1 概要

TTSWAP(token-token swap)是一个建立在以太坊区块链上的自动做市协议，意味着它不依赖于中心化的机构或个人来进行交易。它的核心原理是根据用户的行为，自动触发市场价值的转移，从而构建了一个基于恒定价值交易模型的协议。

这个项目的白皮书解释了TTSWAP的设计逻辑，涵盖了以下几个方面：

1. 商品交易：用户可以直接用一种商品换取另一种商品，而不需要通过其他中间商品。
2. 价值商品投资与撤资：用户可以投资特定的价值商品，并在需要时撤回他们的投资。
3. 普通商品投资与撤资：除了价值商品外，用户也可以投资普通商品，并随时撤回他们的投资。
4. 商品手续费的产生与分配：在交易过程中产生的手续费会按照一定的规则进行分配，以激励更多的人参与到这个市场中来。

总之，TTSWAP为普通用户提供了一个简单、透明、高效的加密货币交易协议，这个协议使用的是一个革新地AMM逻辑——恒定价值交易模型。旨在打造一个方便、安全、低GAS费用的协议。

2 特点

1. 恒定价值交易模型
   这个模型的核心思想是确保交易的价值在整个过程中保持恒定，这意味着无论交易何时进行，都能客观地反映出币种的市场价值，这可让商品自由、简单、快速地交易。
2. 无中转，直接交易
   在这个协议上，任意两种商品之间可以直接交易，而不需要先将一种商品转换成中转商品再进行交易。这样的直接交易模式简化了交易流程，节省了时间和成本。
3. 无滑点交易
   滑点是指在交易过程中由于市场价格波动导致的交易价格偏离预期的现象。在这个协议中，只要交易数量低于特定的阈值，就不会出现价格滑点，这意味着交易在特定条件下是稳定和可靠的。
4. 没有无常损失
   无常损失是指流动性提供者在提供流动性时因市场波动而遭受的损失。这个交易模型通过其设计逻辑上避免了无常损失的问题，这意味着流动性提供者或者商品投资者在撤资时可以保持原有投资的价值，并且还能获得提供流动性所产生的收益。
5. 低Gas费用
   Gas费用是在以太坊网络上执行智能合约时需要支付的费用。由于这个交易模型的逻辑相对简单且运算量较少，因此Gas消耗较低，用户在交易过程中可以节省大量的Gas费用，让交易更加经济高效。相比于其他交易模型，可以节省60%至90%的Gas费用。
6. 手续费按角色分配
   在协议上，手续费根据参与者的不同角色进行分配，这包括商家(商品卖家)、商品投资者（流动性提供者）、门户、推荐者和普通用户。任何人都有机会参与到协议的运作中，并分享协议发展所带来的收益，从而激励更多的用户参与到协议建设中。

7. native ETH支持

   协议中支持Native ETH直接兑换成任何代币.

3 价值守恒交易横型原理

3.1 恒定价值交易模型

$$\frac{V_a}{Q_a} * \Delta a = \frac{V_b}{Q_b} * \Delta b = ... = \frac{V_z}{Q_z} * \Delta z \tag{1}$$

$$V_a：表示协议中a商品的市场价值 \tag{2}$$

$$Q_a：表示协议中a商品的数量 \tag{3}$$

$$\Delta a：表示协议中a商品的购买量或者出售量 \tag{4}$$

$$V_b：表示协议中b商品的市场价值 \tag{5}$$

$$Q_b：表示协议中b商品的数量 \tag{6}$$

$$\Delta b：表示协议中b商品的购买量或者出售量 \tag{7}$$

$$V_z：表示协议中z商品的市场价值 \tag{8}$$

$$Q_z：表示协议中z商品的数量 \tag{9}$$

$$\Delta z：表示协议中z商品的购买量或者出售量 \tag{10}$$

市场价值是衡量用户对于协议中商品的需求程度.用户出售商品,说明对于协议中的商品需求下降,那此商品的市场价值下降.用户购买商品,说明对于协议量的商品需求上升,那此商品的市场价值上升.

3.1.1 计算逻辑

- 交易前a,b商品状态

$$平台中a的市场价值：V_a \tag{11}$$

$$平台中a的商品数量：Q_a \tag{12}$$

$$平台中b的市场价值：V_b \tag{13}$$

$$平台中b的商品数量：Q_b \tag{14}$$

  现在使用Δa购买到Δb后平台中商品状态

$$\text{平台中}a\text{的市场价值}: V_a - \frac{V_a}{Q_a} * \Delta a \tag{15}$$

$$\text{平台中}a\text{的商品数量}: Q_a + \Delta a \tag{16}$$

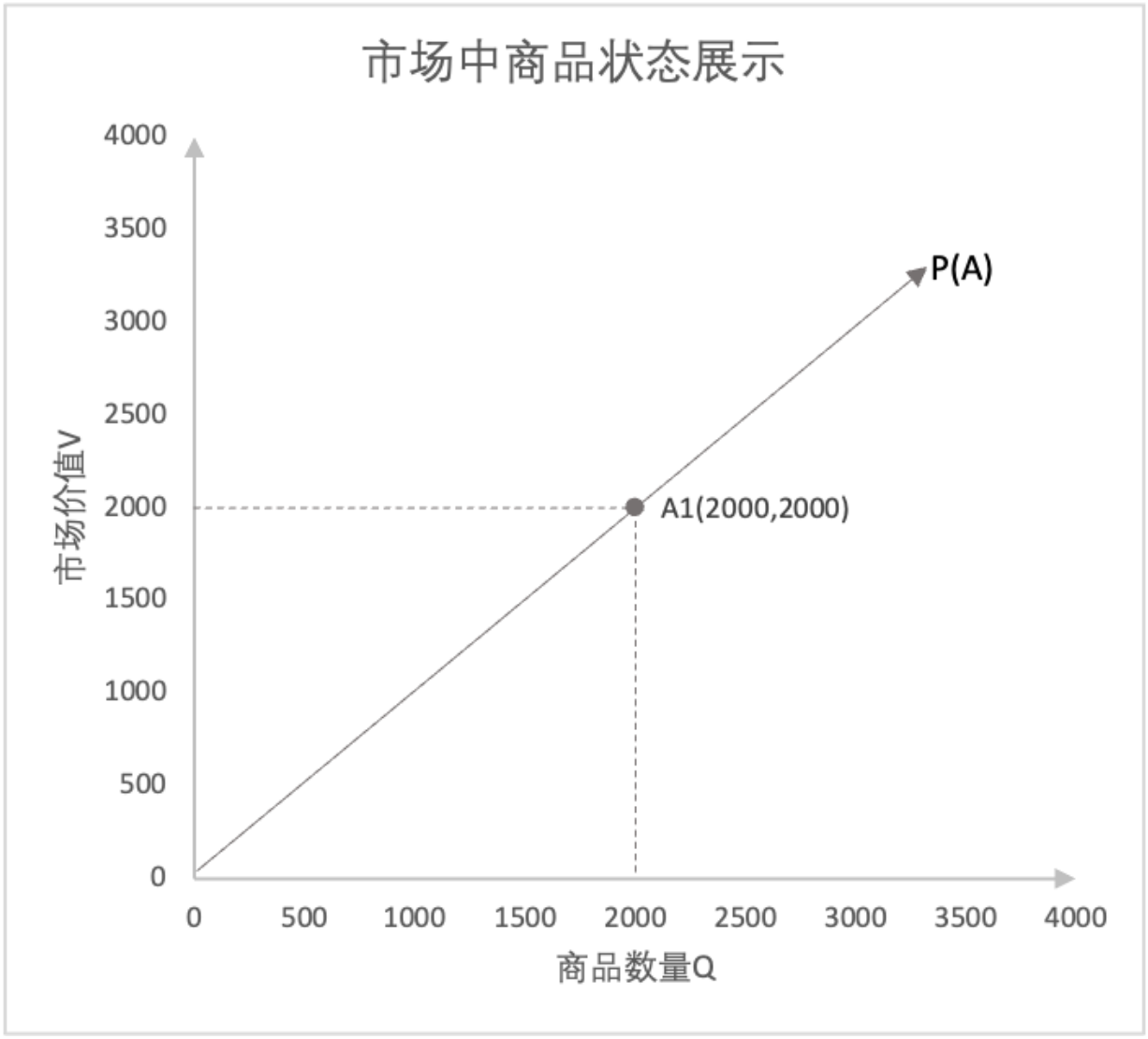
$$\text{平台中}b\text{的市场价值}: V_b + \frac{V_a}{Q_a} * \Delta a \tag{17}$$

$$\text{平台中}b\text{的商品数量}: Q_b - \frac{\frac{V_a}{Q_a} * \Delta a * Q_b}{V_b} \tag{18}$$

$$\text{获得}\Delta b = \frac{\frac{V_a}{Q_a} * \Delta a * Q_b}{V_b} \tag{19}$$

3.2 商品的市场价值

当商品添加到协议时,此时的商品的市场价值与商品的真实价值相同.
例:在协议中添加有2000个商品A1,由于此时的真实价值是2000,那么这个商品的市场价值2000.



