1.引言

近年来，去中心化金融 DeFi 的发展可谓迅速，区块链开发者们基于以太坊 ETH 和各大公链创建了包含交易所、抵押借贷、稳定币、保险、预言机、游戏等一系列应用，形成了愈发完整的去中心化金融生态系统。用户参与热情高涨，链上资产自 2019 年以来一直保持着快速增长，不断刷新着历史记录，各类 DeFi 协议中锁定的资产规模已与 2021 年 5 月突破 1000 亿美金，在过去的一年时间内增长了上百倍。随着更多区块链应用的开发和落地、新用户的不断熟悉和参与，势必将进一步推动 DeFi 的发展和链上资产的持续活跃与增长。

面对更大的用户规模，包括以太坊 ETH 在内的所有公链都会面临同样的问题：

- 第一、高昂的链上交互 Gas 费用，高峰时期 Uniswap 上一笔兑换交易甚至需要上百美金的 Gas 费，这对于普通用户是难以接受的；
- 第二，受制于 TPS 的限制，在使用人数激增时各公链均会出现拥堵现象，导致链上交易、确认时间长，实时性差。

据此，2021 年 2 月上线的 ZKSwap V1 主网版本通过 ZK-Rollups 技术把所有的 ERC20 token 转移到 Layer2 上，基于不断生成的零知识证明来保证 Layer1 和 Layer2 状态的一致性，从而让所有的兑换在 Layer2 上发生，可以做到零 Gas 费用的实时兑换（不再要等待一个区块确认时间），并且具备无限的拓展性，摆脱以太坊 TPS 和区块确认时间的限制，让 DEX 具备 CEX (中心化交易所) 般丝滑的体验，并同时实时掌控自己的资金安全。

在 ZKSwap V1 版本的基础上，ZKSwap 团队发布了 V2 版本并新增了如下功能：

1）"无限 " 上币 - 用户在支付一定费用的情况下，可以自主添加任意 Token，并可创建交易对；

2）优化电路分支的实现，提升电路效率 - 支持一个账户，两个余额的修改；

3）优化提现体验 - V1 版本中，提现的操作和区块验证操作捆绑在一起。由于每笔 Gas 费用的限制，导致区块中的提现的个数受限，特别是在聚合验证的情况下，受限更多。V2 版本将会优化用户的提现体验。

更进一步，ZKSwap 团队还将推进“Layer2 for all”的多链生态战略，在 BSC、HECO、OKChain 上进行部署，为各公链上的生态繁荣添砖加瓦。

2.架构优化

2.1. Token 管理

ZKSwap V2 版本将支持三种类型的 Token：Fee Token、User Token 和 LP Token。总共支持 2^16 个 Token。

Name	Type	编号	Comments
Fee Token	-	0~31	0 - ETH （保留），总共32个
User Token	-	32~16383	16352个
LP Token	-	16384~65535	49152个

2.1.1 Fee Token

Fee Token 只能由 Governor 添加，主要为 ETH、ZKS、USDT、WBTC 。

2.1.2 User Token

User Token 用户可以付费添加。

2.1.3 LP Token

ZKSwap 用户创建交易对时，必须支付费用。LP Token 将在用户创建交易对时自动添加。用户创建的交易对中必须有一种 Token 是 Fee Token。User Token 能创建的交易对个数受限（由 Governor 设置）。

2.1.4 Governor Config

Governor 可以设置添加 User Token 和修改创建交易对支付的费用。

2.2. 账户管理

ZKSwap V2 版本将支持 2^28 个账户。其中账户 0 为 Validator 账户。

2.3. Fee 模型

ZKSwap V2 版本上的 Layer2 交易，用户可以指定 Fee Token 中的一种作为手续费。提现代币、转账超免费次数后、添加移除流动性超免费次数后均可使用用户指定的 Fee Token 来抵扣手续费。

OP name	OP number	Fee	FeeTo	Comments
Noop	0	0		
Deposit（充值）	1	0		Layer 1
TransferToNew（转账到新用户）	2	Fee Token	Validator	charge token for fee
Withdraw（取现）	3	Fee Token	Validator	charge token for fee
Close（关闭账户）	4	-		
Transfer（转账）	5	Fee Token	Validator	charge token for fee
FullExit（退出）	6	0		Layer1 - Withdraw
ChangePubKey（修改L2公钥信息）	7	0		
CreatePair（创建池子）	8	0		Layer 1
AddLiquidity（增加流动性）	9	Fee Token	Validator	charge token for fee
RemoveLiquidity（删除流动性）	10	Fee Token	Validator	charge token for fee
Swap（兑换）	11	Fee Token + 0.25%	LP/Validator	0.25% LP + Validator (fee token only)

