Procedural Principles of Payment Systems

Saeid Rahmatzadeh Poshtiri[1], Ebrahim Abdi Pour Fard[2*], Ebrahim Delshad Maref[3]

1 Pht Student, Department of Law, Faculty of Humanities, Qom Branch, lslamic Azad University, Qom, lran.

2 Faculty member, Department of Private law, University of Qom, Qom, lran.

3 Faculty member, Department of Law, Faculty of Humanities, Qom Branch, lslamic Azad University, Qom, lran.

Abstract

The development of modern banking has provided various payment means and methods followed by several payment systems accordingly. Utility and efficiency of these systems and consideration of each system by the operators including the banks, business owners and consumers depend on observance of legal and procedural rules and principles by the designers and executives of the said systems.

In this paper, the procedural rules and principles of various payment systems, especially e-payment systems, are reviewed. The results of this research which was conducted through descriptive and analytic methods using library resources and experiences of financial systems reveal that efficiency, security and reliability, optimal settlement, risk reduction, constant supervision, and enjoying a legal foundation are among the most significant procedural principles that provide the requirements and features of an optimal and secure payment system. Experiences of financial systems indicate that the more the designers and executives of payment systems provide the required hardware and software facilities for complete and precise implementation and observance of the said principles, the more will the success and utility of a payment system increase.

Keywords: Payment System, Procedural Principles, Efficiency, Security, Risk, Supervision, Settlement.

Tob Regul Sci.™ 2022; 8(1): 1444-1461
DOI: doi.org/10.18001/TRS.8.1.112

INTRODUCTION

If we define payment as a process of transferring monetary value, the payment system is a series of human and material factors that realize this process. BIS (Bank for International Settlement) has defined the payment system as follows: “A payment system comprises a series of banking tools and procedures and mainly banks’ resources that allow for money circulation throughout transfer systems”. (BIS, 2001, 38)

Stating payment system elements, in addition to the payment parties including operators and banks, the money to be paid, payment tools, institutional arrangements such as payment rules and regulations and banking procedures are among the principal elements of a payment system. In bank payment systems, Payment Service Providers (PSPs) should be added to the above.

Today, payment methods and tools, and consequently, payment systems have become extremely diverse and widespread in E-banking payments. In addition to traditional systems such as use of commercial papers and bank drafts, various methods of electronic money transfer, payments based on debit cards and credits cards play an increasing role in payment for commercial and consumer exchanges.

Anyway, optimal and reliable payment systems follow the principles and regulations that secure their efficiency. These principles and regulations can be divided into two categories, namely legal

principles and procedural principles. In this paper, procedural principles and regulations of various payment systems, especially e-payment systems are discussed and reviewed.

The main question of the research which was conducted through descriptive and analytical methods based on library resources and the research works conducted in various financial systems is that "Which principles and regulations does an optimal and reliable payment system follow in a secured payment process?"

Our research hypothesizes that practical experiences of payment systems in traditional banking and e-banking have guided the designers, executives, and operators of payment systems to comply with certain principles and regulations that in fact form the requirements and features of an optimal, reliable and efficient payment system. Research results are provided in 6 chapters in order of findings and accepted principles.

First Principle: Efficiency

Concept of Efficiency

The concept of efficiency is widely used in the study of payment systems. Economists interpret efficiency as choosing one of the payment systems by the operators (based on the aspects they want in that system). These services create the lowest cost for the economy. (ITU-T, 2016, 31)

In practice, it is often very difficult to evaluate the efficiency of the payment systems by the standards of the economists because many of the quality aspects that system operators consider in their choice are difficult to measure (Camenisch, 1996, 91). In addition, the cost of several resources must be calculated accurately. This calculation becomes more difficult due to the fact that efficiency should increase over time. Various factors are involved in providing or increasing the efficiency of the payment system which we will examine hereunder.

The necessity to utilize appropriate technology and the flexibility of the system in facing the changes

Advanced and developed information technology is a requirement for payment systems but it is not always necessary. The use of systems that mainly rely on sophisticated and online communication technology is not common in countries with no suitable and reliable communication infrastructures, because the systems will lose their reliability and efficiency for the operators. Hence, the choice of a suitable system depends on several factors that must be certainly addressed for the efficiency of a system; otherwise, the said system will have neither any economic advantage for the provider nor the necessary application and efficiency for the operators (Flannery, 1996, 805).

It is difficult to ensure that payment systems are useful and efficient and that they will remain the same over time, upon advancement of technology, and change of costs. For example, paper-based processes in the early time of development of financial markets could be efficient and useful in the same level as low scale transactions and those in which time was insignificant, but those systems immediately lost their efficiency and were forgot upon progress of financial markets, significance of time and handling volume in transactions. (BIS, 2001, 44)

Management of costs

Efficiency in the payment system is realized if the resources used for it are not wasted because wastage means additional costs which should not be paid. These costs will be finally borne by the

mediums and end users and the result is that their access to their preferred payment system will be more expensive. Of course, optimal use of resources does not mean hiring less manpower, using a low technology, etc., but it means correct and accurate utilization of all resources. The effective elements in choosing a payment system by the mediums and end users are quite extensive and their choice is pending on the value and significance given to their intended element in that system. Security of payment system, practical applicability and cost effectiveness are among the effective components in choosing a payment system. If a payment system is affordable and has a low cost and it is practically safe and applicable, it will be highly probable that the banks and their customers use that system although sometimes excessive security of payment system increases the costs too much, makes the use of system difficult and the system loses its functional feature. (Cirasino & Garcia, 2008: 36).