定义:
市场价值V_{A1}:2000

商品数量Q_{A1}:2000.
单位价值P_{A1}:1,单位数量的市场价值.

3.3 市场中的商品与用户买卖行为的关系

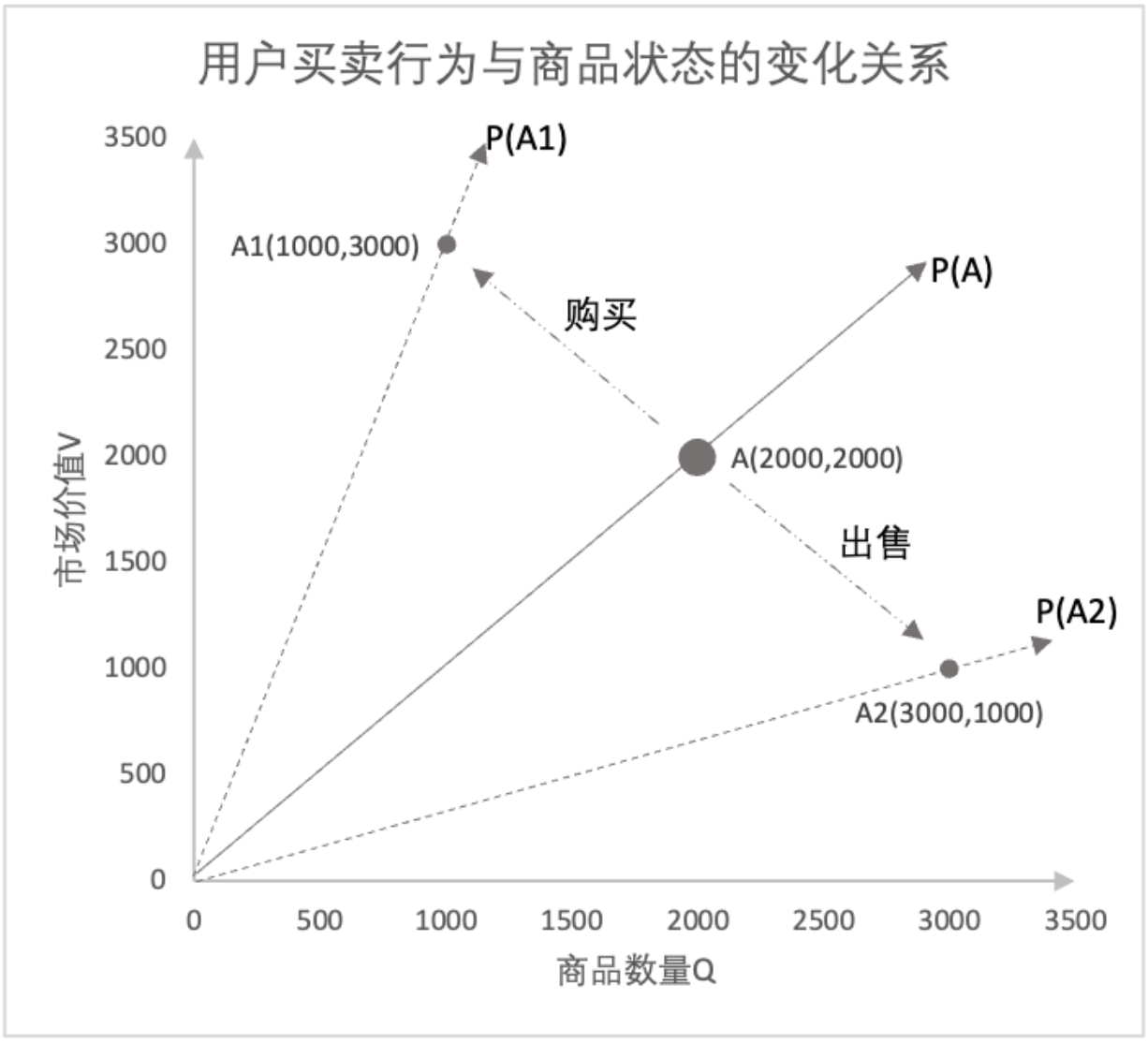
- 例1：用户花费价值1000购买,购买了商品A.

用户购买,说明商品的市场价值V增加.V_{A1}=2000+1000=3000
用户购买,协议中商品数量Q减少.Q_{A1}=2000-1000=1000
协议中商品的单位价值P发生变化成 P_{A1}=3

- 例2：用户出售价值1000购买,购买了商品A.

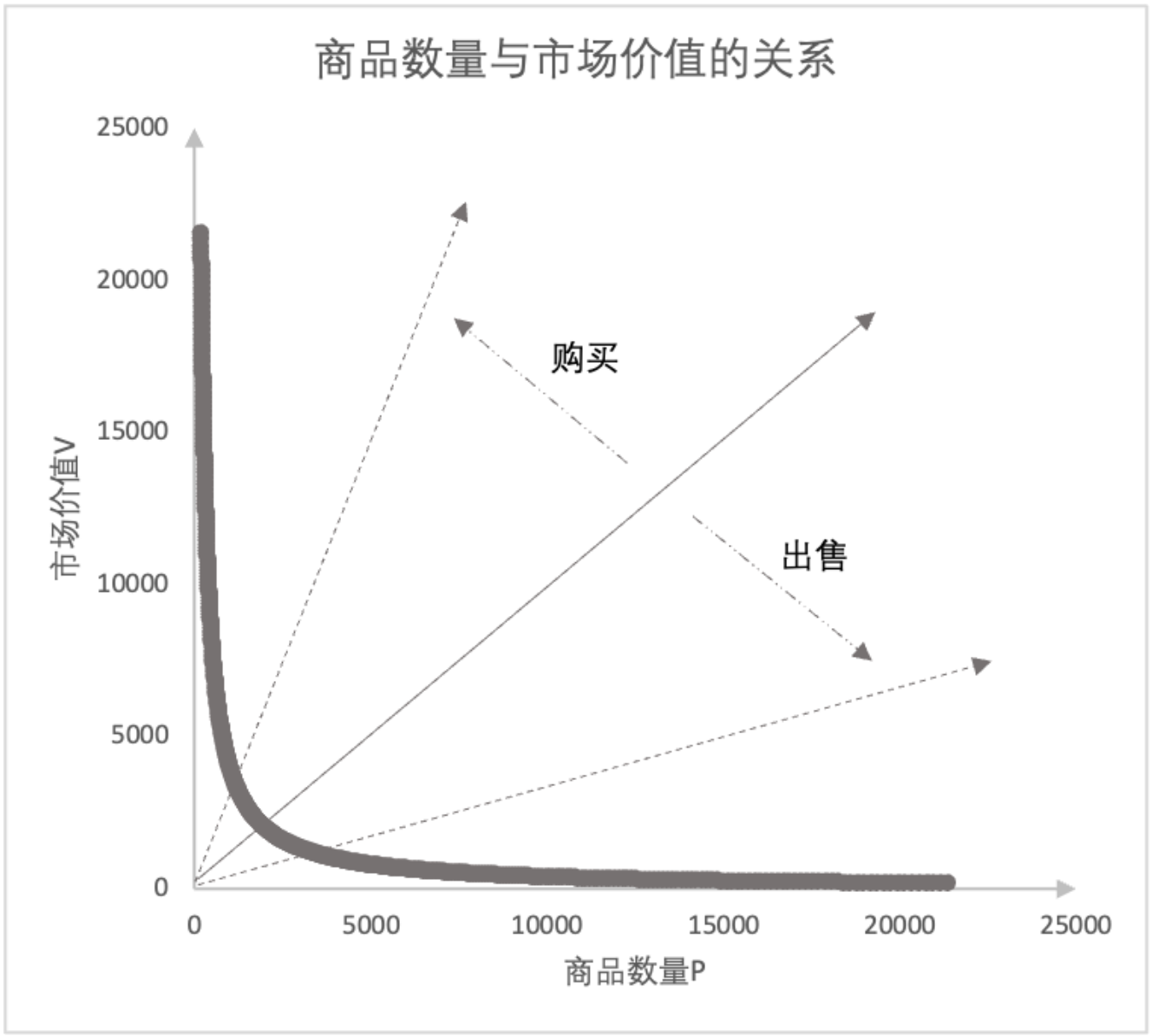
用户出售,说明商品的市场价值V减少.V_{A2}=2000-1000=1000
用户出售,协议中商品数量Q增加.Q_{A2}=2000+1000=3000
协议中商品的单位价值P发生变化 P_{A2}=0.3333

