聚合说明

1. Our Vision

Reduce the user's fee of SpotTrade, increase TPS of SpotTrade under limited resources.

2. Design Introduction

Several considerations:

- as many users as possible
- as many orders as possible
- as many transaction pair as possible
- zkp computing resources are much cheaper than gas resources
- ensure seven significant digits

First, we need to change our inherent way of thinking on SpotTrade. The orders in BatchSpotTrade don' t need to know the specific matching counterparty, but needs to care about the amount of expenditure and income. The expenditureand incomeof all users should reach a break-even state.

Second, for better aggregate more transactions, we preset 6 users, and each user has a different maximum order count, the maximum count is 4, 2, 1, 1, 1, 1, first user have 4 orders, this userwill be an active user.

Third, for reduce the gas consumption of CallData, we abstract the concept of BindToken. BindToken is quote currency which is commonly used. We will register it in smart contract in advance to ensure that their ID is a relatively small value, so we can use less bits when reporting in CallData. At present, we have defined 5bits to represent BindToken.

Fourth, there are at most three tokens in BatchSpotTrade. And only the first user can support three tokens, and the other five users can only support two of the three tokens. We agreed that BindToken would be the third token.

Fifth, we require that the gas fee must be the quote currency. The gas fee is newly added by us compared with loopring.

The following table can better illustrate our design:

		TokenX					TokenY					tokenZ				
	Order	increase	reduce	fee	gas	delta	increase	reduce	fee	gas	delta	increase	reduce	fee	gas	delta
User A	1	IX1	RX1	FeeX1	GasX1	deltaXA	IY1	RY1	FeeY1	GasY1	deltaYA	IZ1	RZ1	FeeZ1	GasZ1	deltaZA
	2	IX2	RX2	FeeX2	GasX2		IY2	RY2	FeeY2	GasY2		IZ2	RZ2	FeeZ2	GasZ2	
	3	IX3	RX3	FeeX3	GasX3		IY3	RY3	FeeY3	GasY3		IZ3	RZ3	FeeZ3	GasZ3	
	4	IX4	RX4	FeeX4	GasX4		IY4	RY4	FeeY4	GasY4		IZ4	RZ4	FeeZ4	GasZ4	
User B	5	IX5	RX5	FeeX5	GasX5	deltaXB	IY5	RY5	FeeY5	GasY5	deltaYB	IZ5	RZ5	FeeZ5	GasZ5	deltaZB
	6	IX6	RX6	FeeX6	GasX6		IY6	RY6	FeeY6	GasY6		IZ6	RZ6	FeeZ6	GasZ6	
User C	7	IX7	RX7	FeeX7	GasX7	deltaXC	IY7	RY7	FeeY7	GasY7	deltaYC	IZ7	RZ7	FeeZ7	GasZ7	deltaZC
User D	8	IX8	RX8	FeeX8	GasX8	deltaXD	IY8	RY8	FeeY8	GasY8	deltaYD	IZ8	RZ8	FeeZ8	GasZ8	deltaZD
User E	9	IX9	RX9	FeeX9	GasX9	deltaXE	IY9	RY9	FeeY9	GasY9	deltaYE	IZ9	RZ9	FeeZ9	GasZ9	deltaZE
User F	10	IX10	RX10	FeeX10	GasX10	deltaXF	IY10	RY10	FeeY10	GasY10	deltaYF	IZ10	RZ10	FeeZ10	GasZ10	deltaZF
		SUM=0					SUM=0					SUM=0				
Token each	token	IX1-RX1+IX2-RX2+IX3-RX3+IX4-RX4+IX5-RX5+IX6-RX6+IX7-RX7+IX8-RX8+IX9-RX9+IX10-RX10 = 0														
User each		DeltaXA, DeltaXB, deltaXC should match: 1. deltaXA = (IX1+IX2+IX3+IX4) - (RX1+RX2+RX3+RX4) - (FeeX1+FeeX2+FeeX3+FeeX4)-(GasX1+GasX2+GasX3+GasX4)														
UserB-F		To make sure user B - F only two of the three token is used: 1.delateXB * deltaYB == 0 or deltaYB * deltaZB == 0 or deltaXB * deltaZB == 0 2.delateXC * deltaYC == 0 or deltaYC * deltaZC == 0 or deltaXC * deltaZC == 0 …														
Order each	sell buy	1. Increase or Reduce is 0: IX1*RX1=0 AND IY1*RY1=0 AND IZ1*RZ1=0 AND (IX1+RX1)*(IY1+RY1)*(IZ1+RZ1)=0 2. sell = IX1 + IY1 + IZ1 3. buy = RX1 + RY1 + RZ1														
	fee	1. FeeX1*FeeY1 == 0 AND FeeY1*FeeZ1 == 0 AND FeeX1*FeeZ1 == 0 2. fee = FeeX1 + FeeY1 + FeeZ1														
	gas	1. GasX1*GasY1 == 0 AND GasY1*GasZ1 == 0 AND GasX1*GasZ1 == 0 2. gas = GasX1 + GasY1 + GasZ1														
	price	P = (amountS / amountB), p = (deltaFilledAmountS / deltaFilledAmountB) , p/P in [0.999, 1.001]														
	fee	fee <= buy * maxFeeRatio														
	gas	gas <= maxGasFeeLeft														

Several important notes：

1. The user's expenditure and income need to reach a break-even state. That is without fees. If the user pays fees, the expenditureand incomemust be unbalanced. The imbalance is caused by trading fee and gas fee.
2. Users B to F have only two tokens, we still calculate the balance change of three tokens, so it is required that the balance change of one of them must be 0
3. For ensure 7 significant digits, we have made special treatment for gas fee. The gas feecharged is specified by the matcher. The circuit only needs to ensure that it is less than or equal to the maxFee which defined in the order.
4. For ensure 7 significant digits, we have made special treatment for trading fee,The trading fee charged is specified by the matcher. The circuit only needs to ensure that it is less than or equal to the calculated value by the feeBips.