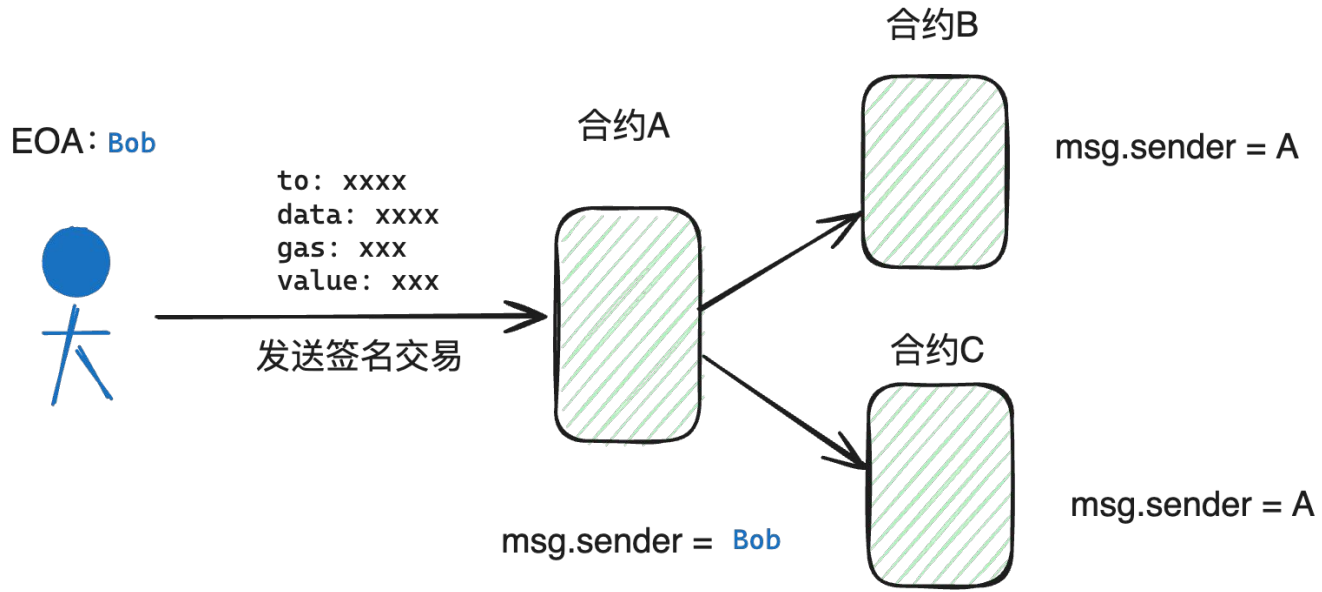
以太坊账户改进之路

Tiny熊

@tinyxiong_eth

EVM 交易工作流



EOA 和合约账户在 EVM 上是一样的，有同样的属性：balance、nonce、code、state

```
function approve(address _spender, uint256 _value)
    allowance[msg.sender][_spender] = _value;
    return true;
}

function transferFrom(address _from, address _to, uint256 _value) returns (bool success) {
     …
    if (_value > allowance[_from][msg.sender]) throw;
    balanceOf[_from] -= _value;
    balanceOf[_to] += _value;
    allowance[_from][msg.sender] -= _value;
    emit Transfer(_from, _to, _value);
    return true;
}
```

EOA

- EOA (Externally Owned Account 外部账号)
  - 用私钥控制的账号（MetaMask / ImToken … ）
  - 特点：链下生产、所有链账号一致