展示如下图



3.4 市场中用户行为与商品状态的关系

用户出售与购买，商品的商场价值V与商品数量Q发生变化，商品的价格也发生相应变化,商品的市场价值V与商品数量Q的变化如图

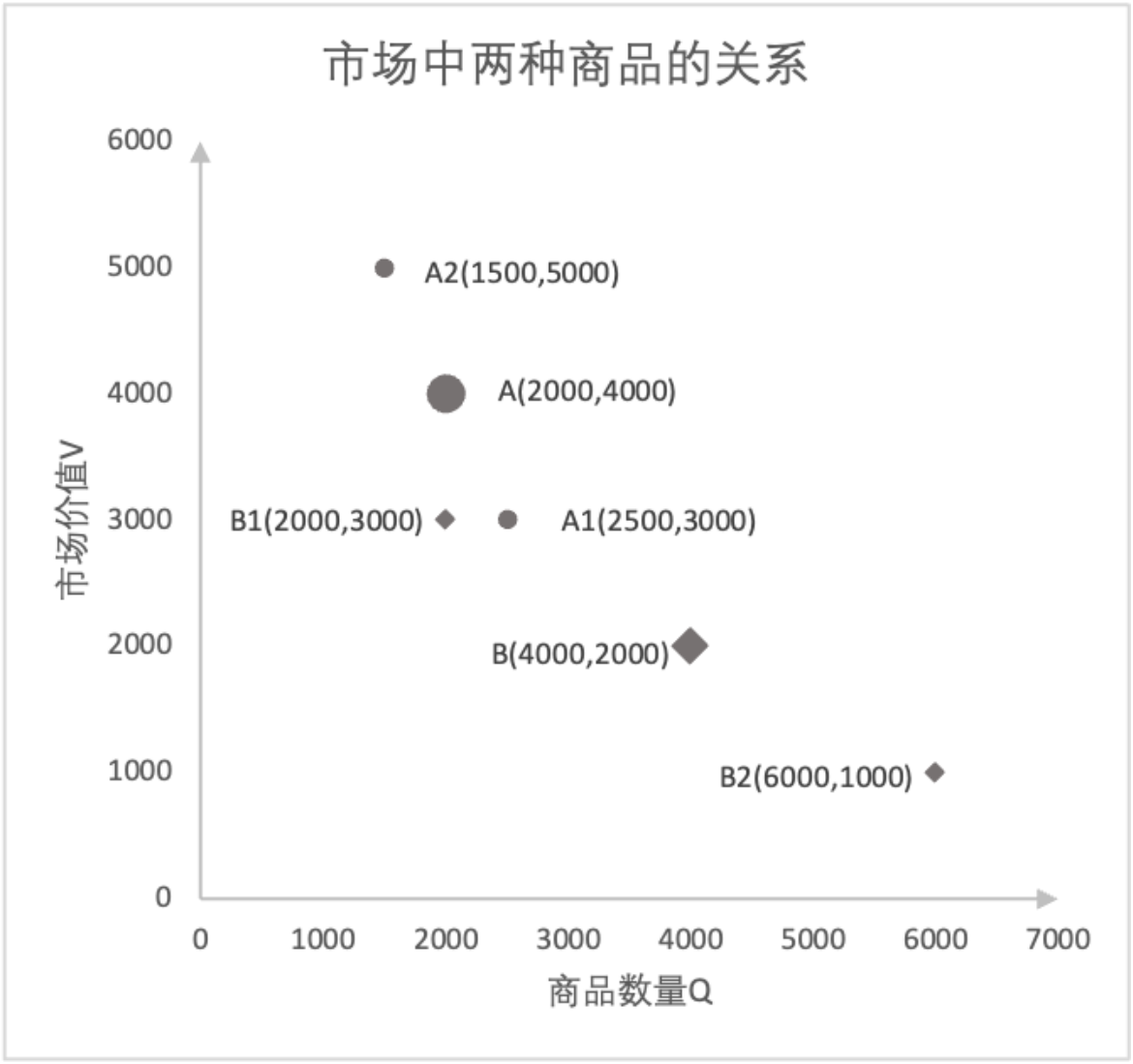


3.5 市场中两种物品的关系

市场中有两种商品,A和B两种商品.A(2000,4000),B(4000,2000).

- 用户使用500商品A,对于的市场价值为1000.市场价值为1000对应的1000个商品B.

当用户购买500个商品A,就要花费1000个商品B,协议中的商品在图中A位置会位移到A1的位置,B会位移到B1的位置.
当用户出售500个商品A,就能得到1000个商品B,协议中的商品在图中A位置会位移到A2的位置,B会位移到B2的位置.

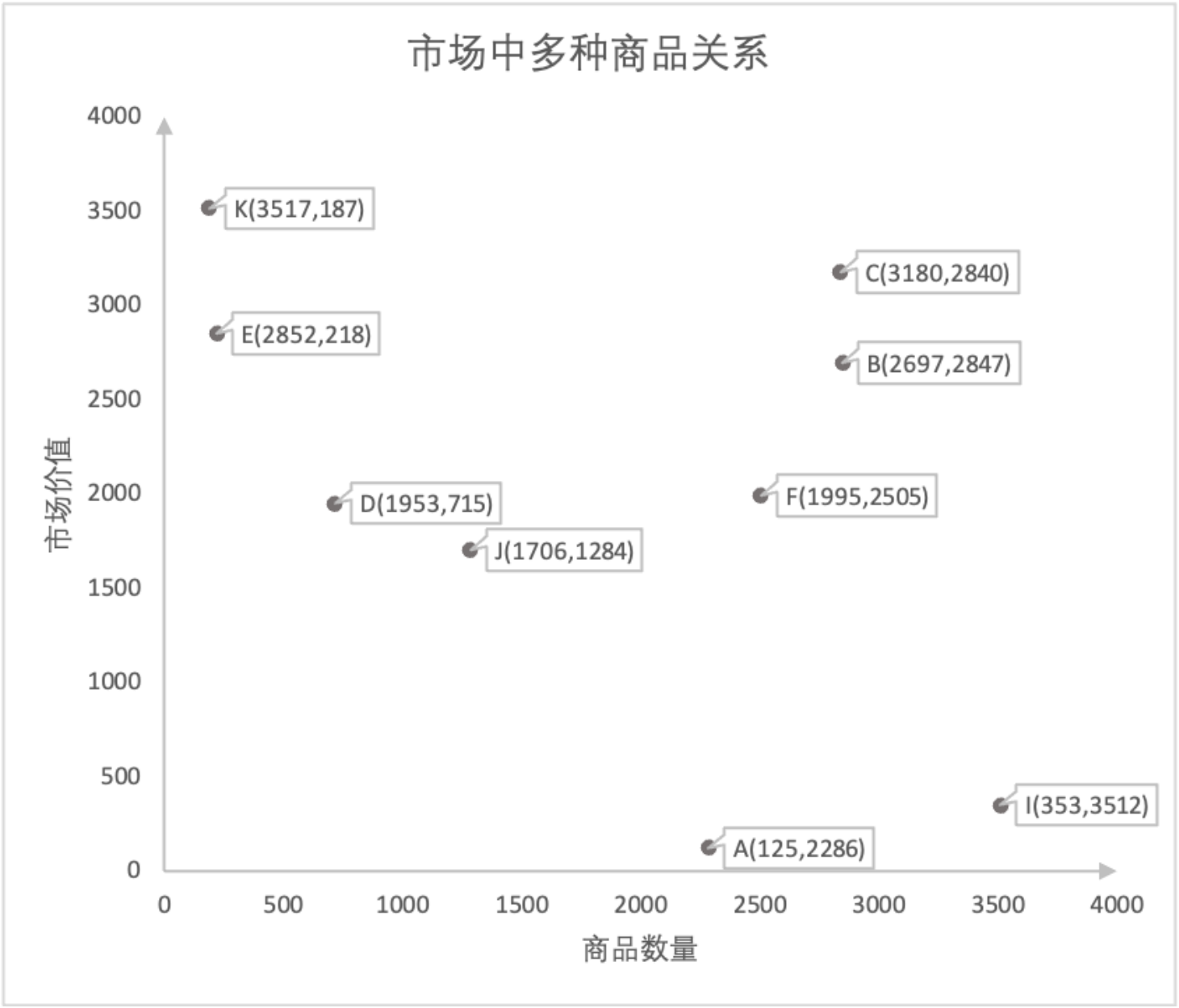


因为位置发生变化,P(A)与P(B)也发生变化，商品B相对商品A的价格也会发生变化,如果与市场外部价格有差异,就会有其它交易促进市场价格与市场外部价格统一.

