Digitaalraha ja selle seos krüptograafiaga

Rene Saarsoo
ifk03

Haapsalu 2004
27 lk

Sisukord

1 Sissejuhatus

1.1 Raha

Raha on üks inimkonna vanimaid kaaslasi, saatnud meid juba tuhandeid aastaid. Algselt olid rahaks kergelt kaasaskantavad väärisesemed – pärlid, kalliskivid, hõbe, kuld—mis algselt niisama ja hiljem väärismetallist müntideks vormituna leidsid pikka aega rahana kasutust. Olles ühtlasi seotud oma reaalse väärtusega oli selline raha raskesti võltsitav—pisut puremist hammaste vahel, ning oli selge, kas tegu on tõesti kuldmündiga või haleda kollaseksvõõbatud võltsinguga.

Selline võltsimatus oli aga petlik, sest ehkki võis olla kerge vahet teha kullast ja mõnest muust metallist mündil, oli väga raske aru saada, kas mitte kümme kuldmünti polnud üles sulatatud ning hoopis üheteistkümneks natuke väiksemaks mündiks vermitud. Arvatavasti just sel põhjusel tuli üle minna rahale, mille väärtus ei seisneks mitte tema tegemiseks kasutatavas materjalis, vaid hoopis riigi poolt kehtestatud kullakursis, ning mille turvalisus oleks tagatud raskesti võltsitava kuningliku profiiliga metalliratta tagaküljel.

Ometi osutus, et ka see ei peatanud võltsinguid—metallraha oli lihtsalt liialt kerge järgi matkida. Tehti järgmine samm, mis eemaldas raha tema kantavast väärtusest veelgi—võeti kasutusele paberraha. Lisaks sellele, et paberraha oli raskem võltsida, oli seda ka tunduvalt kergem kaasas kanda kui münte, rääkimata veel raskemast kullast.

Nagu me kõik tänapäeval näeme, on võltsitud paberraha täiesti tavaline nähtus ning, et eristada head võltsingut ehtsast peab olema tõeline professionaal. Jah, igal kupüüril on ohtralt turvaelemente (alates vesipiltidest ja lõpetades hologrammide ning peensustega, millest tavainimene midagi ei tea), kuid paistab, et ükskõik kui palju turvaelemente me nende paberite peale ka ei lisaks, siis ometi on võimalus seda võltsida. Ainuke, millega võltsimist peatada on see, kui me tõstame rahaüriku valmistamise hinna kõrgemaks, kui tema poolt esindatav väärtus. Milline raiskamine—ja ühel päeval keelavad rohelised meil rahapaberi tootmiseks vajalike puude langetamise...

1.2 Raha, arvutid ja privaatsus

Täna pole (arenenud maades) enam kellelegi üllatuseks, et suhtlemine pangaga ja pankade vahel käib suures osas digitaalselt. Suurte rahavankrite veeremine riikide vahel on peatunud ning selle asemel, et liigutada rahatähti (mis esindavad mingit väärtust) liigutatakse ja hoopis bitte ja baite, mis esindavad mingisugust rahatähtede hulka. Kui näiteks pank Brüsselis tahab osta Londoni pangalt eurode eest naelu, siis kirjutatakse lihtsalt Londoni pangas olevad naelad Brüsseli panga arvele ning Brüsseli eurod Londoni panga arvele—mingit reaalset rahatähtede vahetamist aga ei toimugi.

Internetipangandus on piisavalt turvaline eriti, kui kasutada autentimiseks ID-kaarti. See on märksa, märksa turvalisem kui kasutada sularaha, sest internetipangas olevat raha *pole võimalik* võltsida. Samuti on ühendus pangaga krüpteeritud ja kõrvalised isikud ei saa meie tehinguid pealt kuulata ja/või raha vahelt ära napsata.

Privaatsus on siiski näiline, sest kõigist meie tehingutest on pangal suurepärane ülevaade ning kui tarvis, pääsevad sellele infole ligi ka maksuamet ja politsei, ning pole välistatud, et ka konkurendid. See tõstatab taas nn "suure venna" probleemi: "Kas meid jälgitakse? Ning kui jälgitakse, siis kelle poolt?"

Loomulikult ei soovi meist keegi olla pideva jälgimise all. Sellest hoolimata oleme pideva jälgimise all: kaupluste kliendikaardid, turvakaamerad tänavatel, nuhkvara ja küpsised arvutis... Kübeke privaatsust, kasvõi üksnes finantsleeris, kuluks tõesti ära.

