以太坊钱包开发

熊丽兵（Tiny熊）

登链学院
edu.upchain.pro

我

- 熊丽兵（Tiny熊）
- 深入浅出区块链 learnblockchain.cn
- 《精通以太坊智能合约开发》
- 登链学院创始人

Demo

https://gitee.com/xilibi2003/EthWebWallet

登链学院
edu.upchain.pro

大纲

- 钱包账号、地址、私钥
- 钱包账号管理
- 以太转账
- ERC20 Token转账
- Ethers.js库

(数字)钱包

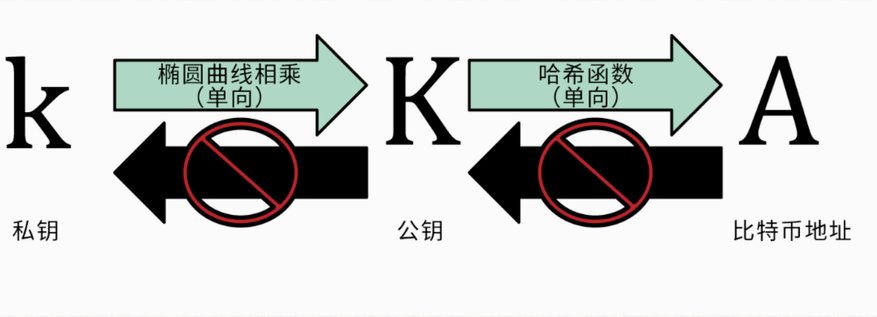
钱包存钱了吗?

钱包实际是一个管理私钥的工具

登链学院
edu.upchain.pro

钱包账号

钱包账号看上去是一个地址，关键是私钥



```
var Crypto = require('crypto')
var secp256k1=require('secp256k1')
var createKeccakHash=require('keccak')

// 一个32字节的随机数（1~2^256-1），直接把他当成私钥
 var privateKey=Crypto.randomBytes(32);
console.log(privateKey.toString('hex'));

// 由secp256k1椭圆曲线算法先计算出公钥
var pubKey=secp256k1.publicKeyCreate(privateKey,false).slice(1);

// 进行keccak256 hash运算再取后40位得到
var address =createKeccakHash('keccak256')
                  .update(pubKey).digest().slice(-20);
console.log("0x" + address.toString('hex'));
```

