JOURNAL OF APPLIED
COMPUTER SCIENCE
Vol. 26 No. 2 (2018), pp. 147-160

Virtual Money for Purchases in School Shops and for Educational Applications: eZloty

Michał Pawlak[1], Jakub Guziur[1], Aneta Poniszewska-Marańda[1], Jan Stolarek[1]

[1]*Lodz University of Technology, Poland*
Institute of Information Technology
Lodz, ul. Wolczanska 215
michal.pawlak@edu.p.lodz.pl, jakub.guziur@edu.p.lodz.pl,
aneta.poniszewska-maranda@p.lodz.pl, jan.stolarek@p.lodz.pl

Abstract. *Recent developments in Polish legislation concerning the healthiness of products in schools shops and results of law compliance verification resulted in a need for a way to supervise purchases in school shops. In this article, a solution for this problem is presented in a form of an online payment platform utilizing virtual currency called eZloty. The platform is based on blockchain technology which allows storing transaction history in an immutable form. As a result, eZloty payment system would enable supervision of products bought in schools, thus creating a possibility for more directed actions promoting healthy food and compliance with ministry regulations.*
Keywords: *virtual currency, blockchain, payment platform.*

1. Introduction

In 2008, an entity hidden under pseudonym Satoshi Nakamoto published a paper describing Bitcoin, a new generation of digital currencies [1]. The main innovation behind it was blockchain, which is a distributed system of ledgers stored in a chain of connected blocks and an algorithm that collectively negotiates and

validates contents of the blocks in a peer-to-peer network [**?**, 2]. The technology is considered by many to be revolutionary and is scrupulously researched [3, 4]. One of the most interesting properties of blockchain is an ability to create a platform for data verification, which can be accessed by anyone [5]. This characteristic is crucial for solving the presented in this paper issue of school shops.

Research conducted in 2017 by Supreme Audit Office (pol. *Najwyższa Izba Kontroli*) in Poland showed that despite regulations, 30% of verified school shops sold unhealthy food [6]. Furthermore, students were still able to buy junk food in other shops outside of any ministerial or parental control. This conclusion resulted in a need for a method for supervision of sales in a school environment. A possible solution could be an online payment platform utilizing virtual currency for conducting and recording transactions. It would allow promoting healthy food by enabling students to make purchases only in verified and accepted shops. In addition, parents would be able to supervise what their children buy and where. Finally, the platform would enable control of products sold in school shops and whether they are consistent with the ministry regulation.

Another advantage of such platform that cannot be overlooked is potential for educational applications. Utilization of virtual currency in a supervised environment would allow students to learn about underling technical solutions and practice its usage. Furthermore, online payment platform with virtual currency would allow students to gain experience with business practices in a safe and controlled environment. Additionally, the inclusion of gamification design principles may further increase motivation and involvement of students, which in turn would help the platform achieve its goal of promoting healthy food [7, 8].

In this paper, an online payment platform utilizing virtual currency based on blockchain technology is described. Its main goal is to promote healthy food by enabling purchases only in certified school shops. The platform allows parents to supervise transactions of their children and use obtained knowledge to influence future purchases. Finally, the platform allows the ministry to control the products sold in the schools shops and to verify whether they follow the ministry directives.

The paper is organized in the following way: section 2 describes the virtual currencies and methods of utilizing them as a payment. Section 3 presents the technical aspects of blockchain technology. Section 4 deals with the original payment platform for verifiable transactions in school shops while section 5 describes an overview of works related to presented field.

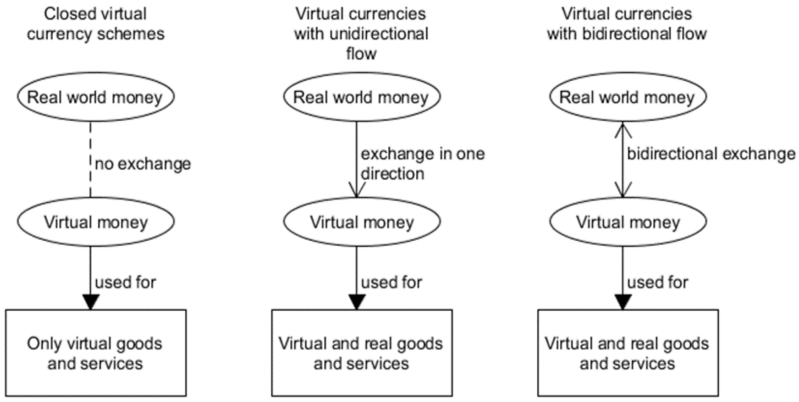

Figure 1: Classification of virtual currencies according to ECB, adapted from [10]

