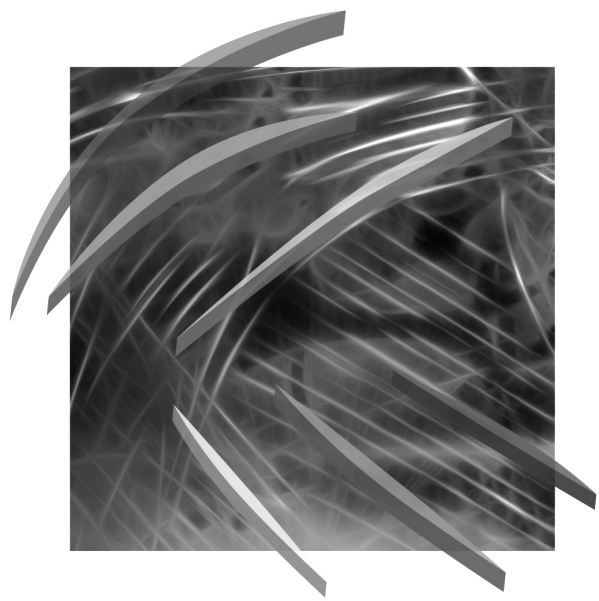
INFORMATYKA EKONOMICZNA

BUSINESS INFORMATICS

2(24) • 2012



Publishing House of Wrocław University of Economics
Wrocław 2012

Copy-editing: Elżbieta Macauley, Tim Macauley, Marcin Orszulak

Layout: Barbara Łopusiewicz

Proof-reading: Aleksandra Śliwka

Typesetting: Beata Mazur

Cover design: Beata Dębska

Publication financed by Ministry of Science and Higer Education

This publication is available at www.ibuk.pl
Abstracts of published papers are available in the international database
The Central European Journal of Social Sciences and Humanities http://cejsh.icm.edu.pl
and in The Central and Eastern European Online Library www.ceeol.com
as well as in the annotated bibliography of economic issues of BazEkon
http://kangur.uek.krakow.pl/bazy_ae/bazekon/nowy/index.php

Information on submitting and reviewing papers is available on the Publishing House's website
www.wydawnictwo.ue.wroc.pl

ISSN 1507-3858

The original version: printed

Printing: Printing House TOTEM
Print run: 200 copies

Table of contents

Streszczenia

INFORMATYKA EKONOMICZNA BUSINESS INFORMATICS 2(24) • 2012
ISSN 1507-3858

Daniel Wilusz, Jarogniew Rykowski
Poznań University of Economics
e-mail: wilusz{rykowski}@kti.ue.poznan.pl

REQUIREMENTS AND GENERAL ARCHITECTURE OF A PAYMENT SYSTEM FOR THE FUTURE INTERNET

Abstract: The advent of the Future Internet contributes to the emergence of new markets of physical objects offering their services. This phenomenon leads to new human-to-machine (H2M) and even machine-to-machine (M2M) markets, which require new payment methods. The goal of the paper is twofold. First, the requirements for a payment system in the Future Internet are identified and discussed, with the emphasis on system efficiency. Second, we propose a novel architecture of a payment system meeting the requirements of the Future Internet. The aim of our proposal is to design an efficient, anonymous, semi-off-line micropayment system by the application of cryptographic techniques as well as proper data exchange among system participants. The main principle of the proposal is the assumption that the system should be designed in such a way that it is pointless for both the payer as well as the payee to behave in a fraudulent way.

Keywords: micropayments, electronic money, Future Internet.

1. Introduction

The Future Internet (FI) is nowadays joined with two modern application areas of networking: the Internet of Things and Service-Oriented Architecture (SOA) together with cloud computing. The Internet of Things (IoT) is a permanently developing concept. It was introduced by MIT Auto_ID Center as an "intelligent infrastructure linking objects, information and people through the computer network, which aimed to allow universal coordination of physical resources through remote monitoring and control by humans and machines" [Brock 2001]. Nowadays the role of the Internet of Things is no more restricted to the electronic identification of objects but is perceived as a way to fulfill the gap between the real word objects and their representation in information systems. Haller, Karnouskos, Schroth [2009] provide a general definition of IoT by placing it in a business context. According to them, the Internet of Things is "a world where physical objects are seamlessly integrated into the information network, and where the physical objects can become active participants in business processes. Services are available to integrate with these smart objects over the Internet, query their state and any information associated with

them, taking into account security and privacy issues" [Haller, Karnouskos, Schroth 2009].

