Bulletin of TUIT: Management and Communication Technologies

Volume 1 | Issue 1 Article 6

1-22-2018

REASONS OF APPEARANCE AND ASSESSMENT FEATURES OF RISK IN ELECTRONIC PAYMENT SYSTEMS

Mahina AbdulAzalova
Tashkent university of information technologies named after Muhammad al-Khwarizmi, bonu444@mail.ru

Mathamat Khaidarova
Tashkent university of information technologies named after Muhammad al-Khwarizmi, haydarova.m@mail.ru

Follow this and additional works at: https://uzjournals.edu.uz/tuitmct

Recommended Citation
AbdulAzalova, Mahina and Khaidarova, Mathamat (2018) "REASONS OF APPEARANCE AND ASSESSMENT FEATURES OF RISK IN ELECTRONIC PAYMENT SYSTEMS," *Bulletin of TUIT: Management and Communication Technologies*: Vol. 1 : Iss. 1 , Article 6.
Available at: https://uzjournals.edu.uz/tuitmct/vol1/iss1/6

This Article is brought to you for free and open access by 2030 Uzbekistan Research Online. It has been accepted for inclusion in Bulletin of TUIT: Management and Communication Technologies by an authorized editor of 2030 Uzbekistan Research Online. For more information, please contact brownman91@mail.ru.

REASONS OF APPEARANCE AND ASSESSMENT FEATURES OF RISK IN ELECTRONIC PAYMENT SYSTEMS

Abdul-Azalova M.Ya., Khaidarova M.Yu.

Abstract: In this era of digital technology, when many new technologies were aimed at integrating new technologies, the blockchain turned out to be the most effective. Blockchain is an innovation in the virtual business world for creating a payment gateway that allows you to create a more secure environment for users. If we are talking about blockchain wallets, they are mainly designed to quickly and securely manage online payments. In this regard, the demand and popularity of the development of blockchain collages is constantly increasing. This article development of electronic payment systems study is devoted. The article discusses the issues of modeling and risk assessment, approaches to risk prevention in the field of electronic payments. In particular, a new blockchain technology wallets is being considered, which will make it possible to prevent a number of risks in electronic payment systems, allow payments to be made at high speed, ensuring a high level of security. Ultimately, companies are looking for convenient, fast and reliable payment systems to streamline processes, and blockchain technology has the potential to make all this a reality - and therefore we expect companies to increasingly look for payment service providers who can help them with access to blockchain . This is likely to be particularly relevant in areas with high levels of exposure, such as multicurrency payments or multi-country payments, which relatively small payment gateways comprehensively cover even in the world, not connected by a single chain. Entering the partner market of other states also apply for legal audits.

Keywords: electronic payment systems, risks, blockchain, bitcoin, security, chain, block.

Introduction

Legal Introduction

The processes of introducing new information technologies affect all areas of the state and the economy. This trend has affected the development of e-business. E-business is an aggregate concept for many classes of information systems that automate the commercial work of an enterprise (a similar definition is given in the law of the Republic of Uzbekistan. "On Electronic Commerce" in Article 3) [1]. In this system, an important financial task is performed by electronic payment systems.

Electronic payment systems (EPS) - a combination of hardware devices, software, information networks and organizational structure that provide one or more types of payments:

- remote electronic money transfer;
- payments using plastic cards with a magnetic strip or smart cards;
- payments by electronic money;
- acceptance or payment of cash from individuals.

EPS can be carried out by both state and commercial organizations. Commercial payment systems are organized by individuals or legal entities. Using EPS, goods, work, services are paid, cash is received from credit organizations, money is transferred from the account of one organization or individual to the account of another organization or other individual. The technologies they use allow settlements directly make calculations between contractors. This excludes the transfer of money from one account to another at a bank or other financial institution. EPS also includes banking and non-banking payment terminals, remote financial services and remote banking services (RBS), including Internet banking and SMS banking, mobile banking, mobile financial services of mobile operators, electronic money.

Main part

Today, EPS are classified as follows:

- state (banking, debit, credit);
- commercial / retail (on the basis of electronic money, on the basis of virtual money, on the basis of virtual currency, electronic wallets, electronic checks, agent points for receiving payments, money transfers).

