Atom跨链交易

介绍：

跨链交易是一个发生在两个持有不同电子货币的用户之间的交易，即：Alice可以发送Bitcoin到Bob的Bitcoin地址，而此时Bob则发送Blackcoin到Alice的Blackcoin地址，然而，这两条链是不相关的，而且交易也不可撤销，这个过程并没有提供防止交易一方不履行他们相关交易的防护措施。Atom跨链交易在不需要第三方的前提下解决了这个问题。

原理：

Alice（initiator，发起方）创建一个交易合约，生成一个secret，然后将一定数量的Bitcoin打到交易合约中，Bob（participant，参与方）只要获知了secret就可以赎回合约输出的币。如果在交易被打包之后，一段时间（通常是48小时）到期，合约的输出没有被Bob赎回，那么合约的输出会退还给Alice。

在Alice发送Bitcoin到合约地址后，Alice需要发送相应的secret hash给Bob，同样，Bob需要发送Blackcoin到该secret hash的相应合约地址。

Alice此时可以用secret赎回Bob发送的Blackcoin。

在Alice赎回Bob发送的Blackcoin的赎回交易中，会暴露secret，此时Bob可以从该交易中提取secret。

Bob利用secret赎回Alice发送的Bitcoin。

详细操作：

1.Alice执行initiate：

./initiate

Query is: {"id":1,"jsonrpc":"2.0","method":"initiate","params":{"amount":1.10,"cointype":"blackcoin","refundaddress":"BLb2fqVG5fd5Aez7zRT44js61V1EmwjTv8","rpcaddress":"192.168.10.184","rpcpassword":"BUG7UEbUkDTnETVnUicmc66iYqQtUuoHhkhwv9pDGphT","rpcport":"55650","rpcusername":"ccrpc","themaddress":"BAJhpjz2e4n7uEagVoXKTAJtnjeeeqFQit"}}

Received: {"Contract address":"bHTUWFDdNZXou6q99iBRwodChnyVdZCmf2","Contract hex":"63a6145a239735fdf216495505a010a7cd69e19a0533cc8876a914403b3c4499be6a5a2e6a535ef8a5970852bfc6da6704970e4f5ab17576a914b102e1819a1e3bfe5993090f237a16cf153b7a3c6888ac","Refund address":"BLb2fqVG5fd5Aez7zRT44js61V1EmwjTv8","Secret":"efb8a37134e254d76731d2623d31f59da5c58c2e1f502dd0a35dbbddce3ed2ac","Secret hash":"5a239735fdf216495505a010a7cd69e19a0533cc","txid":"0c003cd617a7c34fe2791a9c0e760603e0130e70a88a8c24e125ebf4d100e380"}

2.Bob执行participate：

./participate

Query is: {"id":1,"jsonrpc":"2.0","method":"participate","params":{"amount":1.30,"cointype":"bitcoin","refundaddress":"18vmBDq57ZSvjzXKhk375BwRGSZ7eppAT7","rpcaddress":"192.168.10.184","rpcpassword":"BUG7UEbUkDTnETVnUicmc66iYqQtUuoHhkhwv9pDGphT","rpcport":"8332","rpcusername":"bitcoin","secrethash":"5a239735fdf216495505a010a7cd69e19a0533cc","themaddress":"14GVJY42rwMKYQFM6Nkpn8hvC5UPky8q1B"}}

Received: {"Contract address":"32MhjMa1dpG1J6YQCL7rtr7xKMJZJh1x8m","Contract hex":"63a6145a239735fdf216495505a010a7cd69e19a0533cc8876a91423d63e0c6b275bd3d6332c426c2db8c5970834a76704c3c74d5ab17576a91456f3cd8c15d582f370e70f00bb8fe65a1d2edc756888ac","Refund address":"18vmBDq57ZSvjzXKhk375BwRGSZ7eppAT7","txid":"261c2476cfa849cf376d487c26ee6e08cdf5d609f0e5017b929fd7696f8914b0"}