在 ZKSwap V1 版本的基础上，优化了 Swap 交易的计算模型：

资金池创建并注入流动性后，持有相应代币的用户就可以开始在资金池中进行 Swap，这里以用 A 兑换 B 为例。假设兑换前资金池中有 x_i 个 A 和 y_i 个 B 代币，用户向资金池中转入 m 个 A，兑换后资金池中有 x_{i+1} 个 A 和 y_{i+1} 个 B 代币。

若 A 属于 fee token，则系统将先扣除 0.0005m 个 A 的协议手续费，资金池中 A 的数量 $x_{i+1} = x_i + 0.9995m$ ，用户可以对应获得 $y_i - y_{i+1}$ 个 B 代币。根据 uniswap 的 AMM 算法，在扣除 0.0025m 的流动性费用后，应保持 $(x_{i+1} - 0.0025m) * y_{i+1} = x_i * y_i$。因此，用户将获得 $y_i - y_{i+1} = y_i - \frac{x_i * y_i}{x_i + 0.997m}$ 个 B 代币。

若 A 不属于 fee token，则资金池中 A 的数量$x_{i+1} = x_i + m$，用户可以对应获得$y_i - y_{i+1}$个 B 代币，根据 AMM 算法，扣除 0.0005m 个 A 的流动性费用后，保持

（$x_{i+1} - 0.0025m$）$* y_{i+1} = x_i * y_i$ 。输出 $y_i - y_{i+1} = y_i - \frac{x_i * y_i}{x_i + 0.9975m}$ 个 B 代币，在此基础上，由协议扣除 0.05%手续费后，用户将获得的代币数量为 $0.9995 *$（$y_i - y_{i+1}$）。

流动性费用会在交易后自动加入资金池的 reserve，因此交易后整个资金池的 reserve 变为 $x_{i+1} * y_{i+1} = c_{i+1} > c_i$ ，由于没有新的 LP Token 生成或销毁，LP Token 的总量保持不变，即 $n_{i+1} = n_i$。这意味着所有 LP 的份额不变，但每单位份额对应的资金池 reserve 总量增加了。

2.4. Pub Data of Transactions

ZKSwap V2 版本上的所有交易（包括 Layer1 / Layer2 交易）都需要打包提交 Pub Data 到 Layer1。为了保持最优的电路性能，Chunk 大小为 11 字节，兑换和转账只需要 2 个 Chunk。

2.4.1 Noop

ZKSwap V2 版本允许存在空交易，来填充 Layer2 区块。

a. pub data

Data	Type	Size	Comments
OP		1	0

pub data 的总长度 = 1 字节。

2.4.2 Deposit

用户从 ZKSwap Layer1 发起充值操作时，系统会将用户 Layer1 的资产映射到 Layer2。

a. 接口函数

function deposit ERC20 (IERC20_token, uint104_amount,

address_franklinAddr)

function deposit ETH (address_franklinAddr)

b. pub data

Data	Type	Size	Comments
OP		1	1
accountId	ACCOUNT ID	4	Layer2 account ID (**NOT** verified on L1)
tokenId	TOKEN ID	2	Layer2 token ID
amount	AMOUNT	16	
address	ADDRESS	20	

pub data 的总长度 = 1+4+2+16+20 = 43 字节。总共 4 个 Chunk。

2.4.3 Transfer

用户通过 ZKSwap Layer2 发起的转账交易，可实现任意 Token 的转账。

a. pub data

Data	Type	Size	Comments
OP		1	5
accountFromId	ACCOUNT ID	4	from
tokenId	TOKEN ID	2	token id
accountToId	ACCOUNT ID	4	to
amount	AMOUNT_EXPONENT_BIT_WIDTH + AMOUNT_MANTISSA_BIT_WIDTH	5	amount
fee tokenId	FEE TOKEN ID	1	token id
fee	FEE_EXPONENT_BIT_WIDTH + FEE_MANTISSA_BIT_WIDTH	2	fee