Juba üle kümne aasta on mitmed juhtivad krüptoloogid tegelenud digitaalraha probleemiga. Ei, mitte internetipangandusega, tõelise digitaalse sularahaga, mis oleks kasutatav nii üle võrgu kui ka otse tänava peal ja mis võiks olla asendajaks ebaturvaliseks muutunud paberrahale.

Sellise digitaalse raha võltsimiskindlus poleks tagatud mitte kõrgtehnoloogiliste ja peenete valmistamisvõtetega vaid vankumatute matemaatiliste võtetega—krüptograafiaga.

* * *

Järgnevas inglisekeelses referaadis me vaatame kõigepealt, milliseid omadusi peaks üks digitaalse raha süsteem evima, et olla tõesti hea. Seejärel uurime erinevaid probleeme, ja lahendusi neile ning viimaseks toome ära ühe võimaliku digitaalse raha süsteemi.

2 Electronic cash the way it ought to be (Millised omadused peaksid olema digitaalsel rahal)

Different authors describe different requirements and in different order, but the main things, like security and anonymity remain the same. In this section we describe a lot of different requirements in order found from writings of Jon W. Matonis[4] and Melissa Taylor[8].

2.1 Security (Turvalisus)

Money power derives from confidence in it thus the emphasis must be place on security. People have to be convinced that instruments they are offered are reliable and represent the real value. If this requirement fails nothing can force people to use any payment instruments in their every-day transactions.

One can distinguish 6 security levels:

Identification—this is a presentation of all involved parties in order to know who make commitments and who profits from rights. Buyer is obliged to payment (thus risk of no payment) and merchant is obliged to deliver ordered products (thus risk of no delivery).

Authentication—this is a process which verifies that both contractors are those they claim to be.

Authorization—this process indicates the initiator of a transaction.

Confidence—it is important to guarantee that non of all information will be known to the third party. System should be designed in this way that no one has access to the data which he does not need to complete his service.

The example of that can be transaction with payment card. The bank should not have an access to the product or service information and the merchant should not have an access to the card number.

Integrity of data—both parties should be assured that during transmission process, the data was not changed and was delivered on the whole.

Non-repudiation—payment system should ban the customer from the possibility of deny that he/she agreed to payment.

Client solvability—merchant should be sure that his client has money to pay for a product/service.

[7]

2.1.1 No double-spending (Topelt-kulutamise võimaluse puudumine)

To be secure against crooks and rip-off artists, digital cash should be designed in such a way that it can't be forged or reused. We wouldn't want people spending the same money twice, or acting as their own mini-Federal Reserve Systems and creating money from nothing. This cryptological problem is different between on-line and off- line cash systems. In on-line systems the bank simply checks whether a piece of cash has been spent before.[3]

Proposed off-line systems rely on a framework developed by David Chaum. Chaum has been the preeminent cryptological researcher in the field of digital cash. In his framework for off-line systems, one can double-spend the same piece of digital cash only by losing one's anonymity. This has considerable value, because the bank or the person defrauded, knowing the identity of the devious double-spender, can send out a collection agent.[3]

Chaum's framework also has a serious flaw of giving away the anonymity requirement.

Catching thieves and rip-off artists is not the comparative advantage of either banks or the average citizen. (Banks are usually only good at providing transactions services, and charging interest and fees.) Would you really want to see, say, The First Subterranean Bank of Anonymous Digital Cash merge with the Wackenhut Corporation? Luckily, however, there are alternative approaches that will prevent double-spending from ever taking place.[3]

For solutions see section 4 on page 13.

2.2 Anonymity (Anonüümsus)

Customers generally afraid that they will lose their privacy and anonymity so it is an important aspect to find the right combination between security and anonymity. Moreover some businesses can really develop only when clients can profit from a dose of anonymity.[7]

2.2.1 Untraceability (Jälitamatus)

The most important requirement for individual freedom and privacy is that digital cash transactions should be untraceable, yet at the same time enable you to prove unequivocally whether you made a particular payment. Untraceable transactions would make impossible a PROMIS-type data sorting of all your financial activities. In Joe Blowup's financial chronology, discussed previously, you wouldn't be able to connect Joe Blowup's name to any of his purchases. Similarly, no one would know about the money you wired to Lichtenstein, your purchase of Scientology e-meters and the banned works of Maimonides, or your frequent visits to the Mustang Ranch. Privacy-protected off-line cash systems can be made nearly as efficient as similar systems that don't offer privacy.[3]

