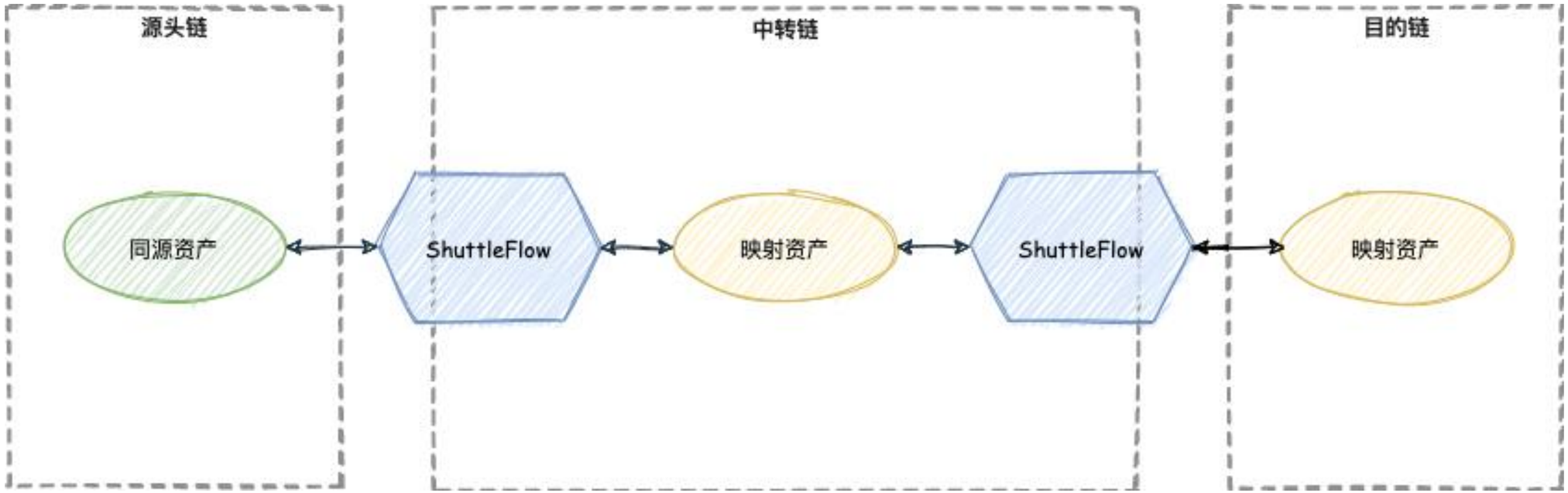
Shuttleflow

跨链技术分享

2020.4.　随Conflux主网第一阶段上线，支持比特币和ETH资产向Conflux的跨链
2020.7.　随Conflux主网第二阶段上线进行数据迁移，更新跨链联盟
2020.9.　支持Moonswap大量资产迁移，服务商功能上线，实现跨链上币自由
2020.10. 随Conflux主网正式上线，拥有了自己的前端入口
2021.2.　支持了Conflux资产反向跨链、币安智能链互跨

