Cryptocurrencies as electronic means of payment without the issuer

Cryptocurrencies as electronic means of payment without the issuer, 2016

Acta Universitatis Wratislaviensis No 3758

Cryptocurrencies as electronic means of payment without the issuer, 2016

Sebastian Bala
Tomasz Kopyściański
Witold Srokosz

Cryptocurrencies as electronic means of payment without the issuer

Computer science, economic, and legal aspects

Wrocław 2016
Wydawnictwo Uniwersytetu Wrocławskiego

Reviewer
Marian Noga

The publication is a part of the project funded by the National
Science Centre based on the decision No. DEC-2013/09/B/HS5/00019

Cover photo: © alswart/Fotolia

ISSN 0239-6661
ISBN 978-83-229-3571-2

Publication prepared at Wydawnictwo Uniwersytetu Wrocławskiego Sp. z o.o.
50-137 Wrocław, pl. Uniwersytecki 15 tel. 71 3752885, e-mail: marketing@wuwr.com.pl

Cryptocurrencies as electronic means of payment without the issuer, 2016

Table of Contents

Cryptocurrencies as electronic means of payment without the issuer, 2016

Cryptocurrencies as electronic means of payment without the issuer, 2016

Introduction

This monograph was created as a part of the project titled "Electronic means of payment without the issuer" financed by the Polish National Science Centre (NSC), based on the decision No DEC-2013/09/B/HS5/00019. The premise of awarding of funds by NCN was to promote interdisciplinarity, hence the research covered three domains: computer science, economics and law. This division was reflected in the monograph, where each chapter is dedicated to a separate aspect of the functioning of cryptocurrencies, which, so far, are the only example of existing electronic means of payment without the issuer. Thus, the methodology, according to which the monograph has been written is not uniform and varies depending on the research area. This heterogeneous methodology, having a significant impact on the differences in the grid of concepts used in each research area, poses the biggest difficulties in the interdisciplinary studies. On one hand, it renders the harmonious cooperation in various disciplines impossible, as the same phenomenon (cryptocurrency in this case) appears to be quite different depending on the point of view resulting from the applied research method. On the other hand, it is impossible to imagine a proper, comprehensive analysis of such a phenomenon as cryptocurrency without the study of computer science, economics, and law. It is striking that so far there is no similar comprehensive monographic paper on cryptocurrencies in the world's literature.

This is the first such a publication in the world.

Basic, but at the same time objective and reliable conclusions in certain areas are enough for in-depth studies in each area; a lawyer or an economist dealing with cryptocurrencies need not have the knowledge of a computer scientist, but should have a basic understanding of IT aspect in the workings of cryptocurrencies. Such a transfer of knowledge should also take place in the opposite direction — from economic and law sciences to computer science. Of course, we should also take into account traditional relationships between economics and the law. Our team hopes that this book will enable this kind of flow of information and contribute to a better understanding of cryptocurrencies. Also, this monograph is the first step on the long way of research on electronic means of payment without the issuer.

Cryptocurrencies as electronic means of payment without the issuer, 2016

Chapter 1

IT aspects of cryptocurrencies

1.1. Cryptographic basics

Understanding of modern engineering of security and computer security protocols requires a great deal of knowledge. This knowledge includes modern cryptography, security of, network protocols, logic and verification of security protocols, access control, secret retention policies, vulnerability analysis, security policy and many other practical aspects of security. Probably the explanation of these areas to someone studying economics or law should not begin with a typical academic course of modern cryptography. Modern cryptography is a mathematical science including advanced algebra, mathematical analysis and the theory of computation. Directing the reader, who does not specialize in mathematics in this direction would require a huge work. However, it seems that there are simpler ways of expressing security rules to non-professionals. They require the introduction of cryptographic primitives in the same way as definitions or primitive concepts. Concepts make the elements which make up more complex security tools.

Understanding the properties of individual components used in security can rely on the description in a formal or even everyday language. With the knowledge on workings of the systems composed of these elements, we can draw conclusions on their properties in a common language. Informal approach provides less assurance as to the correctness of reasoning as compared to the strict mathematical proof, but it can bring security issues to non-professionals at a sufficient level of precision, giving insight on the relations and processes taking place in computer security.

This section explains such cryptographic concepts as a hash function, symmetric and asymmetric ciphers, bit Commitments, and authentication.

1.1.1. Basic concepts

The concept of a string is the basic concept we will use when talking about cryptography. The string means a finite sequence of bits. Finite sequences of

Cryptocurrencies as electronic means of payment without the issuer, 2016

bits are the information carrier in the IT world. We will present them as binary `1010010010001001` or hexadecimal `ef78a7e87998`. Finite sequences of bits can be interpreted as numbers regardless of the system they are stored in. In this case, `1010010010001001` interpreted as a number has the same value as the string `a489`.

We will often use the string concatenation operation. The concatenation of strings x = `1001` and y = `1100` is the string `10011100`, which will be alternatively specified by xy or $x \| y$.

In the everyday sense, the function can be imagined as an h box, which accepts arguments from a certain set, referred to as domain, returning the element from another set, referred to as image. The example of a function is $h(x) = x^2$. When putting 2 into the box, we get 4. The set of real numbers is its domain, and the set of positive real numbers is its image. Elements of the domain are also referred to as arguments, and the image elements are referred to as elements returned by the function. SHA256 hash function whose arguments are strings of bits with the maximum length of 2^{64} — 1 returning the strings of bits with the length of 256 is an example of a cryptographic function.

The concept of practical feasibility is often used in the world of cryptography, thus setting a finite size threshold. This threshold varies with the increase in the computing capacity of machines. This may be, e.g., 2^{100} processor operations. Under this assumption, if the expected time to provide an answer by the algorithm is no less than 2^{100} processor operations, the algorithm is deemed to be ineffective. The problem is deemed not solvable in practice if there is no available method or algorithm that solves this problem in the expected time which is less than the set threshold — e.g. 2^{100} processor operations.

In order to show what is practically feasible at the threshold of 2^{100}, and what is not, let us consider the problem of finding the minimum number for the maximum of 200 natural numbers and the problem of converting the binary form of a two-hundred-digit number to its unary form. For example, for the set of {12, 14, 7, 8, 15, 5, 13, 9}, we can look for the minimum using the following recipe:

— Take the first number and assign it to x.

— Take another number, compare it with x until the set is empty.

If the number is less than x, assign it to the variable of x.

— At the output, return the number in the variable x.

In the case of our input set, x = 12. We do not do anything, because 14 > 12. Taking the next number 7, we know that it is less than x, therefore x will change its value to 7. Now x = 7. Unless we find 5, the value of x does not change, then x will be equal to 5. Because there are only larger numbers after 5, the variable x will be 5, until our set runs out of numbers. The algorithm will return the output value of 5. The algorithm can be deemed effective, because we have not performed more comparison operations than the number of numbers at the input. We will not execute more than 200 comparisons in the case of a set of two hundred numbers. The task should be regarded as practically feasible.

Now the binary form of the number is the input of the problem, and the unary form of the same number is the output. In the case of input of `10101`, the algorithm which solves the problem should return `11111111111111111111`. As `10101` is twenty-one, the algorithm returns twenty one ones — this is the unary form of the number twenty-one.

No particular algorithm has been given in the case of conversion from binary to unary. However, the attempt to convert the two-hundred-digit number into unary form will require writing between 2^{199} and 2^{200} ones to the output. This exceeds our threshold of practical feasibility regardless of the method used.

1.1.2. Hash functions

Hash function is the one with an argument of any length that returns a fixed number of bits. Cryptographic hash functions should additionally satisfy several properties, e.g., they should be one-way, resistant to the second preimage and resistant to collisions.

One way means that finding the argument x which satisfies the equation $h(x) = y$ for a given value of y is not practically feasible. Resistance to the second preimage means that finding another x' satisfying $h(x) = h(x')$ for a given x it is not practically feasible. Resistance to the collision means practical unfeasibility to show two different arguments x and x' satisfying $h(x) = h(x')$.

To show the one-way concept a bit more, let us imagine a million safes with a quadrillion of one-dollar bills in each one of them. Let us also suppose that each one-dollar bill has a unique number and that each is additionally marked with a safe identifier.

There is a total of sextillion of one-dollar bills. We can assume for our purposes that the numbers are numbered from one to sextillion. Their assignment to safes should be entirely random. Let us now take all one-dollar bills out of the safes, throw them into a giant bag, and then mix the contents. The task analogous to finding the argument x for a given $h(x)$ is to find the bill assigned to a specific safe. Can we do it right away, if we reach into a big bag?

Let us reach into the bag, pulling out one bill at a time. The probability that we will pull out a good bill the first time, is one in a million. When we pull out a thousand bills, this probability is still less than one-thousandth. Therefore, we expect that we take a large number of bills before we find a suitable one. The expected work done for the collection of bills and checking safe IDs is the measure of one-way. In the world of computing, reaching into the bag may correspond to finding the bill number in the database and checking the safe ID.

The domain of the h function in the story of safes are all possible numbers of one-dollar bills in one of a million safes. Safe IDs marked on the bills are the image. We assume that each safe has a unique identifier from 1 to 1,000,000, and each bill — a unique number.

Now imagine that the function becomes a slightly different box. We no longer put one argument inside, but a lot of them, one by one, from the X set. We observe what elements are returned one after the other. The set of returned elements is called Y.

Referring to story about safes, let X be the set of one-dollar bills assigned to safes, whose IDs are divisible by 10,000. In this case Y satisfying $h(X) = Y$ is a set of IDs divisible by 10,000. We have discussed earlier how difficult it is to find a bill belonging to a specific safe. In the case which is generalized to safes, we are interested in finding a bill belonging to the safe with a number derived from a subset of numbers. There are few safes of the relevant numbers, only 100. In this case, finding the corresponding bill will require a number of takes from the bag. Finding a bill belonging to the safe which is not divisible by 100,000 is much easier, because there are exactly 999,900 such safes, which is quite a lot.

The one-way property has another generalization for cryptographic hash functions, i.e., there is no efficient algorithm enumerating r_2 for a given $y = h(r_1 r_2)$ and hint r_1. Commitment schemes are implemented thanks to such a property.

Resistance to collision is another of the properties of good hash functions. It means the lack of effective algorithm to find two different arguments x and y satisfying $h(x) = h(y)$. Finding a collision in the story of safes corresponds to finding a pair of bills belonging to the same safe.

Hash functions have many applications in the world of security. There are a few examples of situations in which they are commonly used. These include the storage of passwords, protection against changes, or authenticating the message contents, commitment schemes, digital signatures.

Physical phenomena and hardware errors adversely affect the integrity of the data. Date can be corrupted due to cryptographic attacks. A certain degree of control over the integrity of the messages can be obtained by sending them along with the hash function as a pair (*message*, *h*(*message*)). If any bits of such a pair are changed and the recipient receives a message (*message′, h′*), it is unlikely to be *h*(*message′*) = *h′* after such a change.

Sometimes there is a need to ensure that the message transmitted over the network has been created by a specific user. For such assurance, one can share the secret *key* in a secret way with the user. When it is time to send *message*, send it as (*message*, *h*(*key, message*)). The recipient, sharing a secret *key* with the sender, checks whether the equation *h*(*key*, *message′*) = *h′* is valid for (*message′*, *h′*) after receiving the message. It is practically impossible to counterfeit the contents of such a message by a third party, when they do not know the part of the *key*.

Commitment schemes are used when one of the parties wants to commit to a certain content *m* without revealing the content at the time *s* to the party which takes the commitment.

The commitment should be secret at the time *s* for the recipient. It is no longer a secret at the time *e*, later than *s*, when it is disclosed. *s*, *e* mean, for example dates

with the exact time, and *m* is a bit string. Commitment schemes consists of three stages: taking the commitment, disclosure of the commitment and verification.

Playing morra is an example showing what a commitment scheme is. Suppose that Bob and Alice have to choose two small numbers. Alice chooses *m* and Bob chooses *n*. Suppose that Bob wins if the sum of the selected numbers $m + n$ is even. The difficulty in the commitment scheme is in how both of them reveal the selected number. Disclosure should occur in such a way that neither Bob nor Alice had time to change their mind and show a different number than the one chosen first. Transmission may be implemented using a hash function. Bob can transmit $h(n)$ to Alice, and Alice can transmit $h(m)$ to Bob. At this point, the stage of placing the commitment ends.

Only after sending these values, Bob and Alice go to the stage of disclosure, providing values of *m* and *n*. If the hash function has the property of resistance to the second preimage, when Alice already has $h(n)$, it is difficult for Bob to find the number *k* with a different parity than *n*, satisfying $h(k) = h(n)$.

It is worth mentioning that in the protocols where the commitment schemes take place many times, the participants of the protocol do not create a commitment, sending only the hash functions of commitments. The solution is to send a message to the other message participant in the form of $h(n, r)$. *r* element is an additional random string. If we create commitments many times under a protocol by sending $h(number)$, where *number* is a number selected from a small set, after some time someone watching the flow of data can infer with a high probability that the same number is sent once again. In many protocols, such a capability of predicting the relationship between commitments is undesirable. Selecting a random *r* for each commitment will not allow to guess that the same commitment *n* has been sent in messages $h(n, r_1)$ and $h(n, r_2)$. Messages $h(n, r_1)$ and $h(n, r_2)$ are different with a high probability despite the same commitment. With such a scheme, the disclosure will be based on the presentation of the two values — the number *n* and a non-random element *r*. In such a scheme, resistance to the second pre-image of function *h* again plays the role of a barrier to unwanted attempt to find another pair (n', r'), satisfying $h(n, r) = h(n', r')$.

In order to fully understand the next chapter on digital money, we need to introduce an additional concept of a symmetric difference. The symmetric difference is a binary function designated as *xor*, whose arguments are bit strings of the same length. In case of the length of one the function satisfies $a \; xor \; b = 1$, when *a* and *b* are different, and $a \; xor \; b = 0$, when *a* and *b* are the same. If the *xor* function arguments have more than one bit, *xor* operates locally for each successive pair of bits, such as *xor* with arguments with the length of one. For example, (011 *xor* 101) = 110, because 0 *xor* 1 = 1, 1 *xor* 0 = 1 and 1 *xor* 1 = 0.

xor function has two important properties from the cryptography point of view. Suppose that the user creates the value $P \; xor \; R$ — from a certain bit string *P* and a random bit string *R* — in secret from the third party. It means that the

values of P and R are not disclosed to the third party. In this situation, even if the P *xor* R will be sent explicitly, the undisclosed random factor R "obfuscates" P. This causes P to remain confidential. Another useful property of *xor* are identities A *xor* $B = B$ *xor* A, (A *xor* B) *xor* $C = A$ *xor* (B *xor* C) and A *xor* A *xor* $B = B$.

1.1.3. Encryption and digital signatures

The schema of a symmetric cipher is based on the shared secret K, known as the encryption key. The purpose of a symmetric cipher is to preserve the confidentiality of messages in communication between two participants in the protocol. Confidentiality is when a third party cannot know the contents of the message being sent. A third party means those participants who do not share the secret K with participants communicating using K. Practical protocols typically require complex properties that are a combination of many simpler properties. The confidentiality of the message is one of them.

