Project OtherCoin

Version: *1.1*
Date: *03/08/2015*
Author: *Razvan Dragomirescu (razvan.dragomirescu@veri.fi)*

What is OtherCoin?

OtherCoin is an off-chain Bitcoin payment system based on a tamper-resistant smartcard in microSD form factor. OtherCoin works by securely generating, storing and transmitting Bitcoin **private keys** between parties. Private keys are never revealed to either the sender or the receiver, they can either be used directly in the Bitcoin protocol to sign transactions or securely transmitted to another OtherCoin user. Each OtherCoin smartcard guarantees that the key has either been securely generated by itself or has been received over a secure channel from a similar OtherCoin, with the same restrictions.

Advantages

No trusted third party server – information is secured by each smartcard, there is no central server to be trusted with transaction details or that the system depends on for its operation. The only trusted authority is the issuer of the OtherCoin card – it guarantees that the software running on the smartcard has not been tampered with and that it follows the OtherCoin system rules. Even if this authority goes out of business, any of the OtherCoin cards it has issued can still be used indefinitely. Private keys can always be extracted from the card and used on the Bitcoin network (but will obviously no longer be available for direct off-chain payments).

Privacy/Anonimity –no information is broadcast or registered in the blockchain. Parties communicate directly and are only identified by the public keys of their OtherCoin smartcards. The public keys are sent in an encrypted form between smartcards to preserve privacy.

Speed – No confirmation is needed, the recipient can immediately check the blockchain for funds associated to the newly received private key. Funds are usually already confirmed (more than 6 blocks deep) since the private keys are usually older than 1 hour.

Double spend protection – the recipient gets a private key that is **guaranteed to have never been used** and that is **guaranteed to be immediately deleted** by the sender. The recipient can then post the funds to himself via the blockchain or hold the private key in the OtherCoin smartcard and use it on the blockchain at a later time or transfer it off-chain via OtherCoin to another user.

No transaction fees – Since the blockchain and the Bitcoin network are not involved in the transactions, there are no fees, regardless of the value of the transactions

Less load on the Bitcoin blockchain – transactions are only recorded by the sender and the receiver, no Internet entity needs to know or do anything about them

Instant access to funds – you do not have to deposit the funds with a third party or convert them into an alt-coin denomination. OtherChain moves Bitcoin private keys that can always (and instantly) be used on the blockchain. You do not have to „withdraw" your coins from the system, they are always available. In an off-chain payment, the OtherCoin card simply guarantees that the private key has never been revealed or used to sign a transaction.

What it does

The OtherCoin smartcard is intentionally kept very simple and **only offers 2 basic operations**:

1. ***Bitcoin private key generation*** - securely generate and store a private key (inside a tamper-resistant chip) and release the associated public key to the user
2. ***Establish an encrypted and authenticated channel to another OtherCoin*** smartcard and securely transfer a private key, then delete it from its own storage

What it doesn't do

1. ***It does not sign Bitcoin transactions***. Othercoin cannot generate a Bitcoin signature or authorize a transaction
2. ***It cannot communicate to the outside world by itself***. It only interacts with a software wallet running on the phone or computer the card is inserted in. It cannot establish connections to the Internet or send data anywhere (it has no wireless capabilities either).
3. ***It has no access to your private keys or Bitcoin addresses***. The software wallet running on the computer or smartphone combines the public key that OtherCoin has generated with another public key that it has generated internally to create a new Bitcoin address (similar to the process used to have an external server generate a vanity Bitcoin address for the user). The wallet holds half of the private key (the one it has generated) but has no access to the other half (generated on-card). ***This is the essence of the security of OtherCoin, neither the wallet nor the card have access to the full private key and only the wallet knows the actual public key corresponding to the Bitcoin address.***

Why should I use OtherCoin?

OtherCoin offers all the advantages of off-chain Bitcoin transactions (https://en.bitcoin.it/wiki/Off-Chain_Transactions) with none of the downsides. While it does depend on an issuer to certify the cards initially (ensure that they run the proper firmware on the correct hardware), all subsequent transactions no longer involve the issuer and are not registered in the blockchain or in any other location. This allows for truly anonymous and private transactions, especially in face-to-face situations. At the time the private keys are used to sign a Bitcoin transaction, they might have exchanged hands hundreds of times privately and securely via OtherCoin but the blockchain will only see a single transaction from the final recipient of the funds.

Balance certification and SPV proofs

The current version of the OtherCoin Android application uses a centralized server (based on blockchain.info's API) to retrieve the balance associated with a given Bitcoin address. This is in the process of being replaced by a pure blockchain-based solution using SPV proofs that will remove the last dependency on a centralized service (blockchain.info's API).

Each user will download an up to date set of Blockchain headers but no actual transactions or full blocks. Whenever a key is funded, the application will start listening for a full block containing the transaction. As soon as the transaction is included in a block, the application will store the serialized transaction as well as the Merkle branch connecting that transaction to the block it appeared in. This data (**transaction** + **Merkle branch** + **block hash**) will be transferred between parties as proof of payment. The recipient only has to check the block hash and the transaction outputs, then confirm that the Merkle branch puts the transaction in the given block.