2.3 Infinite duration (Aegumatus)

The digital cash does not expire. It maintains value until lost or destroyed provided that the issuer has not debased the unit to nothing or gone out of business. Alice should be able to store a token somewhere safe for ten or twenty years and then retrieve it for use.[4]

2.4 Portability (Porditavus)

The security and use of the digital cash is not dependent on any physical location. The cash can be transferred through computer networks and off the computer network into other storage devices. Alice and Bob should be able to walk away with their digital cash and transport it for use within alternative delivery systems, including non-computer-network delivery channels. Digital wealth should not be restricted to a unique, proprietary computer network.[4]

2.5 Independent of physical location (Sõltumatus füüsilisest asukohast)

Digital cash should be independent of physical location—available everywhere and capable of being transferred through computer and other telecommunication channels. So we want a smart card that can jack into the communication nodes of the global information network. One should be able to pop into a phone booth to make or receive payments.[3]

2.5.1 Interoperability (Süsteemidevaheline koostoime)

E-payment systems gain super advantage and bear incentives to possess and act with these instruments and systems only when different payment instruments are mutually accepted by different systems and instrument issuers. If not, it creates situation in witch special money is needed for special purpose.

It seems that "e-payment" firms finally understood it and started to create common standards (for example EMV constituted by Europay, MasterCard and Visa).[7]

2.5.2 Scalability (Skaleeritavus)

Payment system should take into consideration the changeable scale of the activity. System can not get stuck with an increase of clients or the transaction value. If not clients will perceive the system as not reliable and will stop making transactions.[7]

2.6 Off-line capability (Võimalus off-line kasutuseks)

You would want the ability to make digital cash payments off-line, just like you can with physical cash. A communication link between every store you shop at and your bank's authorization computer shouldn't be required. Moreover, if digital cash is to have all the desirable qualities of physical cash, you should be able to transfer digital cash directly to another smart-card-carrying individual. Smart cards that could connect directly to other smart cards would be ideal in this respect, and would represent an improvement over physical cash. Even if everyone observed two smart cards communicating, they would have no way of knowing whether the transaction involved $5 or $50,000. There would be no need to slide money under the table.[3]

2.7 Dividability (Jagatavus)

Got change for a dollar for the quarter slots in the pool table? Just as we “make change” or divide physical currency into subunits, so should electronic cash be divisible. Is this a problem? Hmm. Electronic calculators can perform an operation know as division, and so can third-graders. So smart cards ought to be able to handle this also, even if it presents a few difficulties for theoretical cryptology.[3]

2.8 Wide acceptability (Lai kasutatavus)

Clients will be interested in using electronic payments if they can pay anywhere they wish. If not, they would be forced to make some special effort (money exchange, e-money management, equipment expenses, etc.) to be able to make just few transaction. The advantage of the payment system rises more proportionally to the increase of all parties involved.[7]

On the other side, there is no interest in possessing the payment infrastructure and bearing payment costs if only few clients use it.[7]

2.9 User friendly (Kasutajasõbralikkus)

The technological advance and complicated encryption techniques provoke that most clients are unable to understand all technical issues. Thus payment systems should be created in this way that clients understand it by intuition thus systems do not require any special knowledge. All systems which require additional funds, equipment or knowledge are second-rate.

Flexibility (easy and cheap or even free of charge swap between e-instruments)

Clients should be allowed to swap their e-funds for different instruments to enable them to chose the best way of paying.[7]

2.10 Unit-of-value freedom (Ühikuvabadus)

The theme of this paper: the digital cash is denominated in market-determined, non-political monetary units. Alice and Bob should be able to issue non-political digital cash denominated in any defined unit which competes with governmental-unit digital cash.[4]

2.11 Low weight (Kergekaalulisus)

Physical cash is a portable medium of exchange. You carry it in your pocket to give to people when you make purchases. The digital equivalent of this process could be provided by smart cards, which would have the mobility of physical cash and even improve on it. The weight of $1,000,000 in digital money is the same as the weight of $1.[3]

2.11.1 Cheapness (Odavus)

It is very important for merchants to offer new payment solutions at the lowest possible cost in order to be, at the same time, competitive and to decrease their profit margin very little. If they do not offer any extra advantage to customers or the rivalry among them is very strong reality of market economy will force them to accept additional costs. Generally it is price elasticity of demand which will determine who will bear payment cost.[7]

