e-money

Domenico Oricchio

June 25, 2021

Abstract

A secure money transfer in a nation, using files, and without mining to reduce the energy consumption.

I think that it is possible to use use digital currency (e-money): a file that can be exchanged with other like paper-money without bank account[1], only distribuited mail-server[2] with e-mail address[3].

The idea is to use a Simple Mail Transfer Protocol to send some e-money files to the receiver through a central bank: $sender \rightarrow central\_bank \rightarrow receiver$; these files have a name that represent the money value, and a content[4]: for example $0\_01\_AB12598.mny$ is 1 cent of eur with serie AB12598 and $1\_00\_CD482637.mny$ is a eur.

The content of the e-money are some data crypted with open gpg[5]; the bank have a public key and private key for communication, and the person have a public and private key to communicate with the central bank[6][7].

Each person in a nation could have an bank e-mail, a private key, and a bank directory; when a sender sent money to a receiver

- the sender has an encrypted e-money in a directory obtained by the central bank using the central bank public key, and the public key of the sender

[1] without management cost,transport costs, man security, money printing, strong-boxes, cash dispensers

[2] with instant backup between server farms

[3] identical to the national identification number

[4] national identification number, money value, and a random string

[5] or a different public-key cryptography

[6] only the central bank has the clients public key

[7] multiple server farms in different sites to avoid destruction from natural disaster

- the sender take the national identification number of the receiver[8]
- the sender decrypt each e-money using the sender private key, encrypt each e-money and the e-mail address using the central bank public key, and send the file to the central bank
- the central bank decrypt the e-money and receiver address, verify the e-money, change the property address in the e-money file, and encrypt the e-money using the public bank key[9], and encrypt the file using the receiver public key
- the central bank save the file in the receiver directory and fileshred the e-money from the sender directory
- the central bank backup the directory in others distant server
- the receiver send a warning e-mail to the sender
- each operation on the directories must have a warning email

If there is a payment in a restaurant the bank give the change; for each operation are necessary not more of three e-mail sending:

1. $sender \rightarrow bank$
2. $bank \rightarrow receiver$
3. $bank \rightarrow sender\ change$

The cost of the system could be paid by the users without call cost[10]: the central bank can invest a part of the e-money in secure product[11] with a low income over many e-money: the central bank have measured statistically stationary e-money, that the nation can use because not-circulating.

It is possible to promote the e-money, requiring 3 day transfer from e-money to paper-money with a little cost.

It is possible to avoid fun band occupation[12] asking a time delay for each

[8] automatized with smartphone or computer program

[9] this is the e-money

[10] sms exchange cost

[11] for example 10% of moneys in short term ordinary treasury bonds

[12] $A \leftrightarrows B$ using computer

change (for example 30 seconds).

It is not necessary the ownership of the apparatus for the sender, because it is sufficient a memory sim, or memory card, or memory stick, to obtain the private-public key of the receiver, and the public key of the bank.

The e-mail is a common protocol, gpg is a common protocol, so that it is not necessary a program; it may need a program to speed up the procedure.