In the case of symmetric ciphers $E_K(m)$ means the ciphertext obtained by encrypting the message m with symmetric cipher E using a key K. Decryption of the ciphertext c using the key K is denoted as $E_K^{-1}(c)$. The encryption scheme starts at the moment t_0, when two parties of communication, let us call them Alice and Bob, secretly establish a secret bit string K. Symmetric ciphers require both parties to take particular care in storing the key. As long as the key is used for encryption, no one except Alice and Bob can get to know it. Also, the key exchange process should be resistant to leaks.

At the moment t_1 later than t_0 Bob sends Alice information in the form of $c = E_K(m)$, or the message m encrypted with the key K.

There is the equality $E_K^{-1}(E_K(m)) = m$, which means that we get the message m after the operations of encryption and decryption using the same key. From the moment when Alice has received the message $E_K(m)$, she may use the decryption algorithm $E_K^{-1}(E_K(m))$, resulting in the plaintext m. Alice can use the same key K to encrypt the message for Bob. Accordingly, the secret two-way communication channel is established from Bob to Alice and from Alice to Bob.

AES and RC5 are popular symmetric ciphers. These are so-called block ciphers. In the case of AES, a one-time portion encrypted with the same key is 128 bits long. In order to encrypt longer messages in AES, divide the plaintext into 128-bit portions and use one of the so-called block encryption modes.

For example, when we have a string $p_1,p_2,\ldots,p_n$, wherein each p_i has 128 bits, we can use the OFB encryption mode. As the result, we obtain the string $c_0,c_1,c_2,\ldots,c_n$ which is a ciphertext. OFB mode is counted by the formulas:

$$c_i = E_K(c_{i-1}) \text{ xor } p_i \qquad c_0 = IV,$$

where IV is a 128-bit random string.

These symmetric ciphers belong to the class of block ciphers. In addition to the block ciphers, symmetric ciphers include stream ciphers, which we do not cover in this article.

Asymmetric encryption is an invention that does not involve any of the participants in any interactive preliminary operations. In particular, there is no time t_0 when we have to perform the expensive operations, such as key exchange between Alice and Bob. The asymmetric encryption scheme begins from generating a pair of keys K and K' by one participant. One of these keys, e.g. K', should remain the secret of the participant who generated it. The second key may be published or broadcast. The first key is called private key and the other public key. Keys K and K' are mathematically related, but obtaining the key K', if we know the key K, is almost impossible.

String $E(K, m)$ means the message m encrypted with the asymmetric cipher and the key K. String $D(K', c)$ means the decryption of the ciphertext c with the private key. There is the identity $D(K', E(K, m)) = m$ in asymmetric encryption.

In the case of the most popular asymmetric cipher — RSA, encryption is exactly the same as decryption. One can also encrypt using the private key. Encrypting with one key gives the ciphertext of the message m. Encrypting the ciphertext with the complementary key returns plaintext. Thus, the following equalities are valid for RSA:

$$E(K,E(K',m)) = m = E(K',E(K,m)).$$

Symmetric encryption provides two-way confidentiality using a single key shared between Alice and Bob. It is slightly different with asymmetric encryption. When we use one pair of public-private keys, confidential communication is possible in one direction. If Bob publishes his public key K, any Alice, who came into possession of the key K, can send a confidential message to Bob.

Asymmetric ciphers, such as RSA or ElGamal, use expensive arithmetic operations, therefore they are not used in practice to encrypt long messages, for which it is necessary to use block encryption modes. Their main use is encryption when exchanging relatively short secrets. Secrets are used to derivation a key for symmetric encryption, which is used for block encryption of longer messages.

The establishment of a confidential channel between communicating Alice and Bob is not the only task of public key cryptography. It is often necessary to authenticate the communication channel. The purpose of the channel authentication is that Alice, who will receive an encrypted or plaintext information can be sure that the information comes from Bob. The way to obtain an authenticated communication channel is to use a digital signature. A digital signature can be imagined in a simplified way as a pair of $m, Sign(K', m)$. If Bob owns the private key K', he can create such a pair. Alice, when she receives $m, Sig(K', m)$, checks whether $Verif(K, Sig(K', m)) = OK$, making sure that Bob created the pair she received. *Verif* is a mathematical signature verification $Sig(K', m)$ using the key K associated with

K'. This is all done on the assumption that Alice knows that *K* is Bob's public key and only Bob has access to the private key forming a pair with *K*. The validity of such assumptions often results from the context in which signatures are used.

In the case of RSA, the pair m, $E(K', h(m))$ is a digital signature. Private key encryption $E(K', h(m))$ with previous message hashing is what was previously designated as the signature $Sign(K', m)$. Verification reaches *OK* status when $E(K, Sig(K', m)) = m$. Elegant property consisting in the fact that signing is based on encryption with the private key applies to RSA. This property does not appear in the case of other popular digital signatures, such as ElGamal, DSA or ECDSA. DSA and ECDSA algorithms are used only for the creation of digital signatures. Therefore, there is no version of encryption using the public key. The public key for DSA and ECDSA is used only to verify a signature.

The next story illustrates message authentication. Imagine that Zbigniew Preisner wants to submit his new score to the director of the National Philharmonic. The composer insists that noone but the director has the access to it. The director wants to make sure that the score he will receive will come from the composer from whom he ordered it, so that he will not prepare a concert of a well-known composer, in fact performing the music from another author.

The director and composer arrange in advance for the following protocol. The composer will publish his own public key K_P on his Facebook profile. The philharmonic will do the same on their profile, posting the public key K_F. Private keys K'_P and K'_F, which were generated along with K_P and K_F, will be kept secret, according to safety practices. The composer will prepare information (*S F N P*, *Preisner*), where *S F N P* means the Score For the National Philharmonic, and *Preisner* is the information about the author. The pair (*S F N P*, *Preisner*) will be encrypted using the public key downloaded from the Facebook profile of philharmonic, using e.g. RSA cipher. As the result, $E(K_F, (S\ F\ N\ P, Preisner))$ will be created. Then, the signature will be created in the form of:

$$Sig(K'_P, (SFNP, Preisner)).$$

Then the composer will send the message in the form of:

$$E(K_F, (SFNP, Preisner)), Sig(K'_P, (SFNP, Preisner)).$$

After receiving such a message, the director will first decrypt its first part

$$E(K'_F, E(K_F, (SFNP, Preisner))) = (SFNP, Preisner)$$

and will verify the signature by performing the comparison in the form:

$$Verify(K_P, Sig(K'_P, (SFNP, Preisner))) = OK.$$

At that moment, the director concludes the genuineness of the piece.

Authentication of the composer is based on a digital signature, which is created by using a private key. Determining that the private key belongs to the composer does not appear without additional assumptions. The director may assume that

he knows to whom the private key used belongs, only on the basis of a belief that Zbigniew Preisner placed the public key published on his profile by himself, and that the displayed profile belongs to him. Therefore, connecting the key to the user is based on the assumption that the company which handles user profiles has control over their safety. In particular, that no unauthorized person has logged onto the website, placing the public key there, and that the profile is not replaced.

The story of the composer and the philharmonic is simplified compared to the cryptographic practices. However, it reflects what the authentication and verification of a signature is. In fact, no cryptographic tool would use RSA public key for encryption. In practice, first a short secret would be exchanged using the authenticated signature. The secret would help to determine the symmetric key used to block-encrypt the score.

Practical applications of public key cryptography are common. Keys for symmetric encryption are exchanged using public key cryptography. The public key infrastructure is based on it, and it is used for such applications as authenticating Web servers. Browsers installed on our computers contain a large collection of certificates from certification authorities. The certificate consists of data characterizing the entity, the scope of the certificate, identifier of the issuer, the public key belonging to the entity and the signature made on the data by the issuer:

$$data \| id \| K_{id} \| E(K'_{id}, data \| id \| K).$$

Centers can have their own certificate in a way that they verify data of entities reporting to them with an unsigned certificate, and then sign it with their private key to confirm the conformity of the data. Entities can also be centers that will sign certificates to further entities, etc. Thus, a chain of certificates is created.

$$\langle data_1 \| 0 \| K_1 \| E(K'_0, data_1 \| 0 \| K_1) \rangle \langle data_2 \| 1 \| K_2 \| E(K'_1, data_2 \| 1 \| K_2) \rangle \ldots$$
$$\langle data_k \| k-1 \| K_k \| E(K'_{k-1}, data_k \| k-1 \| K_k) \rangle.$$

The Website provides a certificate chain in the process of authentication of the entity that manages it. The role of the client browser is to check whether the first signature was made by a trusted certification center coming from the set placed by the browser manufacturer. For further certificates, one shall verify that the certificate is signed with the private key complementary to the public key embedded in the previous certificate.

1.1.4. Blind digital signatures

Blind signatures is a technology invented by David Chaum[1] in the first half of last century. It was a breakthrough in the design of protocols for electronic pay-

[1] D. Chaum, "Blind Signatures for Untraceable Payments", [w:] *Advances in Cryptology: Proceedings of CRYPTO '82, Santa Barbara, California, USA, August 23–25, 1982*, New York 1982, pp. 199–203.

ments and electronic voting. We have described the idea of ordinary digital signatures in the last section. We will start the explanation of what blind signatures are from a relatively common example. Imagine a postal worker who accepts letters. His stamp is a confirmation of the date of letter acceptance. If we were to also have such a confirmation on the document inside, it is enough to put the carbon paper inside. The stamp would leave the mark with the date. Anyone who would like to replace the document inside the envelope, could not provide conformity between the envelope and its contents. The replaced document would have to be sent at a different time, as the date on the stamp was transferred via the carbon paper on the contents of the envelope. In this situation, anyone who receives the document will see where and when it was sent, even if the envelope was lost. At the same time, the postal worker who put a stamp has not seen the document. We can say that the stamp was put on the document "blind", i.e. without the knowledge of its contents. Blind signatures apply to a similar situation.

We need to need to describe exactly what the RSA cipher is in order to explain the technical side of a classical digital signature.

So far, we have used a general notation $E(K, m)$ and $E(K', m)$, as well as $Sig(K', m)$ designating encryption and digital signature, respectively. The RSA cipher, the public key K and a private key K' are mathematically related pairs of large integers (n, e) and (n, d). Message m is indeed a sequence of bits, but each string of bits can be interpreted as a unique natural number. However, there is a certain limitation when it comes to a choice of m — m number should be less than n. Encrypting a message m in case of RSA consists in raising the number m modulo n to the power of e, denoted as $m^e \bmod n$. Signing the message is to raise m modulo n to the power of e. The signature here is a string of bits representing the value of $m^d \bmod n$. It is worth noting that the mathematical relationship between private and public keys is expressed with the equation $m^{ed} \bmod n = m^{de} \bmod n = m$.

To complete the explanation of the blind signature, let us continue with the example of a post office. Let us consider m being the document inserted into the envelope. Since we are now in the digital world, m is also a number. Putting the document m to the envelope corresponds to the generation of a random number k, encrypting it with the key (n, e), thereby obtaining $k^e \bmod n$, and multiplying it by m. The product $k^e m$ is the equivalent of a sealed envelope with the document m. Ciphertext k^e of a random number is also a random number. The property of such an envelope is impossibility to open it and disclose the document m. This property takes place under the assumption that the random number k was generated in secret by the participant and after generation it is a secret of the participant who generated it. Confidentiality of m to other participants is due to the fact that only the knowledge of the value of k enables to divide $k^e m \bmod n$ by $k^e \bmod n$, resulting in m. For clarification, we should add that the operations of multiplication and division are not expensive.

The digital signature for the message $k^e m \bmod n$ is $km^d \bmod n$. It is the equivalent of putting a stamp on the envelope. However, it is not about the date. The

analogy is not so straightforward. Note that before signing on $k^e m \bmod n$ the message m was "obfuscated" by the random factor $k^e \bmod n$. After signing, $m^d \bmod n$ remains obfuscated by the random element k.

Obfuscating the element $m^d \bmod n$ after signing is important, because knowing $m^d \bmod n$, everyone can get to know m, as e is a public key. The result is a situation in which the person signing is not able to know m, and the person obfuscating the message can divide $km^d \bmod n$ by k at any given time. In particular, the latter may need to present the proof to a third party that the corresponding signature was put on the message m.

In summary, the blind signature scheme using RSA can be presented in the following sections for participants: Sender, Postman, and Verifier:

1. Key generation. Postman generates RSA keys (n, e) and (n, d).

2. Obfuscating. Sender chooses a random number k, then calculates $m' = k^e m \bmod n$ for a given message. Sender can generate m', reaching for the public signature of Postman.

3. Signature generation. Sender submits m′ to Postman for signing. Sender generates $b = (m')^d = km^d \bmod n$. Sender receives the value of d.

4. Removing the obfuscation. Sender calculates $c = k^{-1}b = m^d \bmod n$.

5. Signature verification. Sender sends a pair of m, c to Verifier. Verifier Accepted pair when $c^e = m$.

1.1.5. Proof-of-work

Internet users know CAPTCHA as fuzzy pictures. They appear when logging in to Internet portals and asking for your login and password, in the process of setting up a profile on portals, before entering a comment on blogs online. The purpose of CAPTCHA is to slow down malicious web robots. In these cases, the malware may try to take over the user profile, automatically set up new accounts to send advertisements or append them to blog comments. The reason behind using CAPTCHA was the belief that man, in contrast to programs, copes well with recognizing fuzzy patterns. This is not entirely true today because of the development OCR techniques, but CAPTCHAs are still popular.

CAPTCHA need not be an image, it can also be a riddle to solve in the form of a question on what is the chemical formula of water. A robot trying to answer questions that may belong to basic knowledge of a teenager would have to do a lot work to deduce answers from the knowledge base.

An interesting example of a task which requires performing some work is to find a bit string r, such that there is a prefix of the length k to the string $h(r)$ which consists of zeros only. Symbol h is a cryptographic hash function. The larger k, the more difficult it is to find the correct r. More difficult in this case translates into a longer expected time for the algorithm finding the argument r. We have discussed the analogy to this phenomenon in the story of safes. Remember that it

was harder to find a one-dollar bill belonging to the safe with the identifier divisible by 10,000 than with the ID divisible by 100. In the same way, it is difficult to find the argument r such as that, for example, $h(r) < 100$ — which gives a long prefix of zeros in the value of $h(r)$.

In 1997, Adam Back[2] suggested the way to prevent spamming e-mail based on searching the argument giving a long prefix of zeros.