According to the Law of the Republic of Uzbekistan "On Electronic Payments", the Payment system is the totality of relations that arise between the entities of the payment system when making electronic payments. [2]

Types of payment system:

- interbank payment system;
- intrabank payment system;
- retail payment system.

The development of electronic business is directly related to the active development of commercial / retail electronic payment systems. In the Republic of Uzbekistan, this issue requires refinement due to existing legislative restrictions, for example, according to the decree of the Central Bank of the Republic of Uzbekistan, all transactions conducted on the territory of the republic should be conducted through the banking system, which, in turn, limits the activity of retail / commercial electronic payment systems, as well as on the territory of the republic for settlements, you can use only the national currency - sum, which excludes the possibility of using the services of international retail electronic payment systems.

Published by 2030 Uzbekistan Research Online, 2018

The solution of the issues discussed above will enable the active introduction of retail electronic payment systems, contributing to the development of the electronic business system in the Republic of Uzbekistan. The development of electronic business is an indisputable factor for the development of the economy of the republic and successful integration into the global system of electronic business.

Along with the regulatory aspects of EPS, there are issues of identifying and preventing risks in these systems. Issues of definition, modeling and risk assessment in EPS have received much attention in the past few years. The main reason for this can be called financial globalization and, as a result, the standardization of risk management approaches in payment systems. The most relevant are operational risks.

Operational risk - risk, loss as a result of an inadequate or erroneous internal process, the actions of employees and the system or external event.

This definition includes legal risk but excludes strategic and reputational risks. The definition of operational risk in this form was accepted by all market participants as a standard, it is universal since it can be applied to various financial institutions and, moreover, clearly defines the sources of operational risks.

There are various classifications of operational risk. The most important are technological risks. Technological risk - the risk of loss due to improper data processing as a result of failures, errors, unauthorized access, etc.

To calculate operational risks, a number of indicators must be taken into account. Risk indicators are parameters that allow you to identify possible changes in advance for certain types of operational risks and related control measures that can lead to losses. Risk indicators are objective and quantitative. [3]

At the present stage of determining and developing a model of operational risk, when all aspects are classified and approaches are largely developed, according to their assessment, it is necessary to work not with individual risks, but with the totality of risks to which the entire payment system may be exposed. Therefore, special attention should be paid to aggregation in risk management (risk integration). The key idea of calculating the aggregate (aggregated) risk of a payment system as a financial institution is the existence of a non-zero probability of a simultaneous change in the values of various types of operational risk. Thus, the presence of this relationship between the values of different types of operational risks makes it possible to build competent risk management, taking into account the principle of diversification, when a situation arises in which the overall risk will be less than the sum of individual risks. In the practice of risk management, the concept of non-zero probability of joint implementation of risks is evaluated on the basis of the ratio of values that serve as indicators of different types of risks. The main way is to evaluate the correlation as the mathematical expectation of the simultaneous deviation of two random variables from the average value.

The standard risk correlation assessment is as follows (1):

$$Corr(R_i;R_J)=\rho_{ij}=(E(R_i-E(R_i))(R_j-E(R_j)))/(\delta(R_i)*\delta(R_j)) \quad (1)$$

where E is the operator of the mathematical expectation of a random variable;

δ - standard deviation of a random variable from its mathematical expectations;

R_j - is an estimate of the magnitude of a certain type operational risk;

Then the aggregate (aggregated) risk of RAggregate will bedetermined by the risk aggregation formula in a linear form:

$$R_{Aggregate}\sqrt{\sum_{i=1}^{N}R_i^2+\sum_{i\neq j}\rho_{ij}*R_i*R_j} \quad (2)$$

The aggregate risk values obtained in a similar way in payment systems of various banks will be difficult to match. The question is that even inside the payment system of a bank is difficult to achieve consistency and comparability of aggregate risk assessments, received at different reporting dates. To solve this issue, the most acceptable is the use of blockchain technology for organizing transactions inside and outside EPS. [4-6]

Blockchain is a continuous sequential chain of blocks (linked list) containing information that is built according to certain rules. Most often, copies of block chains are stored on many different computers independently of each other. This technology is a universal tool for building various databases, which has the following advantages:

1. Decentralization: There is no main storage server; All records are stored by each participant in the system; Full transparency; Any participant can track all the transactions that took place in the system.

2. Confidentiality: All data is stored in encrypted form; The user can track all transactions but cannot identify the recipient or sender of information if he does not know the wallet number; For operations, a unique access key is required.

