币安链dapp元交易智能合约开发

产品名称	币安链dapp元交易智能合约开发
公司名称	广州杰肯狸网络科技有限公司
价格	.00/件
规格参数	
公司地址	广州天河区中山大道
联系电话	18125913365 19927739756

产品详情

DApp（Decentralized
Application）是通往去中心化世界的应用程序，让人们真正能够感受到去中心化魅力的工具。但 令人沮丧的是，使用它意味着你需要有一定的对区/块链（以太坊）基础知识的掌握，包括但不限于钱包地址、哈希函数 （散列、Hash）、公私钥、交易、智能合约等。
这对一个对区/块链陌生的用户来说，太可怕了！他需要学大量的知识，只为了使用 DApp。

这阻挠了 DApp 的发展，而
元交易可以减轻普通用户的学习压力，只需要他基本掌握使用一个区/块链钱包，例如
MetaMask、TrustWallet、 ImToken 等等。

元交易（Metatransaction），是一种让用户不需要支付 gas 费就能够使用
DApp、发起交易、调用智能合约的手段。 这意味着用户将不再需要深入了解什么是交易、什么是智能合约，只需要确保自己的钱包是安全的，知道什么是钱包地址 就可以了。这大大的简化了 DApp
的使用流程。

聊元交易之前，首先了解一下什么是交易（Transaction）。一笔以太坊交易由以下内容构成： from – 发送者地址 recipient – 接收地址（如果为一个外部持有的帐户，交易将传输值。
如果为合约帐户，交易将执行合约代码） signature – 发送者的签名。
当通过发送者的私钥签名交易来确保发送者已授权此交易时，生成此签名。

什么是元交易？ 为什么元交易能够让用户不需要支付 gas 费？

– 从发送者向接收者转移 ETH 的金额 （以 WEI 为单位，ETH 的一种面值单位） data –
可包括任意数据的可选字段 gasLimit – 交易可以消耗的 Gas 的*大数量。 Gas 单位代表了计算步骤 gasPrice – 发送者按单位 gas 支付的费用 nonce – 区/块链严格根据 nonce 值从小到大的顺序执行交易 注意其中的

signature
字段，通过它任何人都能够验证这笔交易就是发送者地址签署的。交易会被发送给区/块链节点，发送者会支付 gas 费，通过验证的交易才会被节点包含进自己的区/块链中，并进行广播。

而如果说，这样一笔交易发给某 个中间人/节点，让他帮忙来付 gas 费并执行该交易，我们的目的就实现了。
但问题是，简单的将这样一笔交易发给中间人，中间人也并不能帮你支付 gas 费，因为它是一个普通的交易，它会被验 证通过，并认为是发送者来支付 gas 费。
那我们如何绕过这个限制呢？答案是智能合约。

如果这笔交易发生在智能合约内部，也就是说，在普通的交易内部嵌入一个交易（这个交易就被称作元交易），交易被你 的中间人/节点签署，并指定接收者地址为元交易智能合约的地址，因此 gas 费由中间人/节点支付；而元交易智能合约在 收到一笔元交易后，会验证元交易的签名信息，确认无误后，你的元交易在元交易智能合约中被执行。

举个例子 Alice 想向 Bob 转账 0 ETH，而由于 Alice 账户上没有任何 ETH，即便是转账 0 ETH，但她仍然需要支付一定数额的 gas 费，因此 Alice 无法直接执行这样一笔交易。 而 Alice 知道 Carol 恰好账号上有足够多的 ETH 去支付 gas 费，于是请求他的帮助。 Carol 让 Alice 签署这笔元交易，并将所有内容发送给他；Carol 收到 Alice 的元交易后，构造出一个发送给元交易智能合约地址的交易，广播给区/块链的节点。 区/块链节点将验证 Carol 的交易合法性；元交易智能合约扣除 Carol 的 gas 费作为执行智能合约的费用，并验证该交易 中的元交易是否合法（验证是否为 Alice 的签名，nonce 值是否合法等）。 验证合法后，元交易智能合约执行该元交易，从而 Alice 在没有花任何 gas 费的情况下，通过中间人 Carol 执行了交 易。

元交易是让 DApp 迅速发展的关键性技术之一，它减小了普通用户理解区/块链运作机制的成本，让用户不需要支付 gas 费即可发起交易.