

Forum:[Hack Forums](#)

Thread: [Split wallet?](#)

Armada - June 12, 2015, 7:51 pm

So, Ive been messing about in crypto for a while now and come to wonder this.

Let me lay out a scenario, and I assume one will answer...

I have wallet "A"

Wallet "A" has 5 BTC in it

I CLONE (Copy) wallet file to say a flash drive, for backup.

What happens when I spend say 2.5 BTC from Wallet "A"

Does my clones wallet "A(1)" absorb the change in my block chain?

I assume so, but my question is HOW?

\\Edit:

What is stopping me from cloning a 5 BTC wallet numerous times?

HOW does BTC handle this, and why?

Niko - June 12, 2015, 8:00 pm

I believe what stops it is that every transaction is recorded and every little bit of BTC is accounted for. Therefor denying any currency not accounted for.

Say if Wallet A Gets Copied It can still be used, but they are still in sync. Thats the whole tedious syncing thing the wallet has to do.

afk0 - June 12, 2015, 8:01 pm

Bro I think you just figured out away to make infinite btc wtf???

Niko - June 12, 2015, 8:02 pm

(Jun 12, 2015 08:01 PM)?aron Wrote: [\[CITE\]](#) Bro I think you just figured out away to make infinite btc wtf???

If someone had done that, it would have been patched a real long time ago. I believe that is one reason why the syncing takes longer.

Armada - June 12, 2015, 8:03 pm

(Jun 12, 2015 08:01 PM)?aron Wrote: [\[CITE\]](#) Bro I think you just figured out away to make infinite btc wtf???

The blockchIN lone has verification, my wonder is if I introduce Wallet "A" (Old) to the sequence, how does it sync?

HOW does the blockchain verify from new from old?

afk0 - June 12, 2015, 8:03 pm

(Jun 12, 2015 08:02 PM)LegitBytes Wrote: [\[CITE\]](#) If someone had done that, it would have been patched a real long time ago. I believe that is one reason why the syncing takes longer.

dude it works I just doubled a whole bitcoin omg

Armada - June 12, 2015, 8:06 pm

This thread went full retard before I even got a hint.... awesome...

F-Nuke - June 12, 2015, 8:41 pm

You can copy your wallet numerous time. It is also a good practice to keep your wallet backed up always (just incase your hard disk gets corrupted or anything).

There are no bitcoins. Just transactions. The blockchain is a public ledger of which has a record of every transaction made with bitcoin (not to be confused with the website blockchain.info which provides an easy way to check the transactions with the blockchain. It also provides wallets, merchant APIs and other services, but that's another story).

So if you spend a few coins from wallet 'a', those coins are accounted for in the blockchain. So when you open up the clone of wallet 'a', it gets synchronised with the blockchain automatically and since there is a record of you spending a few bitcoins in the blockchain, you can no longer spend those particular 'already spent' blockchain. Even if you create hundreds of even thousands of wallets, they all get synchronised and you cannot spend those spent coins again.

Wallet Synchronisation is basically downloading the whole blockchain on to your computer and checking it for your transactions. If you use the original Bitcoin-Qt client, it downloads the whole blockchain onto your computer to check the transactions from/to your address. Since the blockchain is very big now and continues to grow (it is about 35,000 MB at the moment). So it is a bit of a hassle. Thus newer wallets like Electrum, Multibit etc., check your transactions with a Bitcoin full node, so you don't have to download the blockchain on to your computer.

I'm typing this from my phone. Let me know if you want me to elaborate or explain anything else.

Hope I helped ?

(Jun 12, 2015 08:01 PM)?aron Wrote: [\[CITE\]](#) Bro I think you just figured out away to make infinite btc wtf???

(Jun 12, 2015 08:03 PM)?aron Wrote: [\[CITE\]](#) dude it works I just doubled a whole bitcoin omg These posts coming from a 'Crypto' member, people expect them to be of a higher quality, at least in the 'Cryptocurrency' section.

Armada - June 12, 2015, 8:49 pm

(Jun 12, 2015 08:41 PM)F-Nuke Wrote: [\[CITE\]](#) You can copy your wallet numerous time. It is also a good practice to keep your wallet backed up always (just incase your hard disk gets corrupted or anything).

There are no bitcoins. Just transactions. The blockchain is a public ledger of which has a record of every transaction made with bitcoin (not to be confused with the website blockchain.info which provides an easy way to check the transactions with the blockchain. It also provides wallets, merchant APIs and other services, but that's another story).