> 备注：如果购买数量占市场中数据比例过大,会造成两商品的相对价格发生强烈波动,因此每个交易会拆分为多个小单进行交易

3.6 市场中多种商品的关系

任意两种商品因为用户交易,造成位置的变化,也会造成这两种商品与其它商品对对位置变化,产生价格的同步变化.



3.7 市场中商品每次交易大小与价格的关系

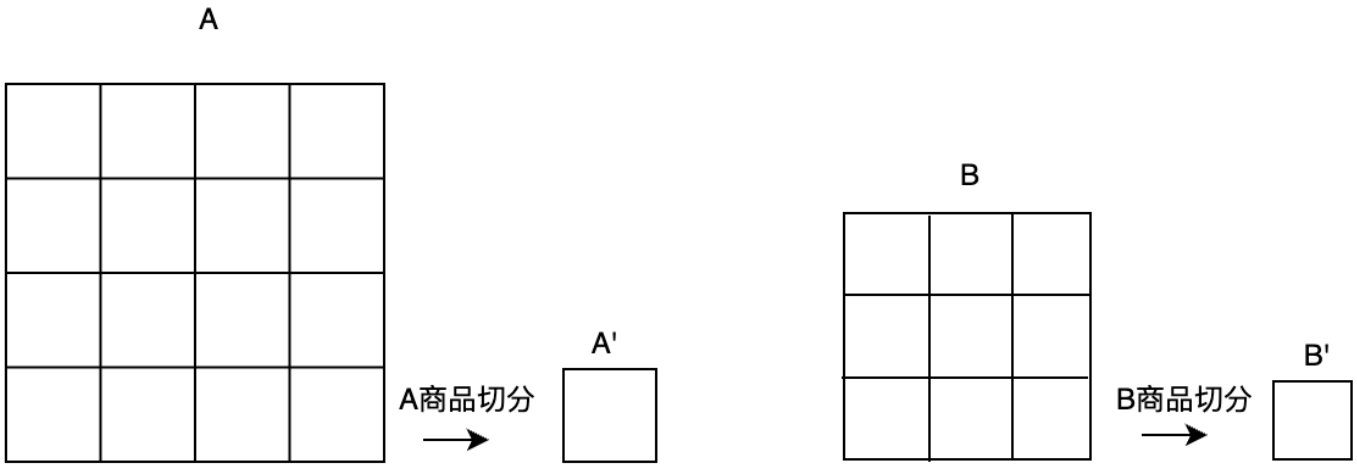
现场中商品数量为100 000 000 ,市场价值为100 000 000.

交易大小	价格变化
10	0.000000200000
50	0.000001000000
100	0.000002000002
500	0.000010000050
1000	0.000020000200
5000	0.000100005000

交易大小	价格变化
10000	0.000200020002
50000	0.001000500250
100000	0.002002002002
500000	0.010050251256
1000000	0.020202020202
5000000	0.105263157895

3.8 无滑点阈值(别称交易阈值)

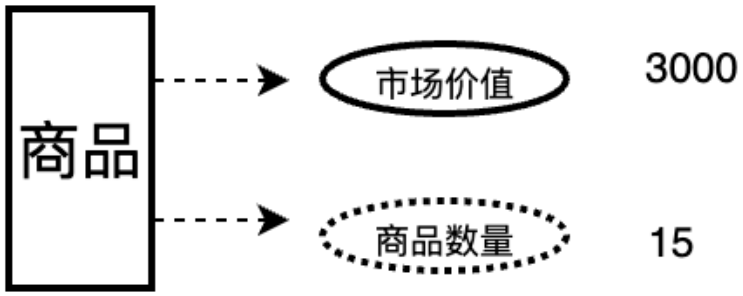
为避免用户交易造成协议商品被挤兑.每个商品在初始化时会设置切分数,每份大小即为这个商品的无滑点阈值。因此当用户交易时,如果交易价值小于商品无滑点阈值,无无常损失.如果交易大于商品无滑点阈值.交易会以阈值为单位,拆分成交.



4 商品

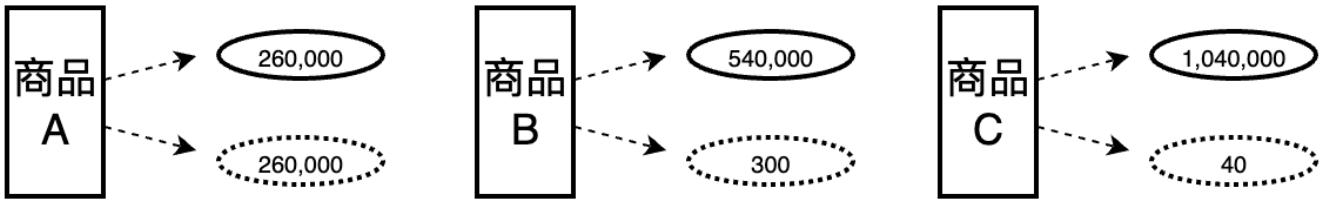
4.1 商品介绍

关于商品的描述:协议拥有市场价值3000的15枚A商品,那么商品就有两个属性:市场价值与商品数量.如下图



- 名词解释
  市场价值:用来衡量用户对协议商品的需求程度的。如果用户购买某个商品，说明用户对这个商品的需求增加,那么这个商品的市场价值就会上升。相反，如果用户开始卖出某个商品，说明用户对这个商品的需求减少,那么这个商品的市场价值就会下降.
  商品数量:记录市场中商品的当前数量。

- 可以如下图描述其它任何商品,例如



4.2 商品分类

商品分类	说明	交易是否 产生手续费	是否可以 单独投资自己	是否可以与其它价值商品 一同投资
元商品	市场中添加的首个商品	是	是	否
价值商品	商品得到市场认可, 有良好的生态及团队	是	是	否
普通商品	个人新增商品, 市场价值待确认	是	否	是

4.3 商品配置

- 商品配置占255位

4.3.1 市场可以调整

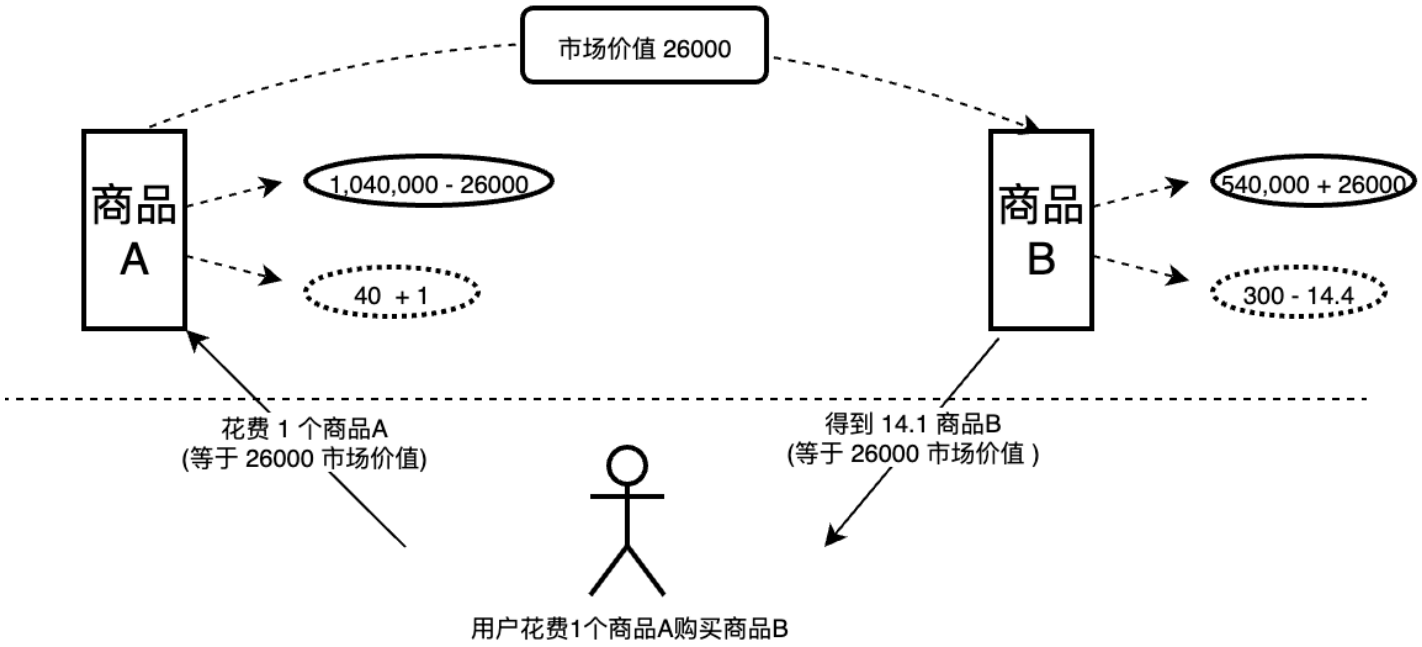
id	配置项	位数	单位	最大值	最小值	起始位	结束位	说明
1	市场价值商品	1	BOOLEAN	1	0	1	1	
1	预留	1	BOOLEAN	1	0	2	2	
1	预留	1	BOOLEAN	1	0	3	3	
1	预留	1	BOOLEAN	1	0	4	4	
...								