2. Current state of virtual currency solutions

Virtual currency (VC) is defined by *European Banking Authority (EBA)* as digital representation of value independent of a central or a public authority, which may be attached to fiat currency and which can be used by natural or legal persons to conduct business transactions and can be stored, traded and exchanged by electronic means [9]. Another definition by *European Central Bank (ECB)* describes VCs as a type of unregulated money in a digital form, which is controlled and issued by its developers, and utilized by a specific virtual community [10]. As can be seen, both definitions are similar. However, the EBA's definition is more specific and will be used for the remaining of this paper.

Virtual currencies are implemented on many different platforms and take many different forms. Due to this fact, there is no single way for their classification. In [10] ECB proposes a method based on interactions and relations between the virtual money and its real world counterpart. Figure 1 illustrates three classes of the virtual currencies schemes.

Closed virtual currency schemes represent forms of virtual currencies in which there is no official relationship between the real world currency and the virtual currency. This type of VCs is most common, but not exclusive, in multiplayer video games and can be spent only on virtual goods and services. For this reason, it is often called "in-game currency" [10]. One of the examples of such currency

is "gold" in massively *multiplayer online role-playing game (MMORPG)* World of Warcraft, which can be used only for in-game purchases and cannot be legally used outside the game [11].

Virtual currencies with unidirectional flow describe VCs which can be purchased with the real money and can be used for both virtual and real goods and services. It is important to note that this type of VC cannot be sold back for the real money [10]. In general, virtual currencies with unidirectional flow work similarly to gift cards offered by many companies. For example, Vale Corporation allows users of their platform (Steam) to buy virtual funds, stored in Steam Wallet, which can be used only for purchases on the platform [8].

Virtual currencies with bidirectional flow consist of VCs which can be freely exchanged with the real money and vice versa. VCs of this type do not differ much from the real world currencies and can be used for purchases of both virtual and real goods and services [10]. One of most illustrious examples of such currency is Bitcoin, which in recent years became one of the most widespread cryptocurrency and can be traded on stock exchanges as any real world currency [12].

It is important to note that virtual money is not the same as electronic money. Electronic money by definition provided by ECB is just representation of the traditional money stored electronically in the same unit of account and with the same value as an equal amount of the real world money, thus preserving the link between the electronic and the traditional representations of money [10]. Virtual currency, on the other hand, changes the unit of account during an exchange and its value may differ over time due to rate fluctuations dependent on the issuer [10].

The main reason for adapting virtual currency is a possibility of generating additional income for issuers by monetizing their applications and services. Moreover, VCs can motivate their users to make purchase by facilitating transactions and reducing their costs by removing the need for repeating transfers from actual bank accounts. Finally, when combined with gamification principles, VCs can ensure constant interest and loyalty of customers with a promise of reward [10].

3. Blockchain technology

Blockchain technology is a result of a combination of two elements [2]:

- blockchain data-structure,
- blockchain algorithm.

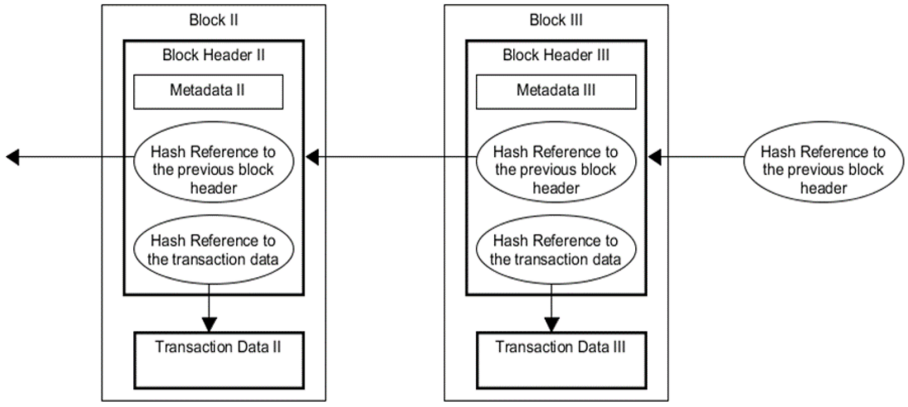

Figure 2: Structure of a blockchain, adapted from [2]

Blockchain data-structure refers to a way of organization of data in units called blocks that are chronologically ordered and connected with each other. This approach results in a chain-like structure made of blocks containing data. All blocks have the same internal structure, which in general consists of: (i) a block header with block metadata (e.g. creation timestamp), a hash reference to the previous block header and a hash reference to the transaction data; (ii) transaction data of various types, for example, money transfer. An exemplary blockchain is presented in figure 2, in which ovals represent hash references in the block headers and arrows point to referenced elements [13].

