Prestare Flash Loan Tool

初衷

目前的借贷协议都是以超额抵押作为整个平台的基础，但是超额抵押带来的资金利用率低的问题。并且由于目前以太坊缺少一个系统的，根据地址及个人信息的信誉机制，因此使得在借贷协议上去做加杠杆的操作不被很多协议原生支持。因此当前交易者想要在一个平台上进行加杠杆，提高自己仓位并且同时进行看空看多操作，就需要使用循坏贷的方式，即超额抵押一笔资金，借出一笔资金重新抵押，再借出资金，循坏以上的操作，直到不可再借出资金。在这个过程，交易者的交易成本是多笔资金交易转账带来的gas费用，如今在AAVE上的存款所需消耗的gas大约在$8，因此假设借款也需要$8，因此一次循环的成本为$16，假设在以太坊主链上，交易员存价值$1000的ETH，循环贷操作5此后，用户当前的仓位约为3689，贷款金额2689，LTV约为72%（以ETH以80%为抵押，借出的资金为ETH，不计算交易成本），计算杠杠为3.689，交易成本是$80，占用户资金的8%。由此可见，循环贷的方式在以太坊是非常昂贵的操作。因此需要一种新的方式完成加杠杆以及看空看涨的操作，从而使得交易成本降低。

AAVE提出的闪贷贷自推出以来，就以其可以高效撬动大笔资金，并且可以保证交易操作的原子性而收到很多好评，当然也成为很多攻击的首选方式，如最近的Euler。我们的目的是使用闪电贷的方式，帮助用户一次完成加特定杠杆的功能。用户使用工具，只需要指定倍数，看空的资产，看涨的资产，以及用户初始存入的资金。工具在链下完成计算，并且得出最大的杠杆数，在链上，使用闪电贷借出看空的资产，然后通过dex交换得到看涨的资产(如用户没有选择，默认为稳定币或WETH)，然后将看涨的资产存回或还回AAVE。同样以上述例子为例，用户可以选择看空UNI，看涨WETH，此时用户可以一次性借出价值$2600的UNI，在uniswap上交换得到最少$2592(按照Uniswap 0.3%的滑点计算)WETH，此时将资产存回AAVE。用户当前的仓位变为3592，借贷为2600，LEV约为72%，杠杆为3.592，用户的交易成本是闪电贷的0.09%的手续费以及gas费，当前的uniswap gas费大约为$7，加上闪电贷的操作gas估算为$10(并非准确估值)，那么交易成本约为$20，占初始成本的2%，成本降低了75%。

实现大纲

AAVE的有两种类型的flash loan，一种是flash loan支持同时多类资产闪电贷，并且只要health factor允许，可以直接将用户的闪电贷转化为debt token，另一种是flash loan Simple，支持单一资产闪电贷，并且必须有足够的资金归还。

目标一：支持在AAVE上进行加杠杆行为。用户在当前界面填入自己的AAVE仓位价格，然后填入目标杠杆，看空资产，看涨资产，可接受滑点。Tool得到信息后，首先获取链上的数据，查看用户当前的仓位价值，检查看空的资产是否可从AAVE中借出，看涨的资产是否可以作为AAVE的抵押品，计算用户当前的杠杆是否可行，检查UNISWAP上是否有对应的滑点等级资产pool。通过以上的信息后，在前端展示用户的最大可借贷资产，当前滑点下转化的资产，构造交易所需的参数，用户确认交易后，使用metamask发起交易，调用合约函数/或直接调用AAVE的flash loan。闪电贷此时借出看空的资产。合约中指定executeOperation函数，在该函数中需要解析用户的需求（通过params传入的数据），分析用户想要看空看涨的资金种类，然后在uniswap上交换资金，交换结束后，计算并判断当前的滑点，最后将资金存回AAVE，完成操作。

目标二：支持使用AAVE闪电贷在别的借贷协议上加杠杆。与目标一相似的步骤，用户需要额外确认自己的平台，链下的计算同目标一。在链上发起操作后，闪电贷借出看涨的资产，合约会解析用户的需求，确定用户的平台，然后将借出的看涨资产存入到借贷协议上，然后在借贷协议上借出看空的资产，通过dex交换为看涨资产，归还到合约账户上，后续AAVE会从合约上提取闪电贷的手续费和本金。