

Forum:[Hack Forums](#)

Thread: [Physical Omnicoin Poll](#)

FantaŠec - April 15, 2015, 8:46 am

I was wondering which people would purchase, please vote in the poll and respond with suggestions. Please note, the keys stored on the database would be encrypted with a key inside the coin and cannot be decrypted any other way, and cannot be accessed by any of the administrators (including myself) and in addition, would have PCI-DSS compliant security, with SSL 128 bit encryption.

Option 1:

Physical coin with private key on the inside

Option 2:

Physical coin sealed with a link on the inside to redeem it on website to get the key. Also comes with the ability to check if it has been redeemed yet and a hologram sticker to guarantee it has not been copied, printed, or x-rayed.

Option 3:

Able to buy both

Abraham Lincoln - April 15, 2015, 8:54 am

From a security standpoint option 1 is much, much safer. The idea of a physical wallet is that all the information needed to receive and spend coins is stored in an offline, physical manner. Extremely safe. (Although when casting the coins the private keys are accessible by the admins)

Option 2 has many risks. Servers can get hacked, disks can become corrupted, admins can go rogue, etc. You have to have full trust that when you want to claim your OMC the servers will still be there and that the private keys haven't been messed with. And the ability to see if a coin has been opened already can be exploited to scam users.

The Scarabian - April 15, 2015, 8:57 am

I like option 1 a lot. It would also be cool to have the address on the face of the coin.

Abraham Lincoln - April 15, 2015, 8:59 am

(Apr 15, 2015 08:57 AM)Manuel Neuer Wrote: [\[CITE\]](#) I like option 1 a lot. It would also be cool to have the address on the face of the coin.

Both options have the public key (receiving address) on the face of the coin.

The difference is in the way the private key (used for sending) is stored.

The Scarabian - April 15, 2015, 9:01 am

(Apr 15, 2015 08:59 AM)Abraham Lincoln Wrote: [\[CITE\]](#) Both options have the public key (receiving address) on the face of the coin.

The difference is in the way the public key (used for sending) is stored.

On your last sentence did you mean private key?

FantaŠec - April 15, 2015, 9:02 am

(Apr 15, 2015 08:59 AM)Abraham Lincoln Wrote: [\[CITE\]](#) Both options have the public key (receiving address) on the face of the coin.

The difference is in the way the public key (used for sending) is stored.
Private key*

Option 2 will have no admins being able to access it, on a RAID 10 drive array, with PCI-DSS compliant security and 512bit encryption only decryptable with a key on the coins inside.

Abraham Lincoln - April 15, 2015, 9:03 am

(Apr 15, 2015 09:01 AM)Manuel Neuer Wrote: [\[CITE\]](#) On your last sentence did you mean private key?

Yea, I did. My bad.

(Apr 15, 2015 09:02 AM)FantaŠec Wrote: [\[CITE\]](#) Option 2 will have no admins being able to access it, on a RAID 10 drive array, with PCI-DSS compliant security and 512bit encryption only decryptable with a key on the coins inside.

Even if the admins don't have access they can still get access. You don't just encrypt a database and throw away the key. It's impossible, actually, if you want to still be able to access the data.

Moen - April 15, 2015, 11:56 am

It could be a secret link and a special password included to a website created by admin. On that website The user can request their OMC sent to their wallet.

telling the customer to add this private key to his wallet might be a problem in itself.

1. Admin might not delete the private keys and in two years he will check if there are any OMC on them and take.

2. The customer might have some problem adding the keys to their wallet.

3. When the customer sends money the part of the money that is not supposed to be sent will be transferred to a random address in the customer's wallet. Having in mind point 1. here admin might even take some more OMC.

FantaŠec - April 15, 2015, 1:58 pm

(Apr 15, 2015 11:56 AM)Moen Wrote: [\[CITE\]](#) It could be a secret link and a special password included to a website created by admin. On that website The user can request their OMC sent to their wallet.

telling the customer to add this private key to his wallet might be a problem in itself.

1. Admin might not delete the private keys and in two years he will check if there are any OMC on them and take.

2. The customer might have some problem adding the keys to their wallet.

3. When the customer sends money the part of the money that is not supposed to be sent will be transferred to a random address in the customer's wallet. Having in mind point 1. here admin might even take some more OMC.

On option 1, no one will have the private key until the coin is opened.

Sniper - April 15, 2015, 2:36 pm

Just in case this sounds familiar to anyone, fanta is working on this for me as I have 0 spare time at the moment. If you have any questions or concerns, or you may want something designed/manufactured/3D modelled feel free to contact me.

FantaŠec - April 15, 2015, 2:40 pm

(Apr 15, 2015 02:36 PM)Sniper Wrote: [\[CITE\]](#) Just in case this sounds familiar to anyone, fanta is working on this for me as I have 0 spare time at the moment. If you have any questions or concerns, or you may want something designed/manufactured/3D modelled feel free to contact me.

Nigga, this is NOT your advertising thread, nonono ?

Doctor Blue - *April 15, 2015, 3:36 pm*

The coin could hold one of two private keys required to spend a P2SH input. That way the balance can be checked on a blockchain explorer, and neither party would be able to spend the coins without the other's private key. Of course this requires swapping public keys/addresses prior to printing the coin.

My favourite option, however, would be not to load anything on it at all. I can imagine it would be cool for decoration, but it's just impractical to actually have coins on them.