解读Stable++：采用CDP机制，RGB++Layer首个稳定币协议

作者：白丁&Vicent Zhao，极客web3

编辑：Faust，极客web3



加缪曾在《鼠疫》中说：“要打听一座城市，无外乎看那里的人怎样工作，怎样相爱，又怎样死去”。如果要考察一条公链的生态，人们最先看的必然是有多少DeFi协议、多高TVL、多少应用场景。可以说，Defi数据直接反映了公链的兴衰，这套评判标准虽然像GDP一样存在诸多不足，但时至今日仍被观察家们奉为首要的参考框架。

在业务模式上，现代DeFi离不开最基础的四套件：DEX、借贷、稳定币、预言机，在此基础上还有LST、 衍生品等，这些东西在EVM生态司空见惯，但在BTC生态却极为稀缺，为此曾涌现出无数打着BTCFi和BTC二层旗号的项目方。

但时至今日，BTCFi和BTC二层身上的诸多缺陷暴露无遗，大多项目只是在比特币生态搭了一条EVM Chain，DAPP基本都是以太坊迁过去的，俨然有把比特币作为以太坊殖民地的味道。这些EVM Chain在同质化内卷的同时，基本没有什么让人耳目一新的东西，也没讲出什么有意思的故事。

相比之下，CKB和Cardano等UTXO公链可能比EVM Chain更具魅力。此前RGB++ Layer创始人Cipher基于UTXO模型的特性，提出了“同构绑定”和“Leap无桥跨链”的方案，一度吸引了无数人的目光；结合Intent且对订单簿友好的UTXOSwap、基于等额抵押的ccBTC、适配多链支持Passkey技术的JoyID钱包显然也可圈可点。

不过，对于CKB和RGB++ Layer生态而言，一大重点在于其稳定币系统，作为各类Defi场景中的枢纽，是否有稳健可靠的稳定币发行协议会直接影响生态格局，此外，能否为稳定币提供合适的流通环境也非常重要。比如USDT最早曾借助比特币的Omni Layer协议来发行，但由于Omni Layer提供的智能合约环境较差，USDT最终放弃了Omni Layer，这说明稳定币只有在完善的智能合约环境下流通才是最合适的。



对此，基于CKB的RGB++ Layer凭借其图灵完备的智能合约环境以及原生AA等周边设施，可以为BTCFi生态的稳定币创造绝佳的流通环境。此外，由于许多大户习惯于长期持有BTC而非用其频繁交互，如果可以在保证安全的同时，使用BTC作为抵押物发行稳定币，可以撬动大户们与BTCFi产生互动的积极性，提高BTC的资金利用率，还可以减少人们对中心化稳定币的依赖。

下文中，我们将对RGB++ Layer生态内的稳定币协议Stable++展开解读，该协议将BTC和CKB作为抵押物生成RUSD稳定币，结合Stability Pool保险池及坏账重分配机制，可以为BTC及CKB持有者提供可靠的稳定币铸造场景。而结合CKB独特的增发方式，Stable++可以在RGB++生态内构建欠阻尼系统，在市场波动剧烈时起到适度的缓冲作用。



### Stable++产品功能与机制设计

从工作原理来看，常见的稳定币基本有四类：



其中MakerDAO是CDP模式稳定币协议的代表，所谓的CDP即债务抵押头寸，即超额抵押ETH、BTC等蓝筹资产来铸造稳定币，由于蓝筹资产共识强价格波动率相对较低，基于其发行的稳定币更能抗风险。CDP模式下的借贷协议类似于AMM的“点对池”，用户的所有动作都与资金池进行交互。

这里我们拿MakerDAO举例。借款人首先在Maker上开立头寸，明确想从CDP中生成的DAI数量，之后超额抵押并借出DAI。当借款人还款时，将借出的DAI还回Maker平台，赎回抵押物，同时根据自己借出的DAI的数额、时间支付利息。这里的借款利息只能用MKR支付，是MakerDAO的收入来源之一。



而DAI的价格锚定机制依赖于“Keeper”。我们可以简单地把DAI的总数视为恒定的，且由两部分组成：MakerDAO资金池中的DAI、平台外市场上流通的DAI。Keeper会在上述两个资金池之间来回套利，维持DAI价格稳定。如下图所示：