The idea was called Hashcache. According to it, the e-mail client should accept extended e-mail addresses. The extension consists in appending the address *emailaddress* with appropriately long string of bits s and the result of a cryptographic hash function:

$$h(s \| emailaddress).$$

In this case, the extended address is:

$$emailaddress \| s \| h(s \| emailaddress).$$

The incoming mail should be accepted only when the component $h(s \| emailaddress)$ contains a sufficiently long beginning filled with zeros. We already know that the more zeros are required, the more difficult it is to find a suitable s, and the more time should be spent on finding it. Since the cryptographic hash functions assign arguments to the elements of an image in a manner similar to a random one, probably the only way to find a suitable s is reviewing candidates in turn.

In order to find an adequate prefix, the client sending the e-mail will calculate the value of the hash function many times. Such calculations will take a second for an ordinary user. Spamming software sends multiple e-mails with the same content to different addresses. One second delay when sending multiple e-mails is the time cost that discourages spamming. In addition, the delays involve the loss of energy to calculate the hash function.

There can be various protocols relevant to the concept of *proof-of-work*. We are only interested in those which follow the following scheme:

— Take a grain, which can also be a challenge sent by another participant in the protocol. Solve a computationally difficult riddle

— Send the result to one or more other participants in the protocol

— Other participants verify the correctness of the riddle, approving its outcome

Such a scheme occurs during the creation of new money and approval of new transactions in systems such as bitcoin. Ideas associated with CAPTCHA and Hashcache play an important role in the development of bitcoin *proof-of-work* based on the hash function.

[2] A. Back, *Hashcash — A Denial of Service Counter-measure*, www.hashcash.org/papers/hash-cash.pdf, 2002.

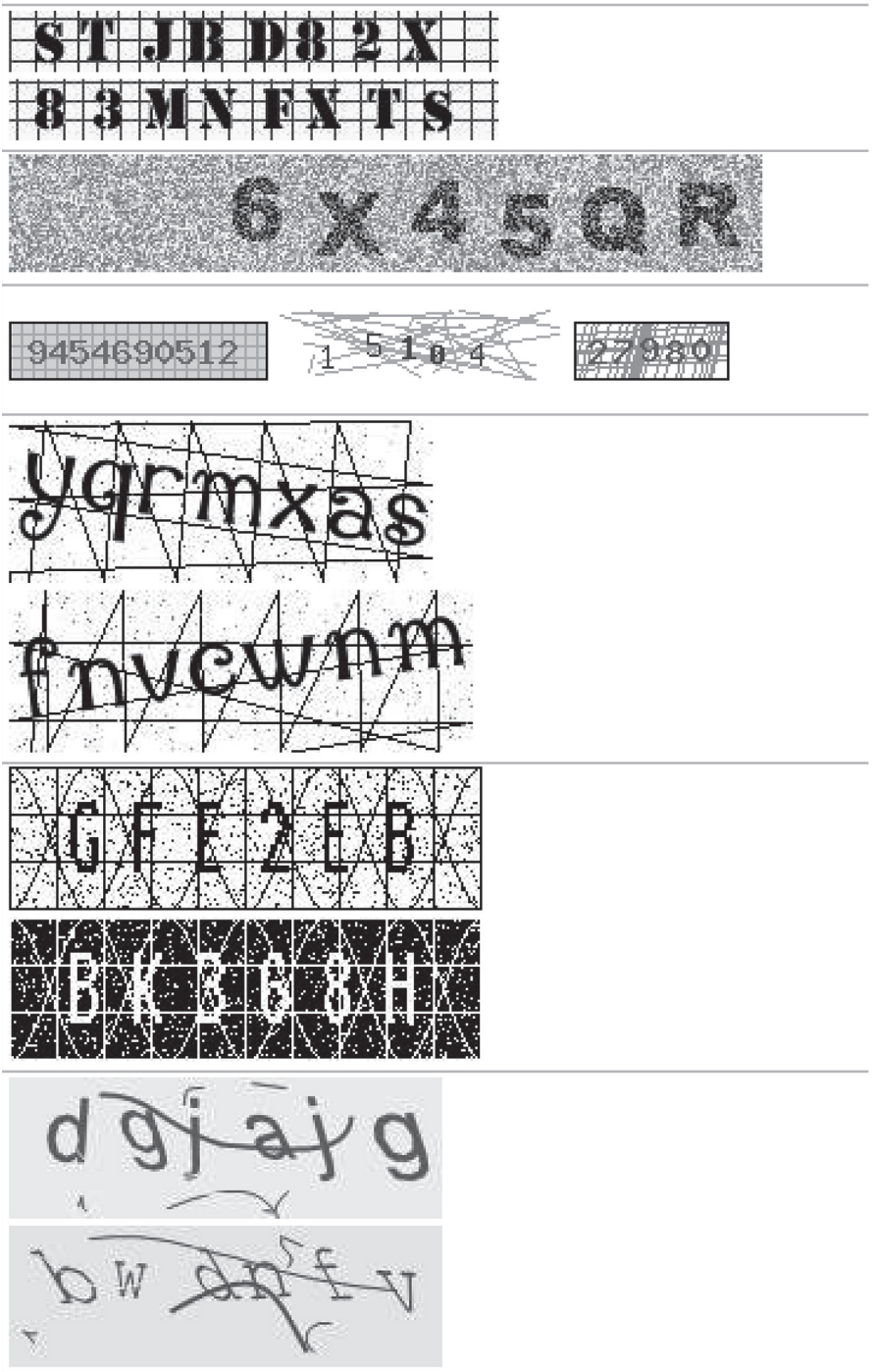

Figure 1. CAPTCHA examples from http://caca.zoy.org/wiki/PWNtcha

1.2. Digital money

This section describes a digital money protocol based on the idea by David Chaum[3]. The participants of the presented protocol are Bank, Customer, and Seller. In the case of the Customer we assume that it is a Customer of the Bank and has a corresponding card, for example a proximity card, which will store digital money. In addition, the Customer has an account at the Bank, from which they can transfer the funds to the card. The protocol we will describe below has several properties in common with paper cash, namely, transaction anonymity and the lack of reusability of the same currency. In addition, the protocol is completely offline for the Customer using money after the stage of negotiations with the Bank.

A negotiation between the Bank and the Customer is the first stage of the protocol. The amount to be transferred to the card is the subject of the negotiation. At this stage the Customer reports to the Bank that they want to transfer a certain amount y on their card. Such a transfer will be called the creation of a digital banknote. First the Bank prepares a unique identifier ID_K for the customer, and the Customer prepares 100 digital documents D_j for $j = 1, 2, ..., 100$. The number 100 is only a helper value, which is to emphasize that there is a lot of documents, and if it was necessary, the Bank can require the Customer to prepare 1,000 or 1,000,000 documents.

A single document consists of a sequence of:

— Bank name or identifier

— Random identifier x of the created banknote

— Amount y

— 100 pairs in the form of $(h(Rij), h(ID_K \; xor \; Rij))$ for subsequent $i = 1, 2, \ldots, 100$, where Rij is a long string of bits (e.g. 256) randomly selected by the Customer during the preparation of the banknote and kept in secret. Let us prepare another set of one hundred different random numbers, each for one banknote. Thus we randomly select a total of 10,000 sequences Rij in the whole process.

After preparing the banknote, the Customer has to remember all digital documents Dj and related random strings Rij. These data should be stored with full attention to their confidentiality.

In the next step, the customer should pack all D_j in envelopes, preparing them to make a blind digital signature. Remember that D_j in the envelope is in fact a value of $r_j^e D_j \bmod n$. The pair (e, n) is a public key of the Bank, and r_j is a random number. Let $E(r_j, D_j)$ denote an envelope with contents Dj. The Customer sends all prepared envelopes to the Bank. There are a 100 sent envelopes.

[3] D. Chaum, A. Fiat, M. Naor, "Untraceable Electronic Cash", [in:] *Advances in Cryptology — CRYPTO '88, 8th Annual International Cryptology Conference, Santa Barbara, California, USA, August 21–25, 1988, Proceedings*, ed. Sh. Goldwasser ("Lecture Notes in Computer Science" 403), London, UK 1988.

In the next step, the Bank checks the contents of 99 envelopes. For this purpose, the Bank should randomly select one from all of them. The Bank asks the Customer to disclose the contents of all envelopes in addition to the selected one. After the disclosure of all elements *Rij*, identifiers *x*, random elements r_j, the Bank alone is able to calculate all hash functions belonging to the selected documents D_j. Then the Bank prepares the envelopes $E(r_j, D_j)$.

If the prepared envelopes look the same as those prepared by the Customer, the Bank considers the verification successfully passed. Otherwise, the Bank launches a procedure in which they refuse to issue the digital banknote or they command to repeat the whole preparation of digital banknotes. Depending on which procedure is followed, the Bank may make an attempt to report a scam when the Customer incorrectly prepared documents several times. However, if prepared envelopes have been positively verified, the Bank blindly signs the selected envelope $E(r_c, D_c)$, while subtracting the amount of *y* from the Customer account. Remember that the blind signature put on $E(r_c, D_c)$ has the value of $r_c D^e{}_d \bmod n$. The Customer can then take off r_c and obtain a pure signature on D_c by division.

Now we will clarify what happened from the point of view of cryptography when signing. Elements of the document D_c have not been disclosed in the verification process. Before putting a signature, the Bank has no way of knowing what is the content of D_c, because D_c is adequately obfuscated by a random number. At the same time, if the Customer tries to deceive the Bank in the preparation of documents D_j, then with the probability of 0.99, the Customer will fail to report a false banknote, which would, for example, have recorded value higher than the predetermined *y*. The Customer also cannot succeed in the manipulation of random elements with any significant probability.

Notice that the described protocol does not rule out that the signed digital banknote may be issued to a larger value than that which was deducted from the Customer account. However, this happens with a very low probability. One should not worry about a lack of certainty, because all cryptography is based on the negligible probability of events which are undesirable. What we can do to strengthen the protocol is to reduce the likelihood of signing the note with the wrong denomination. This can be achieved by increasing the number of prepared documents. We can also use the protocol for micropayments only, preventing recognition of larger denominations. The use of protocol with the parameter 100 for macropayments could make it worthwhile to create a group of people who will prepare one document with a very large amount in order to share it, when one person accidentally manages to pass the verification.

The Customer, having signed the prepared document $D_k{}^{\mathrm{d}}$, can pay using it. The Customer arrives at the Seller with a few banknotes stored on a card. The Seller has an electronic system which will verify the banknotes used. The Seller's system will randomly create a string with one-hundred bits. For the verified banknote D'_k the Customer will provide ID_K *xor Rik*, if the *i*-th bit of the string is one. If the *i*-th

bit is zero, the customer shall provide the value of *Rik*. The Seller's system will save this information along with the explicitly transferred D'_k and a signature D_k^{d}. The Seller's system, having all this information and also knowing the public key of the Bank, may verify that the Bank signed the verified banknote. This operation is very simple. Just raise D_k^{d} to the power of e derived from the public key and check whether the result will is D'_k, which was explicitly specified in the purchase transaction. The seller must save the downloaded data, i.e., both the signature D_k^{d}, banknote D'_k submitted by the customer, and one hundred of arguments for the hash function during the purchase-sale transaction.

The Seller, having gathered information about the banknote, calls the Bank digitally in order to increase their account balance by *y*. The Seller knows which Bank should pay, because the Bank identifier is stored in the digital banknote. The Seller transmits all the collected information to the Bank, which can now verify their own signature and increase the Seller's account balance by *y*. In addition to the signature verification, the Bank verifies whether all hash functions in the banknote have been calculated correctly.

The main problem of a digital money designed this way is that it can be copied repeatedly. The protocol should prevent the double use of the banknote. In our protocol the Bank does this by searching their entire database to find the same identifier of banknote *x*. If they find a duplicate identifier *x*, they take the strings of bits generated by sellers corresponding to both the banknote and duplicate. The first detection of a duplicate occurs when a second banknote has been submitted with exactly the same identifier.

At that point, the Bank has access to two strings of bits $a_1,a_2,\ldots,a_{100}$ and $b_1,b_2,\ldots,b_{100}$. If the strings were random, there are two positions a_l and b_l, which are different, with the probability close to one. One of the bits a_l, b_l is one, the second is zero. This means that the Bank also has access to *Rlk* and ID_K *xorRlk*. We can now calculate the symmetric difference of these values, obtaining ID_K. In this way the Customer trying to use the same digital banknote is exposed. Note that the Customer identifier will not be revealed if the banknote is used at most once.

In conclusion, note that the presented protocol shares two basic properties with the paper money: the anonymity of the holder and the ability to issue a banknote only once. In addition, the Customer is anonymous until they try to submit the digital banknote for a second time. The presented protocol is not perfect, it can be used to support micropayments only, it is expensive, considering the amount of data each participant/party of the protocol must store, and it does not exchange the banknote into smaller denominations. One can find a lot of better solutions in the cryptographic literature, but they require the use of more complex techniques.

The main difference between cryptocurrencies and electronic money is that the value of the latter comes from a regular monetary system. Regular monetary system is centrally controlled by the state and banks. The value transferred to electronic form can be regarded as the same money in another form of banknote

put in circulation. Electronic money presented in such a form in the protocol does not create an additional value on the currency market.

1.3. Bitcoin

The idea coming from a famous article by Nakamoto lived to see many projects. There are already more than a hundred different cryptocurrencies on the market. The implementation of each one of them differs in details, but the idea derived from Nakamoto is in the core of most of them. This chapter shows the essential elements of an architecture based on the original, that is, the bitcoin system. Details of little importance will be skipped, because the objective is to present an outline that will allow to imagine how such a system works.

Bitcoin system data are stored in a sequentially-organized database of records called blocks. Sequentially in this case means that there is the first block. Each next block stores information that indirectly indicates, which block in the database is the previous one. The blocks contain a number of transactions. The maximum number of transactions in the block is limited by the protocol parameters.

1.3.1. Transactions

We will start the explanation of how a block organized and how the included information are related by describing the transactions, which are its components. We will use simplifications. Certain components, which in the implementations are calculated during the block verification process or the transaction, will be presented as if they were stored in the database. In contrast, we will not list the components, which are not significant from our point of view.

There are two types of transactions — regular and base. Figure 2 shows a simple record of a regular transaction. It includes:

— The string of `transaction inputs` with the cardinality of at least one. We will refer to the input string as *vin*. The input string is enclosed in square brackets and preceded by the word "`in`": in Figure 2. The description of each input is preceded by the word "`prev_out`":. The transaction in the figure includes only one input.

— The string of `transaction outputs` consisting of at least one output will be referred to as *vout*. Figure 2 shows two encoded transaction outputs, one has a value of 1.00090000 bitcoin, and the second is 24.75632017 bitcoin.

— The number of transaction inputs and outputs preceded in the drawing by "`vin_sz`" and "`vout_sz`", respectively

— Hash value of the transaction.