pub data 的总长度 = 1+4+2+4+5+1+2 = 19 字节。2 个 Chunk。

2.4.4 TransferToNew

用户通过 ZKSwap Layer2 发起转账交易，可实现任意 Token 的转账。转账对方不需要提前创建账户。

a. pub data

Data	Type	Size	Comments
OP		1	2
accountFromId	ACCOUNT ID	4	from
tokenId	TOKEN ID	2	token id
accountTo	ADDRESS	20	to
accountToId	ACCOUNT ID	4	to
amount	AMOUNT_EXPONENT_BIT_WIDTH + AMOUNT_MANTISSA_BIT_WIDTH	5	amount
fee tokenId	FEE TOKEN ID	1	token id
fee	FEE_EXPONENT_BIT_WIDTH + FEE_MANTISSA_BIT_WIDTH	2	fee

pub data 的总长度 = 1+4+2+20+4+5+1+2 = 39 字节。4 个 Chunk。

2.4.5 Withdraw

用户通过 ZKSwap Layer2 发起提现操作，可实现任意 Token 在 Layer1 的提现。

a. pub data

Data	Type	Size	Comments
OP		1	3
accountId	ACCOUNT ID	4	from
ethAdd	ADDRESS	20	Layer1 address
tokenId	TOKEN ID	2	to
amount		16	amount
fee tokenId	FEE TOKEN ID	1	token id
fee	FEE_EXPONENT_BIT_WIDTH + FEE_MANTISSA_BIT_WIDTH	2	fee

pub data 的总长度 = 1+4+20+2+16+1+2 = 46 字节。5 个 Chunk。

2.4.6 FullExit

用户可直接从 ZKSwap Layer1 发起 FullExit 请求，提取资产，此操作需要 Layer2 提供证明。

a. pub data

Data	Type	Size	Comments
OP		1	6
accountId	ACCOUNT ID	4	from
tokenId	TOKEN ID	2	token id
ethAdd	ADDRESS	20	to
amount	AMOUNT	16	amount

pub data 的总长度 = 1+4+2+20+16 = 43 字节。4 个 Chunk。

2.4.7 ChangePubKey

用户通过在 ZKSwap Layer2 发起提取交易，可实现任意 Token 在 Layer1 的提现。

a. pub data

Data	Type	Size	Comments
OP		1	7
accountId	ACCOUNT ID	4	
pubKeyHash	NEW_PUBKEY_HASH_WIDTH	20	Layer2 address
address	ADDRESS	20	Layer1 address
nonce	NONCE	4	nonce

pub data 的总长度 = 1+4+20+20+4 = 49 字节。5 个 Chunk。

2.4.8 CreatePair

用户通过 ZKSwap Layer1 发起交易池的创建。创建交易池需要在 Layer1 创建对应的智能合约（LP 代币）。

a. 接口函数

function createPair (address_tokenA, address_tokenB)

b. pub data

Data	Type	Size	Comments
OP		1	8
accountId	ACCOUNT ID	4	Layer2 account ID (**NOT** verified on L1)
tokenIdA	TOKEN ID	2	Layer2 token ID
tokenIdB	TOKEN ID	2	Layer2 token ID
tokenPair	TOKEN ID	2	Pair token ID
addressPair	ADDRESS	20	

pub data 的总长度 = 1+ 4+2+2+2+20 = 31 字节。总共 3 个 Chunk。

2.4.9 AddLiquidity

用户通过 ZKSwap Layer2 添加流动性。

a. pub data

Data	Type	Size	Comments
OP		1	9
accountId	ACCOUNT ID	4	Layer2 account ID (**NOT** verified on L1)
accountPairId	ACCOUNT ID	4	Layer2 account ID (**NOT** verified on L1)
amountADesire	AMOUNT_EXPONENT_BIT_WIDTH + AMOUNT_MANTISSA_BIT_WIDTH	5	Layer2 tokenA desired amount
amountAMin	AMOUNT_EXPONENT_BIT_WIDTH + AMOUNT_MANTISSA_BIT_WIDTH	5	Layer2 tokenA min amount
amountBDesire	AMOUNT_EXPONENT_BIT_WIDTH + AMOUNT_MANTISSA_BIT_WIDTH	5	Layer2 tokenB desired amount
amountBMin	AMOUNT_EXPONENT_BIT_WIDTH + AMOUNT_MANTISSA_BIT_WIDTH	5	Layer2 tokenB min amount
fee tokenId	FEE TOKEN ID	1	token id
fee	FEE_EXPONENT_BIT_WIDTH + FEE_MANTISSA_BIT_WIDTH	2	Layer2 token fee