On the other hand, SOA and the cloud computing idea together gained the attention of many Internet users, as a modern tool to provide effective and powerful services across the network. The Internet of Services (IoS) is a natural supplement to IoT systems, making it possible to get access to IoT functionality at a higher level of abstraction.

Both IoT and IoS are applied in different areas such as: manufacturing, supply chains, energy, healthcare, automotive industry and insurance [Haller, Karnouskos, Schroth 2009]. However, FI is expected to emerge beyond companies' internal infrastructures and affect today's economy by creating human-to-machine (H2M) and machine-to-machine (M2M) markets. Yamabe et al. [2010] find the application of IoT in public transport, restaurants or comic cafes.[1] Furthermore, they introduce the concept of Activity-Based Micro-pricing, which means that customers are charged according to the time and sort of services that they use [Yamabe et al. 2010]. In IoT, environment mobile devices may be transformed into the personal servants concluding transactions with machines on behalf of their owners in order to purchase services or goods. However, to enable Activity-based micropayments in the H2M and M2M market, an efficient payment system is required.

The remainder of the paper is organized as follows. In Section 2 basic requirements for a payment system in the Future Internet are identified and described. Section 3 presents and analyses state of the art in the area of micropayments systems. In Section 4 the architecture of an anonymous, semi-off-line, micropayment system for the Future Internet is proposed. Finally, Section 5 concludes the paper.

2. Requirements for a payment system in the Future Internet

As the high transaction cost of electronic fund transfer determines its inefficiency in the case of micropayments, the suitable system should be characterized by properties similar to electronic money.[2] Matonis [1995] distinguishes ten main properties of an ideal electronic money system, which are enumerated below.

- *Security* – the system should prevent money counterfeiting and double spending. Transaction protocol has to be resistant to manipulation by a third party by the application of cryptographic techniques. The e-money provider should be assured that it is impossible or at least very difficult to counterfeit or double-spend electronic monetary value.

[1] Comic cafes are businesses in Japan where customers can rest by having refreshments, using the Internet for playing video-games or reading a book and, e.g., taking a shower at the same time.

[2] Electronic money is defined by [Directive 2009] "as electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions (…), and which is accepted by a natural or legal person other than the electronic money issuer".

- *Anonymity* – the privacy of a transaction should be protected at the highest possible level. The most desirable level of anonymity ensures that only the payer knows all the transaction details and neither the payee nor the e-money issuer is able to trace the transaction. On the one hand, from the legal point of view, anonymity is not a desirable feature of money because of money laundering and terrorism financing issues. On the other hand, transactions in the Future Internet (and especially IoT) are rather of a low value, related with micropayments, and the use of micropayments for illegal transactions appears to be quite inefficient.
- *Portability* – electronic money should not be dependent on physical location or form of electronic storage device as well as proprietary network. Users should be able to perform a transaction using different sorts of devices: PCs, smartphones, smartcards, etc. The payment process should be performed by the utilization of established communication and data description standards.
- *Bidirection* – natural persons should be able to make peer-to-peer payments. On the contrary to bank cards, a micropayment system should allow users to accept payments (acting as the payee). In the Future Internet, user's devices are able to provide payable services, so the user may act as both the payer as well as the payee.
- *Offline capability* – the payer and the payee should be able to exchange electronic money without the use of a network and the involvement of a third party (credit or financial institution). However, pure offline capable systems[3] impose the possibility of multiple spending of electronic money [Hoepman 2010]. As the devices/services in the Future Internet are permanently accessible via the Internet, the offline capability seems to be an irrelevant feature of the system.
- *Divisibility* – a given amount of electronic money should be divisible into as small units as needed. This feature is indispensable in the case of micropayments, where the amount of a payment is of a few eurocents or even less.
- *Infinite duration* – electronic money should not expire so that it would be possible to use it as a store of a value in long term. However, in the micropayment system the electronic monetary value may be of limited validity provided that the issuer will assure the redemption of e-money.
- *Wide acceptability* – Matonis [1995] states that electronic money should be "well known and accepted in a large commercial zone". According to Chmielarz [2005, p. 140], electronic money should be even country- and currency-independent. This feature is important for micropayments systems in the Future Internet, as transactions among dozens of devices/services, located in different places all over the world, should be possible.
- *Ease of use* – electronic money should be easy to use by the payer and the payee as well. According to Matonis [1995], this feature will lead to mass use, which