So if you spend a few coins from wallet 'a', those coins are accounted for in the blockchain. So when you open up the clone of wallet 'a', it gets synchronised with the blockchain automatically and since there is a record of you spending a few bitcoins in the blockchain, you can no longer spend those particular 'already spent' blockchain. Even if you create hundreds of even thousands of wallets, they all get synchronised and you cannot spend those spent coins again.

Wallet Synchronisation is basically downloading the whole blockchain on to your computer. If you use the original Bitcoin-Qt client, it downloads the whole blockchain onto your computer to check the transactions from/to your address. Since the blockchain is very big now and continues to grow (it is

about 35,000 MB at the moment). So it is a bit of a hassle. Thus newer wallets like Electrum, Multibit etc., check your transactions with a Bitcoin full node, so you don't have to download the blockchain on to your computer.

I'm typing this from my phone. Let me know if you want me to elaborate or explain anything else.

Hope I helped ?

These posts coming from a 'Crypto' member, people expect them to be of a higher quality, at least in the 'Cryptocurrency' section.

So, ultimately, I own wallet "A", being all block chain info is public record, when I check in with wallet "A" regardless of state, it verifies with public block chain sequence to account to everything associated with this specific #

Correct?

F-Nuke - June 12, 2015, 8:54 pm

(Jun 12, 2015 08:49 PM)A?mªDa Wrote: [\[CITE\]](#) So, ultimately, I own wallet "A", being all block chain info is public record, when I check in with wallet "A" regardless of state, it verifies with public block chain sequence to account to everything associated with this specific #

Correct?

Yes, it can be simply put in that way. Every wallet you clone has the same private/public key as the original wallet. So it always gets sync'd with your latest transactions and only shows your unspent bitcoins.

Armada - June 12, 2015, 8:54 pm

(Jun 12, 2015 08:41 PM)F-Nuke Wrote: [\[CITE\]](#) You can copy your wallet numerous time. It is also a good practice to keep your wallet backed up always (just incase your hard disk gets corrupted or anything).

There are no bitcoins. Just transactions. The blockchain is a public ledger of which has a record of every transaction made with bitcoin (not to be confused with the website blockchain.info which provides an easy way to check the transactions with the blockchain. It also provides wallets, merchant APIs and other services, but that's another story).

So if you spend a few coins from wallet 'a', those coins are accounted for in the blockchain. So when you open up the clone of wallet 'a', it gets synchronised with the blockchain automatically and since there is a record of you spending a few bitcoins in the blockchain, you can no longer spend those particular 'already spent' blockchain. Even if you create hundreds of even thousands of wallets, they all get synchronised and you cannot spend those spent coins again.

Wallet Synchronisation is basically downloading the whole blockchain on to your computer and checking it for your transactions. If you use the original Bitcoin-Qt client, it downloads the whole blockchain onto your computer to check the transactions from/to your address. Since the blockchain is very big now and continues to grow (it is about 35,000 MB at the moment). So it is a bit of a hassle. Thus newer wallets like Electrum, Multibit etc., check your transactions with a Bitcoin full node, so you don't have to download the blockchain on to your computer.

I'm typing this from my phone. Let me know if you want me to elaborate or explain anything else.

Hope I helped ?

These posts coming from a 'Crypto' member, people expect them to be of a higher quality, at least in the 'Cryptocurrency' section.

So because of the global "cloud" of crypto and the block chains, this is why this process is possible. Im still fubar on my copy theory, I need to know how crypto currency prevents the duplication...

Niko - June 12, 2015, 9:01 pm

Kind of repeating what I said, All bitcoin ever made is accounted for. I will try to make a shitty diagram...

Block > Miners > Wallets > Cloud > More Wallets

Using my address as an example >Wallet A (1LC3R1UaAcgawBCo1guZ9ihATBMhcaEeMa) Has 0.0034

Wallet Gets copied Wallet1<>WalletCopy

Both wallets have the same address so instead of cloud seeing Wallet1 Sent x BTC it sees 1LC3R1UaAcgawBCo1guZ9ihATBMhcaEeMa sent x BTC.

This way all Bitcoin is accounted for and there is no way to "Cheat" it.

Hopefully that clears things up.

Armada - June 12, 2015, 9:04 pm

(Jun 12, 2015 09:01 PM)LegitBytes Wrote: [\[CITE\]](#) Kind of repeating what I said, All bitcoin ever made is accounted for. I will try to make a shitty diagram...

