

分红型 Token 及其去中心化交易所的设计与实现

一，一句话说明核心功能：

实现分红型 Token，并实现该 Token 的去中心化交易所，解决了分红型凭据在以太坊的发行和流通的技术问题。

二，背景和要求：

- 1, 有人尝试定义分红型 Token（参见：<https://github.com/ethereum/EIPs/issues/1726>），我也尽量使用他的术语，以此向这同行致敬。
- 2, 质押分红很流行，典型应用包括寿司（Sushi），但质押分红无法解决持有即分红的需求。Eip-4626(<https://eips.ethereum.org/EIPS/eip-4626>)也能实现质押分红。
- 3, 既然**分红型 Token**有巨大的市场（股票，定期存款，国库券等凭据都可以看作分红型凭据），要方便流通必然需要**有去中心化交易所的支持**。像乌克兰这样的国家，其企业在当前战争期间可能难于融资，使用这种方式融资可能有用。一些交易所和银行也在尝试 STO（和分红型 Token 有交集，绝大部分属于分红型 Token），这是一个潜在的巨大市场。

三, 设计思路:

1, 分红型 Token 的设计, 有人尝试。对照

<https://github.com/ethereum/EIPs/issues/1726> 来说明:

- a) 继承于 ERC20Token, 有资产 Token (类似于 EIP-4626) 用于分红。
- b) 对于每次分红, 无法处理的余额, 可以留作下一次分红, 也可以忽略, 这两种模式都可以。如果选择每次都分红完所有金额 (忽略分不完的金额), 则需要设置 magnitude 值。
- c) Magnitude 值的定义, 我提供了一个算法, 来估计 magnitude 的合适值, 不需要写死指定某个值。可以参见合约中 “function getDivRecommendedDecimals(address AssetToken_) external view returns (uint8)”。
- d) 提出了分红高度的概念。每次分红后, 高度都会递增。可以用分红次数表示高度, 也可以用累加分红金额表示高度。Demo 中使用每股分红金额累加表示高度。
- e) 增加了授权领取分红金额功能, 分红的资产仍然进入持有人账号。

详细的请参阅: IDividendToken, IDividendTokenEx 和 DividendToken0, DividendToken1, ShareToken 等合约。

2, 分红型 Token 的去中心化交易所的设计, 流动性算法参照 UniswapV1 和 UniswapV2, 但要流动性提供者要能得到应有的分红。对照 Uniswap 各个版本, 其相同和不同部分来说明:

- a) 分红 Token 只有一个交易对(Pair), 分红 Token 对应 其资产 Token。

- b) 采用 Uniswap 的恒定乘积流动性算法, 没采用 UniswapV2 使用 Token 表示流动性的方法, 也没采用 UniswapV3 使用多个价格区间并发行 NFT 表示流动性的方法 (主要是因为复杂和版权保护), 更类似于 UniswapV1 的做法和 V2 的做法的结合体。可以改成 UniswapV3 的做法, 这会极大的提高资金效率。
- c) 交易对 (Pair) 里面实现分红功能, 所有的流动性提供者按照流动性值的比例分取红利, 且分红操作不影响交易(交易不中断)。
- d) Uniswap 中的其他功能, 例如 Oracle, FlashLoan, Permit, WETH (会极大的简化合约), Fee, 等辅助功能都没提供。核心点在于展示逻辑; 如果以后有必要可以改善合约和增加功能。

3, 和传统证券联系, 可能会有这些场景:

- a) 某资产管理公司存管了 1000 股特斯拉股票, 以此发行 1000 个分红型 Token。如果有人持有这种分红型 Token, 可以向资管公司要求赎回真实的股票。类似于 USDT 的运营。中心化交易所喜欢这样做。
 - b) 乌克兰某高科技公司, 希望融资生产轮船, 承诺分发红利, 向乌克兰金融管理局申请发行股票, 金融管理局审核并通过了该申请, 允许在以太坊上发行对应的分红 Token。此公司把融资需求、分发红利、财务报表、公司事件等都在以太坊上操作。
 - c) 某银行的大额存单, 可以通过分红 Token 证券化, 并在链上发利息。
- 不仅仅这些场景, 分红型 Token 可以和很多已有的其他金融产品对接。此种情况下, 可以把这类分红 Token 看作 STO, 在大部分国家和地区需要当地法律和金融监管部门的支持与审计。

四，程序：

两部分，包括合约和一个客户端。核心逻辑在合约，是开源的，采用和UniswapV3一样的版权保护“BUSL-1.1 (<https://spdx.github.io/license-list-data/BUSL-1.1.html>)”。但分红Token接口定义是“MIT”版权保护，以后可以提交EIP申请。

客户端是一个APP，不是网页，实现了所有重要功能，还有改善的很大余地。

以特斯拉股份上链为例子，分两部分展示客户端的部分截图：

第一部分，分红Token的详细情况：

1,创建特斯拉股份Token（分红型Token）：

详情

?创建分红Token

name: Tesla

symbol: TSLA

decimals: 3

Asset Token Address: 0x047e8e17e584708f5181d85f8ca2E10cf9a98c21

Tether USD

USDT

?检测

Admin Address: 0xccD87fd57D9640414a84761FDf241C2d84FDBBd3

SuperAdmin Address: 0xEE81a12e57DF714CEB6Ac8279e8681414Cd0F0de

Notice:

以下内容纯属虚构，仅仅用于测试。
钱岸下属子公司美国大财主资产管理有限公司（以下简称大财主）托管特斯拉股票，在链上发行的股票全部和托管的股票一一对应。
链上持有股份Token的人可以向大财主申请赎回股票，持有股票的人可以把股票交由大财主托管并发行对应股份Token，大财主收费标准：股票上链，1ETH一次；赎回股票，1ETH一次。

创建合约

2, 特斯拉股份 Token 被指派给指定人员(挖矿)

⬆️ ?管理员操作

?1, 挖矿(增加股份) | ?2, 执行分红 | ?3, 发布公告 | ?4, 设置Token图标

?新增数量:

?接受地址:

?挖矿公告:

此次挖矿是因为0xccD87fd57D9640414a84761FDf241C2d84FDBBd3托管了1000分特斯拉股票到大财主, 由大财主管理员执行操作。
链下交易凭据单号: 0101010101010101。

3, 特斯拉股份 Token 执行分红

⬆️ ?管理员操作

?1, 挖矿(增加股份) | ?2, 执行分红 | ?3, 发布公告 | ?4, 设置Token图标

?分红金额:

4, 领取特斯拉股份 Token 的分红

⬆️ ?领取分红

Account:

Asset Amount:

5, 特斯拉股份 Token 的分红历史列表

⌵ 分红历史

提示：最多显示300条记录。

刷新

Index	?BlockNumber	?打入分红金额	?执行分红金额	?当前股份	?每股分红	From
2	11	60.000000000000000000	60.000000000000000000	6000.000000000000000000	0.01	0xccD87fd57D9640414a84761FDf241C
1	10	6000.000000000000000000	6000.000000000000000000	6000.000000000000000000	1	0xccD87fd57D9640414a84761FDf241C

6, 特斯拉股份 Token 发布公告（链上公告）

创建 Token 时候有说明信息录入，挖矿的时候也有说明信息录入，这些说明信息都是公告。还可以单独发出公告：

⌵ 管理员操作

?1, 挖矿(增加股份)

?2, 执行分红

?3, 发布公告

?4, 设置Token图标

?公告:

大财主公司今年赚了100越南币，200津巴布韦币，300柬埔寨币。为了庆祝如此丰厚的利润，在2022年8月8日向所有持有特斯拉股份Token的地址随机分发盲盒NFT，盲盒的最大奖励是四千万美金以上。