[3] "Pure offline capable systems" means that electronic money in a form of electronic tokens is exchanged many times and such circulation is not controlled by an institution which issued the e-money.

will result in wide acceptability. In the Future Internet, in order to make payments easy to use, the transaction should be performed by the software agent (an electronic servant), which would act on behalf of the user.

- *Free unit-of-value* – as Matonis [1995] has very liberal views, he states that "electronic money should be denominated in market determined non-political monetary units[4] and that every person should be able to issue non-political digital cash denominated in any defined unit which competes with governmental-unit digital cash". In the micropayment system in the Future Internet, the unit of account should be chosen carefully. Still the internationally accepted currencies as USD or Euro seem to be the most suitable; however, commodity backed units of value could be a reasonable choice.

The properties of electronic money presented above should be treated as a reference model. The currently existing electronic money systems only partially implement those features. The most difficult problem is to ensure the simultaneous security and anonymity of electronic money [Chmielarz 2005, p. 140].

One of the features of electronic money, not mentioned by Matonis [1995], but very important from the economic point of view, is an issue and transaction processing efficiency. For a successful micropayment system the issue and transaction processing efficiency ratio should be as close to 100% as possible to ensure that the use of electronic money even in the case of micropayments is economically justified. Equation 1 and Equation 2 reflect the ideas of issue and transaction efficiency of electronic money.

The electronic money issue efficiency ratio depends on the cost of the e-money issue process – the lowest the cost, the highest the efficiency ratio is. Moreover, the higher the value of issued e-money is at the same time, the higher the issue efficiency is (Equation 1). As a result, the system should minimize the cost of e-money generation and issue e-money of high face value. The conclusion driven from this indicator is that an efficient e-money system should issue e-money of a relatively high value, which can be divisible into smaller amounts (tokens), and the calculations cost and system overload should be minimized.

The electronic money transaction processing depends on the transaction processing cost. The lower transaction processing cost results in higher efficiency. Moreover, the higher the transaction amount processed, the higher the efficiency (Equation 2). This indicator shows that high amounts should be processed, and the cost of processing should be at the lowest possible level. This leads to the conclusion that the transactions should be processed in the maximum possible amount (aggregation of transaction) with calculations and system overload minimized.

[4] GoldMoney is an example of an electronic money system using non-political monetary units. GoldMoney monetary unit is a goldgram which is backed by gold, silver and platinum; as a result, a goldgram is convertible for pieces of precious metal [Gold Money 2011].

$$IE = \left(1 - \frac{IC}{IA}\right) \cdot 100\%$$

IE – issue efficiency ratio
IC – issue cost
IA – value of issued amount

Equation 1. Electronic money issue efficiency ratio

$$TE = \left(1 - \frac{TC}{TA}\right) \cdot 100\%$$

TE – transaction processing efficiency ratio
TC – transaction processing cost
TA – value of transaction

Equation 2. Electronic money transaction processing efficiency ratio

3. State of the art: micropayment systems

The micropayment systems presented in the literature fall into two categories: the first one is anonymity (anonymous or identified micropayments), and the second is the requirement of the connection with the third party processing the transaction (on-line and off-line micropayments). According to these categories, in this section four systems are analyzed and described. First, the Amazon Flexible Payment Service, identified as an on-line system, is described. Then, we examine the probabilistic-identified off-line system designed by Micali and Rivest. Next, the credit based, identifiable and off-line PayWord system is analyzed. Lastly, the anonymous, semi-off-line system of Payeras-Capella, Ferrer-Gomila, Huguet-Rotger [2003] is discussed.