3.Alice赎回Blackcoin：

./redeembcoin

Query is: {"id":1,"jsonrpc":"2.0","method":"redeem","params":{"cointype":"bitcoin","contract":"63a6145a239735fdf216495505a010a7cd69e19a0533cc8876a91423d63e0c6b275bd3d6332c426c2db8c5970834a76704c3c74d5ab17576a91456f3cd8c15d582f370e70f00bb8fe65a1d2edc756888ac","redeemaddress":"16FEXyhpXwAhU1RCVS874H3q3mKWRE2Fgj","rpcaddress":"192.168.10.184","rpcpassword":"BUG7UEbUkDTnETVnUicmc66iYqQtUuoHhkhwv9pDGphT","rpcport":"8332","rpcusername":"bitcoin","secret":"efb8a37134e254d76731d2623d31f59da5c58c2e1f502dd0a35dbbddce3ed2ac","txid":"261c2476cfa849cf376d487c26ee6e08cdf5d609f0e5017b929fd7696f8914b0"}}

Received: {"id":1,"jsonrpc":"2.0","result":"success","txid":"7a87c6267f980591710e806257f7e05e8b309231dd83bf60d303998469a8a42a"}

4.Bob提取secret：

./extractSecret

Query is: {"id":1,"jsonrpc":"2.0","method":"extractsecret","params":{"cointype":"bitcoin","rpcaddress":"192.168.10.184","rpcpassword":"BUG7UEbUkDTnETVnUicmc66iYqQtUuoHhkhwv9pDGphT","rpcport":"8332","rpcusername":"bitcoin","secrethash":"5a239735fdf216495505a010a7cd69e19a0533cc","txid":"7a87c6267f980591710e806257f7e05e8b309231dd83bf60d303998469a8a42a"}}

Received: {"id":1,"jsonrpc":"2.0","result":"success","secret":"efb8a37134e254d76731d2623d31f59da5c58c2e1f502dd0a35dbbddce3ed2ac"}

5.Bob赎回Bitcoin

./redeemacoin

Query is: {"id":1,"jsonrpc":"2.0","method":"redeem","params":{"cointype":"blackcoin","contract":"63a6145a239735fdf216495505a010a7cd69e19a0533cc8876a914403b3c4499be6a5a2e6a535ef8a5970852bfc6da6704970e4f5ab17576a914b102e1819a1e3bfe5993090f237a16cf153b7a3c6888ac","redeemaddress":"BGaMVfYQZLnmu6Hhh2WLaF6E1sspZjMNnk","rpcaddress":"192.168.10.186","rpcpassword":"J6G5vvbmnqDZV5RWnrhFk8pjPZwERhjvCKMbnQ2Jq3E5","rpcport":"55650","rpcusername":"ccrpc","secret":"efb8a37134e254d76731d2623d31f59da5c58c2e1f502dd0a35dbbddce3ed2ac","txid":"0c003cd617a7c34fe2791a9c0e760603e0130e70a88a8c24e125ebf4d100e380"}}

Received: {"id":1,"jsonrpc":"2.0","result":"success","txid":"7c4587d5f5b6f64b108ac6924a353ad8b14063e24580a8ff00f08fc9b8b3b127"}

交易脚本：

OP\_IF OP\_RIPEMD160 29c36b8dd380e0426bdc1d834e74a630bfd5d111（secrethash，20bytes） OP\_EQUALVERIFY OP\_DUP OP\_HASH160 ebcf822c4a2cdb5f6a6b9c4a59b74d66461da581（theirpubkeyhash， 20bytes） OP\_ELSE d728bd59 OP\_CHECKLOCKTIMEVERIFY OP\_DROP OP\_DUP OP\_HASH160 06fb26221375b1cbe2c17c14f1bc2510b9f8f8ff（mypubkeyhash，20bytes） OP\_ENDIF OP\_EQUALVERIFY OP\_CHECKSIG

签名：

对方赎回：

<their sig> <their pubkey> <secret> OP\_TRUE

退还己方：

<my sig> <my pubkey> OP\_FALSE