Bitcore

2022-03-17

# Bitcore

Bitcore est une suite d'outils fournis par BitPay. Son objectif est de fournir des outils faciles à utiliser pour les développeurs Bitcoin. Presque tout le code de Bitcore est écrit en JavaScript. Il existe des modules écrits spécifiquement pour NodeJS. Enfin, le module "node" de Bitcore inclut le code C++ de Bitcoin Core. Veuillez consulter <https://bitcore.io> pour plus d'informations.

# Liste des fonctionnalités de Bitcore

* Nœud complet Bitcoin (nœud bitcore)
* Explorateur de blocs (aperçu)
* Utilitaires de bloc, de transaction et de portefeuille (bitcore-lib)
* Communiquer directement avec le réseau P2P de Bitcoin (bitcore-p2p)
* Génération mnémonique d'entropie de valeur d’amorçage (bitcore-mnémonique)
* Protocole de paiement (bitcore-payment-protocol)
* Vérification et signature des messages (bitcore-message)
* Schéma de chiffrement intégré à courbe elliptique (bitcore-ecies)
* Service de portefeuille (bitcore-wallet-service)
* Client de portefeuille (bitcore-wallet-client)
* Intégration des services directement avec Bitcoin Core (bitcore-node)

# Exemples de bibliothèque Bitcore

## Prérequis

* NodeJS >= 4.x

Si vous utilisez NodeJS et le nœud REPL :

$ npm install -g bitcore-lib bitcore-p2p

## Exemples de portefeuille utilisant bitcore-lib

Création d'une nouvelle adresse Bitcoin avec clé privée associée :

> bitcore = require('bitcore-lib')  
> privateKey = new bitcore.PrivateKey()  
> address = privateKey.toAddress().toString()

Création d'une clé privée déterministe hiérarchique et d'une adresse :

> hdPrivateKey = bitcore.HDPrivateKey()  
> hdPublicKey = bitcore.HDPublicKey(hdPrivateKey)  
> hdAddress = new bitcore.Address(hdPublicKey.publicKey).toString()

Création et signature d'une transaction depuis un UTXO :

> utxo = {  
txId: txId, // identifiant de transaction contenant une sortie non dépensée  
outputIndex: outputIndex, // index de sortie (par exemple 0)  
 address: addressOfUtxo,  
 script: bitcore.Script.buildPublicKeyHashOut(addressOfUtxo).toString(),  
satoshis: satoshis // montant envoyé à l&#39;adresse  
}  
> fee = 3000 //défini de manière appropriée pour les conditions sur le réseau  
> tx = new bitcore.Transaction()  
 .from(utxo)  
 .to(address, 35000)  
 .fee(fee)  
 .enableRBF()  
 .sign(privateKeyOfUtxo)

Remplacer la dernière transaction dans le mempool (replace-by-fee) :

> rbfTx = new Transaction()  
 .from(utxo)  
 .to(address, 35000)  
 .fee(fee\*2)  
 .enableRBF()  
 .sign(privateKeyOfUtxo);  
> tx.serialize();  
> rbfTx.serialize();

Diffuser une transaction sur le réseau Bitcoin (remarque : ne diffusez que des transactions valides ; reportez-vous à <https://bitnodes.21.co/nodes> pour les hôtes homologues) :

1. Copiez le code ci-dessous dans un fichier appelé *broadcast.js*.
2. Les variables tx et rbfTx sont la sortie de tx.serialize() et rbfTx.serialize(), respectivement.
3. Afin de remplacer par des frais, l'homologue doit prendre en charge l'option bitcoind mempoolreplace et la définir sur 1.
4. Exécutez le nœud de fichier *broadcast.js* :

var p2p = require('bitcore-p2p');  
var bitcore = require('bitcore-lib');  
var tx = new bitcore.Transaction('output from serialize function');  
var rbfTx = new bitcore.Transaction('output from serialize function');  
var host = 'ip address'; //use valid peer listening on tcp 8333  
var peer = new p2p.Peer({host: host});  
var messages = new p2p.Messages();  
peer.on('ready', function() {  
 var txs = [messages.Transaction(tx), messages.Transaction(rbfTx)];  
 var index = 0;  
 var interval = setInterval(function() {  
 peer.sendMessage(txs[index++]);  
 console.log('tx: ' + index + ' sent');  
 if (index === txs.length) {  
 clearInterval(interval);  
 console.log('disconnecting from peer: ' + host);  
 peer.disconnect();  
 }  
 }, 2000);  
});  
peer.connect();