As for efficiency based on cost element, a distinction must be made among three categories of costs. The first category refers to costs of the central system which are directly fixed by the operators. The second category includes the costs for carrying out payment operations by mediums and system operators. Although these costs refer to the external layer of payment system, they are often influenced by the design type of system center. The third category includes the costs which are borne by the operators and payment mediums to finance liquidity for payments and settlements. (Camenisch, 1996: 91)

Costs of payment system generally include those for payment, settlement between the banks and recording the accounts and settlements. These processes may be manual, electronic, and/or a combination of both, and all of them need huge investment in equipment, communications, and support. There are also other costs such as system processing, management of communications and general administration of system all of which are manifested in the final cost of system usage and shall be paid by the operators. Internal costs of payment mediums have a significant effect on the final cost of payment system usage. Payment mediums and middle operators of systems provide services in relation to payment which are all costly. Although designers and operators of payment systems have no control over the said costs, operators should know that system design beside the used technology and system process have a significant effect on the aforesaid costs that cover an important part of final costs of the customers to use the payment system and they influence on the customers' opinion in respect of using or not using a system, and when to use or not to use them. Hence, cost decrease and fixing a competitive price are changed to more important issues in the competition between the systems. (Summers, 1994, 126)

In the systems handling a high volume of value, procedural cost of the system has found a less importance for the operators and mediums. Instead, the costs pertinent to liquidity finance become more important during the day. Liquidity costs of mediums and middle operators of the system depend on two factors. The first one is that how much liquidity their payment system has defined for transactions, and the second one is the maintenance cost of the liquidities. (BIS, 2001, 45)

The necessity to evaluate system based on benefit-cost criterion

Benefit-cost evaluation is highly important in carrying out and modification of payment system projects. Adoption of a benefit-cost evaluation method make the designers and modifiers of payment systems to address all the existing costs in the payment process and to examine them in view of the operators, in the manner that the end operator decides either to use the system or to enjoy another method to transfer the monetary value, taking into consideration the security and efficiency of the

system he uses on the one hand, and the costs he pays for that on the other hand. From the customer's viewpoint, the cost he pays is not analyzed. Moreover, the customer does not consider how much is the cost of each part of payment process; instead, he considers the entire amount of money which is paid from his pocket. (Summers, 1994, 120)

The need for transparency in the receipt and payment of subsidies

If it is claimed that the resources are used quite useful and without any wastage, it is very important to clarify the costs of the provided services for the operators although it may seem difficult as there are some upstream costs which should be divided between the number of payment services and other provided services; however, efforts should be made to clarify these costs to the operators. Sometimes, subsidies are accrued to the payment systems. The reason and justification of these subsidies may be different. Sometimes subsidies are accrued because system operators want and/or do not want to bear the operation costs and some other times, subsidies are allocated because the system provider is not able to gain the required profit from service provision. Some other times, the justifications of social benefits led to allocation of subsidy to the payment system. Anyway, the operators who use the subsidy should be informed that they will be treated according to the governing rules and regulations and they will receive no more subsidies if they commit any violation in providing the pricelist of services to the system operators. If granting subsidies to a system becomes a durable procedure, central banks and operators of payment system should be aware that this situation is caused due to no competition and failure to observe market principles which in turn results in inefficiency and wastage of resources. However, if payment system is provided by the central bank, it should clearly declare the documentations for its received costs (BIS, 2001, 47)

Second Principle: Security and Confidentiality

Payment systems are made of various elements and sections. The issue of security and confidentiality is not just related to the payment system center, but all its elements must be secure and reliable, including hardware and software sets, communications, payment mediums, and payment tools. (Rambure & Nacamuli, 2008: 148)

Anyhow, the goals and policies of the payment system security principle should be clearly stated and implemented so that the necessary trust in the system is established. In general, it can be said that due to high sensitivity of business and payments and the need in preservation of their entity, the security goals and policies of payment systems is an issue which is much more sensitive and much more important than other systems which should be defined upon design of system and should be periodically and constantly modified and revised, especially when making major changes to the system and its elements. As it was said, these goals and policies are applied to all those who are involved in payment area and to anyone who has a direct or indirect access to the system or its information. Anyway, system security parameters must be constantly evaluated and controlled (Ojetunde & Shibata & Gao, 2017: 2652). Advancement of technology may cause potential and increasing risks for the system overt time. On the other hand, these advancements provide appropriate and more advanced coping methods. This requires the payment system operators to constantly supervise all technological advancements to ensure that the methods by which they evaluate the system security are still updated and efficient (Mazumder, 2013, 956: ECB, 2013, 2).

Effect of the type of payment system on its security

Traditional payment systems have some disadvantages which are known to everybody. Money can be forged, signatures affixed to the payment orders as well as paper checks may be forged too. Hence, it can be said that the most secure payment system which has been so far designed by man using his past experiences is the e-payment system which is designed properly (Jun and Punit, 2011, 570). This is because payment operations in the said systems are carried out by computer and electronic systems with a high security and because the more the intervention of human factor in payment process decreases, level of security in payment process increases upon decreased effect of bad intensions and/or unintentional errors.

Another advantage of the intervention of computer and electronic systems is to reduce the access of unauthorized individuals to payment system. A good example is the swift network in which the messages are transmitted automatically and they are scattered and unclear until they reach the destination and that unauthorized individuals cannot access to those messages. In swift network, the entry key and the swift code key must be first exchanged by the two brokers. The code is used by a complex mathematical algorithm in which all message letters from the beginning to the end are used in calculating the code and are added to the message. In the destination, the system controls the code and confirms its accuracy accordingly. In other words, encryption and decryption are automatically carried out by the electronic system. In addition, the payment methods that require more identification components enjoy a higher security than other methods (Aigbe and Akpojaro, 2014, 12).

Payment Methods	No. of Identification Components	Type of Identification Components
E-cash	1	Token Encoder
E-check	2	Code Number and Electronic Signature
Smart Card	3	Code Number, Electronic Signature and Fingerprint
Credit Card	2	Code Number and Electronic Signature

Executive confidentiality of payment system

Executive confidentiality standards must be officially defined like security standards and they must be documented by the system operator and operators within the framework of “Service Level Agreements”. Level of services may vary. In the systems using RTGS for example, much time may be allocated to the system’s unanticipated period of failures and no response and as a result, to the decreased level of services. This is while in the systems which are based on settlement at the end of the day, this may only be allocated to the settlement time and not to the length of the day. Therefore, the standards must be planned by considering the governing situation, type of payment system and settlement system (Meharia ,2012: 97).