登链学院
edu.upchain.pro

创建钱包账号

- 随机生成私钥（32字节）
- 分层确定性推倒

登链学院
edu.upchain.pro

随机数生成私钥

随机在1到2^256之间选一个数字

不可预测或不可重复

分层确定性推倒

随机生成的私钥，备份麻烦，不易管理

BIP (Bitcoin Improvement Proposals)　　bip32 提案（HD钱包）

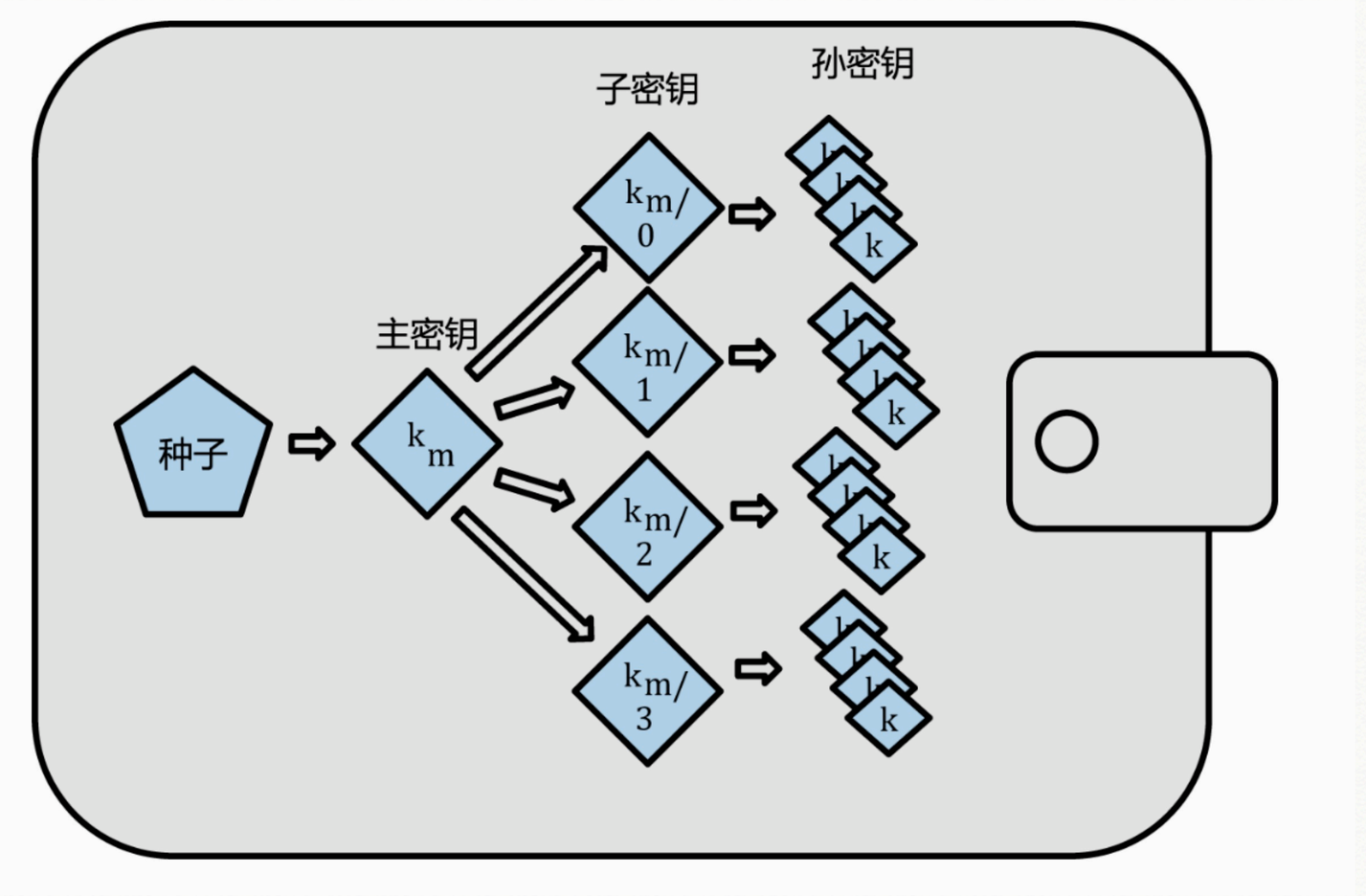
https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki

登链学院
edu.upchain.pro

HD钱包

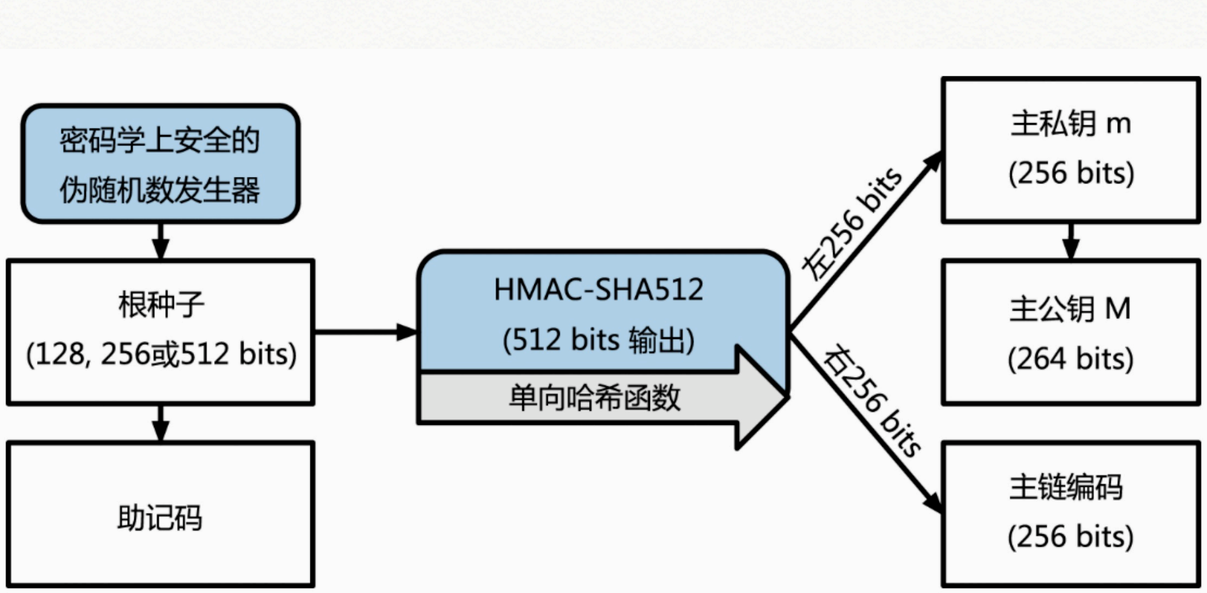
随机数种子推倒生成私钥

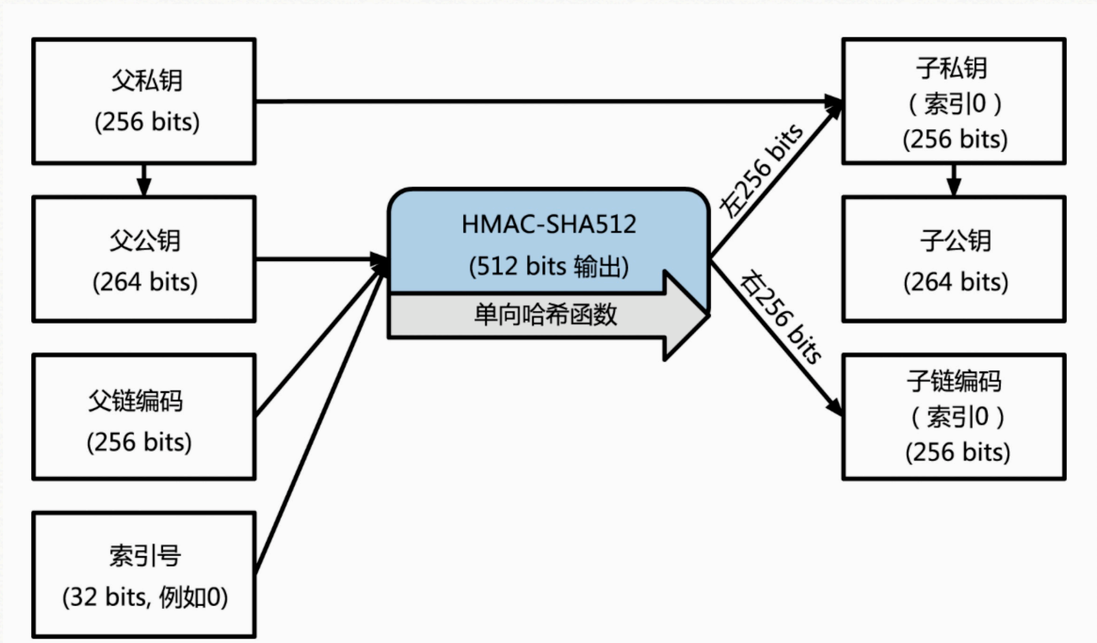
https://learnblockchain.cn/2018/09/28/hdwallet/



登链学院
edu.upchain.pro

分层推倒过程





https://learnblockchain.cn/2018/09/28/hdwallet/

秘钥路径

HD钱包中的密钥是用“路径”命名的，每个级别之间用斜杠（/）字符来表示

如： 第一个主密钥生成的子私钥是m/0。第一个公共钥匙是M/0。第一个子密钥的子密钥就是m/0/1

登链学院
edu.upchain.pro

BIP44

m / purpose' / coin_type' / account' / change / address_index

coin	account	chain	address	path
Bitcoin	first	external	first	m / 44' / 0' / 0' / 0 / 0
Bitcoin	first	external	second	m / 44' / 0' / 0' / 0 / 1
Bitcoin	first	change	first	m / 44' / 0' / 0' / 1 / 0
Bitcoin	first	change	second	m / 44' / 0' / 0' / 1 / 1