3. Reliability: Any attempt to make unauthorized changes will be rejected due to inconsistency with previous copies; For legal data changes, a special unique code is required, issued and confirmed by the system.

4. Compromise: Data that is added to the system is verified by other participants.

Blockchain can be especially useful for international transactions, which has a significant positive impact on the speed, cost and security of international payments. A blockchain based on a payment gateway will allow payments to be made anywhere in the world within 15-20 seconds. This is significantly shorter than payments through traditional banking channels, which can take up to three days. Using the blockchain system as a basis, payments will

be safe and therefore less prone to attack than traditional online payment gateways. [7-10]

Currently, this ability to make business payments or offer batch payment solutions for companies is an option for only a few technology companies (usually limited to fintex space). The financial services sector is stimulating the protection potential to radically change its functioning, but the transition to large-scale implementation will inevitably take time. We must also remember that, despite forecasts, the reality of blockchain is not always so simple - and these contradictions also slow down the pace of implementation. Processing time, transaction costs, and network blocking speed requirements are currently limited by its scalability.

The technologies that blockchain is built on use advanced cryptography, user-specific network protocols, and performance optimization. Today, in addition to bitcoin, there are several more open source blockchain implementations:

- Ethereum: the open source blockchain platform from the Ethereum Foundation;
- Hyperledger: another open source implementation, only from the Linux Foundation. The first implementation was published recently;
- Eris Industries: Tools to help use Ethereum, bitcoin, or fully independent blockchain, mainly to create private networks. Their instructions and guides are a great starting point for a blockchain review.

Blockchain-based wallets maintain a high level of crypto security, because security is the most important task of any business. Although these wallets are implemented in an intuitive user interface, they have complex processes in the background. This causes great interest in how these wallets work with the chain, how secure and simple transactions with these wallets are, how and where they store digital currency, etc. [11-14]

There are basically four types of cryptocurrencies or blockchain wallet available to users:

1. Electronic wallets (software): this type of wallet is software that is installed on a personal computer or mobile device. They give full control over bitcoins, but sometimes it can be difficult for beginners to maintain them.

2. Web wallets. This type of wallet is hosted by a third party. These paper wallets are more like applications / platforms and may be easier to use. Since they are hosted by third parties, the security they provide should be reviewed to ensure that they have systems in place to protect their bitcoins.

3. Hardware wallets. These wallets store user private keys on a hardware device (such as USB). These wallets are compatible with several web interfaces and offer support for multiple cryptography. To use these types of wallets, you need to connect them to any Internet device, enter the PIN code and confirm. Since all funds are stored offline, hardware wallets are the safest wallets available.

4. Paper wallets: a key pair (public and private) is generated for these wallets using a software application, and then printed to complete the transaction. Paper wallets usually work with software wallets for buying and selling. The transfer process is used to transfer funds, which includes scanning a QR code and manually adding keys. [15-18]

For online transactions with blockchain, the wallet stores private and public keys. The wallet interacts with several block chains to check online payments, which allows users to buy or sell one or more cryptocurrencies.

It is important to understand the concept of public and private keys, which are in the blockchain for online payments. The public key can be transferred to anyone, and the private key is kept secret. These keys work very similar to the concept of locking (private key) and key (public key). No matter how many people have keys, they can be useful only if they are used to open the correct block, that is, the private key is correctly mapped to the public key. [18]

By unlocking the vault, you can easily see what is stored in it. Similarly, when the private and public keys used in a transaction match, users can see the contents of their digital assets (bitcoins, ICO tokens, etc.) in their wallets.

The purpose of the blockchain wallet is to simplify the exchange of cryptocurrencies for users. Depending on the frequency and volume of online payments, you can choose between different types of blockchain wallets, as described above.