4.3.2 用户可以配置

id	配置项	位数	单位	最大值	最小值	起始位	结束位	说明
1	投资费率	7	万分之一	127	0	5	11	(1~1023)/10000
2	撤资费率	7	万分之一	127	0	12	18	(1~1023)/10000
3	购买费率	7	万分之一	127	0	19	25	(1~1023)/10000
4	出售费率	7	万分之一	127	0	26	32	(1~1023)/10000
5	交易切片数	10	64	1023	0	33	42	(1~1023)X64
6	撤资切片数	10	64	1023	0	43	52	(1~1023)
7	物品类型	33	1	1023	0	53	85	小于8589934591的数
8	电话号码	48	1	1023	0	86	133	小于281474976710652的数 前4位表示国家号, 后11位表示电话话码
9	经度	48	1	1023	0	134	181	小于2814.74.97.67.10656的数
10	纬度	48	1	1023	0	182	230	小于2814.74.97.67.10656的数
11	预留	26	1	1023	0	231	256	预留字段

5 商品交换

商品的交换实际上就是用户用自己手里的商品A去交换市场上的商品B。当用户选择放弃商品A时，这表明市场上商品A的价值降低，因为用户不再需要它。而当用户选择购买商品B时，这意味着商品B的价值上升，因为用户希望得到它。



- 如图所示,当用户放弃商品A时，协议中的商品A数量增加，而商品A的市场价值降低。而当用户获得商品B时，协议中的商品B数量减少，而商品B的市场价值增加。这就导致了相对于商品A，商品B的价格上升。因此，如果再次进行交易，用相同数量的商品A只能换取比上次少一些的商品B。

5.1 计算过程

$$\frac{V_a}{Q_a} * \Delta a = \frac{V_b}{Q_b} * \Delta b \tag{20}$$

$$交易前P_{ab} = \frac{V_a * Q_b}{Q_a * V_b} = 14.444444444444445 \tag{21}$$

$$\Delta b = \frac{V_a * \Delta a * Q_b}{Q_a * V_b} = \frac{1040000 * 1 * 300}{40 * 540000} = 14.44 \tag{22}$$

$$V_a = V_a - \frac{V_a}{Q_a} * \Delta a = 1040000 - \frac{1040000}{40} * 1 = 1014000 \tag{23}$$

$$Q_a = Q_a + \Delta a = 40 + 1 = 41 \tag{24}$$

$$V_b = V_b + \frac{V_b}{Q_b} * \Delta b = 540000 + \frac{540000}{300} * 14.4 = 566000 \tag{25}$$

$$Q_b = Q_b + \Delta b = 300 - 14.4 = 285.6 \tag{26}$$

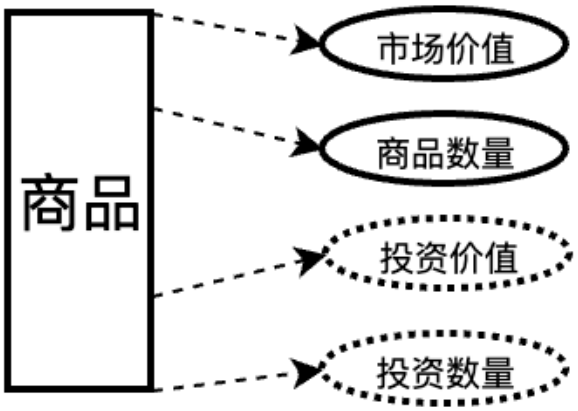
$$交易后P_{ab} = \frac{V_a * Q_b}{Q_a * V_b} = 12.479462208049643 \tag{27}$$

(实际计算中涉及商品切分, 具体参见智能合约) (28)

6 商品投资与撤资

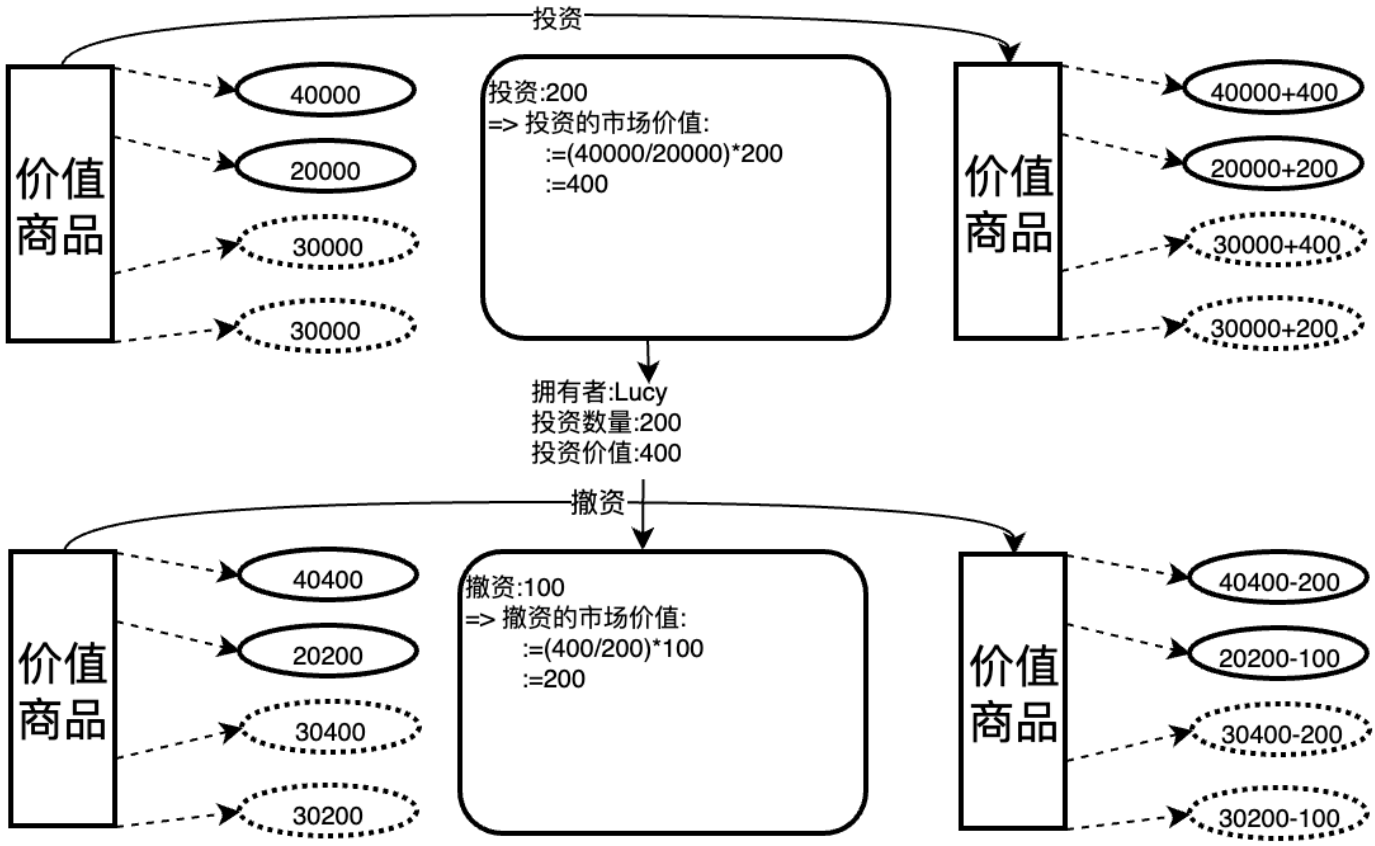
6.1 记录投资和撤资

市场中商品的交易,需有用户提供流动性.就应记录商品投资总市场价值与投资总数量.



- 名词解释
  投资价值:用户投资时商品的市场总价值.
  投资数量:用户投资时商品的总数量.