3.1. Amazon flexible payments service – aggregated payments

Amazon offers merchants a solution to reduce processing fees by the accumulation of micro-transactions into one larger payment. The system is accessible on-line and does not preserve customers' anonymity as they have to register and provide their personal details including the data indispensable to charge their credit cards.

The idea of micropayments consolidation is based on pre-paid or post-paid accounts within the merchant's virtual store. In the first case, the customer has to load his or her account by allowing the merchant to charge his or her credit card with a prepaid value. Then, the customer is able to make the transactions within the merchant's store to the limit of the pre-paid account. In the second solution, the merchant may offer the customer a debt limit, and charge the credit card when this limit is reached [Amazon 2011].

As Amazon's solution is proper for customers who regularly purchase products or services from one merchant, this approach is not applicable in the IoT/IoS transactions, where the purchases happen rather irregularly. Moreover, each purchase has to engage the customer at the lowest possible extent. The strong requirement to authorize a credit card by every merchant decreases the usability of the system.

3.2. Probabilistic micropayment scheme of Micali and Rivest

Micali, Rivest [2002] proposed a micropayment scheme which solves the problem of micropayment processing costs. As there is still no way to aggregate micropayments from different clients into one of a larger value, they proposed a system which with the probability s realizes a payment of $1/s$ to the merchant. Assuming that the system uses function $F()$ to generate random values from an arbitrary bit string, the merchant who makes lots of transaction should receive a payment very close to the value of the sold goods and the customer (in the long run) should be charged an amount close to the value of purchased goods.

The system is constructed in such a way that the merchant is able to determine if the user's "check" is payable or not. The "check" C consists of the transaction details T signed by the user – $C = SIGN_U(T)$. As the transaction details include s, the merchant is able to determine if the C is payable or not. In order to verify if the C is payable, the merchant calculates the output of function $F()$ on the "check" signed by him or her – $F(SIGN_M(C))$. Then the probability is calculated as a binary part of a fraction based on the output offunction $F()$. If the fraction is less or equal to probability s, the merchant demands payment from the bank, while in the other case, he or she does nothing [Micali, Rivest 2002].

One can notice two significant drawbacks of the system. The first is the lack of users' anonymity as they have to sign transaction details. The second is the probabilistic approach, which may be associated with gambling. Moreover, the probabilistic approach is contradictory with the legal essence of a sale, which is "transfer of something (and title to it) in return for money (or other thing of value)" [Hill, Hill 2011]. Although Micali and Rivest's proposition solves the micropayment aggregation problem, it is not likely to be adapted by financial institutions and consumers because of its gambling character.

3.3. PayWord

PayWord is a system utilizing hash chains in order to optimize computations required to produce and process micropayments [Rivest, Shamir 1997]. The system is accessible off-line and is based on a credit assigned by a bank. The bank creates a temporarily valid certificate for the user, which consists of, among other things, the user's public key signed by the bank.

In order to pay, the user presents the certificate to the merchant. Then the user creates merchant-specific pay words, which are a chain of hashes generated by the application of the hash function on the seed *n*-times. Then the user creates the commitment of payment by signing a concatenation of the bank's name, certificate, the last generated (*n'th*) hash value and the current date in order to send all this information to the merchant. The merchant checks the user's signature using the bank's certificate and, if the signature is valid, begins the provision of goods or services. The user pays for every consumed part of good or service a micro-price, by providing *n-1'th*, *n-2'th*, etc., hash value, while the merchant checks if the hash function performed on *n-1'th* hash value is equal to the *n'th* value.

At the end of the business day, the merchant provides the user with a certificate to the bank, together with the commitment of the payment and the *n-m'th* hash value (where *m* is the value of goods or serviced presented in US cents). The bank verifies the user's commitment and performs the hash function on *n-m'th* hash value *m* times in order to compute and compare *n'th* hash value [Rivest, Shamir 1997].

Although the system proposes a relatively fast way to compute electronic money, it suffers from the lack of anonymity. Moreover, the bank takes a risk of users who may exceed their credit.