Moreover, level of executive confidentiality of payment system may depend on alternative ways of payment during serious disturbance in the system’s activities. Executive confidentiality of payment system not only depends on its own elements, but also it is associated with the infrastructures used by the payment system. Another factor affecting the executive reliability of the payment system is that if the activity of any of the elements and components of the system is disrupted, the entire

system will not be disrupted because it is in conflict with the important feature of the market, namely continuity. Hence, when designing the system, it should be considered that a minor system malfunction does not cause the failure of the entire system.

Operators of payment systems must develop their technical and executive facilities and enjoy the best methods and processes in the payment system. This may cover the facilities and processes pertinent to recording, reporting, and analyzing the incidents and events related to the execution process. In this way, payment system authorities and operators will be able to examine the causes of each incident upon its occurrence and to make the necessary changes in the system to improve its function (Jun and Punit, 2011, 570).

As for the changes that occur in each section of the payment system, firstly, these changes must be permissible, and secondly, they must have been controlled and checked. Anyway, development and changes in the system must be such that they do not damage the current and routine activity and do not disrupt it. For example, a new system should be designed separately, taking into consideration all the necessary changes which should be applied to the current system and it should replace the current system in the shortest possible time and with the least delay; of course, with the same level of security and control as in the previous system and not less than that. In any case, the changes must be such that, if necessary, they can be immediately returned to the state prior to making the changes (BIS, 2001, 40).

When designing a payment system, it should be also considered that whether or not that system enjoys such power and capacity to respond with a desirable speed to all demands and expectations at any time and especially, on the peak times and days. The system capacity and function must be constantly measured and evaluated during its lifecycle and a precise planning must be made to make the necessary changes to the volume or pattern to ensure that the system will be able to respond with a suitable speed to any volume of demands (BIS, 2001, 40).

Anyhow, constant supervision of the system by the operator and using the existing standards of the system security, confidentiality and flexibility are some of the ways to increase security and confidentiality of payment systems (Bossone & Cirasino, 2001: 17, Irum, 2011, 32)

Third Principle: Optimal Settlement

The process in the payment system and the transfer of monetary value from the assets of one person to another person, when there are mediums playing roles in this process, require settlement among the mediums. Therefore, settlement can be defined as follows: “Settlement is a process in which the mediums usually transfer monetary value in an open loop system based on network activity to cover the personal transactions they represent” (Benson and Loftesness, 2013, 11).

Open loop systems function based on a Hub-and-spoke model. Almost all large scale payment systems use this model. Open loop system needs the mediums (almost all banks or finance and investment institutions) to join the payment system. These mediums establish work relations with end users (e.g., buyers or merchants) (Benson and Loftesness, 2013, 5). Therefore, settlement in an open loop system is called to a process in which the mediums send or receive money to or from each other. (Benson and Loftesness, 2013, 11)

Types of settlement methods

Settlement process between payment mediums are made in various ways some of which are traditional and old methods and some others are modern and easier methods. Of course, utilization of modern methods requires suitable infrastructures in economy.

Delivered Net Settlement (DNS)

Delivered Net Settlement (DNS) is another settlement method used by payment systems. In these systems, settlement is not made in form of payment by payment; rather, it is made altogether at a certain time of the day which is usually at the end of the day. The banks that use this system for settlement of assets intervene in form of a network of the banks. In this way, at the time of settlement, each bank has just one liability against the settlement system, i.e., it is either debtor or creditor (Summers, 1994, 76). In the following, we will become more familiar with this type of settlement system.

Real Time Gross Settlement (RTGS)

RTGS is a type of settlement system for interbank payments. One of the advantages of this method is that settlement is made between the banks at the time of transaction. Before this settlement method, transactions were conducted among the banks' customers during the day, but the banks did not transfer money until the next day. The result was that the banks owed a huge volume of money to each other. The risk of this case increases when the bankruptcy of one bank affects the other banks and they become bankrupt as well (Kahn & Roberds, 2001: 300).

RTGS eliminates the interval between the start of payment in the transactions and final settlement among the banks and risks pertinent to this interval are eliminated accordingly. In fact, if bankruptcy occurs after payment, it cannot have any effect on payment despite the past. But if there was no zero time principle, this effect would be completed because if the provisions pertinent to bankruptcy were effective as of their issuance date and they were not referred to the past, no risk could threaten payment system in terms of unfinalized settlement. If the bankrupt entity is a bank or a finance institution, the effect of cancellation of transactions will have a destructive effect on the financial and economic system. Some of the institutions may return a part of those amounts, but it is also possible that they cannot return the amounts of money due to granting credits to their customers.

Combined settlement methods

This settlement method enjoys the advantages of both types of the systems mentioned above, i.e., the speed in RTGS and the high efficiency compared to liquidity which is a feature of DNS. Legal basis and executive features of these methods differ from one system to another, but the important feature which is common in all of them is that settlement is made in these systems repeatedly and in certain times and not just one time at the end of the day. Therefore, despite RTGS systems, no separate settlement is made for each payment in any type of the combined systems. Instead, settlement is made in certain intervals by the banks that are present in the network. Despite DNS systems, the combined systems do not make settlement for one time per day, but they do this for several times. In this way, liquidity is efficiently used and settlement is carried out quickly (Willson, 2005, 20).