2021.3.19

以Conflux为中转链实现多链互跨



Shuttleflow现状

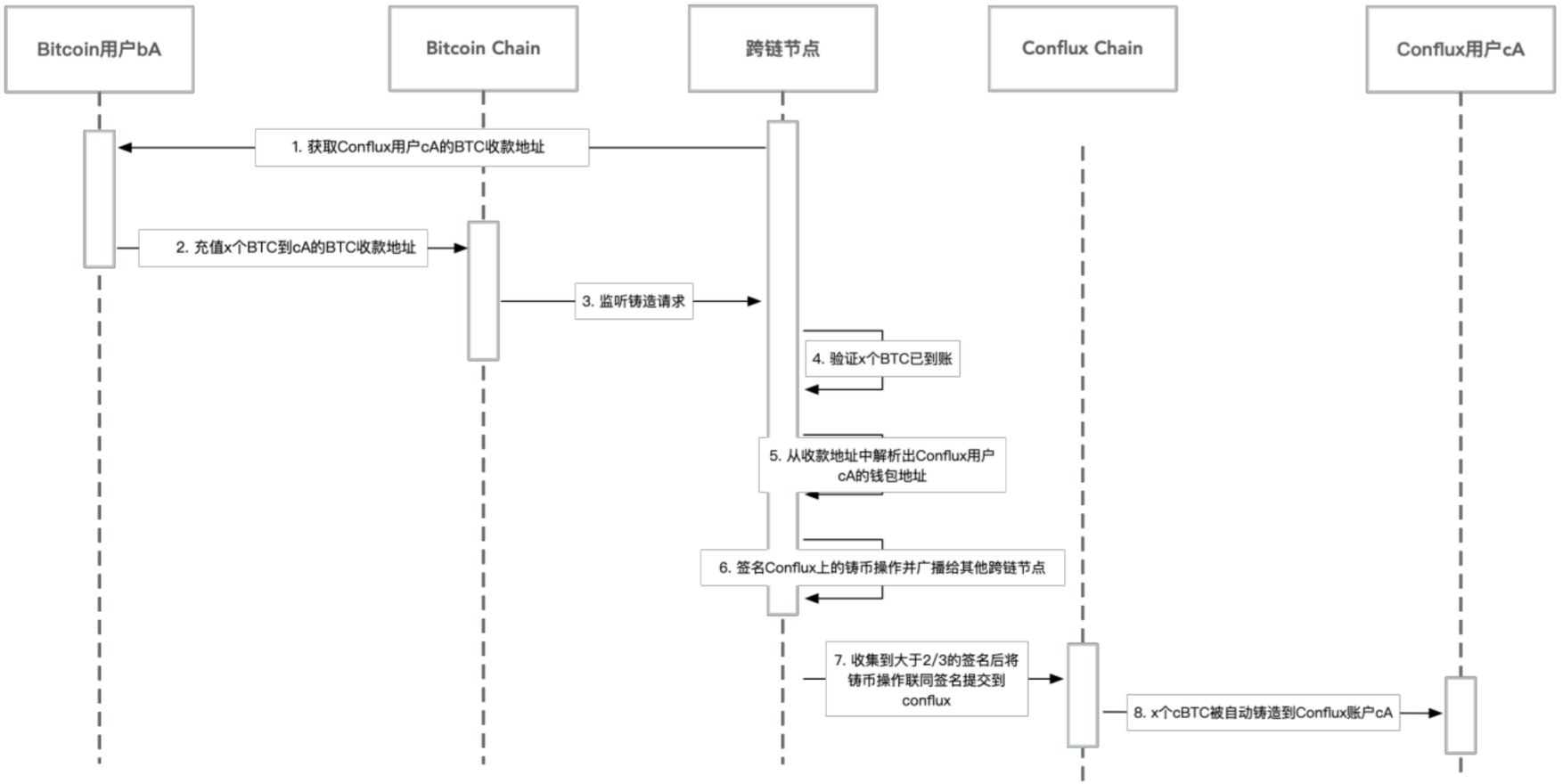
- Bitcoin -> Conflux
- ETH <-> Conflux
  - 支持85种ETH资产向Conflux跨链以及CFX反向跨链
- BSC <-> Conflux
  - 支持Conflux与BSC互跨，其中包含7种ETH原生资产
- Heco、Okex chain
  - 即将上线

Shuttleflow跨链联盟

- 跨链联盟：由知名区块链机构各自运行跨链节点形成的P2P网络

- ShuttleFlow 基于跨链联盟节点 2/3 多签进行资产托管
  - 铸币：在目标链上发行1:1锚定资产 e.g. 1 BTC = 1 cBTC(conflux BTC)
  - 销币：在目标链上销毁锚定资产，联盟在源头链退回原生资产

Shuttleflow跨入流程



Ethereum收款钱包

- 与Conflux地址和跨入场景形成一一映射
- 通过调用跨链节点的API获取收款钱包地址
- Ethereum收款钱包：
  - 通过CREATE2生成的以太坊合约
  - keccak256(0xff ++ deployingAddr ++ salt ++ keccak256(bytecode))[12:]
  - salt=hashFunc(confluxAddress, defiAddress)
- 用户实际充值后联盟才会部署对应收款钱包合约

联盟铸币

- 联盟监听以太坊交易：
  - 每当发现有用户的收款钱包被打入了正确金额，会自动调用收款钱包合约的函数将资产转移进联盟热钱包合约，并生成对应转移事件；
  - 监听收款钱包转移事件，对其进行签名，并在P2P网络中广播给其他节点；
  - 当一个节点收集到足够多的签名后，在Conflux上发起铸币交易，由合约进行多签验证，验证通过后给用户地址铸币。