3.4. Anonymous scheme of Payeras-Capella, Ferrer-Gomila and Huguet-Roger

The authors utilize the blind signature concept of Chaum [1982] in order to preserve users' anonymity. The divisibility of electronic coins is achieved by the application of hash chains. The security of the exchanged information is assured by RSA cryptography. The general operation of the systemis as follows [Payeras-Capella, Ferrer-Gomila, Huguet-Rotger 2003].

The user generates the arbitrary value W_1, which is a proof of coin ownership. Then the hash value of $W_0 = H(W_1)$ is calculated. In order to preserve anonymity, the user blinds the W_0 with a blinding factor, which in turn generates blinded identifier W. In order to have a coin of value Q generated by a bank, the user sends the amount Q and identifier W signed with their own public key to the bank. Then the bank signs the blinded identifier with their own public key, corresponding to the value of Q, and sends it back to the user. The user removes the blinding factor in order to generate a valid universal coin, which is properly signed identifier W_0. However, the universal coin cannot be spent at any merchant.

Before the user begins purchases, he or she has to obtain from a merchant his or her certificate and the identifier for merchant specific coin W_{0m} (the merchant saves W_{1m} in order to prove ownership of the received coin before the bank). In the next step the user generates the hash chain of $n + 1$ values, where the sum of n hash values is equal to the amount the user wants to spend by merchant (Q_2), and the last hash value (W_{0u}) identifies the merchant specific coin M_2. Then, the user contacts the bank and sends the universal coin, the proof W_1, the amount Q_2, the identifiers W_{0u} and W_{0m}, the

number of hash values in chain (n) and identifier W_{0x} of a new universal coin created by the bank from the remains of the previous universal coin ($Q_3 = Q - Q_2$). The bank compares W_0 with the $H(W_1)$ and if they are equal, computes the merchant specific coin by signing the , W_{0m} and n. Next the bank creates another universal coin by signing the W_{0x} with the public key corresponding to the value Q_3.

After receiving the merchant specific and new universal coin, the user is able to begin purchasing. He or she provides the merchant with the specific coin and later during the consumption of goods or services, with the particular hashes from the chain ($W_{1u}, W_{2u,...,} W_{iu}$).

The merchant, in order to deposit the coin, contacts the bank and present his or her specific coin, proof W_{1m} , the latest hash W_{iu} and number of received hashes (i). The bank checks if the merchant is the owner of the coin by comparing W_{0m} with the $H(W_{1m})$ and if they are equal, performs the hash function on the W_{iu} i-times in order to obtain W_{0u}. If the calculated hashes are correct, the bank credits the merchant with i multiplied value of one hash in the chain [Payeras-Capella, Ferrer-Gomila, Huguet-Rotger 2003].

The authors do not explain what happens with the non-spent value of merchant specific coin (hash values n-i). As the coin is anonymous, it is impossible to determine the user both by the bank or the merchant in order to transfer the non-spent value of the coin M_2. It seems that the non-spent value is forfeited in favor of the bank. Moreover, the necessity of contacting the bank by the user before the payment is not suitable for micropayments, especially in the Future Internet. In the IoT/IoS the merchants (objects providing goods or services) are permanently connected to the Internet, and users are rather mobile and bear the higher cost of Internet connection.

4. System architecture

After the analysis of the state of the art in the area of micropayments systems, to our best knowledge, there exists not a single solution suitable to perform micro-transactions in the Internet of Things and Services. Thus, in this section we present our proposal – a new micropayment system meeting the requirements of the Future Internet environment.

The proposed system utilizes the hash chain in order to create divisible coins and the Chaum's blind signature scheme to make them anonymous. The use of RSA signatures is limited to the signing of the coin by financial institution and checking its signature. The payment is semi-off-line with the clearing house preventing double spending. Moreover, the clearing house operates in the cloud in order to allow the efficient processing of payments and to cut the costs. The idea of hash-based one-time passwords [Lamport 1981] allows locking the payment session for the merchant, to prevent double spending and increase system efficiency. The secured communication protocol (e.g., SSL) among all the communicating parties is assured. Moreover, it is