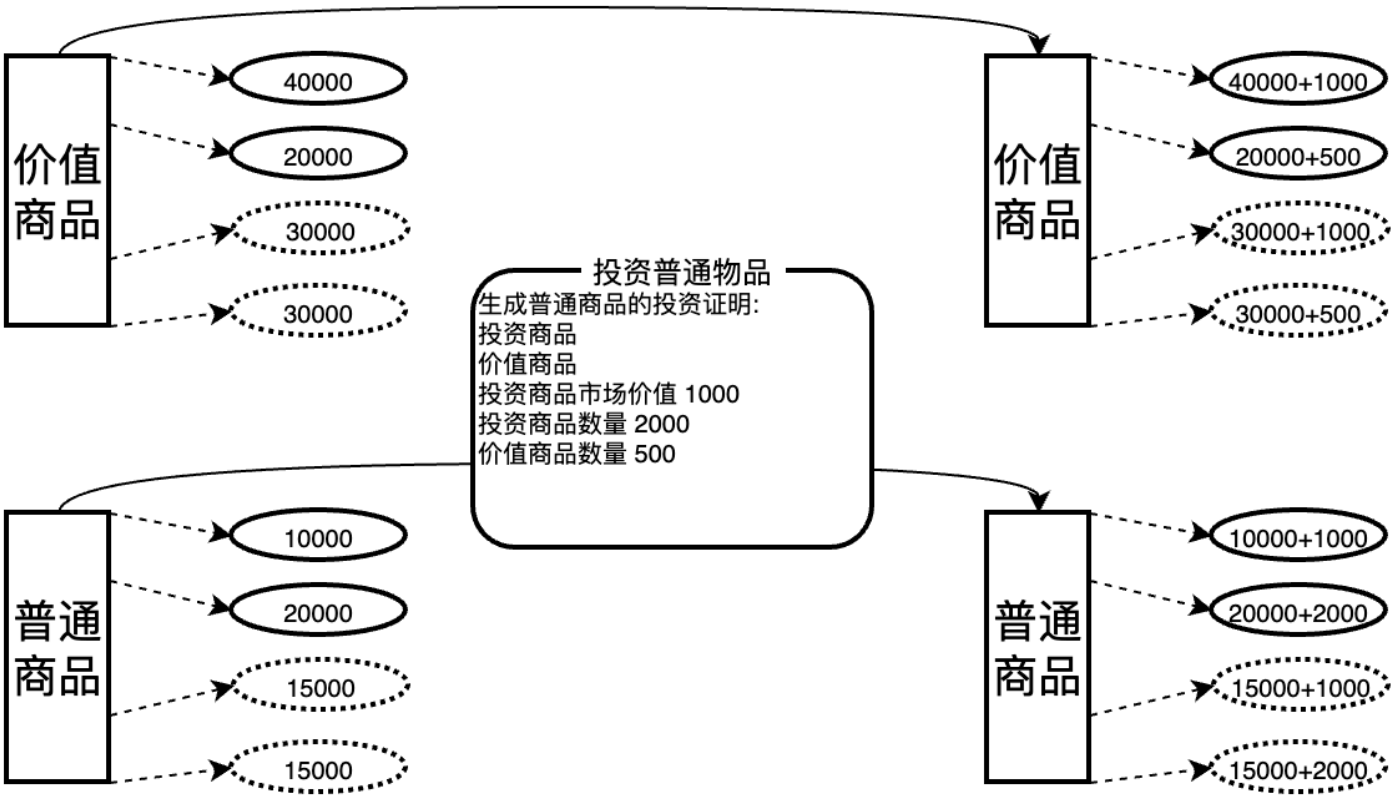
6.2 价值商品投资与撤资流程



- 用户投资价值商品
  用户根据当前价值商品的状态,计算投资数量对应的市场价值.方便撤资时计算收益.
- 用户撤资价值商品
  用户根据投资记录,计算投资产生的收益

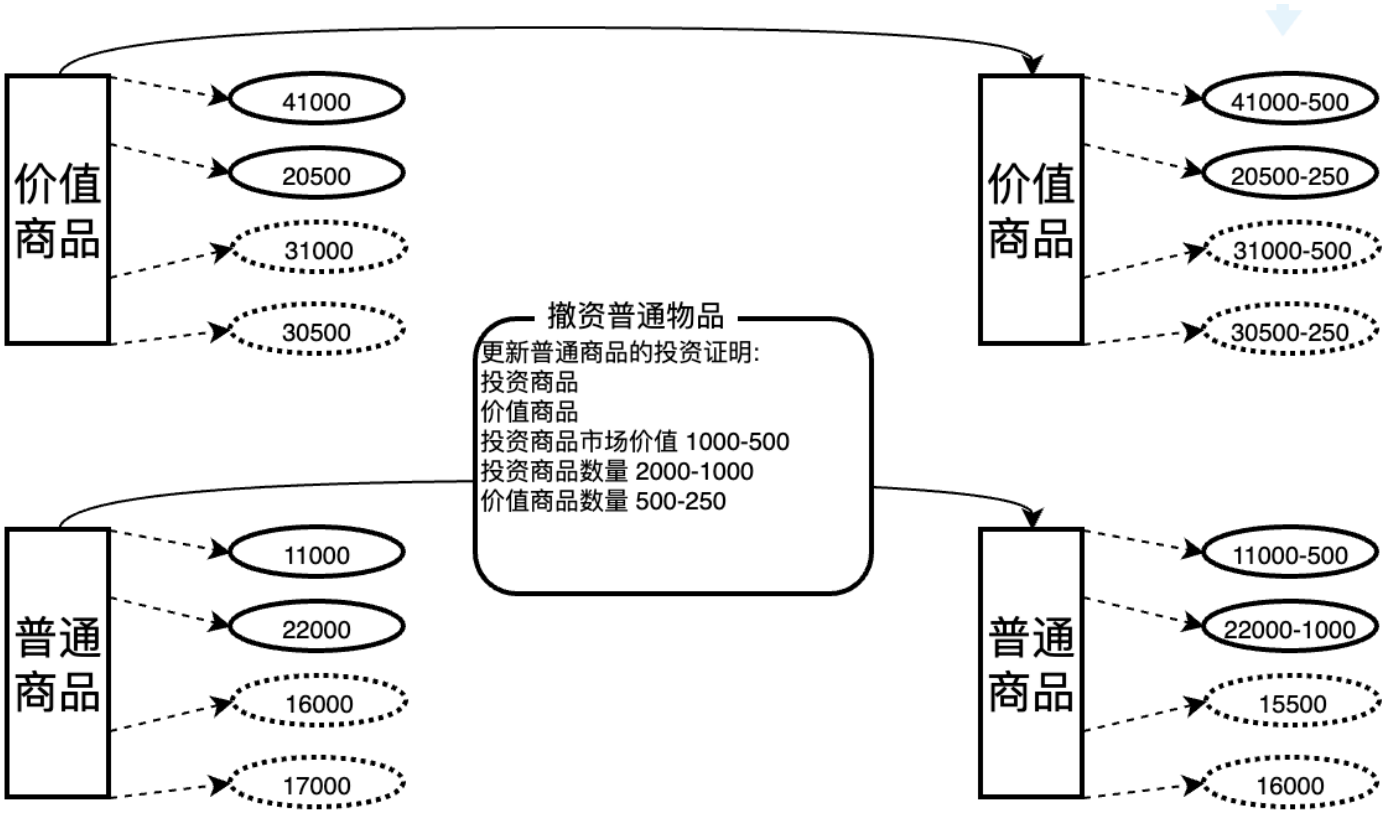
> 撤资商品时,取消数量＜商品当前的总数量/撤资切片数 和 取消数量对应的市场价值＜商品总价值/撤资切片数.

6.3 普通商品投资



- 用户投资普通商品
  由于普通商品的市场价值波动太大,可能会导致协议内套利,造成商品投资者的损失.为避免这种情况的发生,需要投资等市场价值的价值商品.投资的价值商品和普通商品都会产生投资收益,具体参见手续费分配.

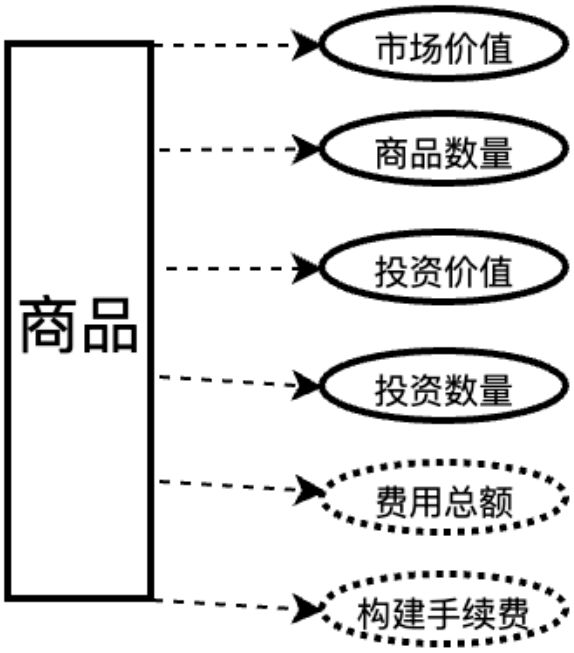
6.4 普通商品撤资



- 用户撤资普通商品
  根据投资记录,计算普通商品和投资商品的收益.具体参见手续费分配.
  撤资商品时,取消数量或者取消数量对应的市场价值需要小于商品当前的总数量或者总价值除以最大撤资比例.