执行发布

7, 特斯拉股份 Token 的公告列表

⌵ 公告历史

提示：最多显示300条记录。

刷新

Index	?BlockNumber	?Notice
4	8	0x00 => mint => 3000000 => 此次挖矿是因为0xDc0227Df3B93Bf8Bf44bA7dA844E8ad1F41Dd49托管了3000分特斯拉股票到大财主，由大财主管理员执行操作。 链下交易凭据单号：010101010101010103。
3	7	0x00 => mint => 2000000 => 此次挖矿是因为0xEE81a12e57Df714CEB6Ac8279e8681414Cd0F0de托管了2000分特斯拉股票到大财主，由大财主管理员执行操作。 链下交易凭据单号：010101010101010102。
2	6	0x00 => mint => 1000000 => 此次挖矿是因为0xccD87fd57D9640414a84761FDf241C2d84FD8Bd3托管了1000分特斯拉股票到大财主，由大财主管理员执行操作。 链下交易凭据单号：010101010101010101。
1	4	以下内容纯属虚构，仅仅用于测试。 钱岸下属子公司美国大财主资产管理有限公司（以下简称大财主）托管特斯拉股票，在链上发行的股票全部和托管的股票——对应。 链上持有股份Token的人可以向大财主申请赎回股票，持有股票的人可以把股票交由大财主托管并发行对应股份Token。 大财主收费标准：股票上链，1ETH一次；赎回股票，1ETH一次。

8,设置特斯拉股份 Token 的图标（链上图标，锦上添花的功能）

管理操作

1. 挖矿(增加股份)

2. 执行分红

3. 发布公告

4. 设置Token图标

图标文件:

C:\Users\abc\Desktop\Tesla.png

Select Image File

更新图标

第二部分，分红 Token 在去中心化交易所的不中断交易（分红过程也不中断）

1,创建特斯拉股份 Token 的交易对：

交易、流动性和分红

创建交易对

请输入分红Token地址:

0x72EA4b062f9BE959e89134596adf500943CDd65b

查询

当前分红地址:

0x72EA4b062f9BE959e89134596adf500943CDd65b

name:

Tesla

symbol:

TSLA

totalSupply:

6000

decimals:

3

Asset Token:

USDT

Asset Token Decimals:

18

请输入 Magnitude 的小数位:

6

推荐的 Magnitude 的小数位:


5

创建交易对

2, 添加和删除流动性:

流动性

?增加流动性 ?减少流动性

Div Token:  TSLA

Ass Token:  USDT 1996.003996003996

?滑点容差 (%) : ?交易截至期限(分钟)

?增加流动性 (Add Liquidity)

流动性

?增加流动性 ?减少流动性

Div Token:  TSLA

Ass Token:  USDT +

?要取出的流动性值(%):


?滑点容差 (%) : ?交易截至期限(分钟)


?减少流动性 (Remove Liquidity)

其中，图上红色部分是可以领取的分红金额和存储金额，在提取流动性时候也一并提出。

3, 交易

?交易

From:  USDT

To:  TSLA 9.921

Price: 0.992100000


?滑点容差 (%) : ?交易截至期限(分钟)


兑换 (Swap)

4, 流动性提供者领取分红

Pair: 0xE478F53297806284a3acB5597388326ebD13a0cA

IsPaused: False

Dividend Token:  TSLA 0.000

Asset Token:  USDT 0.000000000000000000

Price0: NaN

Price1: NaN

Account: 3

0xDc0227DDf3B93BfBBF44bA7dA844E8ad1F41Dd49

Account Balance:

ETH: 100

TSLA: 3000

USDT: 0

交易

流动性

分红和存款

可领取金额:

3,999.999999936754193186

刷新

领取

五, 常见问题公示和答疑:

