A Bitcoin FAQ

andytoshi
19HdsuYDg1Cb3J4ZhgZeqb2pk3dp9GcNTk

1 Transactions

1.1 Where are the coins?

Balances in the bitcoin system are tracked by chains (actually trees) (actually directed acyclic graphs) of linked transactions, starting with an original "coinbase" transaction which grants coins from nowhere to miners as a reward for securing the network.

There is nowhere that coins themselves are stored; there are only trees which may be extended at the leaves. Each leaf node (called a *utxo* internally) has a value associated to it. Your "balance" is the sum of all leaf nodes which you have authority to extend from.

1.2 How is authority determined?

The leaf nodes are constructed so that they can only be extended by digitally signing them. Anyone with the right signing key may extend a leaf, "spending" the money. When you send money to someone, you create a new leaf node which can only be spent by signing with one of their keys.

1.3 So what are addresses then?

Addresses are opaque identifiers used as destinations for bitcoin transactions. (They are never used as sources; so while typical transactions have a notion of a "receiving address" there is no such thing as a "sending address".) From a user perspective, there is **no meaning to addresses beyond this**.

Within the bitcoin network, addresses are used to identify signing keys. Each signing key is composed of two parts, a *public* and a *private* part. Addresses are derived from the public part, and are used within leaf nodes to verify that the signing key used to spend them is the right one.

The act of signing, on the other hand, uses the private part of the key. This is never exposed to the network.

As addresses are in 1-1 correspondence with signing keys, it is advisable to never reuse addresses. Reusing addresses amounts to reusing signing keys, potentially weakening the security of your keys for no benefit to anybody.

1.4 So how is the balance of an address calculated?

Addresses have no balance. They are only used to verify signing authority. This is because there is no such thing as a "sending address" in a bitcoin transaction.

Currently most leaf nodes require only one signature, and have one address associated to them. More exotic leaf nodes may require more than one signature, or use signatures without associated

addresses. Such exotic transactions are possible, do happen in the network, and as infrastructure matures they will become more common.

If you have coins, i.e. spending authority for some leaves in the network, you have no reason to believe that the addresses associated to those leaves' parents (if any such addresses exist) has anything to do with the sender. Nor may you assume that this address can be (or ever could be) safely spent to.

2 Wallets

2.1 What is a wallet?

A wallet is a store of value, typically a collection of signing keys. The reference client stores these keys in a file called wallet.dat; online wallets and exchanges store client balances in a database, which is (hopefully) completely unrelated to key management.

There is also such a thing as a "paper wallet", in which signing keys, or material needed to derive signing keys, are printed or physically imprinted on some medium for permanent storage.

Wallets are not addresses. Wallets are not accounts. Wallets are not balances.

2.2 What is in wallet.dat?

This primarily contains signing keys. It also contains metadata about transactions. It should be encrypted, as anyone in possession of your wallet is also in possession of your signing authority.

It can and should be copied and backed up. It does not "contain coins"; copying a wallet does not duplicate value. But deleting the last copy of a signing key does destroy value. Don't let this happen.

2.3 What are accounts?

In many clients and online wallets, there exist a feature called "accounts", which splits your available balance into various buckets.

Addresses have corresponding accounts: money sent to these addresses will increment the balance of the corresponding account. On the other hand, accounts do not have associated addresses. Specifically, spending money from an account decrements the balance of that account, but does not restrict which available leaf nodes are used. (Remember, there is no such thing as a sending address. It makes no sense for send-from-account transactions to only spend "from" the associated address.)

Similarly, moving value between accounts is purely an accounting activity. It does not touch the network. It has nothing to do with addresses.

Because they are merely an accounting tool, it is possible for accounts to have negative balances. The network itself never works with negative numbers.