2.11.2 Productivity (Produktiivsus)

Payment mechanisms should enable even small value payments so called micropayments (the merchant?s server collects multiple small value payments and after crossing the limit it will send them to the merchant's account). To ensure it one should take into account the relation between security and cost. It is enough to design payment system in this way that a cost of the theft would be higher than value which is stolen.[7]

3 Different Kinds of e-money (Erinevad e-raha liigid)

In general, there are two distinct types of e-money of major importance:

- identified e-money
- anonymous e-money (also known as digital cash)

Identified e-money contains information revealing the identity of the person who originally withdrew the money from the bank. Also, in much the same manner as credit cards, identified e-money enables the bank to track the money as it moves through the economy.[6] So, the way of spending is well known to financial institutions and the latter can easily track the circulation of e-money in the economy.[7]

Anonymous e-money works just like real paper cash. Once anonymous e-money is withdrawn from an account, it can be spent or given away without leaving a transaction trail. You create anonymous e-money by using blind signatures (see chapter 5 on page 15) rather than non-blind signatures.[6]

There are two varieties of each type of e-money:

- on-line e-money
- off-line e-money

On-line means you need to interact with a bank (via modem or network) to conduct a transaction with a third party.[6]

Offline means you can conduct a transaction without having to directly involve a bank.[6]

The real substitute of physical cash in the network is ensured while system is, at the same time, anonymous and off-line.[7] Offline anonymous e-money (true digital cash) is the most complex form of e-money because of the double-spending problem.[6]

We can also divide e-money based on implementation:

- software-based product (SBP)
- card-based product (CBP)

Originally CBP was designed to enable the point-of-sale payments and SBP for network payments. In the case of SBP value is stored on the computer hard disc and it is loaded via network. All protections are focused only on the software and thus SBP is considered as less credible than CBP solution since the latter is supported by special hardware i.e. chip card.[7]

However currently that distinction is a bit artificial because with card reader development (e.g. mobile phones) CBP can be used to make network payments and, on the other hand, the software can be downloaded into a mobile equipment.[7]

4 The Double-Spending Problem (Topelt-kulutamise probleem)

Since e-money is just a bunch of bits, a piece of e-money is very easy to duplicate. Since the copy is indistinguishable from the original you might think that counterfeiting would be impossible to detect. A trivial e-money system would allow me to copy of a piece of e-money and spend both copies. I could become a millionaire in a matter of a few minutes. Obviously, real e-money systems must be able to prevent or detect double spending.

Online e-money systems prevent double spending by requiring merchants to contact the bank's computer with every sale. The bank computer maintains a database of all the spent pieces of e-money and can easily indicate to the merchant if a given piece of e-money is still spendable. If the bank computer says the e-money has already been spent, the merchant refuses the sale. This is very similar to the way merchants currently verify credit cards at the point of sale.

Offline e-money systems detect double spending in a couple of different ways. One way is to create a special smart card containing a tamper-proof chip called an Observer (in some systems). Te Observer chip keeps a mini database of all the pieces of e-money spent by that smart card. If the owner of the smart card attempts to copy some e-money and spend it twice, the imbedded Observer chip would detect the attempt and would not allow the transaction. Since the Observer chip is tamper-proof, the owner cannot erase the mini-database without permanently damaging the smart card.

The other way offline e-money systems handle double spending is to structure the e-money and cryptographic protocols to reveal the identity of the double spender by the time the piece of e-money makes it back to the bank. If users of the offline e-money know they will get caught, the incidence of double spending will be minimized (in theory). The advantage of these kinds of offline systems is that they don't require special tamper-proof chips. The entire system can be written in software and can run on ordinary PCs or cheap smart cards.

It is easy to construct this kind of offline system for identified e-money. Identified offline e-money systems can accumulate the complete path the e-money made through the economy. The identified e-money "grows" each time it is spent. The particulars of each transaction are appended to the piece of e-money and travel with it as it moves from person to person, merchant to vender. When the e-money is finally deposited, the bank checks its database to see if the piece of e-money was double spent. If the e-money was copied and spent more than once, it will eventually appear twice in the "spent" database. The bank uses the transaction trails to identify the double spender.

Offline anonymous e-money (sans Observer chip) also grows with each transaction, but the information that is accumulated is of a different nature. The result is the same however. When the anonymous e-money reaches the bank, the bank will be able to examine it's database and determine if the e-money was double spent. The information accumulated along the way will identify the double spender.