https://github.com/bitcoin/bips/blob/master/bip-0044.mediawiki

https://github.com/satoshilabs/slips/blob/master/slip-0044.md

登链学院
edu.upchain.pro

随机数 or 助记词

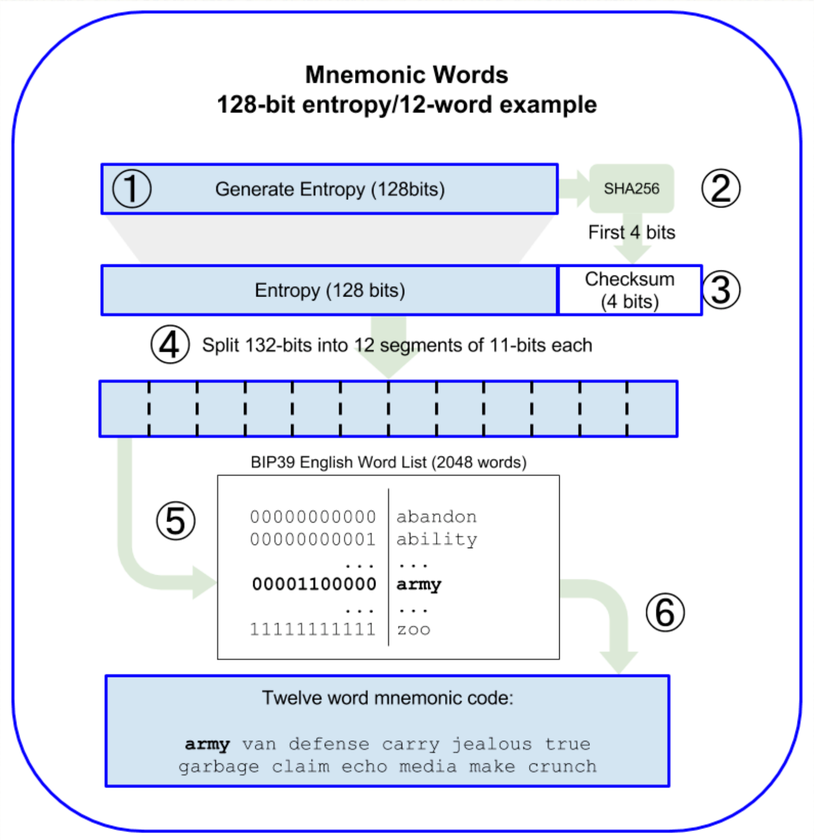
```
090ABCB3A6e1400e9345bC60c78a8BE7
```

```
candy maple cake sugar pudding cream honey rich
smooth crumble sweet treat
```