- 1, 分红型 Token 和对应的去中心化交易所的主要意义有哪些? 在我们链下金融市场, 大部分金融凭据都是持有即受益, 例如: 股票有分红, 存款有利息, 大部分理财也有回报, 等等; 如果这些高价值链下金融产品 (STO) 进入(主)链上, 不会在意手续费, 是巨大市场。在链上这些 xSushi 类质押挖矿的项目, 也是分红型 Token。分红型 Token 在链上还会有更多的新实践; 现在缺的是**分红型 Token 的接口定义**和**对应的去中心化交易所**, 把这个短板补上, 就可以方便分红型 Token 的链上流动。链下分红可能需要暂停交易, 但是链上流通不需要暂停, 这是链上交易的优势之一。乌克兰类国家可能需要此类产品。

- 2, 看这份文档需要哪些基础知识? 建议要理解分红的算法 (可以参见 <https://github.com/ethereum/EIPs/issues/1726>); 了解 Uniswap 的恒定乘积原理; 会一点 Solidity 语言; 了解 ERC20 标准, 等。
- 3, 分红 Token 可以质押吗? 可以, 但怎么处理红利是另外一个问题, 或许需要处理二次分红的问题, 就如本文的交易对一样。
- 4, 分红型 Token 和 STO 的关系是咋样的? STO 可以是分红型 Token, 也可以不是。分红型 Token 是一种功能, 而 STO 是一种业务标准。绝大部分 STO 应该可以做成分红型 Token。
- 5, 质押挖矿型分红 Token 可以上本文交易所吗? 可以的, 但需要满足接口 (IDividendToken) 要求。
- 6, 这些合约可以改进吗? 可以, 我就列了一些改进意见。相比于 UniswapV2&V3, 有一些小细节可以改进 (某些小细节可以减少很少的 Gas 开销), 也可以增加一些有用的辅助功能 (例如 FlashLoan 等); 最好能够避开 UniswapV3 的价格分段计算的版权限制, 采用类似的计算, 才能提高流动性资金效率。现在的重点就是保证安全和准确。
- 7, 合约部署在哪儿? 目前只部署在测试网 (<https://rinkeby.etherscan.io/>) 上, 分红 Token 合约工厂地址是: [0xF182bfAE15B0F77489FBE8f3928F5948bE1c00B6](https://rinkeby.etherscan.io/address/0xF182bfAE15B0F77489FBE8f3928F5948bE1c00B6); 交易对合约工厂地址是: [0x5CdA2aE0A75857e761Dd98f7Af6b4Cc6302A2fDf](https://rinkeby.etherscan.io/address/0x5CdA2aE0A75857e761Dd98f7Af6b4Cc6302A2fDf)。
- 8, 源代码存放在哪里? 在 github 上, 具体网址是: <https://github.com/heddhshan/DividendTokenAndDex/tree/main/Contract>。客户端程序可能过几天也会放上去。

9, 其他人可以使用这些合约用于商业用途吗? 有条件, 参见下面的“出售商业使用许可”段落文档。

六, 出售商业使用许可

如果其他人需要使用这些合约用于商业用途, 可以购买我的许可: 支付 100ETH 就可以商业使用; 支付 200ETH 就把所有权限转让给对方 (我自己放弃所有权限)。购买许可后免费赠送客户端程序源代码, 并提供 8 个小时的技术支持。

支付的方式是在以太坊主网直接往地址 0xC7A9d8C6C987784967375aE97a35D30AB617eB48 打款并发送消息 (消息应该包括接受客户端源代码的邮箱), 可以参照 <https://rinkeby.etherscan.io/tx/0xa27a4176bb3fc6441839d9b97e7831fa4b143e156921fcdc51f9bf7a0f0d5187> (这是测试网的)。金额足够就自动获得授权。我接到 ETH 和消息后, 会把客户端的源代码发到您的邮箱 (我的发送邮箱是 c7a9d8c6c987784967375ae97a35d30ab617eb48@hotmail.com), 并可以补充一个带签名的授权声明。