- 问题：
  - 私钥、助记词、支付 Gas（普通用户太不友好）
  - 一次只能签一笔交易
  - 无法 Social Recovery、无法替换 Key

要大规模采用，不可能

合约账户（CA）

- 由合约代码控制的账户
- 逻辑灵活：其他签名方式、多签、Social Recovery、Gas 代付
- 但是只能被动执行

能否尝试融合两者：账户抽象（Account Abstraction）

先驱：EIP-86 / EIP-2938

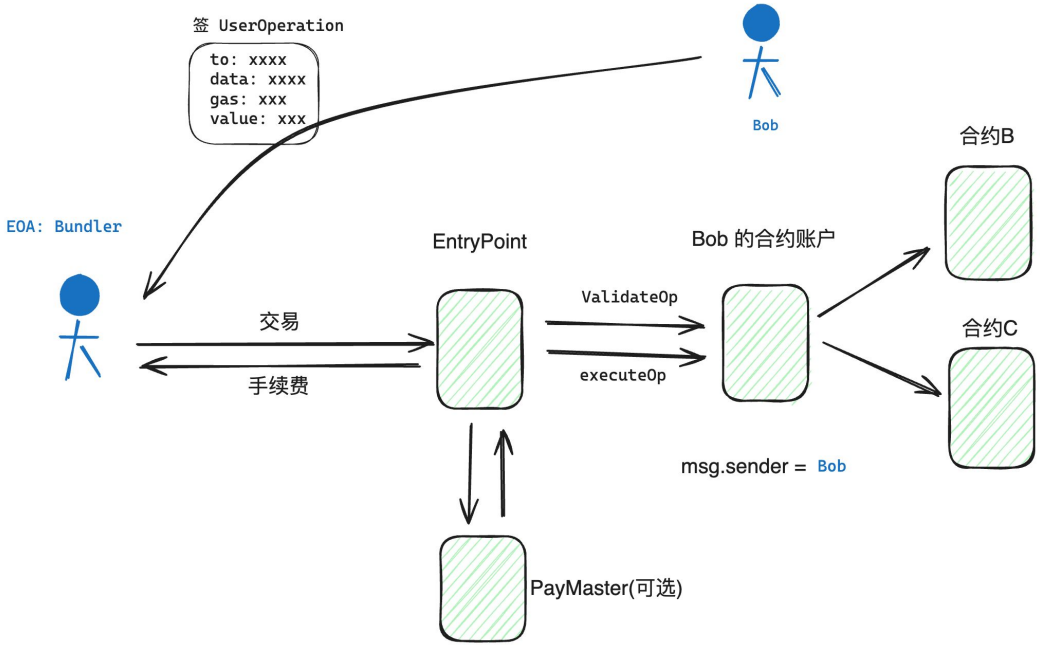
- EIP-86：抽象验证签名逻辑，创建“合约”来验证签名
- EIP-2938：让合约成为一等公民（可支付 Gas 及发起交易）

对核心协议修改太大，暂时搁置

ERC-4337

- 不改变协议(不影响共识)
- 合约作为账户，引入 Bundler 打包发送交易
- 带来了前所未有的灵活性:
  - 多种签名逻辑
  - 批量交易
  - 社交恢复
  - Paymaster 作为付款人