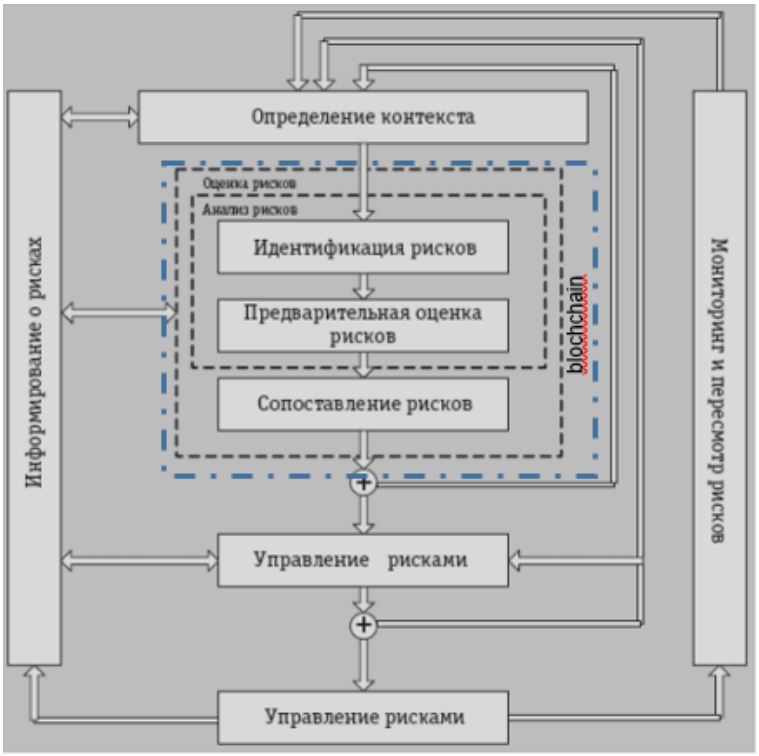

Figure 1. Operational risk management process

As shown in the figure, the risk management process is iterative. The first iteration of risk assessment consists of tasks to determine the context, identify threats and vulnerabilities, and to perform a quantitative risk assessment and risk assessment (comparison). The result of the first iteration of the risk assessment may be satisfactory to support the risk treatment process. If this is not the case, for example, since insufficient information was available, another iteration of the risk assessment should be carried out, which will, for example, include gathering additional information, clarifying the scope and determining the context, further consideration of external influences and limitations, further exploration of vulnerabilities and threats. The goal of the risk treatment process following this is to achieve an acceptable level of risk, for example, by using appropriate controls (countermeasures). These controls typically include controls related to best practices, but more specific controls are often also needed. The success of the risk treatment process depends on the results of the risk assessment. A situation in which the risk treatment process does not immediately lead to an acceptable residual risk is highly likely. In such a situation, another iteration of the risk assessment occurs, followed by risk processing. [19-25]

The following risk-taking process should ensure that the remaining risks are clearly accepted by management. This is especially important in situations where the implementation of controls is not implemented or is delayed, for example, due to cost. It is important that the risk is communicated to relevant parties throughout the entire risk management process, such as management and operations personnel. The use of blockchain technology at the stages of risk identification, preliminary risk assessment and risk comparison will make it possible to conduct risk assessment and analysis at a more effective level, thereby improving the resulting indicators. [10]

Conclusion

Thus, identifying the types of operational risk inherent specific payment system, fixing the response reaction to the occurrence of risk events, the payment system operator will be able to organize risk management and avoid major losses from the implementation of risks. Species assessment and aggregation, on the other hand operational risk is also important, as it affects the estimated reserves for possible losses. All components of the given model important when organizing risk management within the system.

Ultimately, companies and private users are looking for convenient, fast and reliable payment systems to streamline processes, and blockchain technology can make all this a reality, and therefore it is expected that companies and private users will increasingly look for payment service providers that can help them with access to blockchain. This is likely to be especially true in high-risk areas, such as multicurrency payments or payments from several countries, which relatively small payment gateways cover comprehensively even in the world, not connected by a single chain.

The use of blockchain technology will provide an opportunity to improve performance significantly. In turn, this will lead to an improvement in the quality of

the services provided, increased security and reduce the time spent on each transaction.

REFERENCES

[1] Law of the Republic of Uzbekistan "On Amendments and Additions to the Law of the Republic of Uzbekistan "On Electronic Commerce "dated May 22, 2015 No. ЗРУ-385

[2] The Law of the Republic of Uzbekistan "On electronic payments". Adopted by the Legislative Chamber on November 2, 2005, approved by the Senate on December 3, 2005.

[3] Annie Mike. "Towards an ethics of convocation, observation, credibility and timeliness." 2015. Science, Technology, and Human Values 41 (1): 93–117.

[4] Atsori M. "Blockchain technology and decentralized management: is the state still necessary?", 2015. (http://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2709713).