https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki

登链学院
edu.upchain.pro

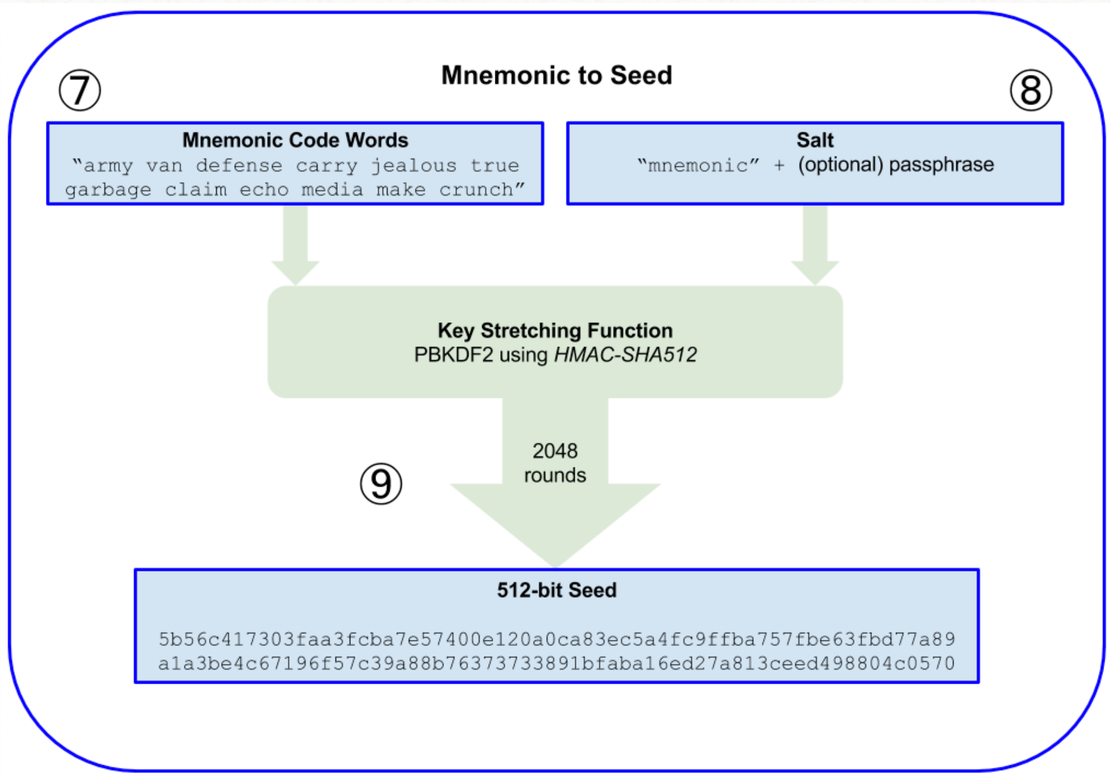
生成助记词



https://github.com/bitcoin/bips/blob/master/bip-0039/english.txt

登链学院
edu.upchain.pro

助记词推倒出种子



密钥拉伸函数：
用来增强弱密钥的安全性

https://github.com/bitcoinjs/bip39

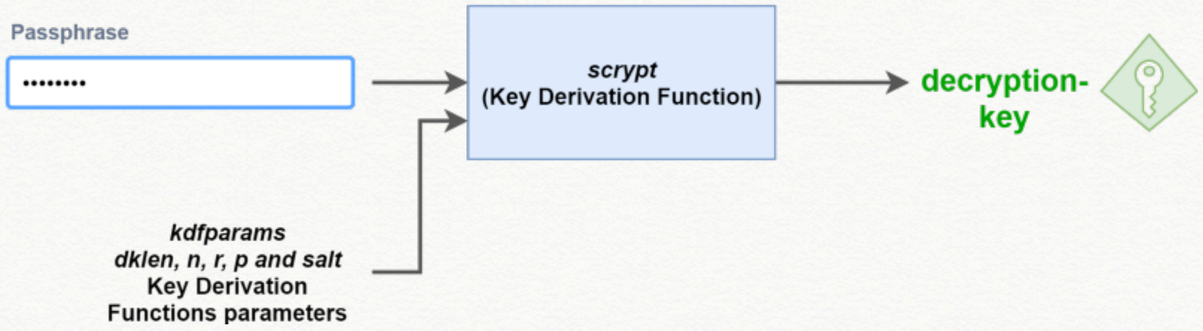
```
var bip39 = require('bip39')
var hdkey = require('ethereumjs-wallet/hdkey')
var util = require('ethereumjs-util')

// 生成助记词
var mnemonic = bip39.generateMnemonic()

var seed = bip39.mnemonicToSeed(mnemonic);
var hdWallet = hdkey.fromMasterSeed(seed);

var key1 = hdWallet.derivePath("m/44'/60'/0'/0/0");
console.log("私钥: "+util.bufferToHex(key1._hdkey._privateKey));

var address1 = util.pubToAddress(key1._hdkey._publicKey, true);
console.log("地址: "+util.bufferToHex(address1));
```

https://iancoleman.io/bip39/

私钥存储

1. 加密存储 - 对称加密私钥

2. 如何选择加密秘钥（KDF）



登链学院
edu.upchain.pro

私钥存储

V3 KeyStore

```
{
    "address":"856e604698f79cef417aab...",
    "crypto":{
        “cipher":"aes-128-ctr",
        “ciphertext":"13a3ad2135bef1ff228e399dfc8d74a....",
        "cipherparams":{
            "iv":"92e7468e8625653f85322fb3c..."
        },
        "kdf":"scrypt",
        "kdfparams":{
            "dklen":32,
            "n":262144,
            "p":1,
            "r":8,
            "salt":"3ca198ce53513ce01bd651aee54b16b6a...."
        },
        "mac":"10423d837830594c18a91097d09b7f2316..."
    },
    "id":"5346bac5-0a6f-4ac6-baba-e2f3ad464f3f",
    "version":3
}
```