ERC-4337 工作流



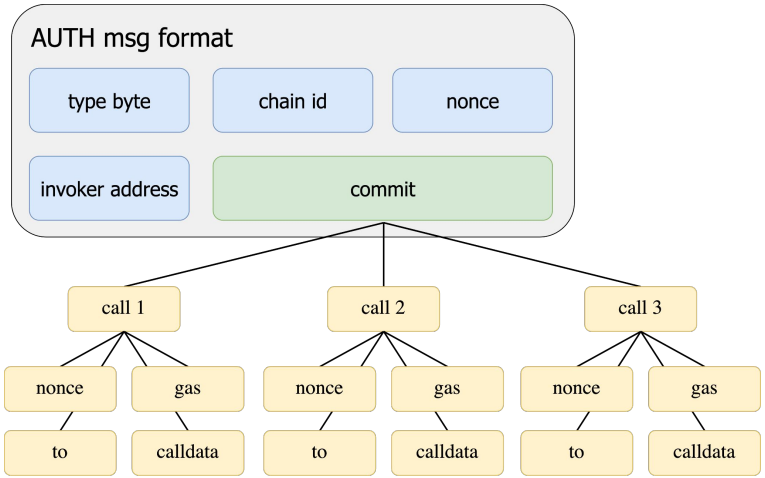
创建账号成本高、交易费高、多链隔离，让 ERC-4377 采用率不够理想。

EIP-3074 - 重新回到视野

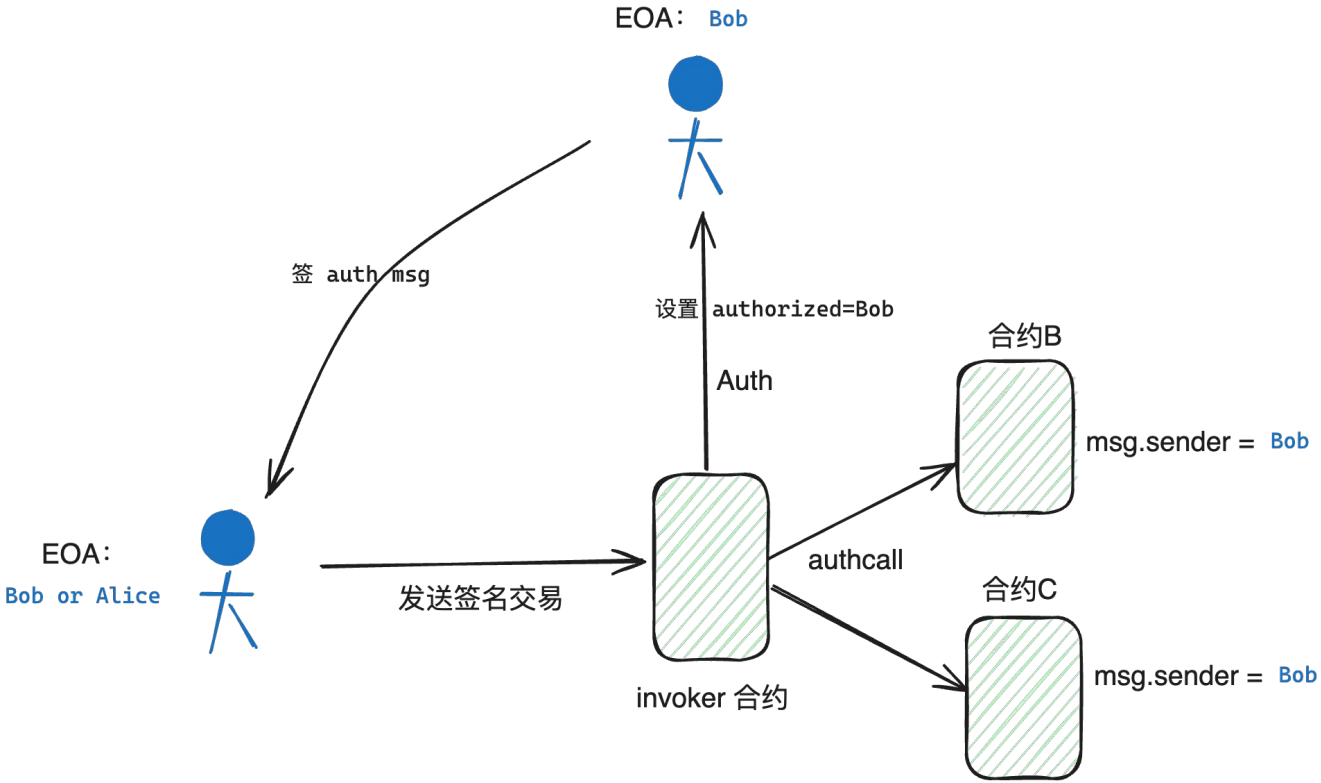
- 引入操作码：AUTH + AUTHCALL
- 允许智能合约代表 EOA（为现有账号添加功能）
- 可实现 Gas 代付、批量交易

EIP-3074

- AUTH：invoker 合约中设置 authorized 变量为 授权签名的账户地址
- AUTHCALL：用 authorized 变量作为调用者地址，再进行 Call 调用



EIP-3074 工作流


EOA： Bob
签 auth msg
设置 authorized=Bob
Auth
合约B
msg.sender = Bob
EOA：
Bob or Alice
发送签名交易
authcall
合约C
msg.sender = Bob
invoker 合约