Hash references are results of an application of a cryptographic hash function on the data stored within each block. The function is one-way and maps arbitrary-sized data to a unique fixed-size bit string, called hash value. A crucial property of this function is change-sensitiveness with respect to input data. Any change of the input changes the hash value, which results in the immutability of the order of blocks of the whole blockchain [14]. Furthermore, changing a single hash reference would force changes in all following blocks. This process is computationally expensive, which discourages any potential attacker. Finally, the correctness of blocks can be verified due to an ability to uniquely identify each block and transaction. Blockchain technology can utilize various cryptographic hash functions, for instance, different versions SHA or RIPEMD algorithms [**?**].

Blockchain algorithm refers to a sequence of instructions in a peer-to-peer net-

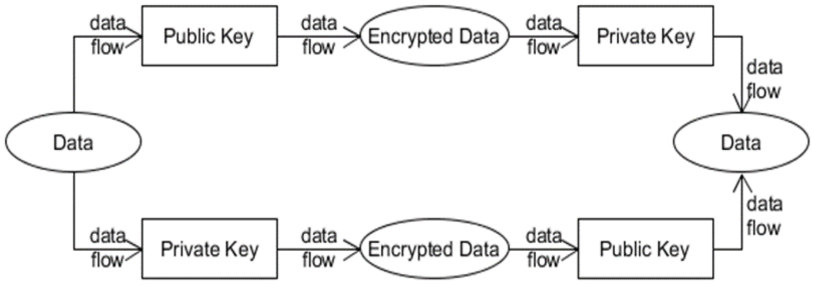

Figure 3: Illustration of asymmetric cryptography, adapted from [2]

work of nodes that negotiates blockchain information content. A separate version of the whole blockchain is maintained by system nodes, which take part in a collective verification of new blocks. More than 50% of all nodes must reach consensus before a new block can be appended to the chain [**?**, 2]. This property makes blockchain highly resistive to manipulation because any permanent change of the data-structure requires taking control of at least 51% of all nodes participating in a validation process.

Another technology used in blockchain is asymmetric cryptography [**?**, 2]. It makes use of two keys: public and private. They can be used for message encryption but a message encrypted with one key can only be decrypted with the other remaining key. Specifically, a message encrypted with a public key can be decrypted with a corresponding private key and vice versa. A schema of an encryption-decryption process is illustrated in figure 3. Ovals represent original data and encrypted data, rectangular boxes mark processes of encryption and decryption, and arrows indicate a data-flow direction.

Blockchain technology combines all these technologies to provide many advantages over traditional transaction storage systems. Blockchain-based systems are censorship-proof because no single entity has control over the whole network of nodes. Such systems are also secure and resistant to both transaction and system level. Another advantage is transparency of data as each transaction is conducted, verified and added to a publicly available blockchain, which copy is stored on every node of the system. Finally, the data can be obtained in almost real time.

4. Payment system based on eZloty virtual currency

eZloty is a virtual currency with unidirectional flow, designed to work with a dedicated payment system for making purchases in school shops. The currency is based on blockchain technology in order to enable parents to supervise their children purchases and ministry to supervise products sold in the school shops. In the following subsections, an overview of *eZloty* payment system components is presented, followed by the system's main interaction overview. The final subsection describes advantages and disadvantages of the payment system.

4.1. eZloty payment system components overview

eZloty payment system is made of four interacting components:

1. eZloty payment platform,
2. eZloty customer wallet,
3. eZloty virtual currency,
4. shops accepting eZloty.

eZloty payment platform is the main component of the whole system. The platform enables users to create accounts with a connected customer wallet and to purchase eZlotys, which are kept in the wallets. Furthermore, it stores information about all transactions conducted through the eZloty platform and preserves it in a form of a blockchain. A single block in the chain stores:

- address of a payer's wallet, which is unique for every user,
- shop wallet address, which uniquely identifies the shop, in which a purchase was made,
- value of a transaction in eZloty,
- list of purchases, which contain IDs and amounts of purchased products,
- timestamp of transaction.