Finalized settlement

The issue of settlement among the banks involved in payment system is one of the critical points of payment systems, where the rules and regulations must clearly indicate that when settlement is finalized and irrevocable and the risks are transferred. Therefore, the rules and regulations concerning the settlement among the banks involved in payment system is one of the most important factors in the success or failure of payment systems and their accurate function. One of the issues which may be quite harmful for payment system is a rule called the Rule Zero which is recognized in the bankruptcy regulations of some of the countries and is implemented accordingly (Devos, 2006, 47)

The rule of zero hour is a rule based on which a debtor and bankrupt person loses its competence and its transactions are exposed to cancellation as of the day its bankruptcy is declared. When this rule enters the area of finance institutions and banks involved in the payment system, it requires risk creation for third parties, i.e., other banks involved in payment system, in the manner that the settlements they assumed to be correct are cancelled and they have to return the received amounts of money. This case can be very nasty for economic relations of the society in a macro level.

The rule of zero hour is regarded as one of the worrying and destabilizing factors in the financial and banking area and payment systems and it faces the principle of settlement finalization with ambiguity. This results in creation of big risks to the extent that the bankruptcy of one of the banks involved in payment system may lead to a huge wave of enormous bankruptcies and losses. Hence, one of the measures which can be taken in line with settlement finalization is to eliminate the rule of zero hour at least concerning the banks and finance institutions involved in payment systems.

Considering that the rule of zero hour in Iran's Commercial Law may be inferred from the articles pertinent to bankruptcy such as articles 418 and 423 of the Commercial Law and this can be a potential risk at least for the banks and finance institutions that are active in the area of economy and payment systems, it is better to remove any regulations that cause this uncertainty at least in relation to the activists of payment systems in line with finalization of interbank settlement. The necessity of this issue in Iran is evident due to the economic condition of our country and in consideration of the financial balances and reports of the banks and finance and credit institutions.

Fourth Principle: Risk Reduction

The necessity to recognize the risks associated with the payment system

Payment system risks are usually divided into 4 groups, namely legal risk, credit risk, liquidity risk, and operating risk. Legal risk refers to the uncertainty of agreements and distribution of responsibilities. The first step in accurate and effective management of financial risks of payment system is to understand the meaning of these risks by all the persons involved in it, from operators to mediums and final customers as well as settlement institutions, especially credit and liquidity risks which are highly addressed in the payment systems. Therefore, the regulations and procedures must be clear and comprehensive and must restate the important issues in writing and in a simple language for those persons who may face a risk when using the system (Ming, 2005, 7)

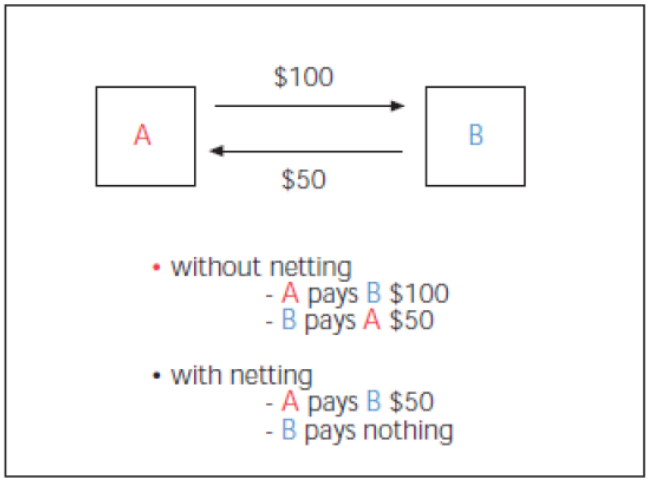
Management of financial risks of payment system (credit and liquidity risks)

Payment system much clearly state the measures it takes to control credit and liquidity risks and to manage them. It must further specify the responsibility of each of the persons who are involved in

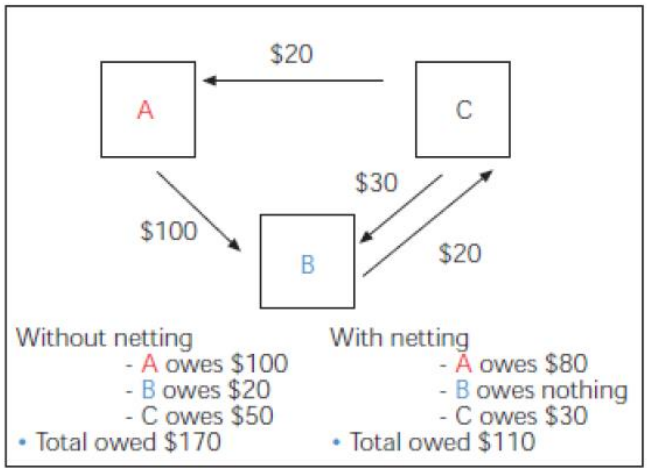
payment system in the said measures. Commercial banks as payment mediums basically undertake the responsibility to conduct transactions and to make payment to the beneficiary. Central bank holds the responsibility to make settlements among the banks. Financial risks are one of the most important risks associated with payment system. The rules and regulations governing the payment system are the main means of dealing with them. Besides covering ordinary and normal situations, regulations and procedures must forecast and cover abnormal incidents and situations as well, such as a situation in which one of the system operators cannot fulfill his liabilities. Method of risk management and distribution of responsibilities among the individuals who are associated with payment system differ depending on the design of each system. For example, type of the settlement method (RTGS or combined settlement methods) used by the system affects risk management (Bergo, 2002, 5).