The big difference between offline anonymous e-money and offline identified e-money is that the information accumulated with anonymous e-money will only reveal the transaction trail if the e-money is double spent. If the anonymous e-money is not double spent, the bank can not determine the identity of the original spender nor can it reconstruct the path the e-money took through the economy.

With identified e-money, both offline or online, the bank can always reconstruct the path the e-money took through the economy. The bank will know what everyone bought, where they bought it, when they bought it, and how much they paid. And what the bank knows, the tax agency knows. You won't have to worry about forgetting those sorts of things, like declaring all the money you have received, when everybody is using fully identified e-money. As a matter of fact, you won't even have to worry about filing a tax return. The tax agency will just send you a bill.

[6]

5 Blind signature (Pime allkiri)

Generally blind signature allows people to sign some information with their digital signature without knowing the content of the message.

The process of the blind signing is a modification of the traditional digital signing process. In essence, the prepared message (e.g. an e-banknotes with the exact denomination) is multiplied by a random factor and thereby the receiver (issuer) knows nothing about the content (i.e. serial number of the e-banknote) except that it carries user's digital signature (to identify user's account for deduction). After signing the e-banknote by the issuer to confirm its validity, it returns to the user who divides e-banknote by the same factor. Now he can use it keeping whole anonymity while the issuer does not know anything about blind factor. However, if user wishes to inform his e-money issuer about blind factor he can do so (e.g. for stopping this e-banknote).[7]

6 The four horsemen of the infocalypse (Neli infokalüptilist ratsanikku)

Tim May writes: "What I call the four horsemen of the infocalypse are being invoked: nuclear terrorists, child pornographers, money launderers, and drug dealers.[5]"

6.1 Money laundering problem (Rahapesu probleem)

There are three main reasons of possible e-money laundering:

- untraceability
- mobility of electronic payments
- no intermediary requirement

To prevent (or to make it more difficult) from laundering there are such proposition as:

- The widening of Financial Monetary Institution definition to encompass non-banks under bank regulations;
- The assurance of traceability of every spent e-coin which has an negative impact on one of the strong advantage of electronic money—anonymity;

[7]

6.2 Who are the bad guys, anyway? (Keda me tegekult peaksime kartma?)

To be sure, strong crypto, anonymous remailers, message pools, data havens, and digital cash will of course be used by some to hide crimes. It would be disingenuous to claim otherwise. But so are locked doors, closed curtains, whispers, and coded signals used to hide criminal activities. And yet in free societies we do not allow random searches, bans on strong locks, or insist that curtains have a special “law enforcement transparency mode” to assist in the “legitimate needs of law enforcement.”[5]

7 Digital cash by example (Näitlik digitaalrahasüsteem)

The description of how Digital Monetary Trust (DMT) works by J. Orlin Grabbe[2].

7.1 The customer's account number and its roles (Kliendi kontonumber ja selle rollid)

When you open an account at an ordinary commercial bank, you are assigned an account number. This number is usually fairly short: 0239446651, for example.

In the DMT, account numbers are long—exactly 1024 bits. For example, here is a DMT account number written as 256 hexadecimal digits:

```
F824500D59C82366 E36EC2C9641BFFFF 4F45CC89C85E153D 087AEC903E54FEE5
6D73ACA4103E752E B43B9DB3C32CED2F 7F2A1C3271C420C1 7E04D456F089B88E
94F82191B4AA4FD3 D77DF22F27F22464 3AFD98F2DBB61148 E38EAE5EF2D99517
5AE684048FDC2FED ADBC057555018AC6 6DA3EE9BA72C8D0A 1EA2840B5A4041A5
```

The client however doesn't have to remember he's account number, or even write it down. The DMT browser software will create it for him and store it. When the account number is needed, the software will also read it and transmit it to the DMT server.

But the reason for the length of the account number concerns two additional roles the bank account number plays.

[2]

7.1.1 Additional Role 1 (Lisaroll 1)

The DMT account number gets hashed to generate a claim number. DMT uses the Secure Hash Algoritm (SHA) hash function. For example, here is the SHA hash of the account number above:

```
5D5F03FF82A4A1BA 58E56D5B135054BF 09A77C0B
```

When you want someone to pay you at DMT, you will give them a claim number. You will select one of your accounts, the software will produce a hash of the account number, and you will copy and paste this number into some secure messaging system that you use to conduct your business—for example, Dodge City Nym-toNym messages, or MailVault PGP-encrypted email, or something similar.