In the figure, the cryptocurrency values are assigned to the outputs of the transaction. The participant, who can create a new valid transaction using outputs

Cryptocurrencies as electronic means of payment without the issuer, 2016

```
hash":"fa13c18e211f8170bf202c4d5d5beeef92c79b462ec065c3005cc10b2c3453f9",
      "ver":1,
      "vin_sz":1,
      "vout_sz":2,
      "lock_time":0,
      "size":227,
      "in":[
        {
          "prev_out":{
       "hash":"ee29667a3cd07c4f4a28d55556b85273f6fc816b681b067992cc224aefd0882e",
            "n":0
          },
          "scriptSig":"3046022100eb882807e980c75c3b6ae10adf2dcdf1a0053ee5b373018
          086995aa819eb32bc02210087832f4c524e063aeac293756962d15973786fd4e6bd82f
          b5ba8bfba470a75e801 038929cc4f548dc81ccb75bafa26bc78bddc3f3f5dd2bc4e6a
          c4ef5c0fb364a50d"
        }
      ],
      "out":[
        {
          "value":"1.00090000",
          "scriptPubKey":"OP_DUP OP_HASH160 c31702be1f2cc089f993c034c2f5443e5e6
          86e82 OP_EQUALVERIFY OP_CHECKSIG"
        },
       {
          "value":"24.75632017",
          "scriptPubKey":"OP_DUP OP_HASH160 1a4eaf51d8eaa4e06811bf173b438d3f759
          1f64a OP_EQUALVERIFY OP_CHECKSIG"
        }
      ]
```


Figure 2. Regular transaction

from transactions already approved by the system, is the owner of the cryptocurrency. When creating a new transaction, the participant indicates which transactions and which outputs are charged. The indication is created by applying a hash function of the transaction and output number, from which it draws its value in bitcoins. Figure 2 shows the issued value derived from transactions with a value of hash functions of `ee29667a3cd07c`... from the first output (indicated by "`n":0`). The indicated transaction may have multiple outputs with different amounts paid to various participants.

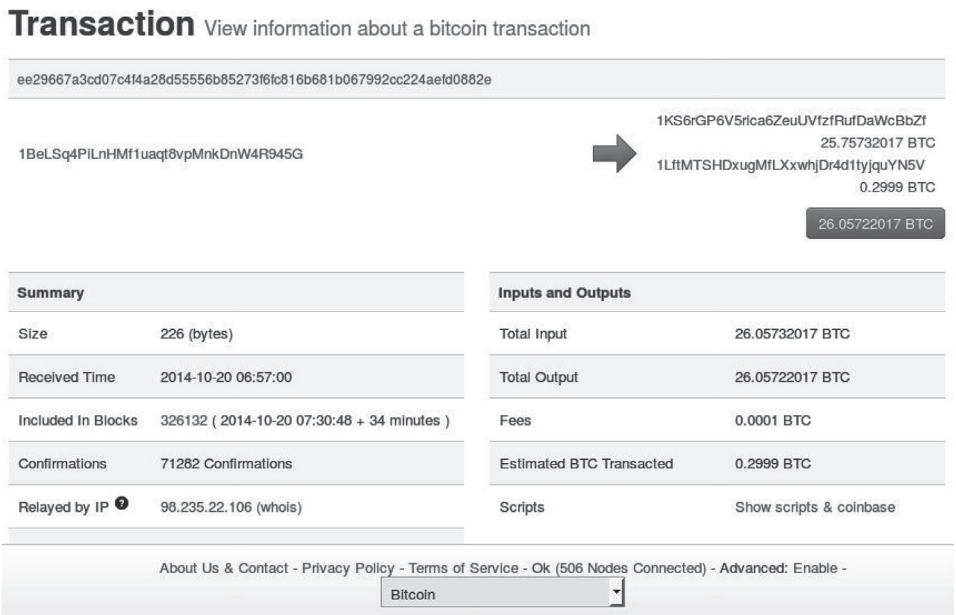

Figure 3. The result of transaction search `ee29667a3cd07c`... on the website https://blockchain.info/pl7

Figure 3 shows the search result of a transaction as a result of hash function `ee29667a3cd07c`... on the website https://blockchain.info/pl.

A careful reader can check that the sum of the amounts for transaction outputs in Figure 3 is less than the amount assigned to the output of the first transaction `ee29667a3cd07c`... by one ten-thousandth. This is exactly the amount that enters to transactions the base transaction as a fee for the participant who solved the block.

Each transactions input also has the so-called signature script. It is designated as `scriptSig` in the figure. Single transaction outputs consist of the actual amount and the public key script, whose main component is the public key of the participant processed twice by the hash function. Putting the public key here enables us to encode the party, to which the right amount is transferred. The result of the hash function mentioned in this section is the identifier of the participant to whom the amount is transferred:

$$\mathrm{ID} = \mathit{RIPEMD}160(\mathit{SHA}256(\mathit{public\ key})),$$

*RIPEMD*160 and *SHA*256 mean cryptographic hash functions here.

Both the public key script and the signature script is a sequence of instructions stored in a special scripting language. The verification of the digital signature can be accurately written using instructions of the scripting language. The semantics of the scripting language is based on a data structure called a stack.

Stack is a structure which includes the so-called bottom of the stack. It enables to perform two operations: download an item from a non-empty stack, and put away an item on top of the stack. Putting element A on top of the empty stack, we get a stack with the value of $\perp A$. If we now put element B on the stack, we get $\perp AB$. Now, pulling an element from the top of the stack, we get $\perp A$ again.

Signature verification begins with placing the contents of the signature script on the top of the stack, according to the order of components. Then, commands from the public key script are executed in sequence. If data appears instead of a command in the public key script, we put it on top of the stack. Scripting language commands apply to, for example, signature verification, duplication of the element on the top of the stack, checking whether the item on the top of the stack and the element under it are equal, etc.

The signature script in Figure 2 has two components: ⟨*SigECDSA*⟩ and ⟨*PubKeyECDSA*⟩. The first is:

```
3046022100eb882807e980c75c3b6ae10adf2dcdf1a0053ee5b373018086995aa
819eb32bc02210087832f4c524e063aeac293756962d15973786fd4e6bd82fb5b
a8bfba470a75e801
```

and is the ECDSA signature (it will be explained later which information is signed), while the second is:

```
038929cc4f548dc81ccb75bafa26bc78bddc3f3f5dd2bc4e6ac4ef5c0fb364a50d
```

and is the ECDSA public key in a compressed form. The uncompressed form of the ECDSA public key consists of two coordinates *x* and *y*, each of which is 32 bytes. In addition, the key in an uncompressed form begins with the prefix 0x04. The compressed form has only 32 bytes and additionally begins with the prefix 02 or 03.

The signature script is ⟨*SigECDSA*⟩⟨*PubKeyECDSA*⟩,, and the public key script is a sequence of instructions and data:

$$OP\_DUP\ OP\_HASH160\ \langle PubKeyHashHex\rangle\ OP\_EQUALVERIFY$$

$$OP\_CHECKSIG,$$

where ⟨*PubKeyHashHex*⟩ is the identifier with the value of

```
c31702be1f2cc089f993c034c2f5443e5e686e82.
```

According to the semantics of the scripting language, the pair ⟨*SigECDSA*⟩ ⟨*PubKeyECDSA*⟩ is placed on the stack. ⟨*PubKeyECDSA*⟩ will be placed on top of the stack, above the signature to be verified. Next, we perform the sequence of operations. First, in accordance with *OP_DUP*, we duplicate the top of the stack, resulting in:

$$\langle SigECDSA\rangle\langle PubKeyECDSA\rangle\langle PubKeyECDSA\rangle.$$

We take *OP_HASH160*, applying the hash function *RIPEMD160* to the top of the stack, resulting in:

⟨*SigECDSA*⟩⟨*PubKeyECDSA*⟩⟨*PubKeyHashHex*⟩.

We copy the data ⟨*PubKeyHashHex*⟩ on the stack and check whether there is equality between the top of the stack and the second element. *OP_EQUALVERIFY* directs us to perform such a step. Two elements remain on the stack:

⟨*SigECDSA*⟩⟨*PubKeyECDSA*⟩,

for which we verify the signature marked in the scripting language as *OP_CHECKSIG*.

The script presented expresses the relationship between the possession some output and the form of transferring of this output using a digital signature. Possession is expressed by the earlier signature and identifier, to which the amount is transferred. The identifier is derived from the public key of the owner. This scheme is called a payment to the address or a payment to the public key hash function.

In the early years of bitcoin development certain restrictions were imposed on the capabilities of expressing payments using a scripting language. The support of five types of transactions was allowed. Payment to the identifier is one of the possibilities. The other is a payment to the public key, payment with multiple signatures, data transfer and a payment to the script hash function (Pay-to-Script-Hash P2SH).

In the case of payment with multiple signatures, bitcoin protocol allows the preparation of transactions that require multiple signatures to pay a certain amount. Let us imagine that Bob wants to transfer his bitcoins to an association. To prevent possible conversion of transferred funds, he may transfer the amount to the management board of the association. He decides that the association will be able to use the amount when three people out of seven board members will submit their digital signatures. Three is sufficient to prevent unfair collusion. At the same time, it is small enough that it does not affect the availability of funds due to the absence of the minority of the board. When creating a transaction, Bob prepares the script of a public key, which this time will not contain a single address or one public key, but the key chain composed of all public keys of board members:

3 ⟨*pubkey*1⟩… ⟨*pubkey*7⟩ 7 *OP_CHECKMULTISIGVERIFY*.

Further transfer of the amount from such a transaction requires the creation of a signature script in the next transaction, which includes at least three signatures of the board members.

OP_0 ⟨*sigA*⟩⟨*sigB*⟩⟨*sigC*⟩.

Verification of such a signature script consists of checking whether the first key matches the first signature. If it does not, then we move on to the next public

key. If it does, we set the next public key and signature for verification. With such a verification procedure, the correct order of signatures must comply with the order of corresponding public keys in the public key script. If the orders do not match, the verification result is negative.

Payments with many signatures are perfect for securing payments with parties of low confidence. If we want to transact with the party towards which we have limited confidence, we can use the protocol where we appoint a mediator as the third participant. In the case of e-commerce, the buyer may pay when ordering goods using their public key, the seller's key, and the mediator's key. In such a case, the key script would require two of the three signatures. When receiving goods in accordance with the specifications and expectations, the buyer and the seller will sign further transfer of the payment to the seller. If the goods is defective, they will need to use the mediator, who will decide whether to return the money to the buyer, or transfer the amount to the seller despite buyer's complaint.

Through transactions with multiple signatures, the idea of wallet protection service is feasible[4]. It is based on using two signatures. One private key belongs to the owner of the wallet, and the other to the wallet manufacturer, who provides the appropriate service. In this configuration, the customer signing a transaction with his or her key receives a partial signature. Partially signed transaction is sent for signing to the service. The service signs and publishes the transaction after the authentication of the owner of the wallet. From security point of view, such a scheme prevents in some way the negative consequences of intercepting the private key of the owner of the wallet. At the same time, however, it requires that the party providing the service was trusted. The site deciding whether to conclude the transaction of their client or not, has a full opportunity to blackmail. It must therefore be assumed that either the one providing the service is a trusted party, or private key is somehow delivered to the recipient. In turn, the recipient holds the key out of his or her computer, which is exposed to attacks.

Already at the beginning of the development of the bitcoin system came the idea to use it not only as a system for financial transactions. The idea was promoted by some developers and rejected by others as incompatible with the original purpose of the system. As a distributed registry with the capability to store data, which includes a time stamp in each block, bitcoin is suitable for the operations of a digital notary. Although bitcoin is not suitable for storing large amounts of data, the digital notary can be carried out using traces resulting from the hash function. A new operator *OP_RETURN* for creating a script that stores data has been introduced since bitcoin version 0.9. This operator allows creating a script data in the following form rather than the public key script:

$$OP\_RETURN\ \langle data \rangle.$$

[4] P. Franco, "Understanding Bitcoin: Cryptography, Engineering and Economics", *Wiley Finance Series* 2015, p. 85.

The size of ⟨*data*⟩ field is limited to 40 bytes. This limitation enables to store, e.g., the result of SHA256 hash (32 bytes) in this location. One does not add values in bitcoins to such a script, because the data script is regarded by the system as unrelated to operations on the cryptocurrency. Therefore, inputs with the operator *OP_RETURN* are not stored in RAM (*UTXO* — Unspent Transaction Outputs register); they are only stored on a central register in blocks on a disk.

The capability to store data is used in the namecoin system. Namecoin system is an extension of bitcoin based on its code that allows the addition of transactions, which store names. The idea, which is an integral part of namecoin, was to provide an alternative to the domain name system based on DNS servers. To use the DNS mechanism which supports its own name, it has to be registered with the namecoin system and wait until the name will be included in a block of sufficient depth. Having the wallet running, one shall start the daemon cooperating with all Internet applications. Namecoin It supports names with the `.bit` suffix.

The capability to store hash values enables to record the cryptographic track of documents. Imagine that the two parties agree on some contents of the document and put two digital signatures. Then the hash function is calculated on the total and reported using *OP_RETURN* operator to the bitcoin system. Some time later, the track becomes a part of the main block of the blockchain.

Payment with many signatures has a different form, which is called the payment to the function script (Pay-to-Script-Hash P2SH). A regular public key script in the case of payment with many signatures is as follows:

⟨*XScript*⟩ = *n* ⟨*PubKey1*⟩…⟨*PubKeym*⟩ *m OP_CHECKMULTISIG*, while the signature script is a sequence of signatures: ⟨*Sig1*⟩…⟨*Sign*⟩. In the case of P2SH script, the signature script is

$$OP\_HASH160\ RIPEMD160(SHA256(X))\ OP\_EQUAL,$$

and the bit string serves as a signature script

$$\langle Sig1\rangle\ldots\langle Sign\rangle\ \langle XScript\rangle.$$

The use of the P2SH script has several advantages over the script with multiple signatures. The participant who wants to pay the entity represented by several signatures can pay directly to a single address $RIP\ EMD160(SHA256(X))$.

The output of such a transaction is significantly shorter than the output of multiple signatures. Transactional fee depends on the size of the transaction, thus the payer will pay a lower fee due to the shorter form. Unspent outputs reside in UTXO (Unspent Transaction Outputs) cache. Relatively shorter output for P2SH will slightly less relieve RAM, which stores UTXO.

As already mentioned, a single output of any transaction has its owner when the payment to the address or payment to the public key is used. There is no telling that the holder is an individual, as transactions are digital, not physical. We call them participants, agents or entities in digital systems. Each of these names can

describe an individual, but in certain situations it may denote a process, program, mechanism, digital card with appropriate software, which are able to perform actions on the system. In particular, the owner is an entity which can create the correct signature script based on the output public key script in a reasonable time to prove its ownership.

It is not entirely clear who owns the cryptocurrency stored in the output with multiple signatures. In this case, a group of people can have the ability to create a valid signature. In addition, a group of people does not have to be specified explicitly, because the requirement of a signature can apply to n of m people. Furthermore, the appropriate keys can be stored in the wallets on several devices. The devices can be in the hands of one or many persons. This slightly complicates the notion of ownership.