本文的主角Stable++在机制设计上同样采用了CDP，并且借用RGB++同构绑定的技术部分继承了比特币的安全性。从产品功能的角度看，Stable++的功能可分为几个部分：

1. 在Stable++中， 用户可以通过超额抵押BTC或CKB，借出稳定币RUSD，以及用RUSD赎回自己的BTC或CKB，抵押和赎回操作会收取手续费；

2.用户可以将借出的RUSD再质押回Stable++，以此获得Stable++的治理代币STB作为奖励，同时获得参与资产清算的权利。这是RUSD的主要通缩场景，接触过Ethena(USDe)的人对这套玩法肯定不陌生。此外，你还可以将治理代币STB也质押回Stable++，若如此做，你可以按照质押STB的权重，从人们抵押和赎回抵押物的手续费中获得一定分成；

3.RUSD支持同构绑定和Leap功能，通过Leap，可以把BTC账户名下控制的RUSD转移至别人的Cardano账户名下，这中间不需要传统跨链桥的介入，安全风险很低而且过程很简洁；

4. Stable++设有LSD板块，NervosDAO用户可以把CKB质押到Stable++上换取wstCKB。这里解释下，NervosDAO是CKB生态的一个重要部分，以一定奖励激励人们将CKB长期质押于此。现在通过与Stable++的结合，NervosDAO用户可以质押CKB获得奖励，同时资产的流动性也没有丧失。



这些功能很好理解，不必赘述。但是我们要知道，一个CDP稳定币协议是否成功，关键要看以下几个方面：

下面我们将着重从清算机制进行展开，解析Stable++的具体设计。

### 清算机制的合理性和效率

可以说，清算组件是借贷协议维持正常运转的关键闸门，Stable++在清算机制的设计上进行了一定创新，规避了传统清算机制中的问题。在Stable++系统中，用户将资产超额抵押到CDP组件中借出稳定币后，如果抵押物价值下降，抵押率跌破阈值，用户不及时补仓就会被清算。

清算旨在确保系统中每一枚RUSD都有足够的抵押品支持，避免系统性风险。在清算过程中，借贷平台要从市场上收回一些RUSD，减少流通中的RUSD数量，最终让平台发行的RUSD有足够的抵押物支撑。

大多数借贷协议的清算以荷兰拍形式进行，平台将抵押品卖给出价最高的买家（即清算人）。举个例子，假设ETH价格4000美金，铸造DAI的抵押率为2：1，系统允许你用1个ETH最多铸造2000美元的DAI，而你实际上铸造了1000个DAI。过了一段时间，ETH价格跌破2000美金，你铸造的1000个DAI抵押率不足2:1，这会引发清算，你抵押的1枚ETH会被自动拍卖出去。

荷兰拍即从最高价开始降价式拍卖，拍卖价逐步降低，直到有买家愿意接盘。假设这些抵押品从1500美金开始拍卖，最终以1200美金成交给清算人，清算人交付1200枚DAI即可获得1个ETH的抵押物，能获得一定利润。之后MakerDAO协议会把收到的这1200枚DAI销毁或锁住，总之会减少流通中的DAI数量。

上述过程在智能合约控制下可以自动执行，确保系统中的稳定币供应始终有足够的抵押品支撑，去除过度杠杆化的头寸。但在实践中，MakerDAO清算机制存在两个问题：

1. 拍卖过程需要时间，当市场剧烈下跌时，有可能出现无法清理掉坏账的情况。自动清算的初衷是通过折价出售抵押物，让渡一定利益来吸引清算人，如果抵押物价值持续下跌，清算人的意愿会大幅降低，平台可能一直找不到合适的清算人。

2. 如果网络极度拥堵，个体户清算人的大量操作都没有及时上链，也会影响到清算流程，这在2021年的5.19事件中得到了实证，当时由于市场剧烈震荡，链上极度拥堵，很多个体户清算人和被清算者的操作都无法及时上链。

上述问题在MakerDAO、AAVE等主流借贷协议身上都有体现，都是因为清算效率低下最终对平台本身和用户造成了损失。针对这个问题，Stable++在清算机制的设计上，倾向于尽量确保清算过程的高效，所以增设了“Stability Pool稳定性池”和“Redistribution重分配”的双重保险机制，这也是Stable++在机制设计上最大的亮点。



