

欧易- 无gas转账功能

背景

- okx官方公告: <https://www.okx.com/cn/help-center/okx-wallet-now-offers-free-gas-transfer>
- 2023年4月18日至香港时间 2023年5月16日中午12: 00, 欧易 Web3 钱包现已推出无Gas转账功能。

免Gas转账活动期间, **每台设备每日可享受一笔免 Gas 转账交易**, 未使用的无Gas次数不会累计, 每日免费次数将在每日 00:00 (HKT) 重置。

免 Gas 转账支持的网络:

目前免 Gas 转账支持: Ethereum、OKTC、TRON、BNB Chain、Polygon、Optimism、Arbitrum One、Avalanche C、Fantom。

减免金额:

不同主网的减免金额上限不同。减免范围内, 用户即使没有作为 Gas 的主网币, 也可以成功转账! (是因为在转账之前, 钱包官方会向用户地址转入主网币、作为gas补贴) 请您注意, 对于超出减免金额的交易, 用户需要支付该笔转账的全额网络费用。

各网络减免金额请参考:

网络	Ethereum	Tron	OKTC	BNB Chain	Polygon	Optimism	Arbitrum	Avalanch	Fantom
等值Gas减免上限	\$ 5	\$ 1	\$ 0.5	\$ 0.5	\$ 0.5	\$ 0.5	\$ 0.5	\$ 0.5	\$ 0.5

原理 (以BSC链为例)

- 转账分为主网币和非主网币两种类型, 其所需的gas费基本是固定的。
 - 主网币转账: gas是固定的: 21000gas
 - 非主网币转账: 需调用token合约的 `transfer()`。token接收者如果是首次接收token, 则合约中需要为该接收者创建一块storage空间, 此时转账交易所需的gas较高, 约为50000个gas; 非首次接收时, 只需更新storage, 此时转账交易所需的gas略少, 约为30000个左右
 - 首次接收USDC交易示例 (花费51115个gas) :
<https://bscscan.com/tx/0x5763fedd9e0bfbe0ca17034d73c01348833c8cca7891272fb39af1519fd05f4e>
 - 非首次接收USDC交易示例 (花费36115个gas) :
<https://bscscan.com/tx/0xe547d90bba7fded2b9f6cfa47e2fb13cbebcbb55aec9346cee609d5e20806a5df>
- 以BSC链为例, OKX官方的Gas减免上限为0.5U。当钱包检测到用户要进行转账时, 用户对转账交易签名后, 钱包先不将交易进行广播, 而是向该用户地址中转入等价于0.05U的主网币 (作为gas补贴), 交易成功后, 再广播用户的真实转账交易。

- gas补贴的具体主网币数量由链下计算；每个设备每日享受一次gas补贴，这一条也是由链下判断控制

OverviewInternal TxnsLogs (1)Comments

⑦ Status:

Success

⑦ Block:

275029023896 Block Confirmations

⑦ Timestamp:

3 hrs 15 mins ago (Apr-20-2023 04:00:30 AM +UTC)

⑦ Sponsored:

Blockscan Chat

Wallet-to-wallet instant messaging platform.

Start Chat

⑦ From:

0x8c3cb9665833fd9f79eb14cba16d82bbab6f22d8

⑦ To:

Contract 0x69ae2a0e4b04e2f20f25ef20431dc64c09c41115

TRANSFER 0.000162462 BNB From 0x69ae2a0e4b04e2f20f25ef2... To → 0x54aba136f6a68e745eb366...

⑦ Value:

0.000162462 BNB(\$0.05)

⑦ Transaction Fee:

0.0005768 BNB (\$0.19)

⑦ Gas Price:

0.00000001 BNB (10 Gwei)

⑦ Gas Limit & Usage by Txn:

500,000 | 57,680 (11.54%)

⑦ Other Attributes:

Nonce: 612Position: 2

⑦ Input Data:

0x71b9139800000000000059b43a51644200054aba136f6a68e745eb366e9b1ab14f31e9aed07

用户地址

View Input As

- 交易示例1（钱包通过与链上合约交互，向用户转账价值0.5U的主网币作为gas。此交易发生在区块高度为27502902。交易发生前，用户的BNB余额为0）：
<https://bscscan.com/tx/0x4609dec5200bec8bf5813f7f25399fe24d075cfe1dae1eb1f82f5a462d9612cb>
- 交易示例2（用户的真实转账交易，此交易发生在交易1的两个区块之后。此交易花费的gas费约为0.02U，交易之后用户地址的BNB余额价值为0.05-0.02=0.03U）：
<https://bscscan.com/address/0x54aba136f6a68e745eb366e9b1ab14f31e9aed07>

相关合约

- 官方合约：<https://bscscan.com/address/0x69ae2a0e4b04e2f20f25ef20431dc64c09c41115>（ETH链合约地址相同）
- 合约的部署者、即owner：0xaa2f15bce9b24662eaa514edec12f0294f07272d
- 此合约 of 欧易钱包官方的合约，作为官方向用户转账的中转点，合约中无资产。
- 主网币流转方向：官方用户地址-->官方合约-->钱包用户地址

- 合约中核心方法：

```
def unknown71b91398(addr _param1) payable:
    require calldata.size - 4 >= 32
    if unknownf75c2664Address != caller:
        revert with 0, '', 0
    if call.value > unknown6216123e:
        revert with 0, 'FG:MAX_GAS', 0
    call _param1 with:
        value call.value wei
        gas 2300 * is_zero(value) wei
    if not ext_call.success:
        revert with ext_call.return_data[0 len return_data.size]
    log 0x4a12d52e: addr(_param1), call.value, 0
```

仅特定地址可调用

校验转账数量

根据 msg.value 进行主网币转账

触发 event

- 此合约中的0x71b91398() 只能由通过合约的setMPC(address _mpc)方法设定的地址进行调用，转账数量也是由参数msg.value决定。此合约最主要的作用应该是 转账+记录事件