pub data 的总长度 = 1+4+4+5+5+5+5+1+2 = 32 字节。总共 3 个 Chunk。

2.4.10 RemoveLiquidity

用户通过 ZKSwap Layer2 移除流动性。

a. pub data

Data	Type	Size	Comments
OP		1	10
accountId	ACCOUNT ID	4	Layer2 account ID (**NOT** verified on L1)
accountPairId	ACCOUNT ID	4	Layer2 account ID (**NOT** verified on L1)
amountToken	AMOUNT_EXPONENT_BIT_WIDTH + AMOUNT_MANTISSA_BIT_WIDTH	5	
amountAMin	AMOUNT_EXPONENT_BIT_WIDTH + AMOUNT_MANTISSA_BIT_WIDTH	5	
amountBMin	AMOUNT_EXPONENT_BIT_WIDTH + AMOUNT_MANTISSA_BIT_WIDTH	5	
fee tokenId	FEE TOKEN ID	1	token id
fee	FEE_EXPONENT_BIT_WIDTH + FEE_MANTISSA_BIT_WIDTH	2	

pub data 的总长度 = 1+4+4+5+5+5+1+2 = 27 字节。总共 3 个 Chunk。

2.4.11 Swap

用户通过 ZKSwap Layer2 实现两种 Token 之间的兑换。

a. pub data

Data	Type	Size	Comments
OP		1	11
accountId	ACCOUNT ID	4	Layer2 account ID (**NOT** verified on L1)
accountPairId	ACCOUNT ID	4	Layer2 account ID (**NOT** verified on L1)
amountIn	AMOUNT_EXPONENT_BIT_WIDTH + AMOUNT_MANTISSA_BIT_WIDTH	5	amount in
amountOutMin	AMOUNT_EXPONENT_BIT_WIDTH + AMOUNT_MANTISSA_BIT_WIDTH	5	min amount out
direction & fee tokenId	FEE TOKEN ID	1	token id, the highest bit indicates the direction (0 - token0->token1, 1 - token1->token0)
fee	FEE_EXPONENT_BIT_WIDTH + FEE_MANTISSA_BIT_WIDTH	2	

pub data 的总长度 = 1+4+4+5+5+1+2 = 22 字节。总共 2 个 Chunk。

2.5. Circuit Optimization

ZKSwap V2 版本为了降低 AMM 相关操作的 Chunk 个数，需要降低“Branch”的个数。原有设计在状态树上的一个 Account 和一个 Token 的 Balance 组成一个“Branch”。在 AMM 相关的操作中，如果采用 Fee Token 的方式，原有的设计效率比较低，需要支持 1 个 Account 和 2 个 Token 的 Balance 的“Branch”。

1) Account Audit Path (aap)

2) 该 Account 下的 2 个 Balance (balance0 / balance1) 在修改前的 Audit Pat（bap0/bap1) 3) 该 Account 下的 2 个 Balance (balance0'/balance1') 在修改后的 Audit Pat （bap0'/bap1')

在修改前电路需要证明：

- balance0 + bap0 ==> b_root0
- balance1 + bap1 ==> b_root0
- account (b_root0) + aap ==> root

在 balance 修改后电路需要证明：

- balance0' + bap0 ==> b_root0'
- balance1 + bap1' ==> b_root0'
- balance1' + bap1' ==> b_root0''
- account(b_root0'') + aap ==> root'