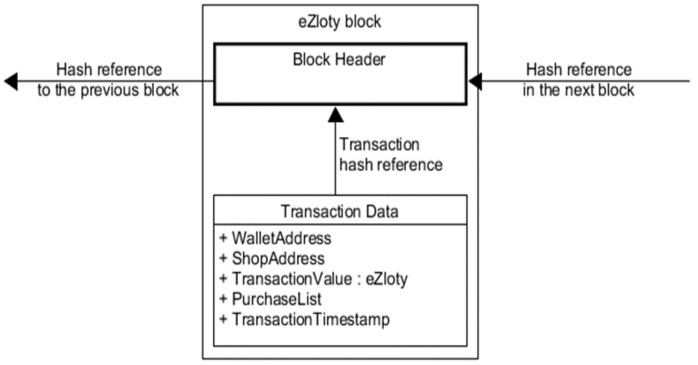

Figure 4: eZloty block model

In other words, each block stores information about a single transaction (Fig. 4). Furthermore, the platform manages operations behind all transactions, mainly delivering real world money to the school shops participating in the eZloty system.

eZloty customer wallet is the second component of the system and it is the main module for clients. The wallet is responsible for providing the owner with an interface for managing owner's account. Moreover, it is responsible for the realization of payments conducted via the eZloty platform. Furthermore, the only operations available are making purchases and adding funds to wallets in order to limit any possibility of an unauthorized exchange.

eZloty virtual currency is a currency of the eZloty platform and can only be used in the shops connected to the system. The virtual currency is available for buyers after they create an account on the platform. eZloty can be bought with real world money and is instantly added to the buyers' wallet.

Shops accepting eZloty are the shops verified and accepted by officials that are allowed to sell their products in schools. They accept payments in eZloty in exchange for available goods.

4.2. eZloty interactions overview

The eZloty payment system involves multiple interactions between components and actors. Figure 5 presents a general view of the interactions within the system. The first and most important action that can be done is creation of an account, which is required for using the platform. The action is marked in the figure

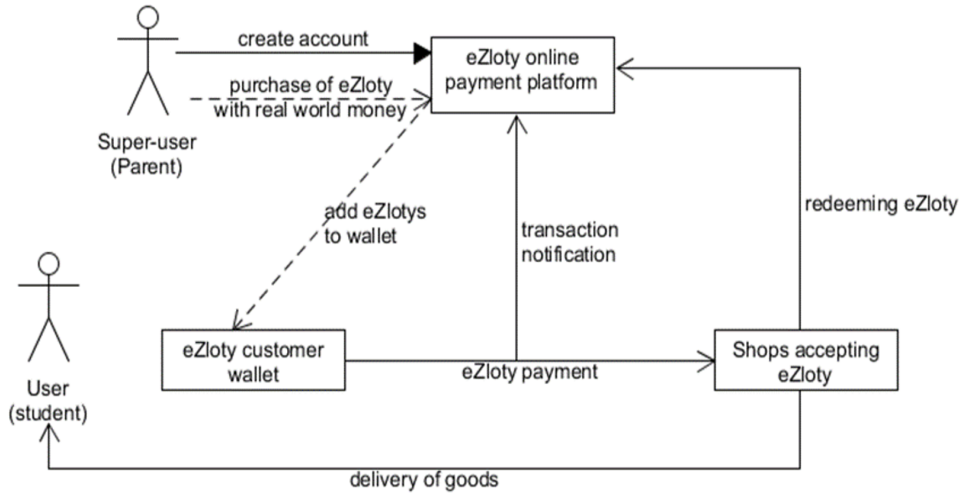

Figure 5: Interactions in eZloty payment platform

by an arrow with a black arrowhead.

Assuming each user has an account, two main operations are possible:

- purchase of the eZloty virtual currency, which is marked with a dotted line,
- making purchases of real goods with the virtual currency, which is marked with continuous lines.

Purchasing the eZloty virtual currency is a straightforward process in which super-users, in this case parents, buy their children (eZloty target users) an arbitrary number of eZlotys at a specified rate. The payment is done with real world money through traditional online payment methods, e.g. e-banking debit or credit cards.

Making purchases using eZlotys is a two-part process. The first part is the one visible to the user and consists of making a payment with the specified amount of the virtual currency in exchange for goods. A customer uses eZloty card, eZloty mobile application or any other payment method which is connected to the customer's wallet and receives desired goods. The second part of the process is invisible to the user and consists of redeeming eZloty for real world money. The mechanism works as follows: each transaction is saved in a blockchain on the eZloty

platform. After a new block is accepted, the platform checks amount of money involved and initiates an e-banking transfer of real money to the shop account. The value of the transfer is equal to the value of eZlotys of the initial transaction.