Probably, creating the signature script is technically the most difficult part of the payment process. The participant of the protocol creates the skeleton of a new transaction by entering all data into it, with the exception of signature scripts. One can say that he leaves free spaces here. Then he rewrites the public key script from the output, which pays in the free space of the constructed input. Then he creates a hash function from the constructed message. He signs it using a private key. He inserts the obtained result in the right place of the previously created skeleton. The location where the public key script is rewritten is not arbitrary. It belongs to such an input, which has a hash and a number indicating the output from which the public key script is retrieved. The method so described is one of several available options for signing the transaction. It is called *SIGHASH_ALL*. We do not present the others here, because they are less important.

In order to understand the payment scheme in more detail, let us imagine two transactions in the form of $T_A = [head_A, vin_A, vout_A]$ and $T_B = [head_B, vin_B, vout_B]$. For simplicity, suppose that the created transaction has exactly three inputs and three outputs, and that Bob is the owner of the amount recorded in the second element of the $vout_A[2]$ string of the transaction T_A. Output $vout_A[2]$ has the form of $skeleton_{voutA2}[PubkeyScript_{A2}]$. String $PubkeyScript_{A2}$ means the signature script saved after the output amount of the second transaction T_A.

If Bob wants to spend a certain amount, which includes $vout_A[2]$, he creates the transaction T_B. Bob should create one input from the inputs of transaction T_B corresponding to the payment of $vout_A[2]$. He achieves this by generating $vin_B[2]$ in the form of $skeleton_{B2}[SigScript_{B2}]$. The $skeleton_{B2}[]$ element includes two pieces of information: the value of the hash function of the transaction T_A and the sequence number of the output, whose amount we are going to spend (in our example this is the second output). There are several ways to output $SigScript_{B2}$ in the bitcoin system. The main and simplest of which is to use the *ECDSA* private key to sign the information in the form of $hash([headB, vin_{B2}, vout_B])$, where $vin_{B2} = [skeleton_{B1}[], skeleton_{B2}[PubkeyScript_{A2}], skeleton_{B3}[]]$, *headB* He is the heading of transaction T_B, $vout_B$ is a string of all outputs of transactions T_B.

We will denote such a signature by Sig_{B2}. Empty parentheses behind $skeleton_{B1}$ and $skeleton_{B3}$ mean unfilled places where $SigScript_{B1}$ and $SigScript_{B3}$ will eventually be. $SigScript_{B2}$ can be thought of as a junction of two components of the signature Sig_{B2} and $PubKey_B$. The first component, Sig_{B2}, is the signature of Bob. The second one, $PubKey_B$, is Bob's public key given explicitly. Explicitly giving public key at this point allows both the verification of the signature Sig_{B2}, and confirming that $PubkeyScript_{A2}$ contains an identifier derived from Bob's public key. The purpose of the latter is to check whether Bob owns the second output T_A.

Each of *SigScript* elements It is calculated according to the same scheme. The result of signing process will be:

$$vf = [skeleton_{B1}[SigScript_{B1}], skeleton_{B2}[SigScript_{B2}], skeleton_{B3}[SigScript_{B3}]].$$

In summary, the newly created transactions are broadcast on the network and are subject to verification by its many nodes. Having the fragment v_f, one should reach for $PubKey_B$, contained within each $SigScript_{B2}$ during verification. Additionally, $skeleton_{B2}$ contains the hash value of the transaction and the number of output paid out by Bob. Such a transaction should be found and checked whether the corresponding output includes $PubkeyScript_{A2}$ with Bob's identifier. If everything is correct, then this is the basis to authorize expenditure from that one output. The verification process should validate all outputs in *vf*.

In addition to checking whether Bob is a valid owner of the respective amounts, it is checked whether the amount transferred from some transactions sum up to the values stored in the output of the transaction T_B and the payment included in the amount of the base transaction.

In the context of the operation on cryptocurrencies, the validity of the created transaction proves that Bob has spent the cryptocurrency, which belongs to him. Is this exactly the amount, which belongs to Bob? A single transaction will not pass the verification, because it moves greater amounts to the output than those assigned to inputs.

In addition, it is subject to verification whether the transaction issues outputs which have not yet been performed. Nakamoto had the idea to prevent the multiple issuance of the same output, which is to leave the entire transaction history in the hands of all the network nodes.

Suppose that the node wants to approve a transaction $T = [head, vin_1, vin_2, vin_3, vout_1, vout_2, vout_3]$. The condition for approval is to find other transactions, maybe some, containing outputs $vout'_1, vout'_2, vout'_3$. Output $vout'_i$ with the amount x and the identifier derived from the public key pk should correspond to the input vin_i, containing a suitable signature script. The signature script is appropriate when a key complementary to pk was used for the signature. However, the most important is that vin_i is generally the only input to the transaction with a signature which

transfers the amount from $vout'_i$. The search of inputs with the signature corresponding to $vout'_i$ applies to the entire transaction history. Searching the registry of many dozen bytes each time could be very costly, and therefore another solution has been introduced. At the very beginning, when saving all approved blocks, the transaction outputs are collected that have not yet been issued (UTXO — Unspent Transaction Output). Such outputs are saved in a separate UTXO database. When the transaction implementing the output from the UTXO database appears, the output is removed and replaced with those from the new transaction. At the moment of checking the transactions, when there is no $vout'_i$ output in UTXO database matching *vout'*, a new transaction *T* should be rejected.

Certainly, the number of transactions in the UTXO database is small compared to all transactions in the history. Nodes outside the main registry maintain the UTXO database in RAM, replacing implemented outputs with new ones on the ongoing basis. The number of outputs held in the UTXO database will be


```
"hash":"b2eacc0f419181bdba58821868525c419adbe3e6765116e9be1b
18bfa83730dc",
"ver":1,
"vin_sz":1,
"vout_sz":1,
"lock_time":0,
"size":157,
"in":[
  {
    "prev_out":{
       "hash":"0000000000000000000000000000000000000000000000000000000000000000",
       "n":4294967295
    },
    "coinbase":"03f9f904062f503253482f04a2be445408564e7efd370400002e522cfabe6d6d8cef5507
     685dee61562e28bf5b9262c9cc6ae871d63d0468df17522188d2366404000000000000000",
     "sequence":0
  }
],
„out”:[
  {
     "value":"25.00370000",
     "scriptPubKey":"OP_DUP OP_HASH160 80ad90d403581fa3bf46086a91b2d9d4125db6c1
     OP_EQUALVERIFY OP_CHECKSIG"
  }
]
```


Figure 4. Base transaction

proportional to all bitcoins available in the system divided by the average value attributable to a single identifier.

Let us now turn to the base transaction. This is a transaction placed on the block as the first one. It is created during the creation of the block in the process of mining a cryptocurrency. The components of the base transaction we are interested in are:

— Data field, which can be stored as any number This number is used to create *proof-of-work* during the process of creating the cryptocurrency. In Figure 4, the places to enter any data are places after the tags "`n`" and "`coinbase`";

— A record of the amount, which is the motivation for creating cryptocurrencies;

— The public key belonging to the participant who created the block.

Previously we have described a shortened specification of regular and base transactions. Looking only at the construction of the transaction, one can find that regular transactions are quite well protected by digital signatures from unauthorized disposition of the amounts in their outputs. To the contrary, base transactions do not contain any cryptographic security. This does not mean, however, that they can be replaced with other data without any calculation effort. In the case of base transactions, security has been imposed at the block level.

1.3.2. Blockchain

The nodes of the bitcoin network are involved in collecting transactions, verifying them and forming blocks from properly verified transactions. The blocks are arranged in a linear form, in which each block except the first one points to its predecessor. A single block consists of many regular transactions and one base transaction. When creating a block, the participant of the protocol, indicates the previous block in the header. The indicator to the previous block is the result of a hash function, which is a *proof-of-work* of the previous block. The participant who creates a new block attempts to calculate the *proof-of-work* of the newly created block. Only blocks, which have obtained a shortcut function with the appropriate number of zeros in the prefix, will be accepted by the network of nodes. In Figure 5, the element

```
"hash":"000000000000000001123b1baca6c065423e10ce1ea524f70f5a69cad9501d380",
```

is *proof-of-work* of the block currently being created, and

```
"prev_block":"000000000000000004cc60b204979965f1106e2ed759741040ed5c3479290657"
```

is *proof-of-work* of the previous block. Both elements have a long string of zeros in the prefix.

The block header contains the value of the root of the Merkle tree. The whole tree is placed at the very end of the block as a sequence of strings. The example

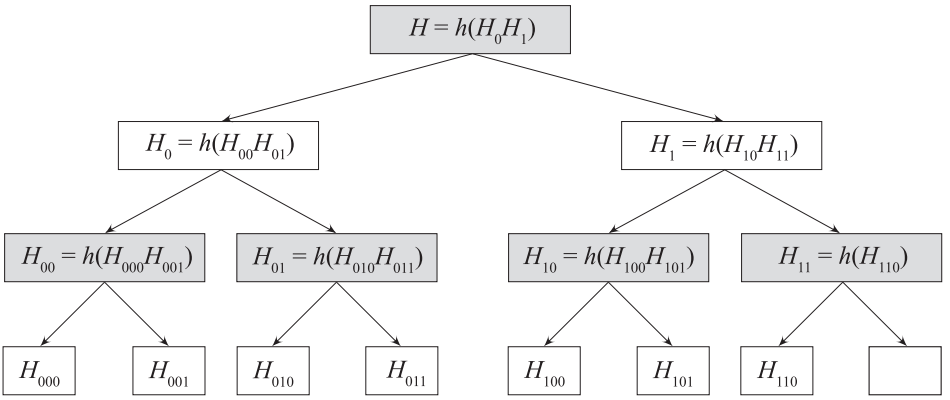

Figure 5. Merkle tree

string may look like this: H_{110}, H_{101}, H_{100}, H_{011}, H_{010}, $H_{001,}$ H_{000}, H_{11}, H_{10}, H_{01}, H_{00}, H_1, H_0, H. Elements of the string with a three-bit index correspond to transactions stored in the block immediately after its creation. Therefore, the sequence corresponds to seven transactions H_{000}, H_{001}, H_{010}, H_{011}, H_{100}, H_{101}, H_{110}. Elements with the longest indexes correspond to the hash function value h calculated for subsequent transactions. Other elements are calculated using the formula $H_x = h(H_{x0}H_{x1})$, provided that it exists within the string H_{x1}. However, if H_{x1} does not exist, then $H_x = h(H_{x0})$. Notice that the string has the structure of a binary tree with the root H.

Merkle tree enables to verify whether a single transaction occurring in the block is valid. The validity of the transaction in this case means the compliance with the tree created when creating the block. Merkle trees are the most useful when transferring large amounts of data in *peer-to-peer* networks as a kind of error detection code. To check if the second transaction is valid, simply:

— Calculate the value of A of the hash function of the transaction under verification

— Check whether the following equations apply: $H_{00} = h(H_{000}A)$, $H_0 = h(H_{00}H_{01})$, $H = h(H_0H_1)$.

In the paper *Bitcoin: A Peer-to-Peer Electronic Cash System*[5] Nakamoto has proposed a solution to the problem of excessive data collection in systems such bitcoin. The idea is to remove the transactions in which all outputs have been paid. The systematic removal of the transaction would result in low growth of memory occupied by the emerging blocks. Old blocks could no longer contain any transactions

[5] https://bitcoin.org/bitcoin.pdf.

Suppose in our example with seven transactions above that all but the first two transactions have been paid out. The other five will be removed, freeing up space. Then the Merkle tree will reduce to the string H, H_0, H_1, H_{00}, H_{000}, H_{001}.

So far, two elements of the block header have been described — Merkle tree root and *proof-of-work* of the previous and current block. The block header contains several other important elements:

— Timestamp, which is a record of the exact time of block creation
— Difficulty factor
— *nonce*, that is, a random number

1.3.3. Discovering addresses in a peer-to-peer network

Client-server computer systems usually have quite large differences between a server and a client. These differences concern both computing power and network bandwidth. Services supported by servers require much more computing power and bandwidth for handling high-intensity traffic. Even the Internet, which initially were to implement an uncentralized structure is a hierarchically organized network. It is hard to imagine e.g. the allocation of Internet addresses without a central coordinator.

Still, *peer-to-peer* systems are common in which every computer on the network acts as a client and server. This does not mean, however, that *peer-to-peer* systems do not use any services running centrally. Often the networks, which are currently working in it, need a service managing the addresses of computers. Sometimes it is supported by multiple servers for efficiency.

To understand how the bitcoin network is organized, one should look at the communication protocol between the nodes of the bitcoin network[6]. Before the network node starts a protocol associated with the exchange of transactions and blocks, the client installed on it should build a database of active network nodes. The communication protocol implemented on the client uses a number of commands and messages, which, when sent, determine how the node that received the message behaves. When building the database, messages *version*, *verack*, *getaddr* and *addr* are important. The message *version* is sent during the first call and contains information about the protocol version, current time, the types of services supported by the node, its own IP address, and the address of the node to which the message is sent. The message *verack* is sent in response to *version* as a declaration of willingness to connect. The message *addr* contains the list of some IP addresses and ports on which a bitcoin client is potentially running. Potentially,

[6] "Satoshi client node discovery", [in:] *Wikipedia*, https://en.bitcoin.it/wiki/Satoshi_ Client_ Node-Discovery; "Network", [term in:] *Wikipedia*, https://en.bitcoin.it/wiki/Network; A. Miller et al., *Discovering Bitcoin's Public Topology and Influential Nodes*, https://cs.umd.edu/projects/coinscope/coinscape.pdf.

because there is never a certainty that the client has not finished running. However, there are mechanisms implemented in the network that are more likely to detect the active nodes. *Getaddr* is a request to send the list of addresses of active nodes.

Right after starting up, the client uses external sites to determine how the IP address is seen by the outside world. For this purpose, the client establishes http connections with sites such as www.showmyip.com. It will later broadcast the received address to other network nodes, but for now it does not know which. Shortly after starting up, the client must also get the first list of network nodes, to which it will send its your address. For this purpose, it will use the addresses of DNS sites entered at the client. Addresses are entered by the manufacturer of the client and it is the manufacturer's interest to ensure that there are currently running sites there. DNS sites, which we call the source sites, are usually run by volunteers. Source sites have implemented various mechanisms to ensure the maintenance of addresses of a useful subset of nodes. Usefulness here means storing only those nodes that are online and the connection to them is readily available. Later on, addresses of DNS sites do not enter the pool of addresses passed on by nodes.

After the stage of acquiring addresses from DNS sites, the client can forget the source sites, because it may ask the nodes, which have addresses stored in the address database, about further addresses.

Each node x maintains a database of addresses — consisting of the assignment of a timestamp to IP addresses. Nodes also keep a list of connections in which the address buffer and the list of known nodes is stored for each node y with which the connection is maintained. The address buffer is a set of pairs of addresses and timestamps prepared to send to the node y, with which the connection is established. The list of known nodes is a registry of nodes, of which a given node y has already been informed. For a given vector of addresses *VecAddr*, the preparation of address buffer of node y to send consists in copying those nodes n which do not belong to the list of known nodes of node y from *VecAddr* to the address buffer.