3.提现优化

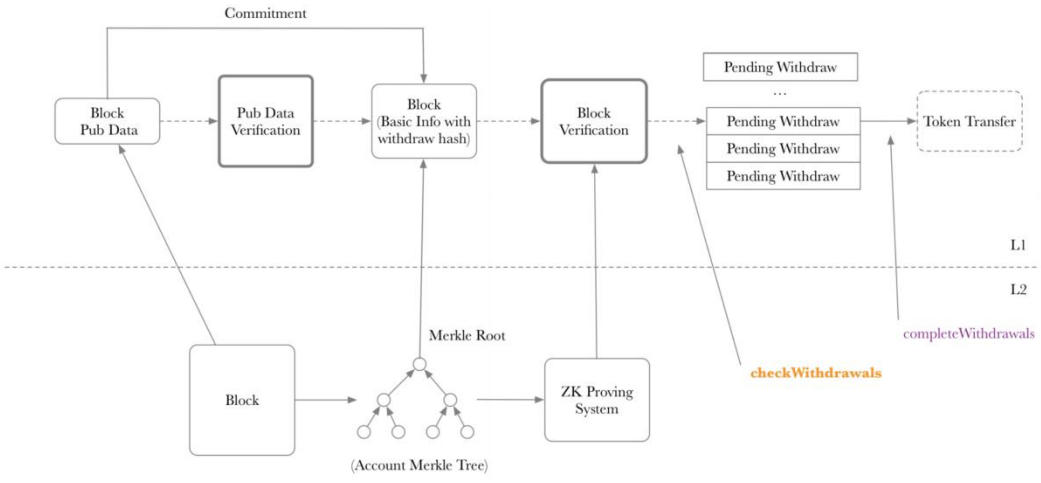
3.1 ZKSwap V1 版本

Withdraw 是指用户从 Layer2 中将 Token 提出，并从 ZKSwap 合约中解锁，发到对应 Layer1 账户的过程。

在 ZKSwap V1 版本中，Withdraw 操作由用户从 Layer2 发起，ZKSwap server 在收到用户对某一 Token 的提币请求后，会更新对应账户下对应 Token 的状态，并把更新后的状态树根节点哈希和 Withdraw 操作应用的证明发送到链上 ZKSwap 合约。ZKSwap V1 版本的 Withdraw 操作和区块 verification 操作捆绑在一起。 由于每笔 Gas 费用的限制，导致区块中的 Withdraw 的个数受限。特别是在聚合 verification 的情况下，情况变得更糟糕。V1 版本中，每个区块中限制 Withdraw 的个数为 4。

3.2 ZKSwap V2 版本

在 ZKSwap V2 版本中，我们将 Withdraw 的操作和区块 Verify 隔离开。区块中的 Withdraw 个数不受限制，可大幅提高提现效率。



在某个区块验证后，通过 check Withdrawals 函数创建 pending Withdraw。再通过 complete Withdrawls 完成提现。complete Withdrawls 函数需要增强可以优先处理某个 pending Withdraw。Block Verification 是针对多区块聚合实现的。check Withdrawals 针对每个验证后的区块进行处理。创建一个 Pending Withdraw 的 Gas 费用在 7w 左右。按照一个交易最大的 Gas 费用 1250w 来说的话，一个区块支持的最大的 Withdraw 个数是 178 笔。

4.总结与展望

ZKSwap 基于 ZK-Rollup 技术，是一套去中心化的 Layer2 代币 AMM 自动化做市商 Swap 协议。ZKSwap V1 版本已经实现了 Uniswap 的完整功能，并且支持超高 TPS 和无限拓展性，用户无需支付 Gas 费用即可便捷实时地完成转账、交易、添加流动性、移除流动性等操作，极大降低了使用门槛与成本。

ZKSwap V2 版本在此基础上，针对 Token 管理、账户管理、Fee 模型、提现流程等进行了诸多优化，对平台支持上线的 Token 数量进行大幅扩容，支持用户自主无限上币（所有符合 ERC20 标准的代币）。并且在免去 Gas 费用的同时，创新性的支持用户自选交易手续费 Token，进一步提升了用户使用体验。

ZKSwap V2 版本仍然由 L2 Lab 支持开发。L2 Lab 团队将推进“Layer2 for all”的多链生态战略，致力于通过密码学、算法来实现去信任的公链扩容，降低用户和生态开发团队的费用成本。

同时，ZKSwap 还将推出以太坊二层网络 NFT 协议，支持用户在 ZKSwap Layer2 上创建和发行 NFT，并实现 Layer1 和 Layer2 互通。ZKSwap 平台上的 NFT 将和 AMM 功能并存，并且支持其他的基于以太坊的 NFT 平台接入该 Layer2 协议。未来，L2 Lab 将在更多领域推进 Layer2 扩展方案，成为安全、通用、开放的 Layer2 金融基础设施。