Shuttleflow跨出流程

- 调用cToken的Burn函数对代币进行销毁：

```
function burn(
        address user_addr,   // 当Defi如Moondex托管用户资产,帮用户跨链时填写
        uint256 amount,  // 销毁金额
        uint256 expected_fee, // 此次销毁最高愿意支付的手续费
        string memory target_addr, // 跨链目标地址
        address defi_relayer // 跨链中转合约地址
 );
```

Bitcoin收款钱包

scriptSig

```
OP_0
${signature_1}
${signature_2}
...
${signature_M}
```

scriptPubKey

```
${user_conflux_address}
${defi_address}
OP_DROP
OP_DROP
${M}
${public_key_1}
${public_key_2}
...
${public_key_N}
${N}
OP_CHECKMULTISIG
```

p2sh地址

跨入流程：

- 联盟热钱包是由各联盟成员组成的2/3多签地址
- 联盟成员监听Bitcoin交易：
  - 实时将用户收款钱包的比特币转移到热钱包
  - 当热钱包收到比特币并经过6个块确认后，在Conflux上铸币

Bitcoin跨出

- 联盟监听cBTC的burn事件，对于已确认的跨出，构造Bitcoin交易并签名
- Bitcoin UTXO模型的特殊性：
  - 联盟成员$1..n$分别看到的热钱包内的已确认UTXO集合为$U_1 \,..\, U_n$
  - 有：$\forall i,j \in [1,n], U_i \subseteq U_j \vee U_j \subseteq U_i$
  - 联盟成员达成共识，挑出一个合适的集合U，使得其中的UTXO能够支付这笔提现且矿工费用尽量优，并保证不同的提现之间UTXO集合无交