对称加密算法

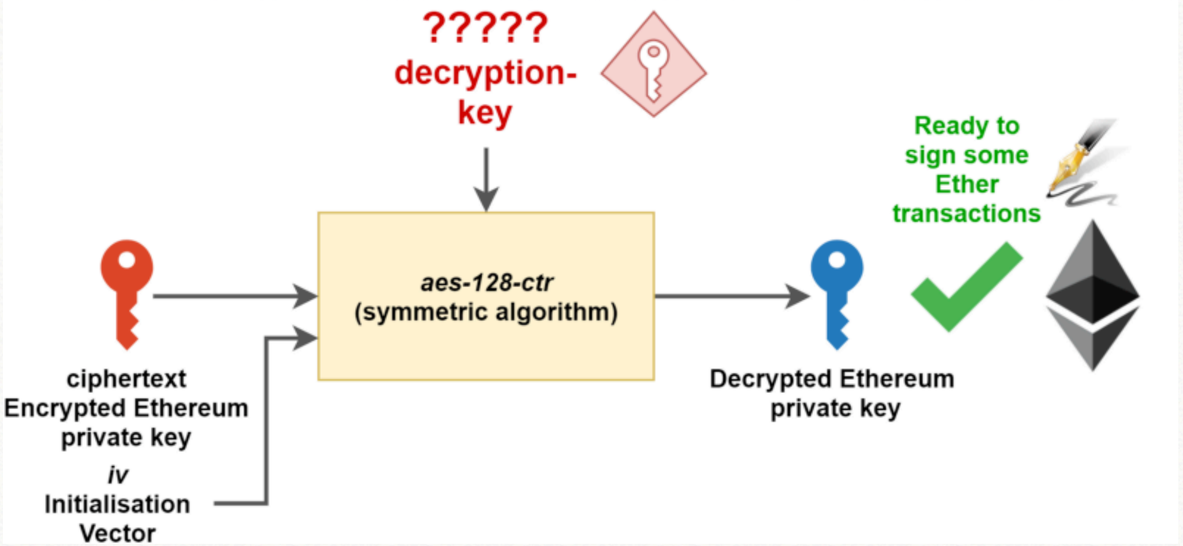
密文

秘钥派生算法参数

校验码

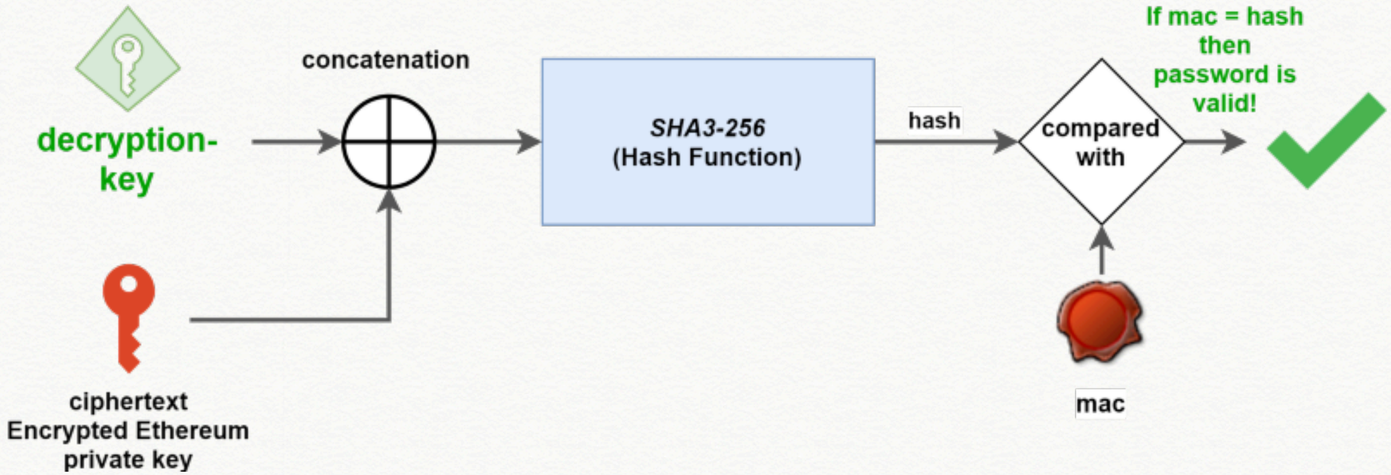
登链学院
edu.upchain.pro

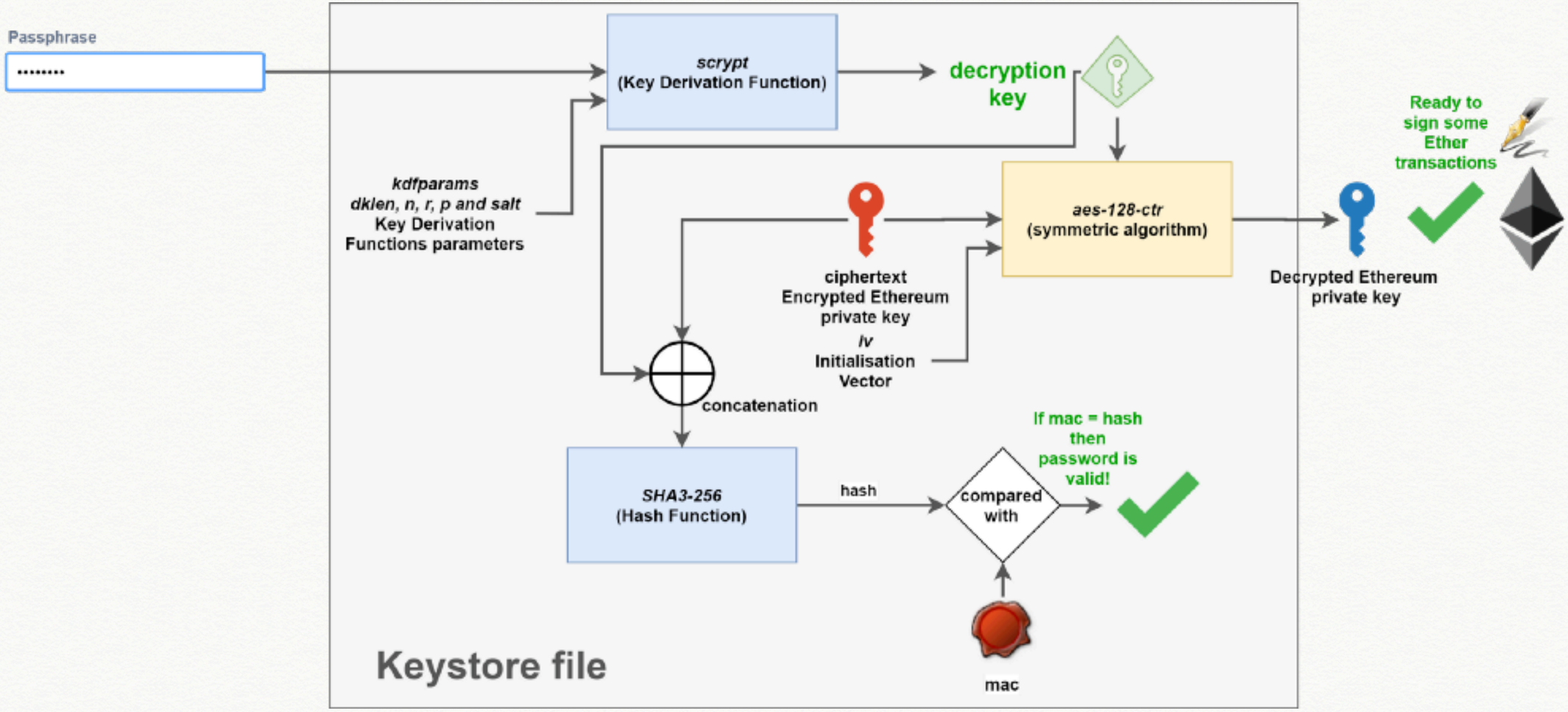
V3 KeyStrore 解密



如何确认密码正确性?

mac= sha3(DK[16:32], ciphertext)




Passphrase
••••••••
scrypt
(Key Derivation Function)
decryption
key
kdfparams
dklen, n, r, p and salt
Key Derivation
Functions parameters
aes-128-ctr
(symmetric algorithm)
ciphertext
Encrypted Ethereum
private key
iv
Initialisation
Vector
Decrypted Ethereum
private key
Ready to
sign some
Ether
transactions
concatenation
SHA3-256
(Hash Function)
hash
compared
with
If mac = hash
then
password is
valid!
mac
Keystore file

