0到1全面认知波卡——跨链可组合性（二）

原创 可达鸭Joie 鸭说区块链 2020-07-16 17:13

上文我们说到波卡就像一个地基，一切基于这个地基建造的区块链都可以实现业务往来，并且可以连接比特币、以太坊等已经建成的区块链。那么从今天开始我们将正式进入到波卡的系统学习中，我同样还是以通俗易懂的语言向大家讲述，今天我们聊聊波卡的**跨链可组合性。**

一、跨链的概念

昨天有小伙伴问我，**波卡是怎么让不同区块链之间进行业务往来的呢**，这里有个专业名称，很多朋友应该都清楚，这种**不同区块链之间进行数据、资产的通信和互操作性**，我们把它叫做**跨链。**

这里划重点，真正的跨链必须要满足以下功能：

1、数据跨链

2、资产跨链

3、互操作性

打个比方，比如比特币和以太坊通过波卡实现了跨链。那么在：

比特币链上的转账记录就可以通过波卡传递到以太坊上（数据跨链）

比特币链上的资产BTC也可以通过波卡转账到以太坊上（资产跨链）

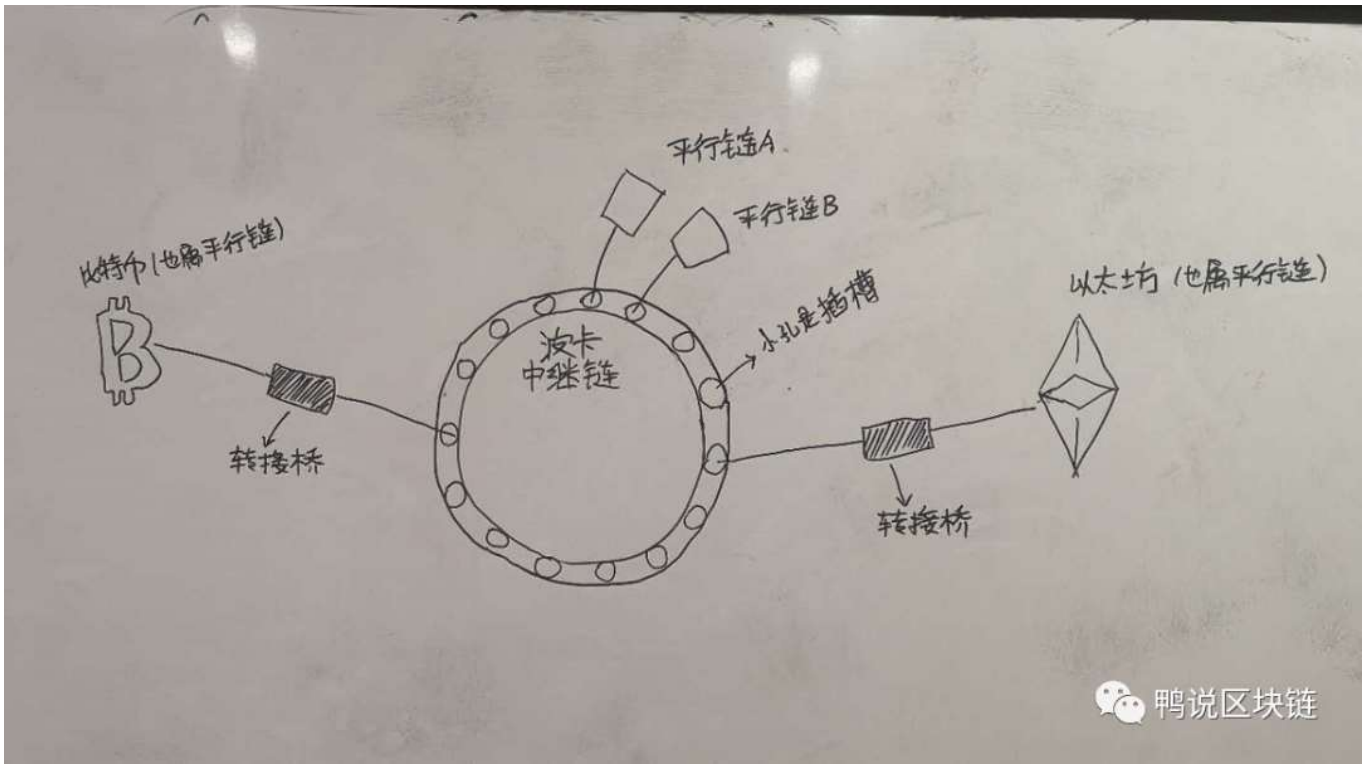
以太坊上的智能合约可以通过波卡控制BTC的转账（互操作性）。

有朋友一直以为所谓跨链，就是资产互换，比如 1BTC兑换了10ETH，这样链上资产就互换了，**大错特错！鸭哥强烈反驳**，这种“跨链”跟在中心化交易所中交易有什么区别？即使是在去中心化交易所（DEX）交易，这与跨链也根本扯不到一起！有些市场上宣称做跨链的项目，鼓吹资产互换就是跨链，实际上就是个交易所，**千万不要混淆概念**。