When the customer of the node x already has the first addresses of the bitcoin network outside source sites, it sends its first *version* type message along with its address and the current timestamp. When it receives a reply from the source site y, it sends a message *getaddr*. It receives the message *addr* with the vector *VecAddr* in response to *getaddr*. Vector *VecAddr* contains up to one thousand addresses. In this situation, we insert each address from the resulting *VecAddr* to the list of known nodes for y. If an address from the vector *VecAddr* has an incorrect timestamp, which is too old or reaching too far into the future, set the timestamp five hours back from now. If an address from *VecAddr* is correct with the timestamp older than 10 min, two nodes are selected and the address is inserted into the address buffer. Each node of the *VecAddr* is also inserted in the address database with a timestamp two hours back.

When the node y, which initiated the connection, sends any information to x and the timestamp in the address database is more than twenty minutes, this

timestamp is set to the current time. If the node *x* receives the message *getaddr* from *y*, the address buffer of the node *y* is reset and up to 2500 addresses randomly selected from the current address database of the node *x* is inserted into it. When the node *y* starts communication with *x*, by sending it the message *version*, the node *x* sends the message *getaddr* back, and the address *x* with the current time is inserted into the address buffer of the node *y*.

Each node *x* sends up to one thousand nodes from the address buffer of the node *p* to a random node combined with it every tenth of a second. The addresses which have been sent are removed from the address buffer and inserted into the list of known nodes for *p*. Node *x* broadcasts its address every 24 hours by inserting the address of each connected node to the address buffer.

1.3.4. Mining a cryptocurrency

The entity storing the full record of blocks from the first block, called genesis, to the currently solved blocks is a complete node of the bitcoin network. If the node is all new, it does not have any block except the first one. Genesis block is supplied with the installed software. The client of such a fresh node starts its operations by loading hundreds of thousands of blocks and building a main blockchain.

Having the genesis block, the node reports the value of the hash function to other nodes. The other nodes send 500 values of the hash function for blocks following the genesis in reply. The node requests the full value of blocks. Now, block 501 is the last block stored in the local registry. With the value of the hash function of block 501, the node can request the network for the next 500 blocks. Building a blockchain continues until the node recreates a full blockchain stored by the network.

Creating new blocks, sometimes called solving the blocks, it plays two roles during mining. The first is the approval of transactions stored in the block by the participant who creates it. The second is the creation of new values of the cryptocurrency, which, after solving the block, belong to the person who created the block and solved it. Solving is the creation of *proof-of-work* described in the first chapter. After collecting a dozen, a few hundred or a few thousand transactions, the participant tries to find the value of the *nonce* and fill in the data field for base transactions in such a way that the value of the hash function for the header block had a prefix composed of an adequate number of zeros. The length of the string of zeros which should be at the beginning of the hash function value depends on the difficulty. The dependence of the length of the string of zeros from the difficulty will be explained later.

Knowing the rules of *proof-of-work* based on hash functions, we know that the solution of the block depends on the work involved and CPU resources. However, when a large number of participants solves a large number of blocks at the same time, the one who hits first can depend on luck, such as in the lottery. After

Cryptocurrencies as electronic means of payment without the issuer, 2016

all, guessing x, such that $h(xy)$ has 30 zeros in the beginning, is possible, but the probability of a quick hit is low. It is hard to imagine how low is the probability of solving the next ten blocks by one participant or a small number of participants.

The nodes of the bitcoin network perform different functions depending on what software is running for them. The node may be full, if it keeps a complete registry of the blocks. It may be a simplified node, if installed on a smartphone with small resources and activates the so-called simplified verification. The participant, who would like to mine cryptocurrency should install the appropriate client. Mining can be done individually or collectively in a number of vertices. A collective managed by special software is called the mining pool.

Since the creation, transactions are broadcast to the nodes of the network. Reaching the subsequent nodes, transactions are verified as to their validity and stored for some time. In the end, they are put in new blocks. New blocks are created by the nodes performing the process of mining a cryptocurrency. The registry of nodes includes many transactions. Which transactions will go to the block depends on an algorithm recognizing the priority of the transaction. The priority of the transaction depends on several factors: the time of creation of the transaction, the fee paid in the transaction, and the size of the transaction. It has already been mentioned that only those transactions in which the value of inputs passed to the transaction is not less than the value of outputs of the transaction have a chance to pass the verification. The difference between these values is the fee paid for block miners. It is widely accepted that the fee should be proportionate to the size of the transaction. There is a limit to the size of data entering the block. In addition to the accumulated transactions, the base transaction, which amounts to a certain bitcoin value, is added to the block as the first one. The value is a certain fixed amount. Currently, it is 25BTC plus the sum of fees paid in all transactions in the block. In Figure 4, fees paid amounted to 0.0037 BTC.

The new block contains the difficulty in the header marked as `bits`. Based on difficulty, we can determine the value, which we will call the target. The main task in the process of mining a cryptocurrency is to determine the hash value that is not greater than the target, and placing it in the block header. The target is determined by the formula

$$target = p \cdot 2^{8\cdot(d-3)},$$

where d is a hexadecimal number composed of the first two digits of the bits coefficient, and p is a hexadecimal number consisting of the remaining digits. In the case of the header in Figure 3 d = 0x18, p = 0x1f6973.

In order to keep up the pace of mining a cryptocurrency, the bits coefficient changes from time to time, adapting to the pace of solving the blocks. It is widely accepted that subsequent blocks should be solved every 10 minutes. Mining of new 2016 blocks should take two weeks. Each bitcoin client measures the time it took to mine these 2016 blocks and changes this number according to the percentage in

two weeks. However, this change is limited — you can not change the difficulty factor more than four times.

We know from the story of safes that hitting the appropriate hash function value requires work. In the case of a new block, this work can be done by incrementing *nonce* in the block header and changing the data field in the base transaction inserted into the block. This is what mining a block is about. Hitting the adequate *nonce* and the appropriate data field statistically requires a huge number of increments. The corresponding hash function should be calculated with each increment.

Complete nodes store a linear block registry. The blocks form the main chain with several branches. The main chain is the longest list of linearly linked blocks. Each block in the list points to the previous block. Mining a cryptocurrency is a competitive process. After collecting the adequate number of transactions and beginning the increment, the node or the mine has a limited time to find a solution. If a solution is found quickly enough, the block is added to the main chain and broadcasted between other network nodes. Other nodes may extend its main chain by this block.

Suppose that we divide complete nodes into the following sets: Dominion, Kingdom, and Realm. Let each set have the same computing power. Suppose that the main chains of each part of the network differ, but they have a common part covering up to the block number 393533:

$$Dominion : \langle 1\rangle \to \ldots \to \langle 393533\rangle \to a_1 \to a_2$$

$$Kingdom : \langle 1\rangle \to \ldots \to \langle 393533\rangle \to b_1$$

$$Realm : \langle 1\rangle \to \ldots \to \langle 393533\rangle \to c_1 \to c_2.$$

Suppose that the Dominion subnet was able to create the next block a_3. The new block a_3 is considered the end of the main chain in the Dominion part. The new discovery is broadcasted and reaches the Realm subnet. This part of the network recognizes the new main chain after a while. The motivation of the Realm subnet to change the main chain is quite rational. Outpacing the Dominion subnet requires solving two more blocks in the same time. This requires computing power, time, and above all luck, because winning in this competition is a matter of probability, which in this case does not work in favor of Realm. As long as the Realm subnet loses, the rest of the network will not recognize fees and rewards arising from the newly mined blocks. Hence the likely scenario is to bring the network to the following state:

$$Dominion + Realm : \langle 1\rangle \to \ldots \to \langle 393533\rangle \to a_1 \to a_2 \to a_3$$

$$Kingdom : \langle 1\rangle \to \ldots \to \langle 393533\rangle \to b_1.$$

News of the new long chain branching have not yet reached the Kingdom subnet. This subnet can work on overtaking Dominion + Realm subnets, however, it is in even worse situation than the Realm subnet before it switched to the main chain of Dominion. Worse situation stems not only from the difference between the lengths of the major chains, but also from the fact that the Kingdom subnet has twice less computing power. In this situation one can imagine that a group of people with hand tools decides to seek ore in a gold mountain, while a company that can afford machines starts mining on the other side of the mountain. The probabilistic consequence of this situation is the Kingdom subnet switching to the chain belonging to the rest of the network, when only the Kingdom subnet learns about the length advantage.

Switching from one branch to another is not immediate from the technical point of view. Rather, it is the process of leaving the branch. Where notifications of new blocks reach a particular subnet, the nodes build a tree of blocks, knowing what is the distance of each block from the first one. It is in the interest of the network to create new blocks by linking them to the longest branch. Once one branch gets advantage over the other, switching is to start creating new blocks in relation to the branch which is currently the longest.

1.3.5. Incomplete nodes

Complete nodes store a chain of blocks, which takes tens of gigabytes of memory. With the increasing popularity of cryptocurrencies, a large number of clients have been designed for devices with limited memory and computing power, such as smartphones, tablets or embedded systems. Along with the restrictions, it became necessary to implement a simplified system of transaction verification, which does not use the entire registry of blocks. At full registry, the verification whether certain output has not been exercised multiple times, requires reviewing of many outputs. Simplified verification system needs to load the headers of blocks without complete transactions. Memory occupancy is about 1000 times smaller in relation to the full registry. Verification in simplified systems is based on a completely different principle of providing on-demand blockchain fragments which are necessary for verification.

The wallet operating on the principle of simplified payment verification can hold a link to the block, which contains the verified transaction and the corresponding indicator in the Merkle tree. Positive verification is equivalent to waiting until some new headers blocks appear that have been approved by the network after the appearance of the indicated transaction. This only proves that a network of complete nodes had time to approve the indicated transaction. As long as an incomplete node is connected to the complete honest vertices, the state of the incomplete node becomes the reflection of the state of complete nodes.

1.3.6. Bitcoin from the point of view of the user

Having a PC with plenty of disk space, we can get started with bitcoin being the complete node. First, we should install one of the available network clients. This may be Armory, Electrum or classic Bitcoin-Qt. The client is a program that connects to the bitcoin network, enables to make transfers and provides some security options. Once installed, the client begins the process of downloading and verification of a blockchain. It takes quite a lot of time, because the entire database is the size of several dozens of gigabytes. Fortunately, downloading a blockchain is a one-time process, which means that we will not have to undergo such a costly process for the second time.

The classic bitcoin client provides us with the option of password-protected encryption. It is worth taking advantage of this opportunity in order to prevent a situation where the wallet file is copied by someone unauthorized or malicious software. The client also provides the option to set the commission during the transfer. Keep in mind that the higher the commission, the faster the transactions will be included in the solved block, and thus — the transfers will be approved faster.

When making transfers in the bitcoin system, the user can be associated with one address. Because the address is derived from the public key, maintaining a single address for too long is an act contrary to good practices. Each pair of private-public key has its life time and a new key pair should be chosen before its expiry. A good rule of thumb is one user having multiple addresses in the context of maintaining a wallet. This prevents in some way traceability and associating receipts with one user. While maintaining multiple identifiers, one user is seen as many protocol participants in the system, which somehow increases the anonymity of the user, by reducing the possibility of associating transfers. This can take place as follows: we want to transfer 5 BTC to the address Y from our address X, where we have 100 BTC. We can do this, transferring 5 BTC to the address Y and 95 BTC to a new address Z or dividing 95 BTC into more addresses. Failure of the wallet when using multiple addresses could have a negative impact, because it is important to take frequent copies of the wallet file.

1.3.7. Definitions for legal and economic purposes

A regular bitcoin user has a client installed on a computer or mobile device. The client includes a wallet, which stores bitcoins. The wallet includes a function connecting to the bitcoin network and enables to make transfers. The user can set the size of the commission in the client, which the user is able to pay for the transfer. It is possible to encrypt the password-protected wallet. The user using the wallet is assigned an identifier, which is a public key processed by a cryptographic hash function. The association of the user with the public key is that the user controls the

private key associated with said public key. Control is based on a confidential storage, which provides conditions for the exclusive use of the private key by the user.

Transaction outputs associated with the value in cryptocurrency, which has not yet been used as transaction inputs, represent an unreleased cryptocurrency. Each output indicates the identifier of the user whom the transaction passes bitcoins. The user is the owner of cryptocurrency stored in the outputs if the user controls the private key associated indirectly with the identifier, and directly with the public key encoded in the identifier.

The user controlling the wallet can initiate a new transaction by making a transfer to the identifier of a different user. The transfer applies to the value which the user initiating the transfer owns. Initialization of the transaction makes the user payer, and the recipient is the user with the identifier to which the transaction is directed. The process of creating a new transaction with an output of corresponding identifier belonging to the recipient is called referring the transaction.

The process of creating new blocks with the selection of a suitable hash function is called mining a cryptocurrency. Finding the right hash value requires work associated with the involvement of computing power. Creating a new block involves the creation of a new cryptocurrency value, which is the fee for finding the right hash value assigned to the resolved block. The newly created value is the result of mining. The user providing the computing power for mining a cryptocurrency is called the miner.

Chapter 2

Economic aspects of cryptocurrencies

2.1. Cryptocurrencies in economic terms — the substance and essential characteristics

From its inception until now, the access to and use of the Internet is growing at a dynamic pace. The number of users worldwide has already exceeded the threshold of three billion[7] and the next levels are a question of time. One of the effects of the development of the Internet are structural changes in social behaviors, affecting the way of life, exchange of information or the method of establishing relationships. The particular manifestation of this is the spread of virtual communities in which people realize mutual goals and meet their needs. The progress in the computerization of society results in moving more and more aspects of everyday life to the realm of virtual reality. This process leads to the appearance of many previously unknown phenomena, including those related to economy[8]. The phenomenon of virtual communities on the Web creating their own means of payment, enabling the exchange of goods and services, is the area of particular interest in the economic and financial dimension. The resulting means of payment become a kind of a new form of digital money, an alternative to the use of traditional currencies in transactions.

In the economic aspect, in addition to technological development and dissemination of Internet, turmoil in the financial market and uncertainty regarding the future shape of the financial system observed in recent years are a fertile ground for the development of alternative forms of payment. The crisis in financial markets has undermined public trust in the traditional banking system, money, principles of operation of financial institutions, the role of financial supervision and the ability to

[7] As of January 1, 2016 there were 3.3 billion users (from: http://www.worldometers.info/pl/ (access: January 10, 2016)).

[8] Ł. Dopierała, A. Borodo, "Znaczenie waluty kryptograficznej Bitcoin jako środka wymiany", *Contemporary Economy* 5, 2014, No. 2, pp. 1–12.

Cryptocurrencies as electronic means of payment without the issuer, 2016

control the situation by the state authorities[9]. Consequently, increased uncertainty regarding the existing rules governing the financial system is a vulnerable ground for new ideas and means of establishing economic relations. One of the manifestations of this is the emergence and development of cryptocurrencies as a potential alternative to traditional means of payment and settlement of transactions settled in the economy.