登链学院
edu.upchain.pro

转账

一个交易长这样：

```
const txParams = {
  nonce: '0x00',
  gasPrice: '0x09184e72a000',
  gasLimit: '0x2710',
  to: '0x0000000000000000000000000000000000000000',
  value: '0x00',
  data: '0x7f7465737432000000000000000000000000000…',
  // EIP 155 chainId - mainnet: 1, ropsten: 3
  chainId: 3
}
```

Gas

矿工费（预算）= gasLimit * gasPrice

gasLimit： 有工作量决定，少了 out-of-gas ， 多了退回。
普通转账是21000

gasPrice: 决定矿工打包的优先级，出价过低打包慢，出价过高不划算。

登链学院
edu.upchain.pro

签名及广播

```
const tx = new EthereumTx(txParams)
tx.sign(privateKey)
const serializedTx = tx.serialize()
```

```
web3.eth.sendRawTransaction(serializedTx, function (err, transactionHash) {
    console.log(transactionHash);
});
```

https://github.com/ethereumjs/ethereumjs-tx

登链学院
edu.upchain.pro

Token转账

Token = 符合 ERC20 接口的合约

Token转账 = 调用合约的转账函数

=

向合约地址发起交易

交易的data 是ABI编码数据

登链学院
edu.upchain.pro

Token转账

ABI: Application Binary Interface
描述合约提供的接口


```
[
    {
        "constant": false,
        "inputs": [{
                "name": "to",
                "type": "address"
            },
            {
                "name": "tokens",
                "type": "uint256"
            }],
        "name": "transfer",
        "outputs": [{
                "name": "success",
                "type": "bool"
            }],
        "payable": false,
        "stateMutability": "nonpayable",
        "type": "function"
    }
]
```

登链学院
edu.upchain.pro

Token转账

ABI: Application Binary Interface 描述合约提供的接口

```
var abi = [...];
var addr = "0x...";
var contract = new ethers.Contract(address, abi, provider);

contract.transfer(targetAddress, amount)
      .then(function(tx) {
         console.log(tx);
     });
```

登链学院
edu.upchain.pro

ethers.js

和web3.js 一样，是一套和以太坊区块链进行交互的库

ethers.js 对BIP32 BIP39 BIP44等相关的提案进行了实现

4个功能模块：

- Wallets & Signers
- Contracts
- Providers
- Utilities

https://docs.ethers.io/ethers.js/html/

登链学院
edu.upchain.pro

ethers.js

随机数私钥创建钱包账号

```
var privateKey = ethers.utils.randomBytes(32);
var wallet = new ethers.Wallet(privateKey);
```

助记词方式创建钱包账号

```
var rand = ethers.utils.randomBytes(16);
var mnemonic = ethers.utils.HDNode.entropyToMnemonic(rand);
var path = "m/44'/60'/0'/0/0";
ethers.Wallet.fromMnemonic(mnemonic, path);
```

登链学院
edu.upchain.pro

ethers.js

KeyStore 加解密

```
wallet.encrypt(pwd.val()).then(function(json) {
    var blob = new Blob([json], {type: "text/plain;charset=utf-8"});
    saveAs(blob, "keystore.json");
  });
```

```
ethers.Wallet.fromEncryptedJson(json, password).then(function(wallet) {
    //
    }, function(error) {
    //
    });
```

登链学院
edu.upchain.pro

ethers.js

连接provider

```
var provider =  new ethers.providers.JsonRpcProvider("http://127.0.0.1:8545");
var activeWallet = wallet.connect(provider);
```

```
activeWallet.sendTransaction({
            to: targetAddress,
            value: amountWei,
            //gasPrice: activeWallet.provider.getGasPrice(),
            //gasLimit: 21000,
        }).then(function(tx) {
});
```

登链学院
edu.upchain.pro

钱包安全性

- 谨慎谨慎谨慎（没有后悔药）
- 强密码 + 离线保存（勿用网络分享）
- 开源钱包 / 硬件钱包 / 多签钱包

登链学院
edu.upchain.pro

现场群：

谢 谢