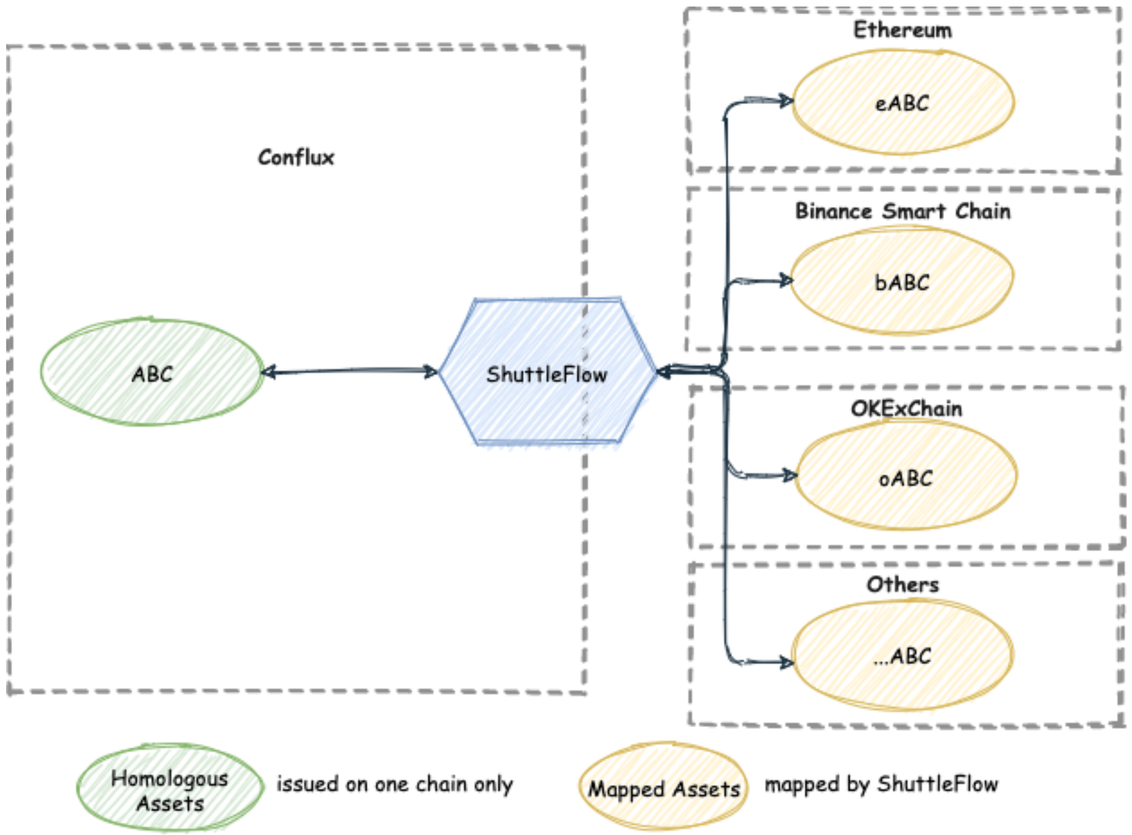
把账算清楚

- Bitcoin：
  - 由于UTXO模型，在跨入跨出过程中没有手续费支出；
  - 所有过程用户承担支付给矿工的交易费，无额外费用。
- Ethereum：
  - 用户给收款钱包转账，自行承担gas费；
  - 如果是新用户，联盟帮忙部署收款钱包合约，联盟支付gas费（钱包费）；
  - 从收款钱包转移资产到热钱包，联盟支付gas费（跨入费）；
  - 提现时联盟在以太坊上发送多签提币交易，联盟支付gas费（跨出费）。