The starting point to determine the economic impact of cryptocurrencies is the explanation of their essence and the indication of their essential characteristics. In the first phase of this treatise at the economic level, we should, distinguish between three concepts simultaneously functioning in the scientific literature and practical studies:

— Cryptocurrency
— Virtual currency
— Digital currency.

In all these three concepts, a key common element is the use of the term currency, which, however, in this sense, is conventional and does not mean official currency that is legal tender in a given country, but rather a currency in the broad sense, i.e. generally understood and used means of exchange. It is also possible to understand this concept more broadly, as a system for the exchange of specific goods[10].

Virtual currencies are the topic which is the most frequently described in theory and in used practice. In the current state of knowledge, the concept of virtual currency has been most extensively defined by the European Central Bank as a kind of digital currency unregulated by law, whose issuance is controlled by its creators and used and accepted among the members of a particular virtual community[11]. It should be noted that that definition does not include all features of virtual currency, and the very concept will undoubtedly evolve in the subsequent years along with the development of the phenomenon. Nevertheless, this definition emphasizes the key features of virtual currencies determining the essential nature of their formation and operation. These include: digital nature, whose manifestation is full dematerialization of virtual currencies, which essentially distinguishes them from traditional currencies which currently still occur simultaneously in the form of cash and cashless, and no direct control of state authorities over the circulation of virtual currencies. Currently, there are many different systems of virtual currency that are not easily classifiable. The most commonly used criterion are interactions of virtual currency with the traditional means of payment and the

[9] See: E. Chrabonszczewska, "Bitcoin — nowa wirtualna globalna waluta?", *International Journal of Management and Economics* 40, Warszawa 2013, p. 51.

[10] J. Czarnecki, "Nie tylko bitcoin, czyli rodzaje wirtualnych walut", [in:] *Wirtualne waluty*, Warszawa 2014, p. 9, http://www.wardynski.com.pl/gfx/wardynski/userfiles/_public/raport_o_wirtualnych_walutach.pdf (access: January 25, 2016).

[11] European Central Bank, *Virtual Currency Schemes*, October 2012, p. 5.

real economy. Taking this into account, we can distinguish three types of virtual currency systems[12]:

— Closed systems existing in isolation from the outside world of real economy. They are closed within the activities of a community usually within the reality of a computer game. The users of the network game can earn virtual money on the basis of results achieved, and the funds can only be spent through the purchase of goods and services offered within the virtual community. Thus, in theory at least, they cannot be traded outside of the virtual community.

— Systems with unidirectional cash flow, which accept cash flows from the outside. Virtual currency can be purchased for real money at a fixed exchange rate, but it is not possible to reverse the transaction. Thus, the system can be charged using funds from outside, and after their conversion to virtual currency they do not return to the real economy, remaining the means of payment only for transactions in the virtual social network. The given system is basically a way to achieve financial income for the creators of the virtual community usually focused around the networked computer game.

— Systems with bidirectional cash flow, in which the virtual currency can be freely exchanged for other currencies. Exchanges, exchange offices and other intermediaries act as input and output. Cryptocurrencies, which are bilaterally exchanged for traditional means of payment, are the example of such a solution.

However, the bidirectional nature of cash flows is not the only differentiator of cryptocurrencies. According to the name and principle of creation extensively described in the previous part of this book, a major factor it is the fact that the system is based on the cryptography principles. In addition, which is an important feature distinguishing cryptocurrencies from other virtual currencies is the inherently decentralized nature of the system, in which there is no central issuer. And it is not only that the issuer is not a state-controlled monetary authority, but also e.g. not a computer game publisher placing means of payment on the market within a virtual community. In addition, the decentralization feature of the cryptocurrency system is a method of verification and processing transactions taking place in a distributed manner in the network of users (e.g. a mining process described in the previous part of this book in the case of bitcoin). In the case of some virtual currencies the system is centralized by creating a central accounting system for the virtual community that conducts and verifies transactions (e.g. in the case of linden dollars as a means of payment in Second Life).

Therefore, comparing the features of cryptocurrency and virtual currency, we can point the differences shown in Table 1.

[12] Ibid., pp. 13–15.

Table 1. Differences between virtual currency and cryptocurrency

Specification	Virtual currency	Cryptocurrency
Form	digital	digital
Controls by the state	none	none
Principles of creating the currency	Use of different technological solutions (one of which may be cryptography)	Default use of cryptographic solutions
Mode of putting the currency in circulation	Centralized or decentralized (depending on the solution used for the virtual community)	Decentralized
Examples	linden dollars, WoW gold, bitcoin, litecoin	bitcoin, litecoin

Source: own work.

Therefore, it can be concluded from the presented comparative analysis that the concept of cryptocurrency is semantically narrower and included in a broader concept, which is virtual currency. Thus, the terms "cryptocurrency" and "virtual currency" are not semantically separate, as it is sometimes suggested in a variety of theoretical and practical papers[13]. Basically, the genesis of cryptocurrency, in addition to the above list, proves that. The idea can be traced in studies dating back to the late twentieth century that presented different visions of the prospective development of money and forms of transactions. In the broadest terms, the concept of cryptocurrency refers to the vision of e-money dating back to 1982, by D. Chaum[14], further elaborated in many subsequent studies[15]. In the principal aspect, e-money, similar to traditional means of payment, was intended to ensure a normal exchange of goods and in this respect the concept has not introduced anything revolutionary for the formation of economic relations both globally and locally. The innovation of e-money manifested more in efforts to create a system that allows high-speed transactions without intermediaries, which also would lower the costs of the payment system. Naturally, various technical solutions which allow to achieve this objective were presented over the years. The idea cryptocurrency is one of them, and the author of the paper published in 1998. Wei Dai[16]

[13] J. Czarnecki, op. cit., p. 9.

[14] S. Barber et al., "Bitter to Better — How to Make Bitcoin a Better Currency", [in:] *Financial Cryptography and Data Security*, ed. A.D. Keromytis, Berlin-Heidelberg 2012, pp. 399–414. D. Chaum, op. cit., pp. 199–203.

[15] T. Okamoto, "An Efficient Divisible Electronic Cash Scheme", [in:] *Advances in Cryptology — Proceedings of CRYPT0' 95*, Berlin-Heidelberg 1995, pp. 438–451; S. Canard, A. Gouget, "Divisible e-Cash Systems Can Be Truly Anonymous", [w:] *Advances in Cryptology — Proceedings of EUROCRYPT 2007*, Berlin-Heidelberg 2007, pp. 482–497, quoted in: M. Polasik, A. Piotrowska, R. Kotkowski, "Waluta wirtualna Bitcoin z perspektywy oferentów interentowych. Analiza wstępna", *Nauki o Finansach* 4, 2013, No. 17, pp. 131–132.

[16] W. Dai, *B-Money*, http://www.weidai.com/bmoney.txt (access: October 6, 2016).

is considered its precursor, who describes cryptocurrency in a visionary way as money, in which cryptographic solutions replace the central government and the monetary authorities regarding the issue of money, and thus create the system to issue money, control the market and carry out transactions that is entirely alternative to modern economics. The use of contemporary methods of cryptography, mathematical algorithms, and computing functions extensively described in the previous part of this book in conjunction with the development of the Internet has become in this case not only a kind of "material" for the development of the idea of digital money, but allowed at the same time to propose solutions, which got cryptocurrency closer to the idea of money without intermediaries, faster and cheaper compared to traditional and existing other virtual currencies. The classical solution — used both by other virtual currencies and payment systems in real economies — introduces a trusted intermediary, e.g. bank, which verifies the correctness of transactions[17]. As follows from the previous section, cryptocurrencies are based on the *peer-to-peer* (P2P) model, in which all completed transactions carried out by users are made public, and the validation of their performance is done by system users themselves. As a result, it is impossible to shut down the system by developers or any third party[18].

Currently, cryptocurrencies are not officially recognized by individual countries, including Poland, as currency units or electronic money. Undoubtedly, this limits the development of cryptocurrencies, causing many legal and tax difficulties. This does not change the fact that cryptocurrencies are used by users from different countries, which automatically makes them a kind of competition to traditional currencies officially recognized by the individual countries. As a matter of fact, the existence of currencies which are competitive for traditional currencies is not a new phenomenon. It appeared in the past, even before the era of the Internet, e.g. in the form of local currencies, separated from the national currency, emerging in different parts of the world. However, the lack of territorial restrictions as the result of using the Internet to develop cryptocurrencies makes the scale of the phenomenon global in this case, which leads to a situation in which cryptocurrencies circulate in parallel with money issued by individual countries.

Specific nature and global reach of the use of cryptocurrencies can have a significant impact on the economy. On one hand, it produces positive impulses associated with the generation of financial innovation and the provision of alternative forms of payment for users. On the other, it is clear that the use of cryptocurrencies can also pose a risk for their users, especially in light of the current lack of regulation and legal provisions regarding trading rules. In fact cryptocurrencies now

[17] P. Everaere, I. Simplot-Ryl, I. Traoré, "Double Spending Protection for e-Cash Based on Risk Management", [in:] *Information Security*, ed. M. Burmester et al., Berlin-Heidelberg 2011, pp. 394–408.

[18] M. Polasik, A. Piotrowska, R. Kotkowski, op. cit., p. 132.

operate as a means of exchange in terms of settlement units being an intermediary in the exchange in the case of transactions carried out by members of a virtual community. However, the following questions arise:

a) Can cryptocurrencies now be treated as money and serve their classic purpose?

b) Can cryptocurrencies replace traditional means functioning as money with the development of the phenomenon?

c) How much cryptocurrencies can popularize and compete with traditional currencies?

d) To what extent the idea of cryptocurrency links to the economic theories of money?

e) How much cryptocurrencies are a safe means of payment?

f) What opportunities and threats the development of cryptocurrencies may entail both for their users and for the economy as a whole?

Answers to these questions determine the nature of the subsequent subsections devoted to the economic aspects of functioning of cryptocurrencies.

2.2. Forms of modern money and cryptocurrencies

The origin of its name clearly reflects the essence of money (lat. *pecunia*) in the economy — in Latin *pecus* means cattle, used in Roman times as an intermediary in the exchange of goods[19].

This suggests that one can establish any commodity as a universal equivalent, solely based on a social contract. Regardless of its external form and the economic system, money is perceived now as legally defined, widely accepted means of payment, which can express, store and accept the values and whose value is closely related with the real GDP[20]. The accepted money is the commonly recognized means of "transferring values in space or time"[21]. This is tantamount to saying that money has many properties and simultaneously satisfies more than one function. The following functions are usually mentioned in this regard:

1) Means of exchange
2) Measure of value
3) Means of hoarding
4) Means of payment.

[19] See: B. Pietrzak, Z. Polański, W. Woźniak, *System finansowy w Polsce*, Warszawa 2008, p. 59.
[20] P. Schaal, *Pieniądz i polityka pieniężna*, Warszawa 1996, p. 26.
[21] B. Oyrzanowski, *Makroekonomia*, Kraków 1997, pp. 122–123.

It should be stressed that these functions of money are not detachable. The literature has perpetuated the belief that some of these functions, namely the functions of measure of value and means of exchange, are original with respect to other[22]. Furthermore, as the history of money shows, the importance of some functions may be permanently reduced in time, while the other will gain significance. At the same time, money does not fulfill all its functions in any conditions. An example would be an inflationary environment where the capability of money to play the role of a hoarding tool and a means of expression of value is limited.

Among various assets, money is especially distinguished by the ability to be used as a means of exchange (circulation)[23]. This happens when it is an intermediary in the transactions of the purchase and sale of goods and services. Thus its existence simplifies economic life, displacing an inconvenient barter[24].

Allowing the regulation of financial liabilities, including taxes, government transfers or loan repayments determines the existence of money as means of payment. Then one can say about the characteristics of money, which is the power of settling obligations[25]. Similar to the means of exchange, money as the means of payment participates in situations where the exchange occurs, but the flow of goods and payments is not simultaneous in this case.

The value of any goods or services is expressed in cash, which manifests itself in determining their prices[26]. Value of goods measured in money changes over time. This is why it is so important that the purchasing power of money was stable. The relation of the size of the circulation of money and the value contained in the commodities market shape the value of money[27], hence the function of the measure of value, which is performed by money, is inextricably associated with the process of exchange. However, this relationship is indirect, because money is in the ideal form as a measure of value. Its appearance in physical form is not necessary in this interpretation — an idea suffices that money expresses the value of commodity[28].

The tool to measure the value does not exist in a barter economy, in which the number of individual relationships between exchangeable goods was infinite, and thus an infinite combination of prices. Thus, the price of each item would have to be expressed in many commodities[29]. To use the language of Aristotle, "all that is exchanged must be able to somehow compare"[30]. Only the creation of

[22] B. Pietrzak, Z. Polański, W. Woźniak, op. cit., p. 57.

[23] F.S. Mishkin, *Ekonomika pieniądza, bankowości i rynków finansowych*, Warszawa 2002, p. 86.

[24] See. more in *Makroekonomia ze szczególnym uwzględnieniem polityki pieniężnej*, ed. M. Noga, Warszawa 2012, pp. 71–76.

[25] Ibid., p. 76.

[26] R. Milewski, E. Kwiatkowski, *Podstawy ekonomii*, Warszawa 2008, pp. 339–340.

[27] S. Owsiak, *Podstawy nauki finansów*, Warszawa 2002, p. 108.

[28] R. Milewski, E. Kwiatkowski, op. cit., pp. 339–340.

[29] F.S. Mishkin, op. cit., p. 88.

[30] Arystoteles, *Etyka nikomachejska*, Warszawa 1956, p. 178.

money made it possible to make such a comparison, strongly facilitating economic decision-making. For this reason, money is identified as the tool to measure value.

From the function for measuring of value follows the function of storing of value. The capability to express the values of all goods using a means called money also includes the ability to add up the values of individual goods and express the assets in this way. This is why the function of money as a means to store value is also called the function of a means of hoarding[31].

Sometimes economic entities do not decide on the location of surplus cash in the financial markets, which would allow to put money into circulation[32]. Today, the function of accumulation of wealth (hoarding) is performed in this way. However, the accumulation of cash savings is considered reasonable only when the condition of stability in the purchasing power of money is met[33]. Therefore, money is realized in this function, when we as buyers trust that it holds a value. Obviously, this function loses its importance with the rapid development of financial markets and emerging alternatives in terms of savings.

The extensive use described and multiplicity of these functions have historically been volatile. Nevertheless, it has been assumed to define money by its functions. Different types of money do not share common properties (features). It is not enough to say that what we call money is usually offered or received when buying or selling of goods, services, and other things[34]. Think of this as an oversimplification.

The basic division distinguishes the form (even shape and material) of money — this is a chronological approach — and is almost identical to the division into money with intrinsic value (commodity, of full value) and fiduciary (symbolic, deficient). The development of forms of money also included primitive money, ore paper money, banking money, digital money[35]. The emergence, development and disappearance of these forms of money proceeded unevenly in space and time. However, they often marked a new quality in economic efficiency.

