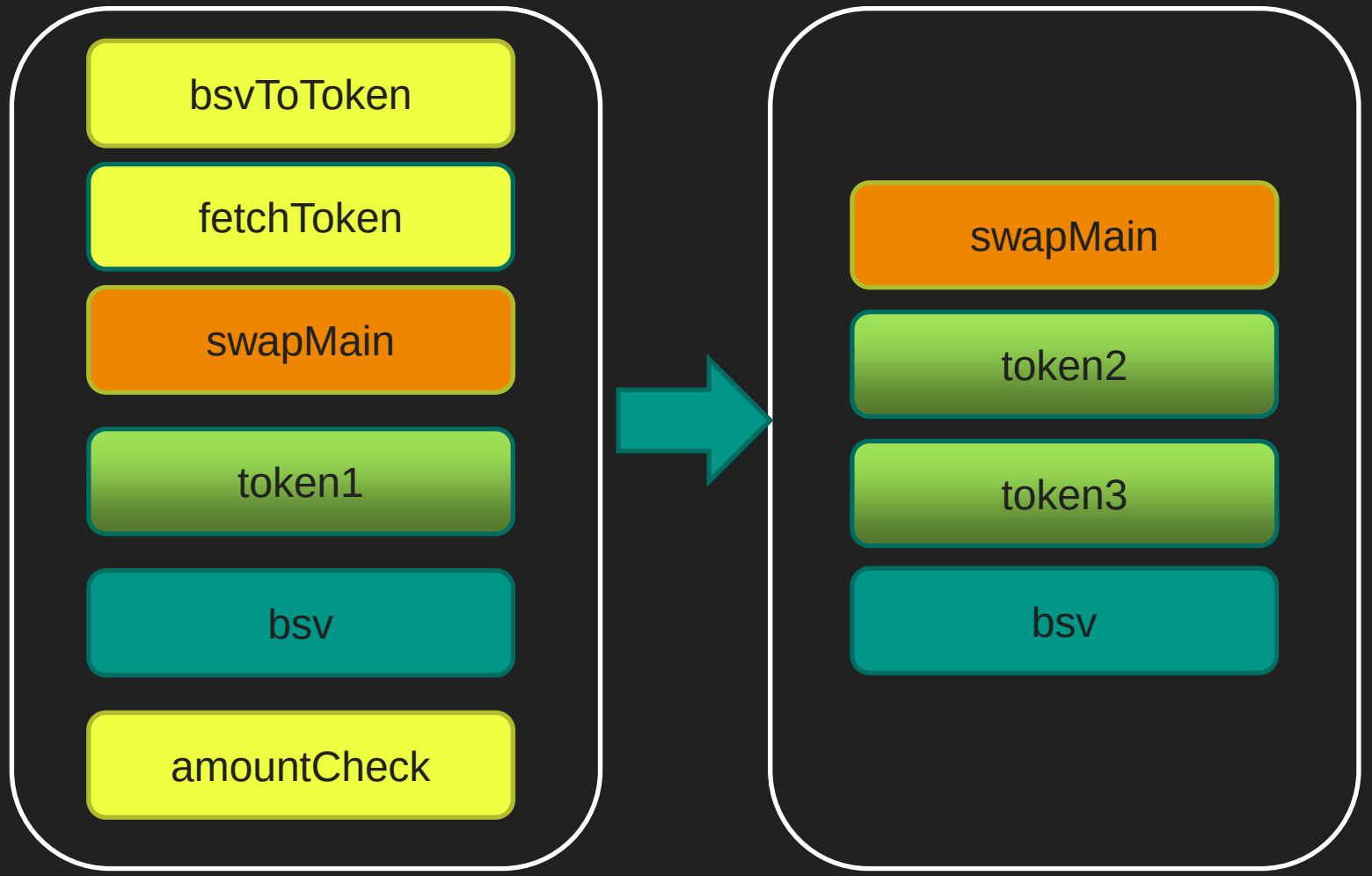
TokenToBsv

swapMain

bsv换取token

- 生成bsvToToken合约tx
- 生成fetchToken合约tx
- 生成token unlokcContractAmountCheck合约tx

bsv换取token



bsv换取token

- token转账给用户
- 输入token数量大于用户换取的token数量，找零到

  fetchToken contract hash

合约拆分

addLiq

removeLiq

bsvToToken

TokenToBsv