Stable++中，用户可以向Stability Pool（下文称之为保险池）存入稳定币，作为“常备军”随时准备清算不良头寸。当清算事件发生时，协议做的第一件事是通过保险池清算掉不良头寸，再将抵押品分配给保险池的LP作为奖励。Stability Pool使清算人角色由“临时找”变成了“常备军”，相当于给协议加了一道高效缓冲，不必等清算发生时临时找清算人。

但这里有两个需要注意的点：

1. Stability Pool目前接受注入的稳定币为RUSD本身。可能有人担心：如果保险池里的储备资产是平台自己发的RUSD，看起来存在自举（自己把自己举起来）。这是否合理？

关于这一点，需要强调的是，保险池中的RUSD在参与清算时会被直接销毁。举例来说：假设RUSD的抵押率为110%，Stability Pool中共有100 RUSD，来自于一位LP。现有一个头寸，铸造了100 RUSD，抵押物价值109美元，已触发清算条件。

该头寸被清算时，保险池中有100 RUSD被直接销毁，这意味着LP将损失100 RUSD，获得清算头寸内109美元的抵押品，利润9美元。之后，被清算者不再需要偿还100 RUSD的债务。

显然，市场上流通的RUSD中有100枚被销毁，平台上也少了109美元的抵押品，触及110%抵押率红线的不良头寸直接消失了，平台上其他头寸的抵押率还是健康的。对此，我们可以如此总结概括Stable++的保险池设计：

本质就是让部分借款人把自己的RUSD锁仓，当某个头寸被清算时，平台需要销毁部分RUSD并移除不良抵押品，来维持健康。MakerDAO的清算模式下，被销毁的DAI由市场上随机的清算人提供，而Stable++直接由保险池提供待销毁的DAI。所以，对于Stability Pool这种模式来说，可以只用Stable++自己发行的稳定币作为储备，不必担心自举问题。

上述例子同时还解释了作为Stability Pool的LP，获得的抵押品折扣率怎么计算，这和系统设定的CR相关。如果按照上述案例中110%的抵押率来看，参与清算的LP相当于用100U获得了109U的抵押品，折扣率约为9%，和常规的清算折扣差不多（这里只是简单举个例子，并不代表Stable++的真实参数）。

但因为Stable++用的是常备保险池，所以在清算速度和效率上好很多，不需要临时去市场上寻找清算人。反过来说，如何维持Stability Pool有充足的流动性来应对清算，也是需要着重考虑的问题。



2. 如果Stability Pool没有足够的稳定币来参与清算，那么Redistribution就会启动，被清算头寸涉及的债务和抵押品将按比例在当前所有头寸中重新分配。比如说，当保险池也无法处理坏账时，坏账部分的债务就会成为global debt，分散给所有借款人，例如：

现在有100个借款人，而某个待清算头寸有100 RUSD的坏账，Redistribution就会让每个借款人多承担1 RUSD的债务，但同时也会获得相应份额的抵押品作为收益。这一点和Synthetix等老牌Defi平台的重分配机制不一样。Synthetix只会把坏账部分的债务分配给现有借款人，把借款变成global debt，每个借款人只承担额外债务，而不获得对应收益。

通过上述两道保险，Stable++保证只要清算事件发生，都可以在第一时间被迅速消化，这种高效清算可以有效解决传统借贷协议中的坏账问题。并且，这种双管齐下高效的清算方式代表Stable++可以以一个较低的抵押率（比如110%以内）让用户借贷，大大提高资金利用率。

总结来说，CDP本质上是借贷的一种形式，因为是借贷关系，所以一定会出现坏账，也就是抵押品价值下跌导致“资不抵债”的情况发生，就需要清算。在下面谈及的两种清算方式上，双方又各有优劣：

以MakerDAO、Aave为例的传统拍卖清算方式久经考验，无需维护庞大的“保险机制”，通常只要确保抵押资产的流动性足够好，市场接受度高，就可以实现大规模的清算。但是缺点就和之前提过的一样，遇到极端行情效率不高，而且除了ETH等特定的几种资产外，其余抵押品的流动性并不高，没有足够的清算者来快速帮助协议回到正常债务水平；

以Stable++和crvUSD为例的“清算池”，本质都是以协议控制的资产池作为清算者，通过挂反向订单的形式，在发生清算时快速进行清算，使得协议整体债务水平达到健康值。只是在具体做法上每家各有千秋。比较有趣的是，AAVE最新的Safety module --umbrella 也采用了不出售保险池资产，而是通过燃烧的方式来减少坏账。