1- Credit Risk

In general, credit risk is called to a risk based on which it is probable that payment obligor fails to completely fulfill its liability on the specified date and on any date thereafter (ITU-T, 2016, 102). Credit risk is sometimes put forth in the relation between the payer and payee, especially in the assumption in which a timed or noncash payment means is used to fulfill the corresponding liabilities, and sometimes it is put forth in the relation between the banks and failure of a bank in settlement of its debt. As for the second assumption, credit cards may be referred to, because the issuer of the credit card (loan card) accepts an apparent credit risk if the cardholder fails to pay its debt. Credit issue arises among the payment system operators once there is a time interval between accepting to make payment by the system and its final settlement. This case is not put forth in the systems that use a RTGS system which has been designed well, because there is no time difference and delay between the two events (Perold, 1994: 23). The difference between RTGS system and DNS system is related to the settlement form and time and not to the payment method. The systems that enjoy RTGS method settle the payments on a transaction by transaction basis and separately ASAP and within the shortest time interval with payment operations. In contrast, payment is made promptly in the systems that use DNS systems, but its settlement is made altogether on a specified time which has been already agreed upon and it may be during the day of operations or postponed to the end of the day. (BIS, 2001, 26). This puts at risk those who have used the system during the time period ended on the settlement, because inability of one of the operators to fulfill his liability leads to changes in the condition of others and they may even fail to fulfill their new liabilities. The following figures clarifies this case well.



The above figure shows a DNS system between two banks. Thus, if Bank A owes a total amount of 100 dollars to Bank B due to all the payments it has made during the day and Bank B owes 50 dollars to Bank A for all the payments it has made during the day, irrespective of the settlement relation, Bank A must pay 100 dollars to Bank B and Bank B must pay 50 dollars to Bank A. But, by using the DNS system, the two banks decide to postpone the payment and receipt of their debts and claims to another time and to offset them as much as possible. In addition, if one of the parties still owes to the other, it will pay that amount to the other party. As you see in the above figure, Bank A pays 50 dollars to Bank B and their debts and claims are offset in this way. Now, the case becomes more complicated if there are more than two banks involved in this process. The following figure shows a three-sided relation which is the simplest multilateral relationship.



In the above figure, the present banks in the payment system use DNS system and establish a network relationship to settle their accounts by the least money displacement. Thus, Bank A must pay 100 dollars to Bank B and receive 20 dollars from Bank C. Bank B owes 20 dollars to Bank C and claims 30 dollars from the said bank. As it was said, Bank C owes 30 dollars to B and 20 dollars to A. If there were no settlement system governing the relationship of the said three banks, Bank A must totally pay 100 dollars, Bank B must totally pay 20 dollars and C must totally pay 50 dollars and the total amounts which must be transferred would be 170 dollars. This is while by DNS system, Bank A will totally pay 80 dollars, Bank C will totally pay 30 dollars, and Bank B will not have to pay any money and the total amounts to be paid will be totally 110 dollars which shows a decrease of 60 dollars. Of course, this amount can be much less than that depending on the case. Having explained the above relationships, the risk governing the payment systems that use DNS method is specified.

Now, let's assume that in the above figure, Bank C fails to fulfill its liabilities, i.e., it fails to pay its 30-dollar debt to Bank B and its 20-dollar debt to Bank A. If this happens in this system, all the corresponding equations are interrupted and the banks that are involved in this payment system will face new liabilities. As if was said, if this situation is not properly managed, there will be a high risk for the banks involved in this payment system. If Bank C fails to fulfill its liabilities and the settlement system is disrupted, Bank B will not pay its debt (20 dollars) to Bank C due to its direct relationship with the said bank and will also include 10 dollars as its claim considering the 30-dollar debt of Bank C. Bank A that must receive 20 dollars from Bank C as claim should pay its entire debt of 100 dollars to Bank B as the relationship between banks B and C has nothing to do with Bank A (it is probable that Bank A fails to do this due to shortage of credit) and it still claims 20 dollars from Bank C as the debt of the latter. In this way, although Bank B is in direct relationship with the breaching bank, it will receive all its claim and will save itself. But Bank A which has no direct relationship with the breaching bank will suffer from credit risk and it may even fail to fulfill its new liability which is 20 dollars more than the previous one (DeSourdy, 1999, 61).

In contrast, those systems that enjoy RTGS method will create no credit risk for their operators as each payment is settled separately and immediately. Hence, in the systems where there is a difference between the time of accepting to make the payment and the time of final settlement and they use DNS systems, the case of credit risk is quite important and it should be controlled and managed. In this regard, there should be some limitations for the maximum credit risk that each operator can create for the payment system. These limitations can be fixed by considering the financial credits of operators, available liquidity, and executive materials of the system. When a payment system uses DNS method and it sets a credit limit for its operators, it is very important to legally support and cover the communication network of the operators, because if it is probable that the payment is not settled on the due date by the obligor and it remains unprotested, credit risk may be intensified since a recalculation may probably increase the debts of some of the operators, exceeding their credit limit, and one or more operators may accidentally face a credit risk. This will discourage them in respect of risk control as it is not clear which operator will face a credit risk (BIS, 2001, 23).

2- Liquidity risk

Liquidity risk refers to the inability of a system operator to fulfill its short-term financial liabilities before another operator. In bank payment systems, end users are financially liable before the bank (payment mediums), the mediums (banks) hold the same liability before the members of settlement network, and the settlement network in turn holds a financial liability before the banks. This position is regarded as a key position and function for settlement system in the open loop payment system. It means that when a bank enters into a payment relationship with another bank, it does not have to worry about the liquidity of the transmitter bank. However, settlement system has to worry in this regard. If one of the network members in a debtor position fails to fulfill its liability, settlement system (in most cases) must fulfill the liability of that member before the other members. This is one of the reasons that limits most of the membership settlement systems to those group of financial institutions that observe certain capital standards and are under constant legal supervision (Benson and Loftesness, 2013, 25).

Liquidity risk occurs differently in the systems that do not use DNS system. An operator who uses RTGS system must have the required liquidity in its account with the settlement institution so that

its payment request is fulfilled; otherwise, the routine process of the payments of the corresponding system ceases and the payments of that operator face a traffic and the routine process of its payments are locked (Gridlock). This is the same for DNS systems and it occurs when a credit ceiling is defined for the operator and the volume of its requests exceeds the credit defined for that. Repetition of traffic and gridlock of the routine payment process results in distrust with the system and the individuals may use more unsecured alternatives.