Now the presence of such a number is standard business practice anyway. Frequently, when paying a bill, you have to include an invoice number, or some similar reference number. The difference for the DMT system is that the claim number determines who gets the payment. You don't make payments to an identified individual. You make payments to a claim number.

Anyone can make a payment to one of your claim numbers. But only you can collect the payment, because only you know the account number from which the claim number was created. You can easily derive a claim number from an account number. But this path is one-way: no one given your claim number will be able to create an account number that corresponds to it. Therefore they can't collect payments intended for you.

The DMT account number is a *pre-image* of the claim number. To prove that money paid to a claim number belongs to you, you have to produce its pre-image—namely the DMT account number from which the claim number was derived.

[2]

7.1.2 Additional Role 2 (Lisaroll 2)

The DMT account number is also a public key. It is the public key corresponding to a public-private key pair. This enables it to be used in a challenge-response protocol.

Don't misunderstand the use of the word "public" here. This public key, your DMT account number, is never given or shown to anyone. Rather, it is only stored on your computer by the DMT browser, and is also stored on the DMT server. But, for example, the DMT server could encrypt something to the DMT browser (such as a random number) using the customer's public key, and only the customer would be able to decrypt it. The private (secret) key corresponding to the public key (DMT account number) is known only to the customer.

As illustration, here is the private key corresponding to the public key (account number) above:

`5DBCA9A911BDA5C8 6288FA2575E95057 C4FBA1D4.`

In order to be able to collect a payment made to a claim number, it is not sufficient just to be able to show the pre-image (the account number) from which the claim number came. It is also necessary to prove knowledge of the private key corresponding to the account number (the account number being a public key).

So, after the DMT server verifies that your account number corresponds to the claim number, it next issues a challenge—a number calculated using both a random number and your public key. In order to answer this challenge properly, your browser will have to use your private key to make the calculation. When it is asked to do this, it will ask you for your passphrase, which is required to decrypt the private key for this account.

Having two separate ”proof”mechanisms that one is the proper recipient of a payment gives the system confidence that it is dealing with the real McCoy, and not with an imposter. But there is a separate reason for having two mechanisms. The first proof involves your showing you have the pre-image (the account number) from which the claim number came. This proof (the account number) is something written down—a number stored on your hard drive. It is possible someone could get access to your hard drive and steal this account number. But they still wouldn't be able to use it to collect your payments because they wouldn't know your private (secret) key. That's because the private key is protected by a separate layer of encryption, and you have to enter a passphrase to get access to your private key when you answer the challenge-response protocol. The private key is decrypted in computer memory just long enough to respond to the challenge-response protocol. Then it is erased, leaving only the well-encrypted version. But the passphrase is stored in your head. So a thief would have to rob both your hard drive and your head to be able to make transactions in your DMT account.

[2]

7.2 DMT signatures (DMT allkirjad)

When DMT signs an account, a hash is made of the account balance, the account number, and a random number. This hash is used along with the DMT's private key to create a bank signature.

If anyone alters your account balance or account number, the wrong hash will be obtained, and the signature will not verify. Moreover, an attempt to create a valid bank signature will fail because it requires DMT's private key, which corresponds to the DMT public key. Finally, and in addition, any altered data will not correspond to the data at the server.

For example, suppose we have the following bits of financial data:

Account Balance: $5000. This number is the same as 1388 in hexadecimal.

Account Number:

```
F824500D59C82366 E36EC2C9641BFFFF 4F45CC89C85E153D 087AEC903E54FEE5
6D73ACA4103E752E B43B9DB3C32CED2F 7F2A1C3271C420C1 7E04D456F089B88E
94F82191B4AA4FD3 D77DF22F27F22464 3AFD98F2DBB61148 E38EAE5EF2D99517
5AE684048FDC2FED ADBC057555018AC6 6DA3EE9BA72C8D0A 1EA2840B5A4041A5
```

Random Number:

```
197CCB886FBB1EC8 CAC2BA62A59D7715 7B9D51F1203278A7 1AC4BE69F7DF2529
9695E752D2EF048B 8921F3FB6FED702C 3129C9A76F9EC8E3 2108A4B81FFDA53D
A98DE1172282BA23 CF17EB14CF680E99 3BB76E607C11FE58 804942748F41EFBB
2E27B28ED0137A57 CC30D60223F4C0A8 3D1F159B4BED9ED3 BF1A9C3938F79968
```

