**EIP-1271 讓你的合約也可以簽名**

[[](https://medium.com/@wiasliaw?source=post_page-----dc4e1c9c84a0--------------------------------)](https://medium.com/@wiasliaw?source=post_page-----dc4e1c9c84a0--------------------------------)

[[Taipei Ethereum Meetup](https://medium.com/taipei-ethereum-meetup?source=post_page-----dc4e1c9c84a0--------------------------------)](https://medium.com/taipei-ethereum-meetup?source=post_page-----dc4e1c9c84a0--------------------------------)

[Wias Liaw](https://medium.com/@wiasliaw?source=post_page-----dc4e1c9c84a0--------------------------------)

·

[Follow](https://medium.com/m/signin?actionUrl=https%3A%2F%2Fmedium.com%2F_%2Fsubscribe%2Fuser%2Faf88987a8fbb&operation=register&redirect=https%3A%2F%2Fmedium.com%2Ftaipei-ethereum-meetup%2Feip-1271-%E8%AE%93%E4%BD%A0%E7%9A%84%E5%90%88%E7%B4%84%E4%B9%9F%E5%8F%AF%E4%BB%A5%E7%B0%BD%E5%90%8D-dc4e1c9c84a0&user=Wias+Liaw&userId=af88987a8fbb&source=post_page-af88987a8fbb----dc4e1c9c84a0---------------------post_header-----------)

Published in

[Taipei Ethereum Meetup](https://medium.com/taipei-ethereum-meetup?source=post_page-----dc4e1c9c84a0--------------------------------)

·

3 min read

·

Aug 5, 2022

82

2

*越來越多 Dapp 或是合約需要依賴簽名來使用，像是 EIP-2612 以簽名代替 approve 使用。換到合約錢包上要怎麼簽名呢？*

首先，要先強調的是「合約沒辦法產生簽名」，合約沒有私鑰可以做簽名，做不到從簽名驗證簽名者是誰。EIP-1271 設計一種方式可以讓合約錢包可以去調用需要傳入簽名的函式且能正常使用。

**Example in EIP**

直接來看一個合約錢包需要實作什麼函式。isValidSignature 要實作在需要簽名去調用其他函式的合約裡，像是合約錢包。

驗證的實作可以很彈性，這裡沒有限制一定要使用什麼哪種驗證方式。如果驗證正確則回傳一個 magic value(0x1626ba7e)，也就是 isValidSignature 這個函式的 function selector。以合約錢包為例，則驗證這個錢包 owner 為哪個 EOA 即可。

// solidity  
// implemented in Wallet Contract  
function isValidSignature(  
 bytes32 \_hash,   
 bytes memory \_signature  
)  
 public  
 view   
 returns (bytes4 magicValue)  
{  
 (uint8 v, bytes32 r, bytes32 s) = split(\_signature);  
 address signer = ecrecover(\_hash, v, r, s);  
 require(signer == wallet.owner);  
 return 0x1626ba7e;  
}

至於需要驗證簽名的合約，像是 ERC2612，需要區分 EOA 和合約調用(Address.isContract)，如果是合約則需要去調用合約錢包實作的 isValidSignature 來驗證簽名，舉例如下。EOA 和原本一致即可。

// solidity  
// implemented in Contract need to verify signature  
function callERC1271isValidSignature(  
 address \_addr,  
 bytes32 \_hash,  
 bytes calldata \_signature  
) external view {  
 bytes4 result = IERC1271Wallet(\_addr)  
 .isValidSignature(\_hash, \_signature);  
 require(result == 0x1626ba7e, "INVALID\_SIGNATURE");  
}

**Implementation**

更為簡略的實作可以看ㄧ下下我用 Foundry 寫的版本，省略很多實作只留下簽名和驗證的部分。

**[GitHub - wiasliaw/wallet-signature](https://github.com/wiasliaw/wallet-signature?source=post_page-----dc4e1c9c84a0--------------------------------" \t "_blank)**

[research and implement for some eip about signature SimpleWithPermit.sol simplified implementation of EIP-2612…](https://github.com/wiasliaw/wallet-signature?source=post_page-----dc4e1c9c84a0--------------------------------" \t "_blank)

[github.com](https://github.com/wiasliaw/wallet-signature?source=post_page-----dc4e1c9c84a0--------------------------------" \t "_blank)

**Reference**

**[EIP-1271: Standard Signature Validation Method for Contracts](https://eips.ethereum.org/EIPS/eip-1271?source=post_page-----dc4e1c9c84a0--------------------------------" \t "_blank)**

[Externally Owned Accounts (EOA) can sign messages with their associated private keys, but currently contracts cannot…](https://eips.ethereum.org/EIPS/eip-1271?source=post_page-----dc4e1c9c84a0--------------------------------" \t "_blank)

[eips.ethereum.org](https://eips.ethereum.org/EIPS/eip-1271?source=post_page-----dc4e1c9c84a0--------------------------------" \t "_blank)