There are several ways to solve the problem of payment traffic due to shortage of liquidity. The main solution is hidden in the system design. For example, in a sequential system designed based on the order of entries, macro payments may cause unnecessary delays in the payment system. In contrast, a more advanced algorithm for queue management system can reduce the need in liquidity, decrease the system delays and makes the use of liquidity more efficient (BIS, 2001, 24). Users may use the liquidity provided to them by the central bank to settle their accounts during the day. Here, it is the central bank that should decide how to manage and control the risk of providing this liquidity. First of all, all conditions and provisions for granting liquidity must be clear and explicit. Moreover, some of the central banks obtain pledges and/or set limitations for the users when granting liquidity to control the liquidity risk. In addition, central bank must adopt policies and procedures (for example, regarding the pricing and its services and conditions) to control such cases where the granted liquidity may not be returned to the central bank during the day or on the closing hour of the system. Moreover, special attention must be paid to the role and responsibility of payment system operators in respect of controlling and smoothing the process of payment in the system. These roles and responsibilities must be clearly stated in the corresponding procedures and provisions. One of the tools in this regard is the guidelines provided regarding the operations process of the system by which the operators are encouraged and/or required to take actions in this relation (for example, the operators are required to ensure that averagely, a certain proportion of the payments made by them has been processed by the system within the specified deadlines). Anyhow, development of the systems related to supervisory information and processes plays a significant role in supporting and guaranteeing the implementation of the regulations and procedures pertinent to the control and supervision of financial risks. This information can be effective in determining the credit ceiling of operators, controlling their credit balance with the central bank and borrowing the same and it finally results in management of the financial risks related to the payment system (BIS, 2001, 25).

3- Operating risks (nonfinancial)

Nonfinancial or operating risks may be associated with the payment system, its users or human error and/or it may be related to the influence or misuse of unauthorized individuals and scammers. Systemic operating risk may be caused by failure of compute system or communication lines among the systems.

Risk of fraud

A person who has entered a payment-based relationship may have been cheated and suffers from financial loss (ITU-T, 2016, 31). There are various types of fraud risk in payment. Some specific cases are for special payment systems and some others are more general. Some of the payment systems such as card payment systems have defined high levels of fraud management for the transactions. Other systems such as check payment system and ACH system leave the fraud risk management to the mediums and end users (Sullivan, 2014: 53).

Implementation of accreditation and authentication standards and technical methods in e-payment systems such as Password, Digital Signature, and Secured Communication Channels sharply reduces the risk of fraud and misuse of unauthorized individuals (Jarupunphol, 2013, 279; Omariba, 2013, 438). Although scammers try to profit from technologies and businesses of economic activists, banks or buyers through innovative methods, fraud management system of payment systems enjoys scam neutralization loops and this feature has resulted in emergence of new scam methods and immigration of scammers to other payment systems or mediums (Benson and Loftesness, 2013, 27).

Operating risk

This risk occurs when a transaction user either fails to handle a job who is expected to do or makes a mistake. A wide range of situations fall into this category: Expiry of payment deadline, files with wrong formats, failure or malfunction of devices (such as such as a check stuck in the separating device), etc. If the money that should be legally received by another user remains with the sender as the result of an operating error, the operating error can be followed by serious financial consequences (Benson and Loftesness, 2013, 28). The Bank for International Settlement (BIS) defines operating risk as a risk arising from inefficient local processes, human error and/or foreign systems and/or events. (Hassanzadeh et al., 2014, 418)

Each payment system has a combination of work rules and procedures through which the mediums present in the system try to help each other to compensate for the errors and to avoid financial losses. However, it is not always possible to completely compensate the operating errors. Processors and other third parties (nonbank mediums in the value chain) play an important role in understanding the risk of operations. A third party often expresses in its cooperation contract that it accepts on behalf of a processor the official and legal responsibility to carry out a certain duty under the supervision of payment system laws. If the third party violates in any way from its commitment, the bank which is a party to contract with that third party will remain responsible. For this reason, several payment systems confirm the role of third parties and set some rules to require their direct parties (banks) to control and sometimes to guarantee the third party in the system (EBC, 2013, 3).

Data security risk

The risk threating the data of a final payment user which is available to the bank, processor, network or final users is the risk of probable use of the data. The measures taken by the card networks to establish and implement PCI-DSS standards (Payment Card Industry Data Security Standard) are an effort to effectively manage this case. PCI has recently used the issuer's marking method for more protection of the validity of this type of cards. Today, the leakage risk of important data of payment systems can be minimized by using technical tools, such that only authorized persons can view or receive the data and messages that contain important information on the corresponding transaction. A secured electronic transaction is realized by using the combined encryption and decryption method on the data of messages (Irum, 2011, 32, T Sikis, 2005, 12).

Fifth Principle: Constant Oversight

Central Banks have always addressed security and efficiency in payment and settlement systems (Bossone & Cirasino, 2001: 17) as they not only provide settlement and payment services to other banks but also, they supervise the same in a systematic and official manner, where parameters such

as security and efficiency increase through supervising the systems, evaluating and measuring them by the said goals and if necessary, requiring them to change (BIS, 2006, 3).

The central bank's interest in the security and efficiency of payment and settlement systems is not a new issue. They have played a prominent role in the systems since the past by establishing a secured asset settlement mechanism (by operating one or more payment systems, participating in other systems, concluding agreements and trying to set standard rules and regulations for the systems. Central banks have gained considerable expertise and experience regarding payment systems and probable disorderliness and failure in the market by performing their duties as the bank of the banks and their unique role in maintaining public trust in respect of national money. Their have always used their experience to improve the systems and it has been a good means to establish a monetary discipline which in turn results in economic stability (BIS, 2006, 16).