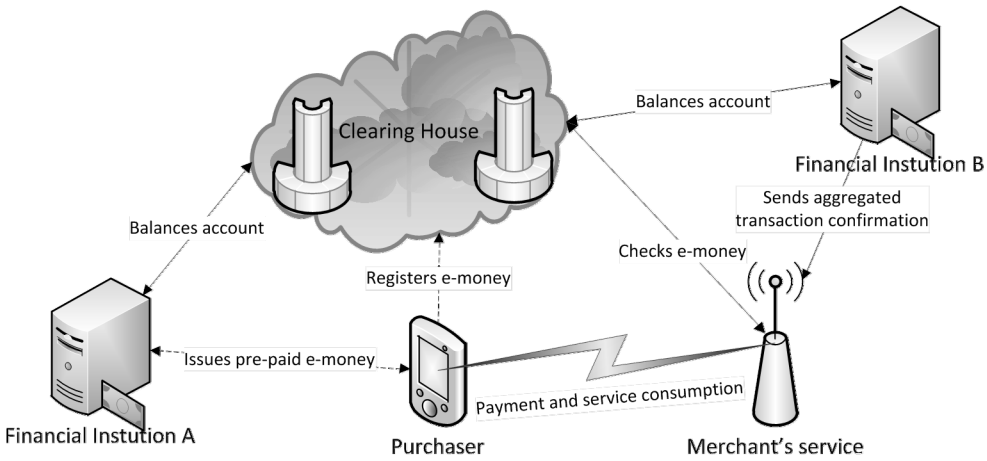


Figure 1. System participants

Source: Lamport [1981].

assumed that financial institutions and the clearing house trust each other and that they are supervised by the legal authorities.

The participants of the proposed system are presented in Figure 1 and described below.

- The purchaser is an entity who obtains valid pre-paid electronic tokens from a financial institution, registers them anonymously in the clearing house and spends them at the merchant.
- The financial institution signs e-tokens generated by users and debits their accounts. The presented architecture allows many financial institutions to participate in the system.
- The clearing house is a participant which registers newly issued electronic tokens, prevents double spending and balances the accounts of financial institutions by compensating their mutual liabilities.
- The merchant accepts electronic tokens and checks their validity by the clearing house. The merchant in order to accept payments has to establish an account at the clearing house.

4.1. Issue of the electronic coin

In the proposed scheme the electronic coin is assumed to be of fixed value V. However, the application of value connected signatures of a financial institution, like in Payeras-Capella, Ferrer-Gomila, Huguet-Rotger [2003], could be considered. The electronic coin is divisible into n tokens each of value equal to V/n.

In the first step, the user generates seed consisting of timestamp and random value ($S = T||Rv$). Then the user performs hash function (i.e., SHA-512) on the seed n times to produce coin identifier $CId = H^n(S)$. Next the user calculates the blinding factor r – the number relatively prime to the N parameter of financial institution RSA public key. Then the user blinds the identifier by calculating $CId \cdot r^e (mod\, N)$, where e is the second parameter of the financial institution RSA public key. In the next step, the user asks the financial institution to debit his or her account and sign the blinded coin.

The financial institution does not hesitate to sign the blinded token because the user has no benefit in sending a wrongly formed identifier as such a coin would be useless (only the user knows the seed is able to spend the coin). For further registering purposes, the financial institution multiplies the blinded coin with number-expressed date (D) (this solution prevents double spending and allows the user to revoke the coin in the very unlikely case of collision of hash function[5]). There are two elements signed by the financial institution. The first is the blinded identifier ($CId \cdot r^e (mod\, N)$), and the second is the blinded identifier multiplied by date $(CId \cdot r^e (mod\, N))D$. The signed blind coin is in the form of $CId^d r^{ed} (mod\, N)$, where d and N are parameters of the private key of the financial institution. After signing the blinded coin, the financial institution sends it to the user together with the signed identifier multiplied by date and the value of date.

In the next step, the user removes the blinding factor from the coin. As was proven by Chaum [1982], $r^{ed} \equiv r\, (mod\, N)$, so the user multiplies signed the blinded coin by $r^{-1}\, (mod\, N)$ in order to obtain the identifier (CId) signed by the financial institution $CId^d \equiv CId^d r^{ed} r^{-1}\, (mod\, N)$. Moreover, the user checks the timestamp by applying the financial institution public key to the signed identifier multiplied by timestamp $\left(CId \cdot r^e (mod\, N)\right)D = \left(\left(CId \cdot r^e (mod\, N)\right)D\right)^{ae}\, (mod\, N)$ and divides the result by D in order to receive the blinded identifier. If the calculation results in the proper value, the user has a proof of the time when his or her account was debited, which allows revoking the coin in the very unlikely case of hash function collision.

