

# Token合约

## 常量

变量名	类型	描述
MINTER_ROLE	bytes32	增发行为角色
PAUSER_ROLE	bytes32	暂停行为角色
BURNER_ROLE	bytes32	销毁行为角色
DEFAULT_ADMIN_ROLE	bytes32	管理员角色

## 状态变量

变量名	类型	描述
PAUSER_ROLE	bytes32	暂停行为角色
BURNER_ROLE	bytes32	销毁行为角色
excitationAddr	mapping	治理激励合约地址

## 构造函数

- 描述：
  - 部署合约时需要化传递参数。
- 参数：

•	参数名	类型	描述
	name	string	Token名称
	symbol	string	Token符号

# 方法

## 增发Token

- 方法名：mint
- 描述：
  - 实现增发功能。
- 注意：
  - 该函数只能被具有 MINTER\_ROLE 角色的账户调用。
- 参数：

参数名	类型	描述
_to	address	接收Token的账户。
_amount	uint256	增发的Token数量。

- 返回值：
  - 无
  -

## 销毁Token

- 方法名：burnFrom
- 描述：
  - 实现销毁功能，允许授权用户进行销毁，要求授权用户需要有足够多的授权Token。
- 注意：
  - 该函数只能由具有 BURNER\_ROLE 角色的账户调用。
  - 授权用户需要事先调用 approve 函数授权给调用者足够多的授权Token。
- 参数：

参数名	类型	描述
-----	----	----

_account	address	待销毁Token的账户地址。
_amount	uint256	待销毁的Token数量。

- 返回值：
  - 无

## Token转移

- 方法名：transfer
- 描述：
  - 实现 ERC20 标准中的 transfer 函数，增加暂停交易的判断，函数用于从当前合约的地址向另一个地址转移Token。
- 注意：
  - 转移操作会消耗发送者的Token。
  - 当前合约需要有足够的Token进行转移。
  - 转移操作受到暂停交易的限制，若交易被暂停则无法进行转移。
- 参数：

参数名	类型	描述
_recipient	address	接收者的地址。
_amount	uint256	要转移的Token数。

- 返回值：

类型	描述
bool	转移操作是否成功。如果成功，返回 true；否则，返回 false，并且不会进行Token转移操作。

## Token转账

- 方法名：transferFrom
- 描述：

- 实现 ERC20 标准中的 transferFrom 函数，增加暂停交易的判断，函数用于从一个地址向另一个地址转移Token，前提是发送方已经获得了发送方授权的Token数量。
- 注意：
  - 该函数只能在交易未被暂停的情况下调用。
  - 如果转账发起方不是Token拥有者，该函数需要在Token拥有者先调用 approve 方法授权。
  - 调用该函数将会减少发送方的Token数量，并且增加接收方的Token数量。
  - 该函数会返回一个布尔值表示是否转账成功。

- 参数：

参数名	类型	描述
_sender	address	发送方的地址，即Token拥有者的地址。
_recipient	address	接收方的地址。
_amount	uint256	要转移的Token数量。

- 返回值：

返回值	类型	描述
success	bool	转账是否成功的布尔值。如果转账成功，返回 true；否则返回 false。

## 授权转移Token

- 方法名：approve
- 描述：
  - 允许 spender 从当前账户转移指定数量的Token。如果之前已经存在授权，那么该函数将会覆盖之前的授权。
- 注意：
  - 需要确保 spender 代表的账户是可信的。
  - 如果授权的数量小于之前已经授权的数量，那么之前授权的数量将会被覆盖。

- 参数：

参数名	类型	描述
_spender	address	被授权转移Token的账户地址。

_amount	uint256	允许转移的Token数量。
---------	---------	---------------

- 返回值：

类型	描述
bool	授权是否成功。如果成功，则返回 true。

## 增加授权额度

- 方法名：increaseAllowance
- 描述：
  - 增加授权额度，允许 spender 可以从当前账户中转移更多的Token数量。
- 注意：
  - 当前账户需要先授权 spender 才能增加授权额度。
  - 该函数只能在未暂停交易时调用。
- 参数：

参数名	类型	描述
spender	address	需要增加授权额度的账户地址。
addedValue	uint256	需要增加的授权额度。

- 返回值：

类型	描述
bool	表示授权额度是否成功增加的布尔值。

## 减少授权Token数

- 方法名：decreaseAllowance
- 描述：
  - 减少spender可以从当前账户中转移的Token数量。

- 注意：
  - 该函数只能在交易未暂停的情况下调用。
  - 减少授权的数量不能使授权的余额小于0。

- 参数：

参数名	类型	描述
spender	address	被授权的账户地址。
subtractedValue	uint256	减少的授权Token数量。

- 返回值：

类型	描述
bool	操作是否成功。

## 授予角色权限

- 方法名：grantRole
- 描述：
  - 实现权限配置功能，只有具备 DEFAULT\_ADMIN\_ROLE 角色的账户才有权限调用该方法。
- 注意：
  - 该函数只能被 DEFAULT\_ADMIN\_ROLE 角色调用。
  - 授予的角色必须预先在合约中定义。

- 参数：

参数名	类型	描述
_role	bytes32	被授权角色的哈希值。
_account	address	被授权的账户地址。

- 返回值：

- 无

## 批量分配角色

- 方法名：setupRoles
- 描述：
  - 批量分配角色。
- 注意：
  - 该函数只能被管理员调用。
- 参数：

参数名	类型	描述
_roles	bytes32[]	角色数组。
_addresses	address[]	地址数组。

- 返回值：
  - 无

## 撤销角色权限

- 方法名：revokeRole
- 描述：
  - 撤销指定账户的指定角色权限。
- 注意：
  - 该函数只能被管理员调用。
- 参数：

参数名	类型	描述
_role	bytes32	待撤销的角色。
_account	address	目标账户地址。

- 返回值：

- 无

## 暂停交易

- 方法名：pause
- 描述：
  - 用于暂停交易。
- 注意：
  - 该函数只能被具有 PAUSER\_ROLE 角色的账户调用。
- 参数：
  - 无
- 返回值：
  - 无

## 查看余额

- 方法名：balanceOf
- 描述：
  - 查看账户地址的Token数量。
- 参数：

•

参数名	类型	描述
account	address	账户地址

- 返回值：

类型	描述
uint256	Token余额

## 查看总额

- 方法名：totalSupply
- 描述：
  - 查看Token总量



- 参数
  - 无
- 返回值：

•	类型	描述
	uint256	Token总量

查看Token名称

- 方法名：name
- 描述：
  - 查看Token名称
- 参数
  - 无
- 返回值：

•	类型	描述
	string	Token名称

查看Token符号

- 方法名：symbol
- 描述：
  - 查看Token符号
- 参数
  - 无
- 返回值：

•	类型	描述
---	----	----

string	Token符号
--------	---------

查看Token精度

- 方法名：decimals
- 描述：
  - 查看Token精度
- 参数
  - 无
- 返回值：

•	类型	描述
	uint8	Token精度