Supervision of payment systems by the central bank has found a more distinct and more official concept in the recent decades as compared to the past. Today, the activities of the central banks are not just focused on payment and settlement systems; rather, development of payment systems managed by the public sector and the concern to avoid payment problems in the market have made central banks to address supervision more than ever. Advancement, complexity and focus of several payment and settlement systems as well as the high and increasing volume of the credits transferred by these systems indicate the high importance of supervision quite well; whether this system has been designed, manufactured, and implemented by the private institutions or by the central bank. Such development in payment systems and a high volume and concentration in their activities led to the concern that any problem and inefficiency in the design and implementation of payment systems will be followed by several risks.

Regarding the concept of supervision, it can be said that “Supervision of payment and settlement systems is one of the duties of the central bank. Security and efficiency will increase by constant control of the exiting systems as well as those under development, evaluation of the systems with the corresponding goals and if necessary, making changes.” This definition encompasses the goals of public order including supervision (security and efficiency), scope of supervision (payment and settlement system) and supervision activities (constant monitoring or control, evaluation and requiring changes). The elements named in the said definition may be used from the responsibilities, goals and duties of the central banks. It also excludes the supervisory duty of other institutions and authorities in respect of payment and settlement system (BIS, 2006, 17).

The central bank’s supervision and control of its payment systems follows certain principles and provisions. Clarification is the first principle. Central banks must publicly release their supervisory policies including system prerequisites and standards. Moreover, they must set an index to recognize which index has the said prerequisites and standards so that the operators of payment systems become aware of the prerequisites and standards pertinent to the applied supervisory policies and match themselves with such policies. Applying clarification, the central banks will be able to prove the extent of integration in their supervisory approach. Moreover, clarification provides the ground for examining and judging the effect of the policies adopted by the central banks and the possibility of trusting in their performance of supervisory duties (BIS, 2006, 2).

The second principle is to comply with and to implement supervision standards. Central banks must apply the international recognized and confirmed standards regarding the payment and settlement systems as much as possible. Utilization of international standards pertinent to the security and

efficiency of payment and settlement systems can increase the central bank's supervision of the said systems (Sangeetha, 2016, 3).

The third principle is an effective power and competency. The central banks must have the required power and competency to implement their supervisory duties effectively and efficiently. They must have such power to ensure that they are able to obtain any information in relation to payment systems in line with their supervisory duties and to require the payment and settlement systems to make some changes. Central banks mainly use tools in line with fulfillment of their supervisory tasks. What is important in relation of the said tools is their effectiveness and not their forms and shapes. In practice, many of the central banks use the convincing and consulting methods in daily supervisions to obtain information and to make changes in the systems. Some others use other tools in addition to the said tools with the same adequacy to obtain information and to make changes in the systems. And some of the central banks enjoy statutory powers that can be used whenever necessary (BIS, 2006, 3). Central banks must have sufficient resources to fulfill their supervisory task. One of the said resources is trained and skilled manpower. Effective efficiency of these resources requires the central bank to have an integrated structure for supervision.

Nondiscrimination is the fourth principle which means that the supervisory standards must be applied equally and free from any discrimination to all similar settlement and payment methods including those payment systems administered by the central bank. Equal application and implementation of supervisory standards and prerequisites free from any discrimination by the central bank which also covers the systems under the supervision of the central bank itself is quite vital because various payment and settlement systems might be involved in direct competition and the payment and settlement system of the central bank might be one of their competitors (for example, card payment systems that are provided by various payment systems). Central banks must clearly declare their parameters for evaluation and measurement (BIS, 2006, 3). Hence, the central banks must make a distinction between their traditional duty including the provision of payment services on the one hand, and their relatively new duty which is the supervision of payment systems provided by the private sector on the other hand. Therefore, supervision system of the central bank must act independent from the other section.

Cooperation is the fifth principle of supervision. In line with increase of security and efficiency of payment systems, central banks are required to cooperate with other relevant sections and authorities as well as other central banks and to provide the necessary assistance. Supervisory cooperation in local and international cooperation sections can be addressed in this regard. cooperation of central banks with different authorities involved in supervision, such as legislators, security authorities and supervisors of the banks provide a mechanism that empowers them in fulfilling their duties through cooperation. Moreover, there will be no interference between their duties with the responsibilities of other authorities involved in supervision. This can create a strong supervision in payment and settlement systems (BIS, 2006, 4). In addition to the cooperation of supervisory systems and authorities inside the borders of a country, the same cooperation must be present in an international and extraterritorial level where extraterritorial and multicurrency payment systems deal with more than one central banks. The respective guidelines have been provided in this regard accordingly (such as CPSS and Lamfalussy principles) (BIS, 2006, 3). Collaborations the central banks lead to continuation of supervision and decreases the risk of consideration of contradictory requirements for the system by various central banks. Application of international recognized supervision standards plays an important role in reducing the risks arising

from contradictory supervisory policies and it has a significant effect on successful application of a collaborative supervisory approach among central banks. Lamfalussy Principle is one of the principles designed and set in line with collaborative activities of central banks in supervision. Since the time Lamfalussy Principle was released in 1990, some of the central banks used it as a basis and fundamental for international supervision collaboration. The main element of this principle is that central bank shall hold the main responsibility of supervising the system and consider the interests of all the corresponding central banks in this respect (BIS, 2006, 28).

Sixth Principle: Legal Framework

Payment systems must have a good legal foundation in all legal systems within which they act. A legal foundation is quite effective for a payment system and its general function. For example, some of the effective rules in development of a legal framework for payment system include those related to laws on liabilities, contracts, bankruptcy, bank rules and regulations, and commercial documents. In some cases, the rights of competition and the laws on supporting the consumers may be regarded as effective rules for a legal framework for payment system. In addition, there are certain rules which are much more effective than the said rules in formation of a legal framework for the payment system, such as the rules and regulations related to the central bank, the rules concerning payments including e-payments, the rules governing final settlement and settlement network. Where the case of payment has an extraterritorial aspect, the rules of the countries other than the host country of the system may be effective in the system function (BIS, 2001, 16). A precise legal basis in payment system provides a framework based on which all the parties involved in payment system, ranging from operators, mediums and end users to legislators understand their rights and obligations in this relation. It is the understanding of the said rights and obligations that forms the basis of risk management mechanisms as the said mechanisms are designed and managed based on the assumptions they have regarding the rights and obligations of the individuals involved in payment system. Hence, the management efficiency of payment system risks is rooted in the high confidentiality of the rules that develop the rights and obligations of those who are associated with payment system. Evaluations made regarding the good performance of risk management mechanisms have always referred to the questions concerning the efficiency of the legal foundation of payment system (BIS, 2001, 16).