4.2. Registration of the electronic coin

In order to use the electronic coin, the user has to register it at the clearing house. The user sends $CId^d T^d\, (mod\, N)$, T and shared secret s (randomly generated number) to the clearing house. The clearing house checks if CId exists in the data base. If this value is unique, the service registers the coin under the identifier CId, the date, signed coin; number of coin tokens (n) and secret (s) are stored as well. There is no user authentication required, as only the user has knowledge (tokens) to use the coin

[5] At the same time, anonymity is preserved as the date is probably common for many requests incoming during the same day.

(prove the ownership by performing hash function over tokens, which are kept secret until they are spent at the merchant).

In the case of the doubled coin identifier, the user performs the proof of the time and financial institution which signed the coin. After positive proof, the service refuses registration and prepares the coin revocation by signing the electronic coin. The revocation allows the user to have a newly created coin signed by the financial institution without bearing additional costs.

4.3. Payment process

The user who wants to consume a service provided by the merchant agrees to the fee $h = l\frac{V}{n}$ (l is the number of tokens of a value equal to v) for a service unit and presents the coin identifier and the lock – hashed secret $H(s)$ encrypted with the clearing house public key. Then the merchant forces a checkby the clearing house to validate $H(s)$ and requests a lock to the coin. Then, after consuming a fraction of the service, the user presents the unspent token of the coin $T_1 = H^{n-l-m-1}(S)$, where m is the number of already spent tokens and $m < n$. In the next step, the merchant presents this token and l to the clearing house. The service calculates the hash function over the token l times. If the result is equal to the last spent token, the clearing house sends to the merchant the information on the remaining value of the coin. If the user wants to continue consumption of service, he or she provides the token $T_2 = H^{n-2l-m-1}(S)$ to the merchant. If the remaining value of the coin is higher than v, the merchant does not have to check the next bunch of tokens again – it is enough that the hash function performed on the other token l times results in the value of previous token $T_1 = H^l(T_2)$. When the user stops consuming the service, the merchant presents to the clearing house only the last received token (T_r) and the total value of consumed services ($xl\frac{V}{n}$). Then the clearing house performs the hash function over the last spent token (T_0) xl times to verify the credibility of the merchant and, if equation $H^{xl}(T_r) = T_0$ is met, the clearing house debits the value of coin by xv (diminish the number of remaining tokens by xl), credits the merchants account, removes the lock, replaces T_0 by T_r, replaces the secret with hashed value of the secret and sends confirmation to the merchant.

5. Conclusions and future work

In this paper we presented the basic architecture of a payment system for the Future Internet. The main achievement of the proposal is to effectively serve micropayments. The use of a computationally effective hash function allows the generation of divisible e-coins, which in turn engages the computing resources of financial institution only during signing the coin. Moreover, the concept of the blind signature allows preserving users' anonymity. The main advantage of the proposal is the semi-

off-line character of the system. Contact with a third party is required only during the first check of the coin and the remaining tokens of the coin may be off-line checked by the merchant. This was achieved by a new application of one-time passwords in order to lock the coin at the clearing house.

As this is one of the very first approaches towards the general payment system for modern networks, it was not possible to discuss several important issues, such as prototype implementation and efficiency analysis. We are now working on the implementation of the proposed architecture within the scope of the Internet of Things, intelligent (Java-based) smart cards and mobile devices. However, as implementation is at an early-stage, we are not able to say anything about targeted system usage (application scenario) and efficiency. We do hope, however, that according to our best knowledge the proposal will be effective even in the cases of massive hardly-repetitive micropayments.

References

Amazon, *Amazon FPS Aggregated Payments Quick Start*, Amazon.com, 2011, https://payments.amazon.com/sdui/sdui/business?sn=devfps/aggregated (accessed: 21.11.2011).