The process can be automated through implementation of smart contracts into the system. They can be defined as an agreement between two parties that is automatically enforced without involvement of intermediaries. From the points of view of blockchain, smart contracts are fragments of code which execute when certain defined conditions and terms are met. Operations conducted via smart contracts are fully traceable and irreversible as they are saved within blockchain itself [15, 16, 17].

5. Related works

Financial and business sectors greatly benefit from developing technologies. As a result, there exist many publications concerning applications of new technologies in these sectors. In recent years, virtual currencies received a lot of attention due to a boom in cryptocurrencies started by the development of Bitcoin and blockchain.

Alghamdi and Beloff in [18] present a thorough overview of different aspects of virtual currencies. They present various types of it from two different points of view: (i) how VC can be obtained and what are methods for it; (ii) what are methods and ways for spending VCs. Furthermore, the authors describe challenges and threats faced by all virtual currencies. Lastly, the article presents an overview of the chosen national and international laws concerning the topic.

In [19] the authors examine the role of virtual currencies in loyalty programs of various companies. The paper presents how VCs are used in case of four online platforms: (i) Miles & More introduced by Lufthansa; (ii) Groupon Bucks offered by the Groupon platform; (iii) Facebook Credits; (iv) Viking Points implemented by Mobile Viking. The authors mainly focus on the business aspects of the examined platforms and currencies.

The authors of [20] research models of virtual currency circulation for small value payment systems in Chinese e-commerce. The paper presents an overview of VCs and their mechanisms. Finally, the authors examine various different circulation models based on an ideal VC circulation model.

Mitsuhara and Shishibori in [21] describe a virtual currency system "Knowlegeonaire" utilizing gamification principles to encourage revisiting a Disaster Mu-

seum in Japan. *Knowlegeonaire* presents its users with quizzes concerning exhibits and rewards them with a fixed amount VC for correct answers and punishes them for incorrect answers by taking some amount of VC away. The users can use their virtual currency to buy hints for questions and gifts at the museum's shop.

In [10] European Central Bank presents a detailed overview of virtual currencies, their business schema, their advantages and their risks. Moreover, the report contains two case studies on Bitcoin and the virtual currency in Second Life virtual community. Further analysis is presented in [22], which describes results of research on Bitcoin and other cryptocurrencies.

Finally, the authors of [23] propose a classification of blockchains and blockchain-based systems. The paper presents a taxonomy based on the most important archi- tecturally-relevant characteristics and quality attributes of such systems. The main goal of the work is to provide support with architectural decisions concerning implementation of blockchain-based systems.

6. Conclusions

Recent developments in Polish legislation concerning the healthiness of products in schools shops and results of law compliance verification create a need for a method to supervise purchases in school shops. As a result, an idea for an online payment platform utilizing virtual currency was born. Such platform should provide a way for parents and ministry to supervise transactions between children and school shops. In order to accomplish this, a usage of two technologies was proposed: virtual currencies and blockchain.

As defined by EBA, virtual currency is a digital representation of value independent of a central or a public authority, which may be attached to fiat currency and which can be used by natural or legal persons to conduct business transactions and can be stored, traded and exchanged by electronic means [9]. There are different ways in which VC can be obtained and used. What is more, there are different possible relations between VC and real world money. This technology allows limiting transactions only to specified traders and to keep more detailed transaction information.

On the other hand, development of blockchain technology created a possibility of creating immutable public record of transactions, which provides a simple way for transaction supervision.

In this paper, eZloty payment platform is described. It is a payment platform

using a unidirectional flow of a virtual currency called eZloty. It allows making purchases only in certified and verified shops. Furthermore, it allows supervision of transactions due to the use of a public blockchain, which stores transaction history.

The eZloty platform fulfils all requirements that were presented. However, in the future, it would be potentially beneficial to transform it into a fully independent virtual currency. This would allow using it for more educational purposes, for example, by creating simulated stock exchanges based on real data, in which children would learn about financial instruments.

References

[1] Satoshi, N., *Bitcoin: a peer-to-peer electronic cash system*, Tech. Rep. https://bitcoin.org/bitcoin.pdf, 2008.

[2] Drescher, D., *Blockchain Basics: A Non-Technical Introduction in 25 Steps*, Frankfurt am Main: Apress, 2017.