Block > Miners > Wallets > Cloud > More Wallets

Using my address as an example >Wallet A (1LC3R1UaAcgawBCo1guZ9ihATBMhcaEeMa) Has 0.0034

Wallet Gets copied Wallet1<>WalletCopy

Both wallets have the same address so instead of cloud seeing Wallet1 Sent x BTC it sees 1LC3R1UaAcgawBCo1guZ9ihATBMhcaEeMa sent x BTC.

This way all Bitcoin is accounted for and there is no way to "Cheat" it.

Hopefully that clears things up.This some what confirms my original suspicion. ?

Im not looking for a way to cheat the system, I just want to understand how it accounts for itself. ?

F-Nuke - June 12, 2015, 9:12 pm

(Jun 12, 2015 08:54 PM)A?mªDa Wrote: [\[CITE\]](#) So because of the global "cloud" of crypto and the block chains, this is why this process is possible.

Im still fubar on my copy theory, I need to know how crypto currency prevents the duplication...

Well you see a transaction gets 'confirmed' ? Confirmations are basically validating a transaction by thousands of miners across the world. Even if you edit the blockchain present in your computer (which is near impossible because of every block mined has its own block number and hash which is unique to itself) and send bitcoins, your transaction will not get confirmed and it will not go through. But as I said, it is near impossible to edit or put duplicate entries into the blockchain.

(Jun 12, 2015 09:01 PM)LegitBytes Wrote: [\[CITE\]](#) Kind of repeating what I said, All bitcoin ever made is accounted for. I will try to make a shitty diagram...

Block > Miners > Wallets > Cloud > More Wallets

Using my address as an example >Wallet A (1LC3R1UaAcgawBCo1guZ9ihATBMhcaEeMa) Has 0.0034

Wallet Gets copied Wallet1<>WalletCopy

Both wallets have the same address so instead of cloud seeing Wallet1 Sent x BTC it sees 1LC3R1UaAcgawBCo1guZ9ihATBMhcaEeMa sent x BTC.

This way all Bitcoin is accounted for and there is no way to "Cheat" it.

Hopefully that clears things up.

"No way" is a bold statement. There are several ways to do a double spend. But they will eventually get detected. There is race attack, Finney attack and the infamous 51% attack (which unfortunately happened to our very own OmniCoin). But as I said, they will get detected and those fake coins will be invalidated. But you need lots and lots of mining/computing power to do a 51% attack on a large coin like bitcoin.

Armada - June 12, 2015, 9:19 pm

(Jun 12, 2015 09:12 PM)F-Nuke Wrote: [\[CITE\]](#) Well you see a transaction gets 'confirmed' ? Confirmations are basically validating a transaction by thousands of miners across the world. Even if you edit the blockchain present in your computer (which is near impossible because of every block mined has its own block number and hash which is unique to itself) and send bitcoins, your transaction will not get confirmed and it will not go through. But as I said, it is near impossible to edit or put duplicate entries into the blockchain.

"No way" is a bold statement. There are several ways to do a double spend. But they will eventually get detected. There is race attack, Finney attack and the infamous 51% attack (which unfortunately happened to our very own OmniCoin).

"Thousands of miners"

- Thus my confusion. If My waller is already confirmed for a specific block chain (\$) how does the system differentiate my original wallet from a clone of the same block chain?

I take "Wallet "A" and it has BTC, I spend 3.5 BTC from wallet "A"
Before I spent this, I duplicated the wallet file however.

How does BTC sync to correct from such obvious flaws?

F-Nuke - June 12, 2015, 9:28 pm

(Jun 12, 2015 09:19 PM)A?mªĐa Wrote: [\[CITE\]](#) "Thousands of miners"
- Thus my confusion. If My waller is already confirmed for a specific block chain (\$) how does the system differentiate my original wallet from a clone of the same block chain?

I take "Wallet "A" and it has BTC, I spend 3.5 BTC from wallet "A"
Before I spent this, I duplicated the wallet file however.

How does BTC sync to correct from such obvious flaws?

Read my first post again.

(Jun 12, 2015 08:41 PM)F-Nuke Wrote: [\[CITE\]](#) There are no bitcoins. Just transactions.

You duplicated your wallet. Not the transactions. And wallets are not confirmed. Transactions are. Do you understand SQL? I can give you a better example using a few SQL statements.

Armada - June 12, 2015, 9:56 pm

(Jun 12, 2015 09:28 PM)F-Nuke Wrote: [\[CITE\]](#) Read my first post again.

You duplicated your wallet. Not the transactions. And wallets are not confirmed. Transactions are. Do you understand SQL? I can give you a better example using a few SQL statements.
Thanks for the confirmation ?