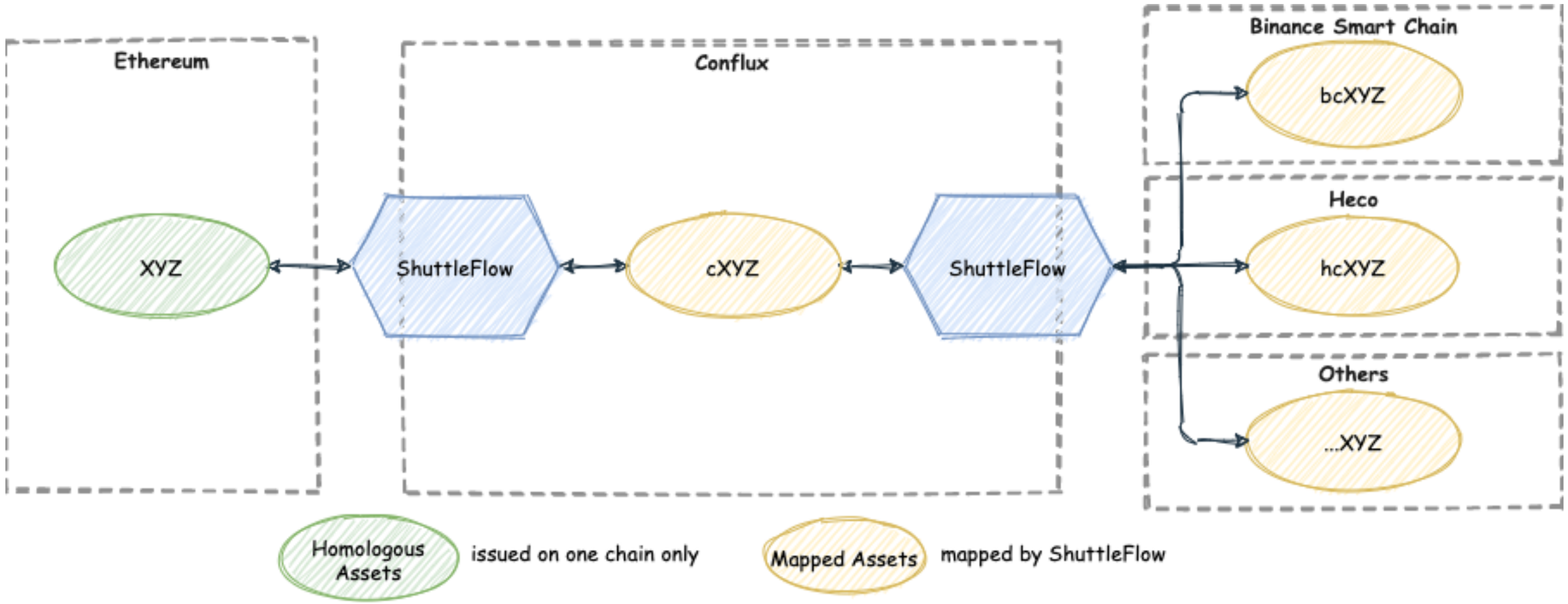
服务商机制

- 问题：联盟为了Ethereum的跨链交易垫付了大量的gas费用，且需要为币种单独设置手续费，上新币需要联盟审核
- 如果一个币种想要通过Shuttleflow跨链，它必须有一个服务商
- 服务商：
  - 为特定币种抵押cETH在Conflux上的跨链合约中；
  - 为该币种制定手续费参数：最小跨入/跨出，钱包费，跨入费，跨出费；
  - 每当联盟垫付了以太坊的gas费，就会去合约中找对应币种的服务商报销这笔gas费用，同时从用户这次操作的币中抽取对应的数量支付给服务商；
  - 除了ETH、USDT，其他币种的服务商是开放竞争的，当满足条件时可以被其他人顶替。
- 允许无许可的资产互通，任何人都有能力添加资产的跨链而无需联盟许可。

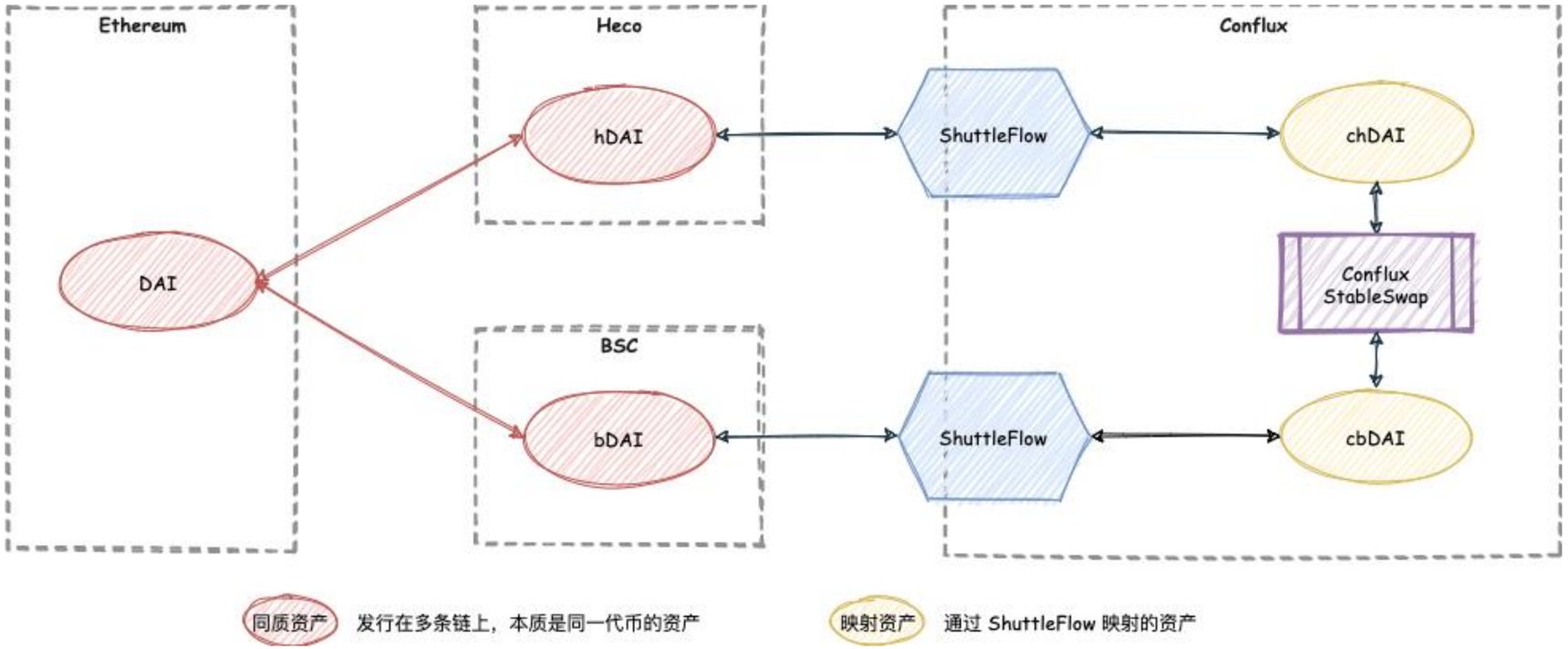
Shuttleflow



Shuttleflow



Shuttleflow 2.0



Q&A