[3] Zhao, J. L., Fan, S., and Yan, J., *Overview of business innovations and research opportunities in blockchain and introduction to the special issue*, Financial Innovation, Springer Berlin Heidelberg, 2016, pp. 2–28.

[4] Risius, M. and Spohrer, K., *A Blockchain Research Framework – What We (don't) Know, Where We Go from Here, and How We Will Get There*, Business & Information Systems Engineering, Vol. 59.

[5] Ojo, A. and Adebayo, S., *Blockchain as a Next Generation Government Information Infrastructure: A Review of Initiatives in D5 Countries', Government 3.0 – Next Generation Government Technology Infrastructure and Services*, Springer, Vol. 59, No. 6, 2017, pp. 283–298.

[6] of Poland, S. A. O. R., *NIK o zdrowym żywieniu w szkołach – Najwyższa Izba Kontroli*, Tech. Rep. https://www.nik.gov.pl/plik/id,14600,vp,17065.pdf, Supreme Audit Office, 2017.

[7] Zichermann, G. and , C., *Introduction in Gamification by Design: Implementing Game Mechanics in Web and Mobile Apps*, O'Reilly Media, 2011.

[8] Corporation, V., *Steam Wallet – Knowledge Base – Steam Support*, Tech. Rep. https://support.steampowered.com/kb_article.php?ref=1122-RTSC-0478#transferred, Valve Corporation, 2017.

[9] Authority, E. B., *EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf*, Tech. Rep. https://www.eba.europa.eu/documents/2014.

[10] Bank, E. C., *Virtual Currency Schemes*, Tech. Rep. Frankfurt am Main, 2012.

[11] Blizzard Entertainment, I., *Virtual Currency Schemes*, Tech. Rep. http://eu.blizzard.com/pl-pl/company/legal/wow_tou.html, Blizzard Entertainment, Inc., 2012.

[12] CoinDesk, *CoinDesk*, Tech. Rep. https://www.coindesk.com/, CoinDesk, 2018.

[13] Poniszewska-Maranda, A., Pawelska, J., and Majchrzycka, A., *Selected aspects of security mechanisms for transactions in Bitcoin virtual commerce*, In: Software Engineering Research for the Practice, PTI, Polish Information Processing Society, Warszawa, 2017, pp. 91–104.

[14] Stallings, W., *Chapter 11 Cryptographic Hash Functions*, Cryptography and Network Security: Principles and Practice (6th Edition), Pearson Education, Inc., 2013, pp. 313–354.

[15] Tar, A., *Smart Contracts, Explained*, Tech. Rep. https://cointelegraph.com/explained/smart-contracts-explained, Cointelegraph, 2017.

[16] Narayanan, A. and Clark, J., *Bitcoin's academic pedigree*, Communications of the ACM, Vol. 60, No. 12, 2017, pp. 36–45.

[17] Alimoğlu, A. and Özturan, C., *Design of a Smart Contract Based Autonomous Organization for Sustainable Software*, In: Proc. of IEEE 13th International Conference on e-Science (e-Science), Auckland, New Zealand, 2017.

[18] Alghamdi, S. and Beloff, N., *Virtual currency concept: Its implementation, impacts and legislation*, In: Proc. of Science and Information Conference (SAI), London, UK, 2015.

[19] Buchinger, U., Ranaivoson, H., and Ballon, P., *Virtual currency for online platforms: Business model implications*, In: Proc. of International Conference on e-Business (ICE-B), Reykjavik, Iceland, 2013.

[20] Shang, W., Wu, H., and Ji, Z., *Virtual Money As a Small Payment System in E-Commerce in China: An Economic Analysis*, In: Proc. of 4th International Conference on Wireless Communications, Networking and Mobile Computing, Dalian, China, 2008.

[21] Mitsuhara and Shishibori, M., *Virtual Currency as Gamification for Learning in a Disaster Museum to Increase the Number of Revisitors*, In: Proc. of 25th International Conference on Computers in Education, Christchurch, New Zeland, 2017.

[22] Bank, E. C., *Virtual currency schemes – a further analysis*, Tech. rep., European Central Bank, Frankfurt am Main, Germany, 2015.

[23] Xu, X., Weber, I., Staples, M., Zhu, L., Bosch, J., Bass, L., Pautasso, C., and Rimba, P., *A Taxonomy of Blockchain-Based Systems for Architecture Design*, In: Proc. of IEEE International Conference on Software Architecture (ICSA), Gothenburg, Sweden, 2017.