二、波卡的跨链架构

波卡就像一个地基，那么波卡的主链就像这个地基一样，可以让很多区块链加入进来，我们把**波卡的主链叫做中继链，加入进来的区块链叫做平行链。**

中继链为了让更多区块链能加入进来，所以它上面会有很多的**插槽**，上文说过，比特币和以太坊这种已经建设完毕的区块链，没法直接插入插槽，只能通过桥梁的方式连接波卡，**我们把这个桥梁叫做转接桥。**我画个画给大家演示一下，大家应该就明白了：



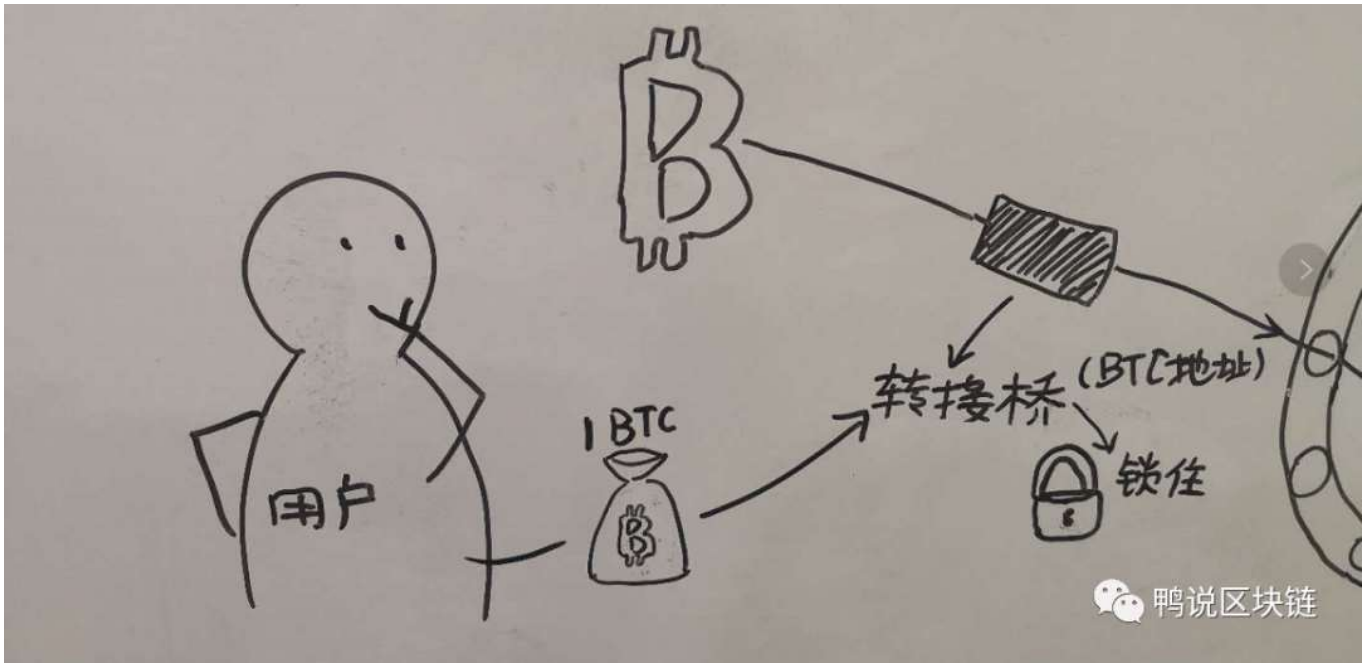
图中波卡**中继链**就是个大圆环，上面有很多小孔作为**插槽**，其他区块链可以插入插槽成为**平行链**，比特币和以太坊没法直接插入插槽，只能通过**转接桥**的方式成为平行链。