Brock D.L., *The Electronic Product Code (EPC) A Naming Scheme for Physical Objects*, Auto_ID Center, 2001, http://www.autoidlabs.org/uploads/media/MIT-AUTOID-WH-002.pdf (accessed: 18.11.2011).

Chaum D., Blind signature for untraceable payments, [in:] *Crypto '82*, Springer-Verlag, Berlin/Heidelberg 1982, pp. 199–204.

Chmielarz W., *Systemy elektronicznej bankowości*, Difin, Warszawa 2005.

Directive 2009, *Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC*, Official Journal of the European Union L 267.

Gold Money, *Convenient Gold & Silver Investment*, 2011, http://www.goldmoney.com/why-goldmoney-convenient.html (accessed: 18.11.2011).

Haller S., Karnouskos S., Schroth Ch., The Internet of things in an enterprise context, [in:] *Future Internet – FIS 2008*, Springer-Verlag, Berlin/Heidelberg 2009, pp. 14–28.

Hill G., Hill K., *The People's Law Dictionary*, 2011, http://dictionary.law.com/Default.aspx?selected=1878 (accessed: 22.11.2011).

Hoepman J., Distributed double spending prevention, [in:] *Security Protocols 15th International Workshop, Brno, Czech Republic, April 18-20, 2007*, Springer-Verlag Berlin/Heidelberg 2010, pp. 152–165.

Lamport L., Password authentication with insecure communication, *Communications of the ACM* 1981, vol. 24, issue 11, ACM, pp. 770–772.

Matonis J.W., *Digital Cash & Monetary Freedom*, Internet Society (ISOC), 1995, http://www.libertarian.co.uk/lapubs/econn/econn063.pdf (accessed: 18.11.2011).

Micali S., Rivest R., Micropayments revisited, [in:] *Topics in Cryptology CT−RSA 2002*, Springer-Verlag, Berlin/Heidleberg 2002, pp. 149–163.

Payeras-Capella M., Ferrer-Gomila J., Huguet-Rotger L., An efficient anonymous scheme for secure micropayments, [in:] *Web Engineering International Conference, ICWE 2003 Oviedo, Spain, July 14–18, 2003*, Springer-Verlag, Berlin/Heidleberg 2003, pp. 80–83.

Rivest R., Shamir A., Pay Word and MicroMint: Two simple micropayment schemes, [in:] *Security Protocols International Workshop Cambridge, United Kingdom, April 10–12, 1996*, Springer-Verlag, Berlin/Heidleberg 1997, pp. 69–87.

Yamabe T., Lehdonvirta V., Ito H., Soma H., Kimura H., Nakjima T., Activity-based micro-pricing: Realizing sustainable behavior changes through economic incentives, [in:] *Persuasive Technology 5th International Conference*, *PERSUASIVE 2010*, Springer-Verlag, Berlin/Heidleberg 2010, pp. 193−204.

WYMAGANIA I ARCHITEKTURA SYSTEMU PŁATNOŚCI W INTERNECIE PRZYSZŁOŚCI

Streszczenie: Nadejście Internetu Przyszłości powoduje pojawienie się nowych rynków, na których obiekty podłączone do sieci oferują swoje usługi. Zjawisko prowadzi do powstania dwóch nowych rynków człowiek−maszyna (H2M) i maszyna–maszyna (M2M), na których dotychczasowe metody płatności nie mogą być efektywnie wykorzystane. W artykule zostały zidentyfikowane i omówione wymagania dla systemu płatności w Internecie Przyszłości ze szczególnym naciskiem położonym na efektywność systemu. Co więcej, artykuł przedstawia propozycje architektury systemu płatności dostosowanego do wymagań Internetu Przyszłości. Celem artykułu jest zaprezentowanie efektywnego, anonimowego i semi-pracującego-w-odłączeniu (ang. *semi-off-line*) systemu mikropłatności, który został zaprojektowany przy wykorzystaniu technik kryptograficznych oraz odpowiednich schematów wymiany danych między jego uczestnikami. Co ważne, architektura systemu uniemożliwia próby oszustwa, ze strony zarówno płatników, jak i beneficjentów.

Słowa kluczowe: mikropłatności, pieniądz elektroniczny, Internet Przyszłości.