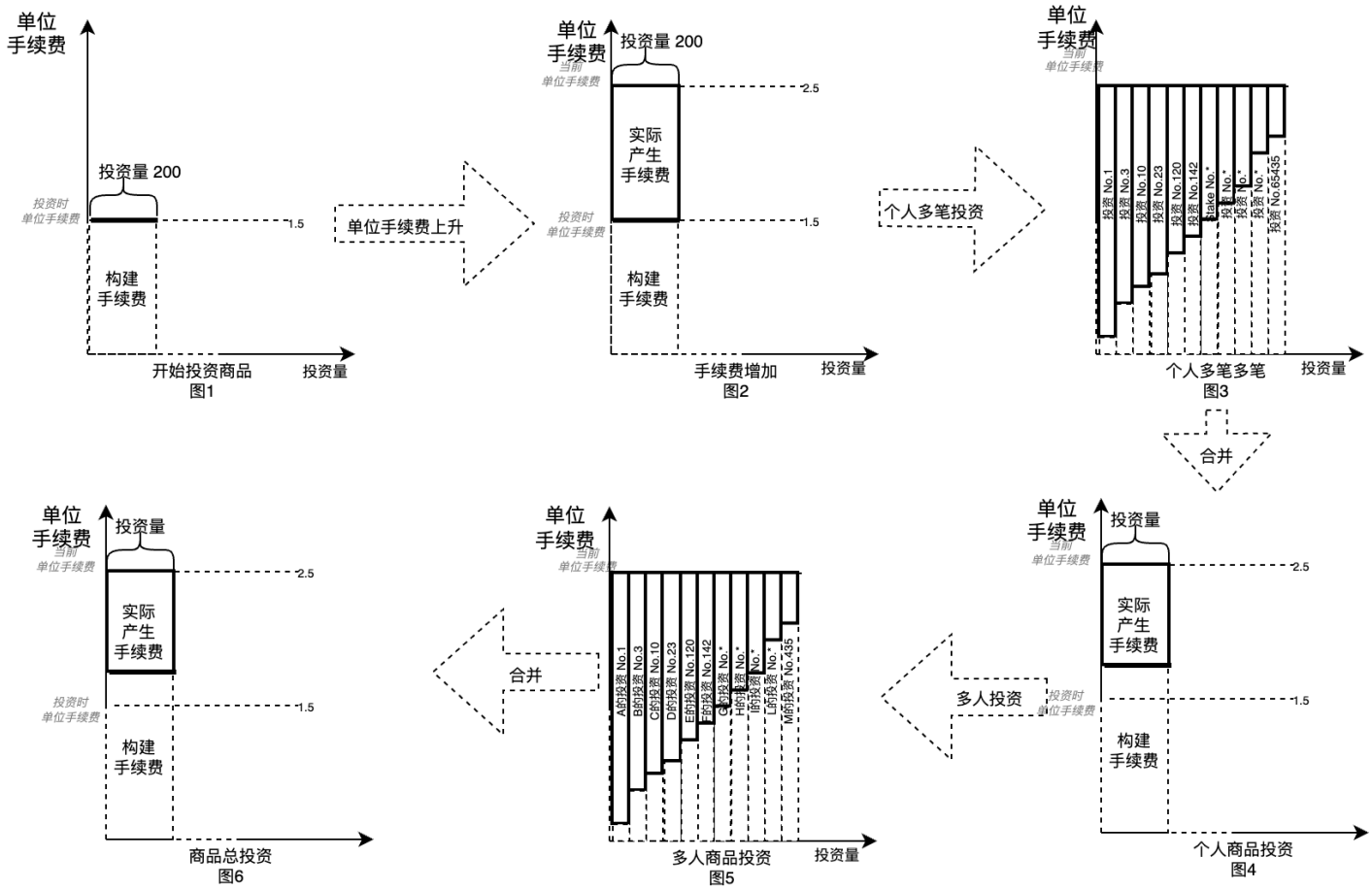
7 商品手续费

7.1 商品手续费记录方式



- 名词解释
  费用总额=实际产生的手续费汇总+构建手续费汇总
  构建手续费=计算用户投资产生的利润而引入虚拟手续费,不实际发生的手续费.具体参见7.4与7.5.

7.2 手续费来源



手续费(实际手续费)的来源是根据商品的费率,当用户进行操作时,计算得到.