CONCLUSION

In monetary economy, financial markets and payment systems reciprocally depend on each other. Settlement procedures in the markets and in some cases, commercial procedures are directly related to design and implementation of payment systems. Hence, design and function of payment systems must address the demands of financial markets and end users of payment systems to meet the requirements for an efficient financial system and economic efficiency and to control and mange financial risk in payment and banking systems by using the technology and legal means. Fulfillment of payment services may require provision of more than one payment means and settlement mechanism to meet various preferences in consideration of payment cost, settlement acceleration and distribution of operating and credit risks in payment process.

Today, payment system is still exposed to quick changes. Newly emerged technologies, new participants, revised regulations and globalization has caused this complicated issue to lead us towards companionship. Central bank is legally responsible to upgrade efficient payment systems.

This responsibility is more claimed upon swift change of systems because concentration on the central bank's responsibility is quite different from that of the market activists and especially the banks.

Based on the conducted studies and experiences of the financial system, efficiency, security and confidentiality, optimal settlement, risk reduction, constant supervision of the Central Bank and enjoying legal foundations are among the most important procedural principles of payment system. A proportion between the costs and quality of services, optimal use of resources, security and risk reduction, competitiveness, capacity for activation of added-value of services, implementation schedule and speed of action, dominant payment standards, integrity, scalability and adaptability are among the indexes of payment system efficiency.

Confidentiality and efficiency mean that payment means should be provided to meet the demands of end users of payment systems with the costs that the operators are willing to pay, as risk management, license of the payee, payment finalization, settlement method, dealing with disputed payments, sharing fraud information, security controls, tolerance, protection of end user's data, verification of the identity of the end user/provider, and partnership requirement are among the elements of payment system security and safety.

In addition to effective and comprehensive supervision of central bank, legal framework, data privacy, payment system rules, supporting the rights of consumers, and international legal framework are among the legal prerequisites of an optimal and reliable payment system.

REFERENCES

[1]. Hassanzadeh, Ali et al., 2014. **Money and Modern Banking**, Tehran, Jangal Publications, 1st edition.
[2]. Aigbe, P., & Akpojaro, J. (2014). Analysis of security issues in electronic payment systems. International journal of computer applications, 108(10).
[3]. Benson, C. C., & Loftesness, S. (2013). Payments Systems in the US: A Guide for the Payments Professional. Glenbrook Partners.
[4]. BIS(Bank for International Settlements)(2001). Core Principles for Systemically Important Payment Systems, Basel(Switzerland).Press &Library services.
[5]. BIS(Bank for International Settlements)(2006). Principles for financial market infrastructure, Basel(Switzerland).Press &Library services
[6]. Bossone, B., & Cirasino, M. (2001). The oversight of the payments systems: a framework for the development and governance of payment systems in emerging economies. The World Bank.
[7]. Camenisch, J., Piveteau, J. M., & Stadler, M. (1996, January). An efficient fair payment system. In Proceedings of the 3rd ACM Conference on Computer and Communications Security (pp. 88-94).
[8]. Cirasino, M., & García, J. A. (2008). Measuring payment system development. Payment Systems Policy and Research, Financial Infrastructure Series, World Bank, Washington, DC.
[9]. DeSourdy, L. (1999). New legislation on netting and payments finality. Reserve Bank of New Zealand Bulletin, 62(2).
[10]. Devos, D. (2006). Legal Protection of Payment and Securities Settlement Systems and of Collateral Transactions in European Union Legislation. In Seminar on Current

Developments in Monetary and Financial Law–Law and Financial Stability, hosted by the International Monetary Fund, Washington, DC.
[11]. ITU-T(International Telecommunication Union)(2016). Focus Group Digital Financial Services: Payment System Oversight and Interoperability.
[12]. Jun S. and Punit A. (2011), The more secure the better: A study of information security readiness. Industrial Management and Data Systems. 111(4), pp.570-588.
[13]. Kahn, C. M., & Roberds, W. (2001). Real-time gross settlement and the costs of immediacy. Journal of Monetary Economics, 47(2), 299-319.
[14]. Meharia, P. (2012). ASSURANCE ON THE RELIABILITY OF MOBILE PAYMENT SYSTEM AND ITS EFFECTS ON ITS'USE: AN EMPIRICAL EXAMINATION. Accounting and Management Information Systems, 11(1), 97.
[15]. Ming, S. (2005). Risk Management of Payment System and Fedwire's Practice [J]. Studies of International Finance, 8.
[16]. Ojetunde, B., Shibata, N., & Gao, J. (2017). Secure payment system utilizing MANET for disaster areas. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 49(12), 2651-2663.
[17]. Perold, A. (1994). The payment system and derivative instruments.
[18]. Rambure, D., & Nacamuli, A. (2008). Securities Settlement. In Payment Systems (pp. 148-157). Palgrave Macmillan, London.
[19]. Sullivan, R. J. (2014). Controlling security risk and fraud in payment systems. Federal Reserve Bank of Kansas City, Economic Review, 99(3), 47-78.
[20]. Summers, M. B. J. (Ed.). (1994). The payment system: design, management, and supervision. International Monetary Fund.
[21]. Willison, M. (2005). Real-Time Gross Settlement and hybrid payment systems: a comparison.