[5] Dong Hye et al. "Virtual Currencies and Beyond: Initial Considerations," 2016. Washington, D. S.: International Monetary Fund.

[6] http: //www.reglament.net/bank/raschet/2005_4_article.htm

[7] "Blockchains: A Big Chain of Confidence in Things," Economist. October 31, 2015 "The technology underlying bitcoins allows people who do not know or do not trust each other to create a reliable ledger. it has consequences far beyond cryptocurrency"

[8] Morris David Z. "A venture fund without blockchains based on a blockchain attracts $ 100 million and counts." Fortune. Source May 23, 2016.

[9] http://www.it.ru/press_center/publications/3818/

[10] Brito Jerry, Castillo Andrea. Bitcoin: a textbook for politicians. Fairfax, VA: Mercatus Center, George Mason University. October 22, 2013.

[11] Aliev, F.A., Niftiyev, A.A., Zeynalov, J.I. (2011). Optimal synthesis problem for the fuzzy systems in semi-infinite interval. Applied and Computational Mathematics, 10(1): 97–105.

[12] Hasanli, Y., Hasanov, F., Mansimli, M. (2010). Equilibrium prices model for sectors of Azerbaijan economy based on input-output tables, EcoMod. International Conference on Economic Modeling, Istanbul, Turkey, July 7–10, 2010.

[13] Kerre, E.E. (2011). The impact of fuzzy set theory on comtemporary mathematics (survey). Applied and Computational Mathematics, 10(1): p. 20–34.

[14] Yager, R.R., Zadeh, L.A. (ed.) (1994). Fuzzy Sets, Neural Networks and Soft Computing. Thomson Learning. p.440.

[15] Avital, M., Hedman, J., & Albinsson, L. (2017). Smart Money: Blockchain-based Customizable Payments System. Dagstuhl Reports, 7(3), p.104-106.

[16] A. K. Koç, E. Yavuz, G. Dalkılıç, "Towards Secure E - Voting Using Ethereum Blockchain", 2018.

[17] L. Thomas, C. Long, P. Burnap, J. Wu, N. Jenkins, "Automation of the supplier role in the GB power system using blockchain-based smart contracts", CIRED - Open Access Proc. J., vol. 2017, no. 1, pp. 2619-2623, 2017.

[18] M. Turkanović, M. Hölbl, K Koščic, M. Heričko, A. Kamišalić, "EduCTX: A blockchain-based higher education credit platform", IEEE Access, vol. 6, no. March, pp. 5112-5127, 2018.

[19] O. Novo, "Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT", IEEE Internet Things J., vol. 5, no. 2, pp. 1184-1195, 2018.

[20] J. Gao et al., "GridMonitoring: Secured Sovereign Blockchain Based Monitoring on Smart Grid", IEEE Access, vol. 6, pp. 9917-9925, 2018.

[21] X. Huang, C. Xu, P. Wang, H. Liu, "LNSC: A Security Model for Electric Vehicle and Charging Pile Management Based on Blockchain Ecosystem", IEEE Access, vol. 6, pp. 13565-13574, 2018.

[22] M. Hossain, R. Hasan, S. Zawoad, "Probe-IoT: A public digital ledger based forensic investigation framework for IoT", IEEE INFOCOM 2018 - IEEE Conf. Comput. Commun. Work. (INFOCOM WKSHPS), pp. 1-2, 2018.

[23] L. Kan, Y. Wei, A. Hafiz Muhammad, W. Siyuan, G. Linchao, H. Kai, "A Multiple Blockchains Architecture on Inter-Blockchain Communication", Proc. - 2018 IEEE 18th Int. Conf. Softw. Qual. Reliab. Secur. Companion QRS-C 2018, pp. 139-145, 2018.

[24] P. D. S, K. Singi, V. Kaulgud, S. Podder, "Evaluating complexity and digitizability of regulations and contracts for a blockchain application design", Proc. 1st Int. Work. Emerg. Trends Softw. Eng. Blockchain - WETSEB '18, no. 1, pp. 25-29, 2018.

[25] F. P. Hjalmarsson, G. K. Hreioarsson, M. Hamdaqa, G. Hjalmtysson, "Blockchain-Based E-Voting System", 2018 IEEE 11th Int. Conf. Cloud Comput., pp. 983-986, 2018.