三、波卡如何实现跨链

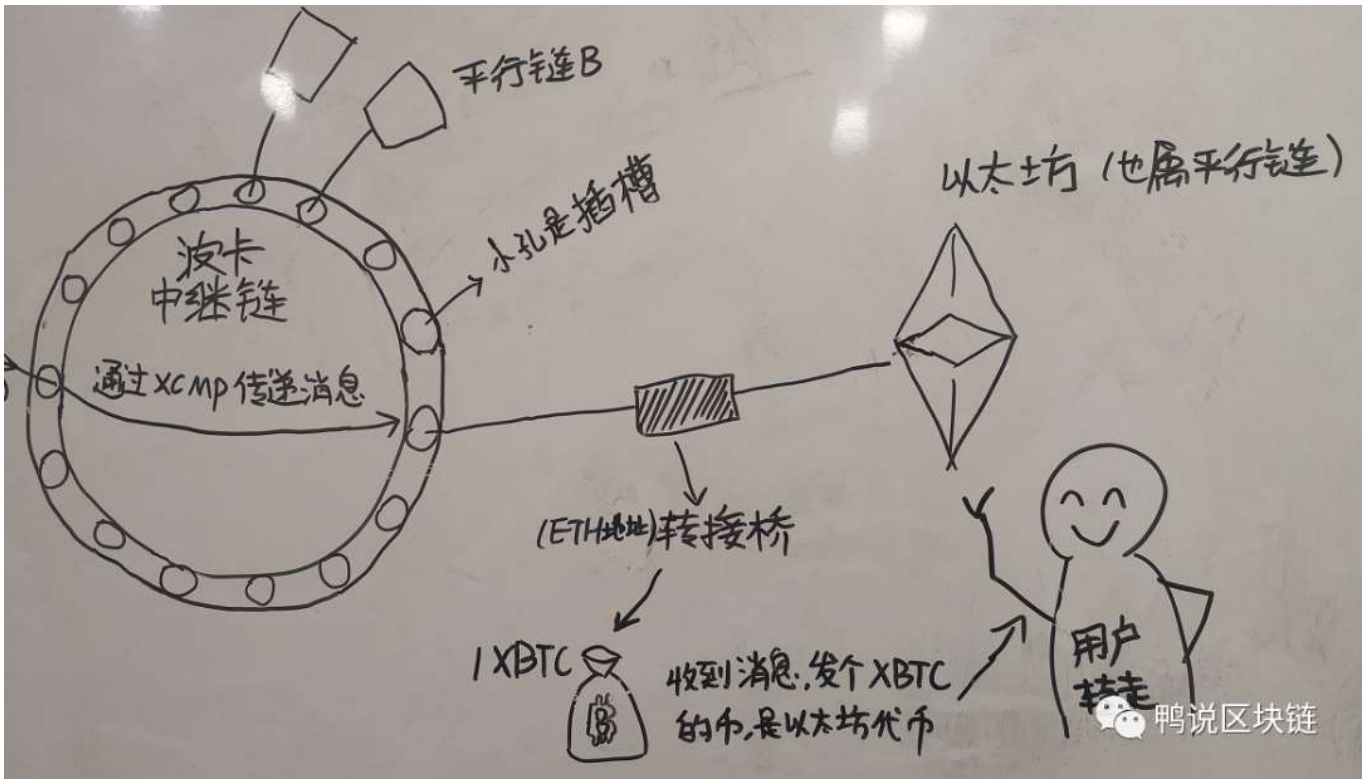
上图中波卡中继链好像一个插排一样，不同区块链可以插入插槽成为它的平行链，那么这个插排**有个数据传递的协议**，我们把它叫做**XCMP协议。**

正是因为有了XCMP协议，插入插槽的平行链之间才可以互相发送消息，互相通信，实现数据跨链。

那么比特币又是如何转账到以太坊上的呢？很多人跟鸭哥一样匪夷所思，只有数据跨链如何让资产也能跨链呢，这里我们继续画画说明：



一个比特币用户拥有1个BTC，他想把这个BTC转账到以太坊上参与以太坊的去中心化金融活动。那么首先，**他会把1BTC转账到转接桥的BTC地址，转接桥收到后会锁住，**没有任何人可以动这个BTC，**然后提交一个以太坊地址。**



紧接着，转接桥会把锁住BTC的消息，**通过波卡XCMP协议**传递消息，把消息传递到以太坊那边的转接桥上。
大家都知道，**以太坊上的智能合约可以发币**，因此以太坊那边的转接桥接收到消息后，立即通过智能合约**铸造一个XBTC的以太坊代币，发送到用户提供的以太坊地址上。**
这个XBTC代币，代表那边转接桥锁住的BTC。那么用户就可以把这个XBTC代币转账到以太坊的生态中，参与各类去中心化金融活动了。这样就把比特币转账到了以太坊上，实现了资产跨链。