EIP-3074 争议

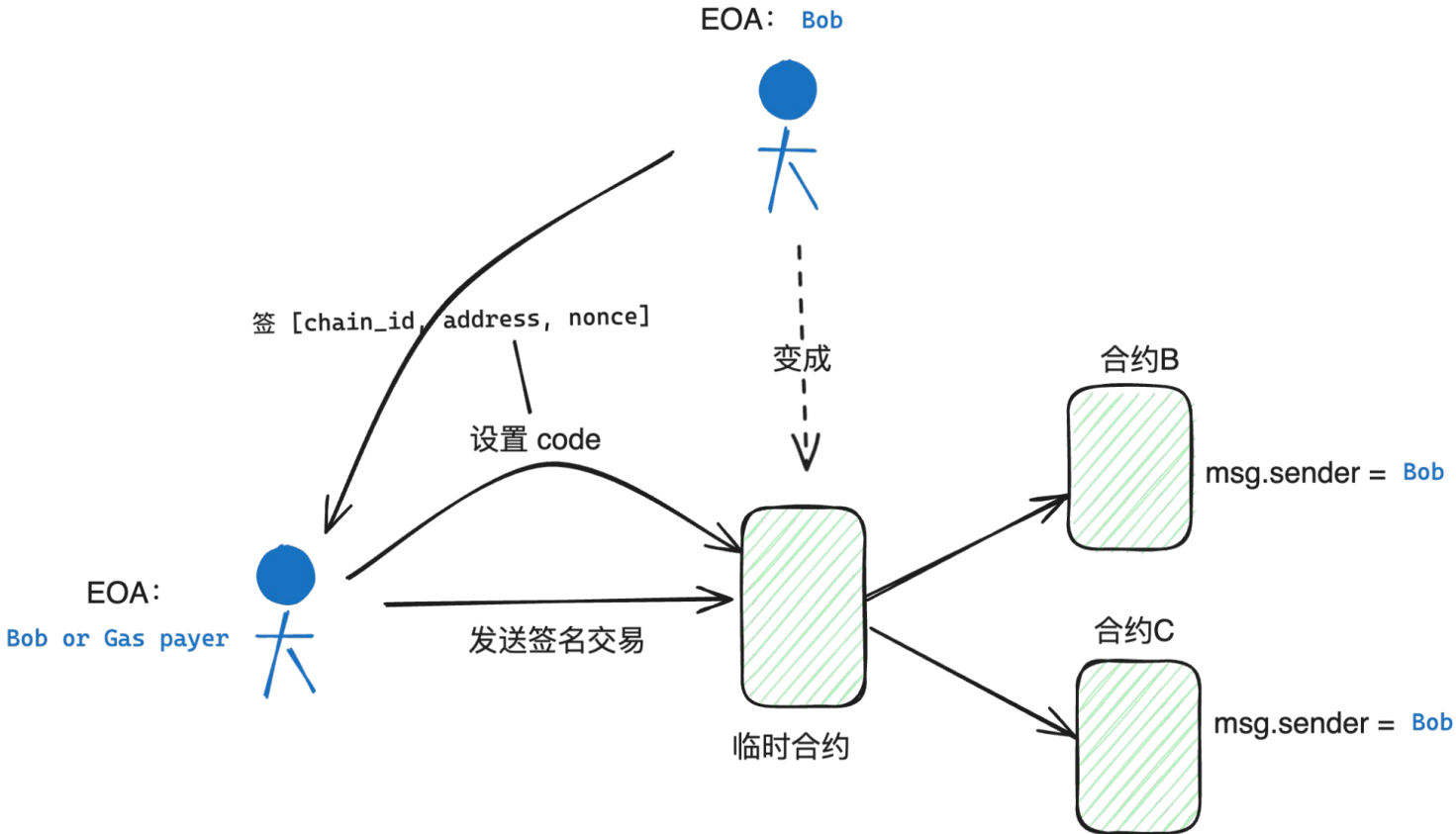
- 优点：
  - Gas 低
  - 可快速应用（利用现有的 EOA及基础设施）
- 反对：
  1. Invoker 权力过大，不利于抗审查
  2. 依旧依赖 ECDSA
  3. 在 EOA 到 SA 迁移后（被认为是 endgame），3074 引入的操作码将无用，但会遗留在 EVM 代码中，造成技术债务。

https://docs.zerodev.app/blog/4337-and-3074-disagreements
https://ethereum-magicians.org/t/eip-3074-is-unsafe-unnecessary-puts-user-funds-at-risk-while-fragmenting-ux-liquidity-and-the-wallet-stack/19662

EIP-7702

- 作为 EIP-3074 的替代方案提出
- 添加新的交易类型（基于EIP-2718），可设置代码，让EOA 可以变成临时合约账户（transient smart wallet）
  - 具体是在交易中加入一个 authorization_list
  - authorization_list 为 [chain_id, address, nonce, y_parity, r, s]

EIP-7702 工作流


EOA: Bob
签 [chain_id, address, nonce]
变成
设置 code
合约B
msg.sender = Bob
EOA:
Bob or Gas payer
发送签名交易
合约C
临时合约
msg.sender = Bob

EIP-7702 - 中庸之道

- 向后兼容现有钱包，向前允许转为合约钱包（可兼容 ERC4337）
- 实现批量交易、Gas 代付，但不引入技术债务

总结对比

ERC-4337	EIP-3074	EIP-7702
无协议变更	引入操作码	引入新交易类型
创建独立的合约账户	合约代表 EOA	(瞬时)给 EOA 添加代码
需要资产迁移	复用现有资产	复用现有资产
可不依赖 ECDSA	依赖 ECDSA	依赖 ECDSA
Gas 较高	Gas 较低	Gas 较低

其他的账户 EIP

- RIP-7560：ERC-4337 在 Rollup 的实现（实现 Native AA）
- EIP-7377：添加新交易，将 EOA 迁移到智能合约
- EIP-5003：在 EOA 上发布代码（加指令AUTHUSURP）
- EIP-6913：SETCODE 指令，合约升级

Thanks