If we concatenate these three numbers, we get:

```
1388F824500D59C8 2366E36EC2C9641B FFFF4F45CC89C85E 153D087AEC903E54
FEE56D73ACA4103E 752EB43B9DB3C32C ED2F7F2A1C3271C4 20C17E04D456F089
B88E94F82191B4AA 4FD3D77DF22F27F2 24643AFD98F2DBB6 1148E38EAE5EF2D9
95175AE684048FDC 2FEDADBC05755501 8AC66DA3EE9BA72C 8D0A1EA2840B5A40
41A5197CCB886FBB 1EC8CAC2BA62A59D 77157B9D51F12032 78A71AC4BE69F7DF
25299695E752D2EF 048B8921F3FB6FED 702C3129C9A76F9E C8E32108A4B81FFD
A53DA98DE1172282 BA23CF17EB14CF68 0E993BB76E607C11 FE58804942748F41
EFBB2E27B28ED013 7A57CC30D60223F4 C0A83D1F159B4BED 9ED3BF1A9C3938F7
9968
```

The hash of the above concatenation is:

```
5E394BEB853CADCF 68660E1B582A3625 8E050E99
```

If DMT's public key were:

```
B0CC79A888766222 C29E0244BBBDDE96 A7E4E9C97337C93C 2C62CF5AA10489FC
D2D8FC953EA977B7 529E1F3ADD1237BA FAB2E683EBF57354 06E91835B3174C9A
C262DF7C30447088 B6603452EDBCF6E2 FF7F6AAB772CFE3C 7BF0DCF641283AE5
16DE8BA7EBED9A44 D2FA051DF5497D76 F2745AC31C295817 CDD008C720427ADD
```

Then the bank signatures on the data would be, first, the random number just given above, and also the number

```
8459A92761A569C3 CD5B72139DF81FDA 82F2077F.
```

Change any of the input numbers, such as the account balance, and this number will not verify.

[2]

7.3 Receiving Payments (Maksete laekumine)

When a transaction is made with the server to claim a payment, the browser must show the proper account number corresponding to a claim number, and then must also respond to a challenge by using the private (secret) key corresponding to that account number. In responding to the challenge, the user must enter a passphrase to decrypt the secret key. Then the same account is decrypted at the server, and the same financial information verified by comparison with the server information. If all these tests are successfully passed, then the payment is added to the account balance, and the new balance is stored on the browser, along with bank signatures corresponding to the new amount. The new account balance is also recorded by the server.[2]

7.4 Making Payments (Maksete sooritamine)

When a transaction is made with the server to make a payment, a claim number to which the payment is to be made must be entered. The server then checks the DMT signatures on the account and verifies that these correspond to the account number and account balance. The server next sends a challenge to the browser, which must be responded to by using the private key (again, protected by a passphrase) corresponding to the account number. Then the same account is decrypted at the server, and the same financial information verified by comparison with the server information. If all these tests are successfully passed, then the payment is deducted from the account balance, and the new balance is stored on the browser, along with bank signatures corresponding to the new amount. The new account balance is also recorded by the server.[2]

7.5 Communication with the Server (Suhtlemine serveriga)

When data is sent from the browser to the server, a hash is made of some of the key variables in the data, and some key variables are also encrypted at this point.[2]

Next, the variables are diced into packets for sending to the server. These packets are encrypted under the TLS[1] protocol and sent to the server. The server checks each received packet to see that it hasn't been altered in transit. It then decrypts the packets and obtains the underlying variables (some of these still in encrypted form). It then decrypts the encrypted variables. Next it makes a hash of some of the key variables, and compares this to the hash made by the browser. All of this ensures that the data at the server is the same as the data in the browser.[2]

7.6 The Server Network (Serverivõrk)

DMT servers communicate with each other over the Internet, using an encrypted protocol which creates a Virtual Private Network. In addition to software security, the servers have physical security. The server locations are

[1] Transport Layer Security

housed in guarded, shielded, fortified facilities, with power provided by at least two independent power grids, along with backup battery power and gasoline generators.[2]

8 Kokkuvõte

Nagu me nägime on võimalik krüptograafia vahendeid kasutades luua turvaline ning samas ülimalt privaatne finants-süsteem. Siinjuures on oluline märkida, et kasutusele tuleb võtta pea kõik moodsa krüptograafia vahendid: salajase ja avatud võtmega krüptoalgoritmid, räsifunktsioonid, digitaalallkiri ja pime digitaalallkiri. Viimased kaks pole küll iseseisvad meetodid, ent toovad esile kuivõrd keerukas üks digitaalne rahasüsteem on.