Stabl++采用的是燃烧机制，清算池中的资产会直接被销毁，所得抵押品也直接分发给保险池的LP。而crvUSD则是完全交易的思路，清算时用crvUSD购买抵押品，抵押品价格上升后又会卖出这些抵押品，回购crvUSD，整个抵押品的所属权是在Curve本身。

### 能否在所属生态内构建欠阻尼系统

首先要讨论一下，一个健康的经济系统是什么样的？它的必要条件之一是：一定要有对抗币价变动趋势的“欠阻尼机制”。欠阻尼（力）借用了物理学中的概念，指“阻碍”但不足以“阻止”物体运动趋势的力，会使物体的变化趋势减缓，在代币经济学中指无论币价涨跌，经济系统中都有阻碍但无法阻止其变化的缓冲机制。这样的经济系统既能维持发展，又不会过度杠杆化，具备软着陆的条件。

比特币的交易手续费、以太坊的Gas费计价模型，都会随着实时的热度变化而动态调节， 这就是一种“欠阻尼机制”。反之，如果一种资产快速上涨或下跌，系统中缺乏有效缓解其变化趋势的方案，那就是不健康的经济系统，这样的系统最终会因过度杠杆化而崩溃，这也是一众以太坊LSD、Restaking项目被人诟病的原因。

由于Stable++支持的抵押物主要是BTC和CKB，而且其部署在RGB++ Layer上，那么我们就要考察Stable++和CKB代币之间形成的关联对于整体生态是否有益。

除创世区块外，CKB的发行方式有两种。第一种即PoW挖矿产生，上限为336亿枚，新增的CKB每4年减半一次，上次减半在2023年，年发行量由42亿枚降为21亿枚。这种方式叫做“基础发行”。

另外CKB还有一个独特的机制，即用户要锁住一些CKB才能在链上存放数据（你在CKB链上持有资产，会有相应的数据要存储，要支付一定的存储费用）。但网络并不直接向锁住CKB的人收取存储租金，而是通过发行CKB，用通胀的方式稀释用户手中的代币价值，变相收取租金，这叫做“二级发行”。二级发行每年的总量固定为13.44亿，这部分Token的分配方式如下：

1. 矿工：分配给矿工的二级发行CKB，与用户在链上占用的存储空间成正比

2. NervosDAO

3. 国库：分配给国库的二级发行CKB，与流通中CKB/总发行量的比例成正比，这部分会直接销毁

Stable++可以让用户质押CKB生成wstCKB，或使用CKB以较低的抵押率借出RUSD。CKB价格上涨时，将有更多人用CKB抵押铸造RUSD，这可以让很多CKB被锁住；而铸造出的RUSD会增加链上Defi系统的活跃度。总体而言，相当于间接降低了CKB通胀率，又增加了链上活跃度，也可以让矿工获得更多利益，调动其积极性提高整个网络的经济安全。

所以与其他资产抵押类稳定币不同的是，Stable++与CKB的发行机制组成了一个较为健康的代币经济系统，可以形成“欠阻尼机制”，而不是单纯的加杠杆。配合已有的CKB LST，其可组合性和流动性将会进一步提高。

### 总结：从市场角度看Stable++的必要性

从市场角度看，BTCfi生态上也需要一种规模较大的去中心化稳定币出现。

第一，当前加密市场中的稳定币，USDT和USDC几乎占据了90%的市值，但它们的中心化风险难以忽视。如上文所言，BTCfi用户最注重的就是安全，一个能满足大户对交易和安全的综合需求的去中心化稳定币如果出现，是撬动这些人参与到BTCFi中的必要条件。



第二，稳定币的市值总和大概是800多亿美元，只有比特币总市值的零头，从这个角度看，还有很多BTC可以作为抵押物生成稳定币，基于BTC的稳定币还有很大的发展潜力。



但之前比特币生态也出现过一些稳定币，却都未引起市场的较大反响。究其原因是出现得过早，当时没有足够的技术作为支撑。如今，随着RGB++ Layer生态的日渐繁荣，以及UTXOSwap、Stable++、JoyID等项目的逐步完善，BTCFi在CKB上的大基建才刚刚开启序幕，基于比特币的稳定币协议必将为BTCFi生态带来新的想象空间，CKB这片价值洼地将成为创业者的沃土，一切愿景都未来可期。