PIN-based escrow

The OtherCoin system offers a primitive escrow mechanism that allows the payer to prevent the payee from spending the funds associated with an OtherCoin key until the payee actually performs the services or ships the goods. When a key is transferred, it is internally encrypted with a random 4 digit PIN. The PIN is displayed to the payer at the time of the key transfer.

The payee can receive the key and verify the funds but it will show as „locked" until the 4 digit PIN is entered. In its locked state, the key is unusable to both parties (payer has the PIN but not the key, payee has the key but not the PIN), so they have to agree in order to spend the funds (or lose them altogether).

Supported hardware and protocols

As of May 2015, the OtherCoin smartcard application runs on any NXP JCOP or Infineon secure elements. We have confirmed it to be working on the microSD secure elements sold by Device

Fidelity (NXP), Swissbit (Infineon) and Certgate (NXP), the Yubikey Neo by Yubico (NXP) and the Famoco FX100 dedicated Android device (embedded secure element by NXP).

Communication between parties is supported over NFC, Bluetooth, QR codes and TCP/IP (via relay server). You can mix and match protocols, even during the same transaction (for instance send the initial handshake over Bluetooth but receive the payment over NFC or as a QR code to scan).

Frequently Asked Questions

1. ***What happens if I lose my OtherCoin smartcard? Do I lose all my funds?***
   In the initial release, losing the OtherCoin smartcard means losing access to the private keys that it stores. Since the keys are not duplicated anywhere, this means you lose access to the funds.
   Future versions of OtherCoin will allow users to operate an OtherCoin card remotely (over a secure Internet connection). The OtherCoin could then be left at home (plugged into a computer), safe from physical theft. A classical private key backup should be used for the private key parts that the smartphone wallet has generated since they are needed in addition to the OtherCoin parts to generate the real private keys used in transactions.

2. ***Will it be open source?***
   Probably not. The main reason for this is that most of the Elliptic Curve crypto functionality used in the OtherCoin firmware is only available as a set of proprietary crypto functions by the secure chip manufacturers (NXP and Infineon). We are bound by NDAs and contractual terms with them to not expose any proprietary and confidential information and that covers the crypto functionality inside the OtherCoin.
   However, as noted above, the OtherCoin has no access to your keys, it does not sign transactions or communicate to the outside world by itself in any way. Its only purposes are to generate Bitcoin keys, keep them safe and certify that they haven't been revealed or securely send them to another card.

3. ***If someone steals my card, will they be able to steal my funds?***
   No. First of all, all smartcard operations are protected by a 6 digit PIN code. Second, the OtherCoin only stores the private keys it has generated. These need to be combined with the private keys generated on the wallet to determine the actual private keys and Bitcoin addresses used. So they would need to steal your smartphone (or computer) as well.

4. *Will you steal my funds? How can I trust you / the OtherCoin card?*

No we won't. And you don't need to trust the card since it never has access to your actual keys or can sign away any of your Bitcoin funds. It is simply a helper for your wallet, a way to allow it to safely send private keys (and the associated funds) to another party, without going through the Blockchain or another server/service. The OtherCoin never touches your funds and never communicates to the outside world. It cannot leak or transfer any information, it is under the full control of the wallet application and the device it is inserted into. Think of it as a „Bitcoin off-chain server in your pocket".

5. *Can I try the service before I buy the OtherCoin card?*

We plan to offer an „OtherCoin in the cloud" service that would act as a remote OtherCoin card hosted on secure Internet server. It would offer the exact same functions and API as the real card but it will require a connection to our server. Once you are ready to migrate to the more secure physical OtherCoin card, you can purchase one and transfer your keys to it using the OtherCoin protocol, just as you would with two physical OtherCoin cards.

6. *Who are you?*

My name is Razvan Dragomirescu, I am a developer/entrepreneur based in Romania. I am also the author of the first offline QR-code based Bitcoin wallet (VisualBTC – www.visualbtc.com), the VeriFi phone transaction verification system (www.veri.fi), the miniature AutoMonitor Jump 3G router (http://www.automonitor.net/jump/), the first background sound generator for phone calls – SounderCover (http://www.nytimes.com/2004/04/22/technology/news-watch-audio-sorry-i-can-t-talk-now-they-re-ready-for-my-root-canal.html) and a bunch of other stuff (Windows Mobile file sharing - http://www.theregister.co.uk/2004/06/03/pocket_rendezvous/ , Node.JS library for Iridium satellite comms - http://rockblock.rock7mobile.com/?p=332).

I own a small software development company called Cayenne Graphics SRL, we've been in business since 2002, focusing mostly on mobile applications.

You can reach me at razvan.dragomirescu@veri.fi .

Bitcoin donations are welcome, you can send them to
1Razvan4KEK2q5DNxemvsHwGncF1T3NqR