Samuti nägime, et anonüümne ja jälituskindel digitaalraha võib endaga kaasa tuua mitmeid probleeme seoses kuritegijate jälitamisega. See ei tohiks olla aga olla takistuseks digitaalraha levikul, sest siiamaani pole inimkond jätnud leiutamata ja kasutusele võtmata veel midagi, mis võiks endast meie turvalisusele ohtu kujutada. Võrreldes nugade, püsside, pommide ja mürkidega näeb digitaalraha välja vägagi süütuke—pealegi pole sellega võimalik kellelegi vähimatki otsest kahju tekitada (erinevalt näiteks sellistest tapariistadest nagu konserviavajad ja munalõikurid). Digitaalraha head omadused—võltsimatus, anonüümsus, jälitamatus ja turvalisus—kaaluvad siiski jõudsalt üles tema potentsiaalsed halvad küljed. Ehkki on ka digitaalrahasüsteeme, kus iga tehing on jälgitav, mis kahtlemata sümpatiseerib võimustruktuuridele, on privaatsust tagavad süsteemid kodanikule kahtlemata märksa ahvatlevamad.

Mõned digitaalrahasüsteemid on juba realiseeritud, ent nende populaarsus on hetkel veel väike, pealegi pole paljudes süsteemides veel implementeeritud võimalust “off-line” tehinguteks, mis peaks olema just see, mis masse ahvatleks.

* * *

Digitaalse raha temaatika on märksa laiem, kui käesolev põgus referaat on ehk suutnud edasi anda. Kasutatud materjalid esindasid mitmesuguseid erinevaid seisukohti ning kirjeldasid palju erinevaid süsteeme. Meie vaatasime eelkõige anonüümset digitaalraha, kui kõige erinevamat praegusest pangandusest, ent samapalju on ka materjale mitteanonüümse e-raha kohta. Kuna e-raha kui selline on siiski suhteliselt uus temaatika, siis tõeliselt vananenud allikaid praktiliselt polegi. Pealegi pole antud töö sisuks mitte praktiline e-raha süsteemi ehitamine vaid teoreetilise ülevaate andmine digitaalraha valdkonnast.

* * *

Nagu ikka uute krüptograafiliste meetoditega, kulub ka digitaalse raha puhul enne üksjagu aega kui see jõuab laiade massideni. Kogu ajalugu on meile näide sellest, et kui on midagi, milles me kahelda ei pruugi, siis on selleks tehnoloogia arengu jätkumine. Kui aga tehnoloogiline progress jätkub, siis oleks lausa patt, kui selline suurepärane tehnoloogia, nagu seda on digitaalraha, meie laia kasutusse ei jõuaks.

Digitaalraha tuleb, kohe päris kindlasti.

Viited

[1] Grabbe, J. Orlin: *Cryptography and Number Theory for Digital Cash*, 1997, http://www.aci.net/kalliste/cryptnum.htm

[2] Grabbe, J. Orlin: *How DMT*[2] *Works. A Simple Explanation*, 2001, http://freedom.orlingrabbe.com/lfetimes/DMT_simple.htm

[3] Grabbe, J. Orlin: *The End of Ordinary Money, Part II*, 1995, http://www.aci.net/kalliste/money2.htm

[4] Matonis, W. Jon: *Digital Cash & Monetary Freedom*, 1995, http://www.isoc.org/HMP/PAPER/136/html/paper.html

[5] May, Tim: *Untraceable Digital Cash, Information Markets, and BlackNet*, 1998, http://www.privacyexchange.org/iss/confpro/cfpuntraceable.html

[6] Miller, Jim: *E-money mini-FAQ (release 2.0)*, 2004, http://www.ex.ac.uk/ RDavies/arian/emoneyfaq.html

[7] Stabla, Witold: *Electronic Payment Systems*, (mitte varem kui) 2001, http://ws19.webpark.pl

[8] Taylor Melissa: *Digicash*, dateerimata, http://www.infosystems.eku.edu/student/TaylorMelissa/SecondPage.htm

[2] Digital Monetary Trust