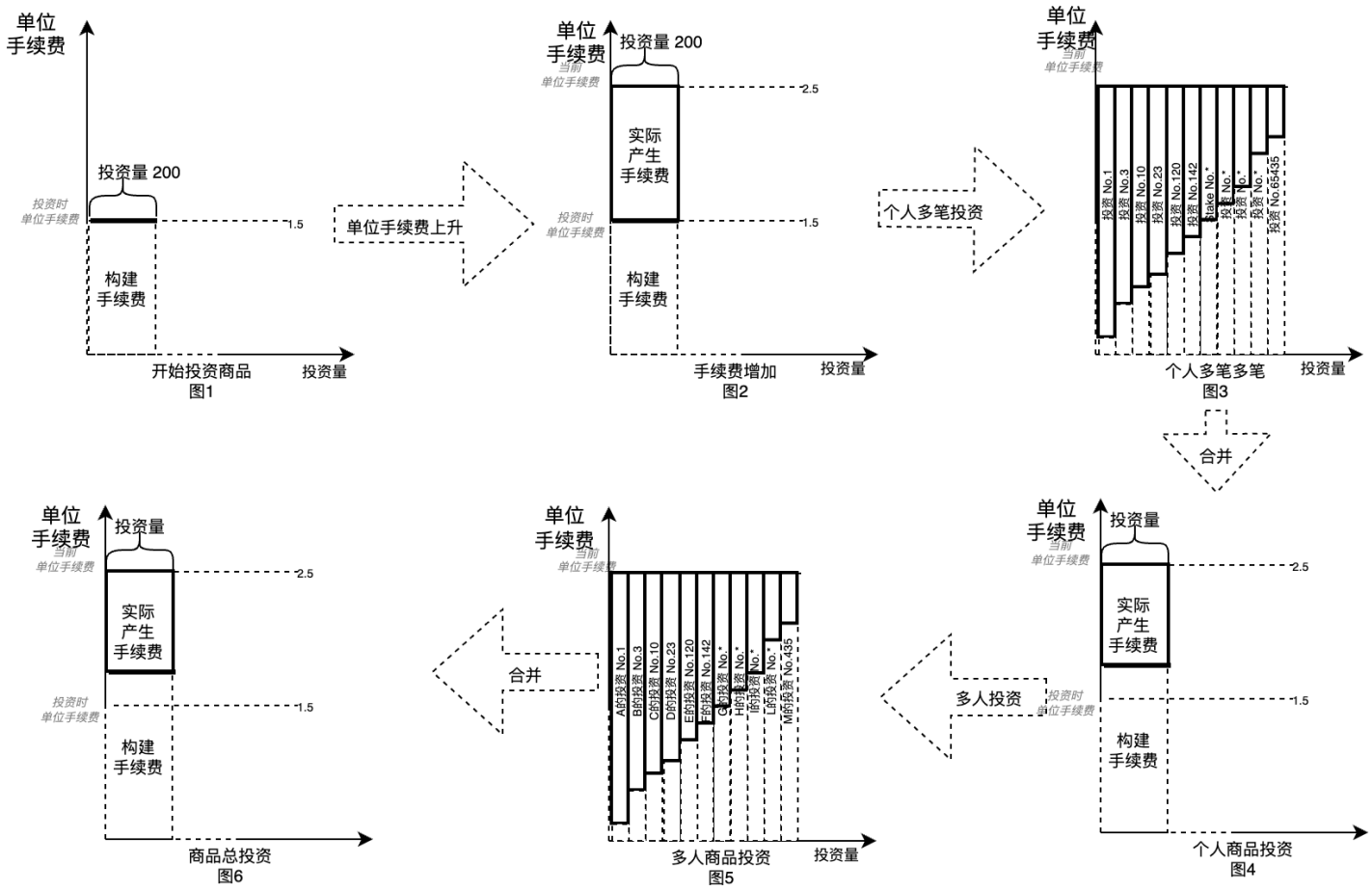
7.3 手续费分配

Alt text

协议中涉及协议技术,门户运营,推荐人,用户以及流动性提供者.协议会合理分配利润.
其中流动性提供者的手续费分配参见 7.4与7.5手续费流程

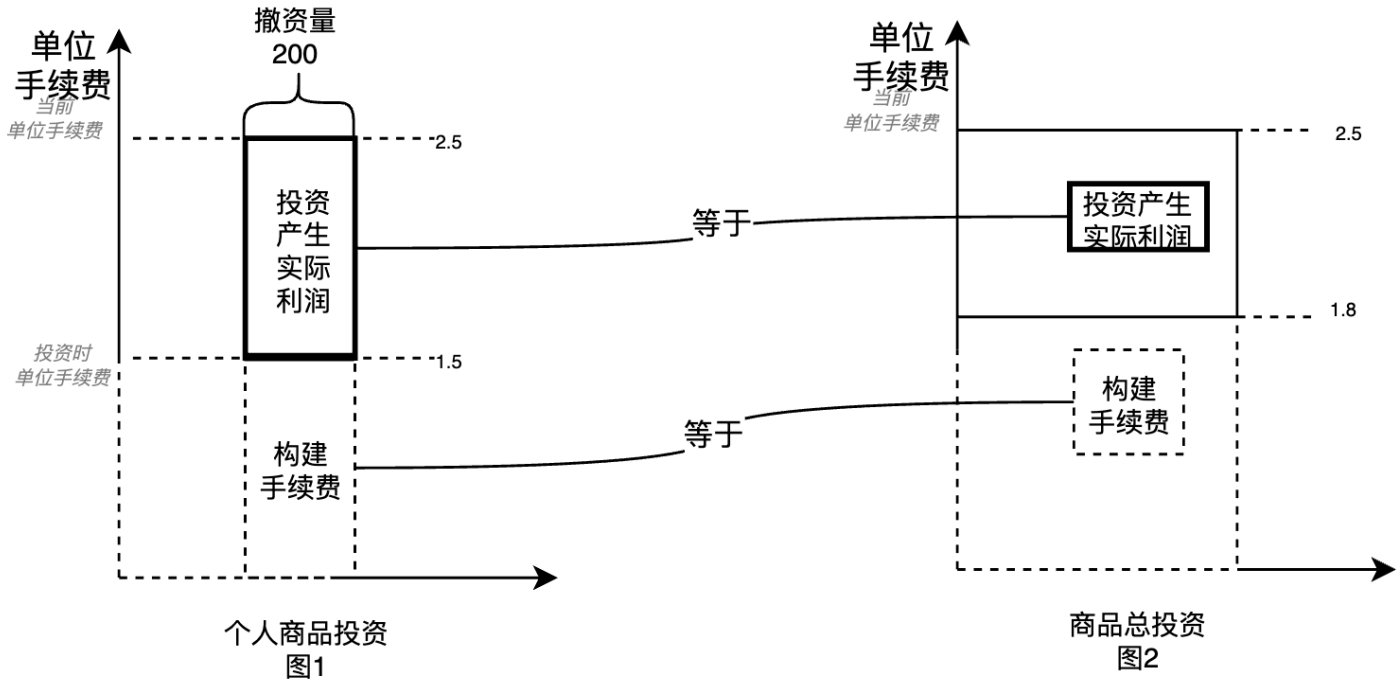
- 如果用户填写了推荐者.
  按用户的相关角色进行实时分配.
- 如果用户未填写推荐者.
  手续费分配中用户所占比例划归于商家角色.
  手续费分配中推荐者所占比例划归于门户角色.

7.4 手续费计算流程(投资)



- 图1 用户投资前商品状态
  单位手续费指单位投资应该得到多少手续费,单位手续费=手续费总额/总投资数量;
  随着交易的进行,手续费不断产生,手续费总额增加,单位手续费就增加.
  构建手续费提用户开始投资时,为记录用户不应该享受的手续费总额.
  构建手续费=投资数量X投资时单位手续费
- 图2 用户投资后手续费积累增加
  当协议中不停有手续费产生时,单位手续费会不停增加.
  用户投资产生的收益=单位手续费x投资数量-构建手续费.
- 图3 个人在商品上的多笔投资
  当用户在同一下商品上,进行多笔投资,可以合成同一条投资记录.
  合并后的构建手续费=合并前的构建手续费汇总
  手户投资产生的收益=单位手续费x投资数量-汇总后的构建手续费
- 图4 个人在商品上多笔投资进行合并
  该图展示合并后的投资情况
- 图5 多人在商品上的投资
  当多个用户进行投资时,就可以汇总成这个商品总投资数量,总投资市场价值,总构建手续费.
  该商品当前总共实际投资利润=当前总费用-汇总构建手续费.
- 图6 多人在商品上的投资进行合并

7.5 手续费计算流程(撤资)



- 图1 个人商品投资(此图表示如果提供流程性时无无常损失)
  此图是个人在此商品的投资情况,当用户进行撤资时,计算逻辑:
  商品当前单位手续费=商品当前手续费总额/商品当前投资数量
  撤资时构建手续费=构建手续费X(撤资数量/用户投资总量)
  当用户撤资时,获得利润= 当前单位手续费X撤资数量-撤资时构建手续费
- 图2 商品总投资
  在商品减去用户撤资时的计算逻辑:
  商品当前手续费总额=原商品当前手续费总额-用户撤资时利润-撤资时构建手续费
  商品构建手续费=商品构建手续费-撤资时构建手续费
  商品投资数量=原商品投资数量-用户撤资数量

8 市场配置

id	配置项	位数	单位	最大值	最小值	起始位	结束位	说明
1	商品投资者分佣	6	百分之一	63	0	256	251	
2	商家分佣	6	百分之一	63	0	250	245	
3	门户分佣	6	百分之一	63	0	244	239	
4	推荐者分佣	6	百分之一	63	0	238	233	

id	配置项	位数	单位	最大值	最小值	起始位	结束位	说明
5	用户分佣	6	百分之一	63	0	232	227	
6	协议费率	6	百分之一	63	0	226	221	
...								

9 主要代码实现(参见代码)

9.1 合约部署GAS

Deployment Cost	Deployment Size
4877267	24752

9.2 合约函数(部份主要函数)GAS

Function Name	min	avg	median	max	备注
buyGood	46836	138059	60565	329943	购买商品
disinvestNormalGood	49425	128844	124744	204344	撤资普通商品
disinvestNormalProof	48432	128221	124121	203721	撤资普通证明
disinvestValueGood	38356	73889	91656	91656	撤资价值商品
disinvestValueProof	36955	92016	97816	126116	撤资价值证明
initNormalGood	332431	359376	356331	405431	初始化普通商品
investNormalGood	54892	122094	113028	192628	投资普通商品
investValueGood	36041	116896	155177	279577	投资价值商品
setMarketConfig	1125	1125	1125	1125	更新市场配置
updateGoodConfig	3098	3098	3098	3098	更新商品配置

当第用户第一次交易一个商品时,GAS费消耗在MEDIAN,用户第二次或者后续交易这个商品时GAS消耗一般在MIN.

10 法律许可

10.1 说明

为了维护项目正常权利,同时也方便其它用户了解协议,对于不同文件不同开源协议.违反协议将得到法律追究.

10.2 协议说明

采用MIT协议的文件供大家自由使用
采用BUSL-1.1协议的文件才协议有效期内只能用户于学习目标,不能运用于商业用途.具体协议内容参见:
项目中LICENSE文件:https://github.com/tt-swap/ttswap-core/blob/529db0eb94ac1c5631beb03c4697222a6ce1cd79/LICENSE.
如因项目在未知的情况违反其它项目开源协议,及时联系我们,我们尽快调整.

10.3 文件开源协议信息

├── GoodManage.sol(BUSL-1.1)
├── MarketManager.sol(BUSL-1.1)
├── ProofManage.sol(BUSL-1.1)
├── RefererManage.sol(BUSL-1.1)
├── Multicall.sol(GPL-2.0-or-later)
├── interfaces
│ ├── I_Good.sol(MIT)
│ ├── I_MarketManage.sol(MIT)
│ └── I_Proof.sol(MIT)
└── libraries
├── L_Good.sol(BUSL-1.1)
├── L_GoodConfig.sol(MIT)
├── L_MarketConfig.sol(MIT)
├── L_Proof.sol(BUSL-1.1)
├── T_BalanceUINT256.sol (MIT)
├── T_Currency.sol (MIT)
├── L_Struct.sol (MIT)
└── L_ArrayStorage.sol(MIT)

11 参与和合作联系方式

X:@ttswap_exchange
TG:@ttswap01
Email:ttswap.exchange@gmail.com

Discord:https://discord.com/invite/GZyEPZmk
github:https://github.com/ttswap/