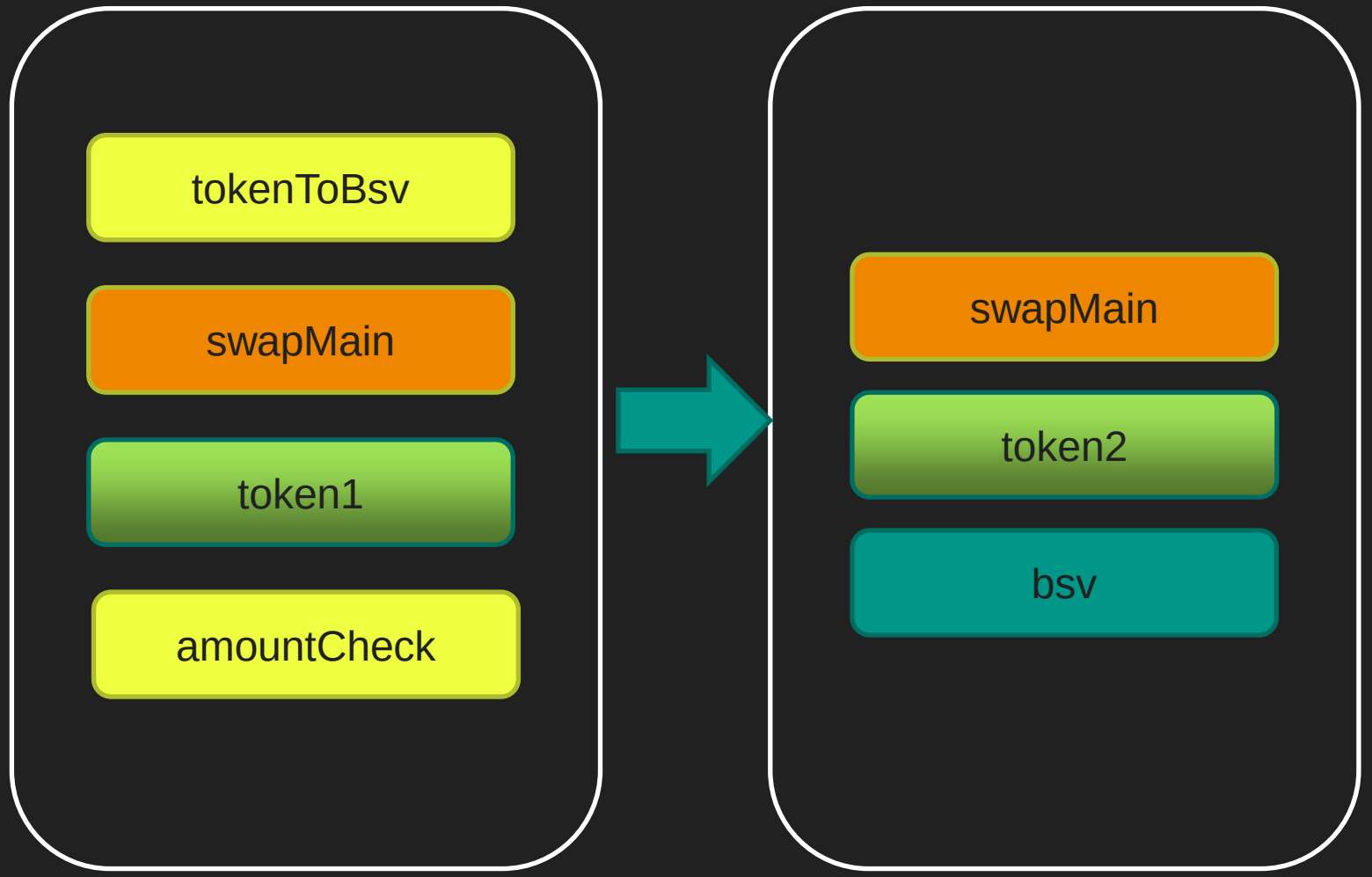
swapMain

Bitcoin SV BOOTCAMP

token换取bsv

- token从用户转账到tokenToBsv contract hash
- 生成tokenToBsv合约tx
- 生成token unlokcContractAmountCheck合约tx

token换取bsv



token换取bsv

- token转移到fetchToken Contract Hash
- bsv转账给用户

谢谢

https://sensiblecontract.org

Bitcoin SV BOOTCAMP