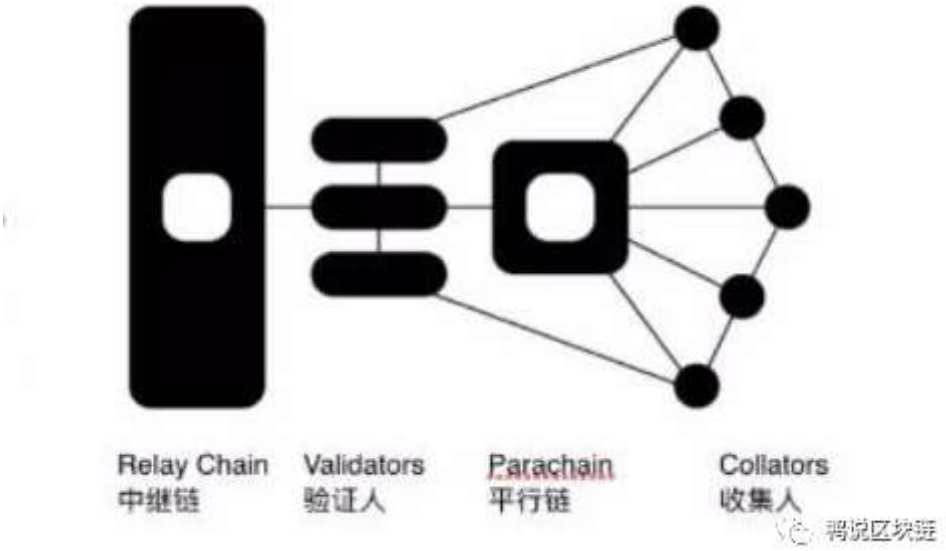
如果用户想赎回自己比特币链上的BTC怎么办呢？其实也很好实现，只需要把**XBTC代币转回以太坊的转接桥，并提交一个接收比特币的地址**，转接桥收到XBTC后，立即通过智能合约**销毁。**
同样经过波卡XCMP协议，把销毁的消息传到比特币的转接桥上，**解锁释放BTC到这个用户提供的比特币地址上**，这样用户就拿到了原来的BTC。

四、如何确保转接桥的安全

可以看出，比特币和以太坊的资产跨链主要依赖于转接桥。有人问鸭哥，如果转接桥跑路了或者不工作了怎么办？
其实转接桥并不是中心化的，**它也是属于去中心化的区块链**，在这个桥链上存在**收集人**这个角色，每个平行链都有属于它自己的收集人，这些收集人收集平行链的消息传给中继链验证，并监控平行链的情况，防止作恶事件的发生。

要成为收集人是需要质押该平行链的代币的，比如作为比特币转接桥的收集人，需要质押BTC，如果运行收集人节点掉线，或者作恶，系统将会惩罚质押的BTC，当然如果收集人表现良好，**系统也会有奖励作为收集人的激励。**

因此在比特币和以太坊的转接桥，**资产跨链是要收取手续费的，这些手续费作为收集人的奖励**，比如用户转到转接桥上1BTC锁定，实际在以太坊转接桥上可能只会收到0.99 XBTC代币，扣掉的0.01BTC就是作为收集人的奖励了，**这样通过去中心化的方式就能保证转接桥的安全。**



五、总结

不知大家有没有发现波卡整个跨链系统中最核心的部分是什么，鸭哥认为**波卡跨链系统中最核心的就是XCMP协议**，事实上，所谓资产跨链，也是因为通过数据跨链，**通过数据的链间通信来操作两个不同区块链之间资产的锁定、解锁、铸造和燃烧的过程。**
回归本文的标题——**跨链可组合性**，其中可组合性又是指什么呢？其实，波卡的平行链范围非常广泛，包括公有链、私有链、联盟链甚至不是一个区块链，只要它的技术足够优秀，可以为波卡生态的繁荣增添新的功能，都可以加入到波卡这个庞大的跨链系统中。所有波卡生态下的平行链都可以互相跨链通信、资产转移、互相操作。

正如上文文末我们对波卡进行的定义：

所以你说波卡是什么，它什么也不是，但是加入它的区块链多了，它就什么都是了。

——END

鸭哥创办了Polkadot新纪元社区，后续有千元红包和抽奖送DOT的活动，有一手消息或争取到的波卡生态项目的糖果也会作为福利发给社区，扫描二维码马上加入：
更多交流请加鸭哥V: cui1kcan2

知识星球

Polkadot新纪元

星主： Joie

长按扫码预览社群内容
和星主关系更近一步

鸭说区块链