Currently, money comes in two forms:

— Cash money (real), occurring in the material form of paper money (banknotes) or in the form of coins issued by the monetary authorities of the country concerned

— Cashless money, having no material physical form, which is the subject of the accounting records of the banks and created in a banking system as a credit

Of course, the presence of money in present forms does not in any way exclude the emergence of new means of payment, which evolutionarily may replace

---

[31] P. Schaal, op. cit., p. 23.

[32] S. Owsiak, op. cit., p. 109.

[33] *Makroekonomia…*, p. 76.

[34] J.K. Galbraith, *Money: Whence It Came, Where It Went*, Boston 1976, p. 6.

[35] W. Piaszczyński, *Anatomia pieniądza*, Warszawa 2004, p. 19.

the currently accepted forms, compete with them, and even displace them. Cryptocurrencies can emerge just as a possible alternative from this perspective, and not only for cash, but also for non-cash forms of crated in the banking system. Undoubtedly, however, as the history of economics shows, a set of features and characteristics of a given commodity, which qualifies it to play the role of money, favors the capability of performing the aforementioned functions. The following are mentioned most often in the literature:

— Durability — money should retain its physical properties in time and should not be subject to easy destruction

— Divisibility — money must be divisible into smaller units without loss of value

— Scarcity in the economic meaning — i.e. it should have limited availability (supply) relative to the goods and services occurring on the market

— Homogeneity — money should be similar to each other

— Convenience — money should allow relocating its significant values

— Originality — money should be difficult to forge

Referring to the technological aspects of creation and operation of cryptocurrencies described in the previous section, we should conclude that cryptocurrencies meet all of these features, and some of them even to a much higher degree than a traditional currency. This applies in particular divisibility, which in the case of bitcoin is guaranteed up to eight decimal places, while quoting of traditional currencies is limited to four decimal places, and only to two decimal places in the case of cash (pennies, cents, etc.). Certainly, cryptocurrencies are also scarce, which is provided almost automatically by the established limit of created units assumed by the algorithm. Convenience obtained by a digital nature and originality (provided by cryptographic security) are also indisputable. Somewhat more controversial may be the perception of durability because of the risk factor, which is the stability and security of computer systems and the Internet. However, in comparison with the cashless money, cryptocurrencies undoubtedly feature at least comparable durability (after all, similar technological conditions and associated risk factors appear in the creation of money in the banking system), and even far greater when compared to cash.

Seeing the money in pure economic terms as a commodity to meet the needs, it should be emphasized that money, unlike other economic goods, has its individual specifics. If we analyze money in terms of the market, the market mechanism reflecting the supply and demand for money determines its price, as in the case of other goods. However, unlike other goods money is specifically isolated from the economy, i.e. when there is something unfavorable going on in individual markets, in any way this does not have to adversely affect other markets, and certainly not the whole economy. For example, a sudden increase in the market price of potatoes will affect the decisions of consumers and producers, it will partly affect the markets for substitute and complementary goods, and will not affect the behavior

of all other markets of other goods[36]. In contrast, in the case of money every change in the demand and supply of money translates directly or indirectly into other markets. For example, if the money supply in circulation rises or falls, it will affect the situation of each market — some more quickly, others more slowly, but undoubtedly each market will be affected. Similarly in the case of rapid changes in the demand for money (the desire to possess and buy). Decisions of the holders of the funds will also affect all markets for goods and services. Even if the impact is uneven, it will certainly occur[37]. This fact makes any potential appearance of possible new forms of money should be subjected to particularly careful analysis due to the effects it may bring about for the economy. For this reason, the economic analysis of the phenomenon of cryptocurrencies is necessary to establish the legal conditions related to their functioning and possible distribution further in this book.

2.3. Cryptocurrencies and a theory of money

2.3.1. Theories of money in the mainstream economy — factors affecting the demand for money

The extensive use described and multiplicity of these functions raises the demand for money. The demand for money in the most general terms adopted in the literature should be understood the demand raised by businesses or households. However, currently it is considered that the demand for money is determined by the amount of money in real terms, for which the demand was submitted by market entities[38]. In theoretical considerations it is most often assumed that the stock of money includes cash and bank deposits on demand as assets with the highest degree of liquidity[39].

As keeping a cash reserve involves the alternative cost, whose expected size is determined by the market interest rate[40], the existence of subjectively conceived benefits inducing the loss of potential income in exchange for liquidity represented by money is suggested[41].

This situation is associated with functions of money in the economy[42].

---

[36] M. Machaj, *Krótki przewodnik po teorii pieniądza*, http://mises.pl/blog/2012/03/29/machaj-krotki-przewodnik-po-teorii-pieniadza/ (access: January 12, 2016).

[37] Ibid.

[38] See: *Makroekonomia…*, p. 76.

[39] See: R. Milewski, E. Kwiatkowski, op. cit., p. 343.

[40] On risk-free, fixed-rate investments, and the most common — the yield rate of treasury bonds. More on this topic: D. Begg, *Ekonomia*, Warszawa 1994, p. 131; R. Milewski, E. Kwiatkowski, op. cit., p. 345.

[41] See: D. Begg, op. cit., p. 131.

[42] See more: S. Owsiak, op. cit., p. 93.

Concepts relating to the factors shaping the demand for money are constantly evolving. The reference to the specificity of functioning of cryptocurrencies requires an abridged chronological analysis of various trends relating to this subject.

One of the first theories to clarify the essence of money is the so-called quantitative theory of money. Its first historical reference is found in the *Treaty on coining money* by Nicolaus Copernicus. Although it is based more on the metallistic theory of money (in which ore, from which coins are made, is considered their source), but the assumption regarding the function of money (measure of value, means of circulation, means of hoarding), and especially the law of bad money, inspired subsequent promoters of the quantity theory of money. The Law of bad money, now called Copernicus-Gresham's law, assumes that worse money, i.e. made of precious metal of inferior quality, and therefore having less value, displaces better money in the circulation. For this reason, Copernicus is sometimes considered a precursor of the quantity theory of money based on the conclusion that the coin (money) loses value as a result of an excessive amount of money in circulation[43]. Fundamentals of the quantity theory of money were also reflected in the works of late Scholastic school from Salamanca (sixteenth century), D. Hume (eighteenth century), J.S. Mill (nineteenth century)[44].

The most famous development of the classical quantity theory of money is the contribution of I. Fisher finally expressed in the following equation[45]:

$$M \times V = P \times T,$$

where:

M — The amount of money in circulation

V — The rate of circulation

P — The average level of prices

T — The number of transactions in a given period

It is pointed out that the condition for the validity of the equation is the same value on both sides that is the cash sum of commodity transactions[46]. Note that Fisher only analyzes money in its transactional function (exchange). According to the quantity theory[47]:

— Money supply is fixed (due to the decisions of monetary authorities)

— The number of transactions in the short term is constant (because the utilization of labor, capital, and land change gradually)

— The rate of circulation of money is constant (due to undergoing slow changes in the technological and institutional conditions)

---

[43] E. Lipiński, *Historia powszechnej myśli ekonomicznej do roku 1870*, Warszawa 1981, p. 81.

[44] Z. Fedorowicz, *Teorie pieniądza*, Warszawa 1993; Z. Polański, *Pieniądz i system finansowy w Polsce*, Warszawa 1995; A. Kaźmierczak, *Pieniądz i bank w kapitalizmie*, Warszawa 1994.

[45] See: A. Kaźmierczak, *Polityka pieniężna w gospodarce otwartej*, Warszawa 2008, p. 85.

[46] See: W. Stankiewicz, *Historia myśli ekonomicznej*, Warszawa 1998, p. 439.

[47] See: R. Milewski, E. Kwiatkowski, op. cit., s. 347; *Makroekonomia*..., p. 79.

When the above conditions are met, one can infer a proportional dependence, which exists between the nominal resource of money in circulation and the average price level. Then the size of the demand for money is given by[48]:

$$M^D = \frac{T}{V} \times P,$$

where:

M^D — The demand for money.

The demand for money depends on the evolution of the average price level (P), which means that the growth of prices, and thus increasing the value of transactions, is accompanied by the resulting increase in the demand for money.

Translating the quantity theory of money into the plane of use of cryptocurrencies in trade leads to an interesting reflection. The algorithm for creating many cryptocurrencies (including the most famous, such as bitcoin or litecoin, as referred to further below), assumes reaching the predetermined number of units, which will be constant over time. According to the quantitative theory, in particular, the cited Fisher equation, it should therefore lead to limiting the increase in the price level in the long term.

An attempt for a different interpretation of the quantity theory was made by A.C. Pigou and A. Marshall. Determining the factors influencing the demand for money in this concept proceeded on the basis of determination of the proportion of the distribution of current income between the stock of money and other forms of deposits[49]. As a result, it became possible to determine the rate of money circulation based on determining which part of the income is held in cash. Therefore, the rate of money circulation was understood as the number of turns made by the unit of money in a given period[50]. The assumption is expressed in the ratio:

$$\mathrm{K} = \frac{1}{V} = \frac{M}{D},$$

where:

D — Global income in the economy

k — The factor which determines what part of the income Y the entities of the economy want to keep in the form of cash.

The transactional version was replaced by the theory of quantification of reserves by the abandonment of the transactional value, which is difficult to measure, in favor of the national income, which can be expressed as:

$$M^D = kPY,$$

where:

Y — Real national income.

---

[48] *Makroekonomia...*, p. 79.

[49] W. Stankiewicz, op. cit., p. 439.

[50] See: A. Kaźmierczak, *Polityka pieniężna*…, p. 86.

It should be noted that the terms of this equation with respect to Fisher's exchange equation remain unchanged[51]. Thus, the assumption was made that *k* is a constant, which is tantamount to saying that global real income is established as the factor, which has the biggest impact on the demand for money. It is considered stable in the short term, therefore the money supply affects the changes in prices[52]. In this way, the basic assumption resulting from the quantity theory was upheld. With respect to cryptocurrencies, which assume, as mentioned, a fixed and limited supply of created units, this may result in a deflation nature of cryptocurrencies on one hand. On the other hand, it may raise concerns about the capability of handling transactions in the conditions of economic growth, which in the light of the quantity theory raises doubts whether cryptocurrencies can displace traditional currencies and replace them in the role of a universal intermediary in transactions in the situation where the increase in global real income creates an increased demand for transactions.

A contribution to the quantity theory by representatives of the school in Cambridge, who distinguish more than one (transactional) reason of having money, is important considering the idea cryptocurrency. Money is also considered as a means of savings, and the need to create a reserve for contingencies is a reason to keep it[53]. This plays a special role in the theoretical consideration of cryptocurrency as a potential alternative to official money. On one hand, the limited supply of cryptocurrencies may in time cause increased hoarding tendencies in a market. On the other hand, full virtualization, and uncertainty as to the economic stability and legal regulations as it is now, may constitute a somewhat mental barrier to keep purchasing power in this form. This also signifies an important need for research for the evaluation of the use of cryptocurrency as a way to accumulate savings, which will be reflected in the empirical part of this chapter.

Undermining the main objectives of the quantity theory occurred with the publication of *The General Theory of Employment, Interest and Money* by J.M. Keynes[54]. In particular, the theory of money presented there includes the claim that the money supply is determined by the demand for money. By referencing the specific functions of money to determinants of demand for money, Keynes distinguished between three reasons embedded in psychology:

— Transactional
— Precautionary
— Speculative.

Following these reasons, analogous types of demand are defined, which added together designate the demand for money in the economy.

---

[51] See: S. Guzdek, "Historyczne ujęcie klasyczno-neoklasycznej teorii pieniądza i poglądów", *Zeszyty Naukowe* 2010, No. 8, p. 212.

[52] See: A. Kaźmierczak, *Polityka pieniężna*..., p. 87.

[53] W. Stankiewicz, op. cit., p. 439.

[54] J.M. Keynes, *Ogólna teoria zatrudnienia, procentu i pieniądza*, Warszawa 1956, p. 125.

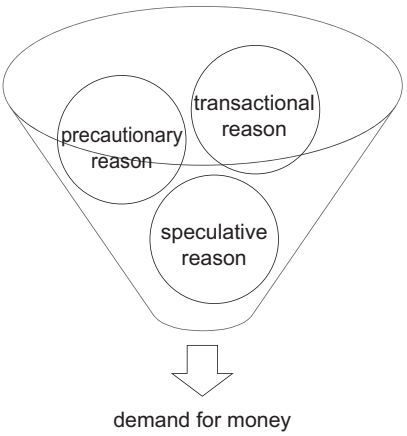

Figure 6. The reasons for the demand for money by J.M. Keynes

Source: own study based on *Makroekonomia*…, p. 77.

The source of transactional reason is the foreseen need to pay for purchased goods and services, and this in turn is related to the use of the general equivalent (money) in exchange processes. In this perspective, keeping money results only from imperfect synchronization of revenues and expenditures of economic entities in time[55]. These temporary differences will influence the amount of funds, which entities strive to possess, but they are not decisive[56]. According to Keynes, the volume of transactional demand, identical to the value of transactions, remains positively and strongly correlated with the size of national income[57].

The prevalence of money as a medium of exchange involves the precautionary reason. Caused by uncertainty regarding the development of income and expenditures in future, depends in particular on keeping cash reserves to cover unforeseen expenses. Strong positive correlation occurs between income and the size of precautionary demand[58].

The causes of the speculative (portfolio) reason are believed to be in the perception of money as a means of accumulation. That's why J.M. Keynes, using the assumption of substitutability of money and bonds (or financial assets in a broader context), proposed a comparison of the cost of keeping money and possible gains/losses resulting from investments in bonds, in order to decide on the size of individual speculative demand based on the expected future level of interest rates[59]. The portfolio reason thus applies to investment decision-making under conditions of uncertainty regarding the evolution of interest rates in future.

[55] See: D. Begg, op. cit., p. 131.
[56] See: ibid.
[57] See: S. Owsiak, op. cit., p. 94.
[58] See: R. Milewski, E. Kwiatkowski, op. cit., p. 349.
[59] See: *Makroekonomia*..., p. 78.

Speculative reason is particularly important for the analysis of phenomenon of cryptocurrencies. Note that keeping the money for purposes other than trading and possibly precautionary (Cambridge school — a way of collecting savings) was not addressed in the quantity theory[60]. Moreover, Keynes believed that the accumulation of savings in the form of money is risk-free, which can become an incentive to resign from a part of the investment in risk assets when market interest rates are low (in favor of liquidity). Thus diversified portfolio includes money, which due to its basic feature — liquidity — can be quickly converted to any assets characterized by higher profitability. This is equivalent to keeping the money resource for the purpose of speculation, thus achieving a profit[61].

An inverse relation which exists between the level of market interest rate and the demand for money resulting from the portfolio reason emerges from the reasoning presented above. The phenomenon called liquidity trap resulting from the expectations associated with changes in interest rates is the consequence of the speculative reason. The occurrence of this situation would make monetary policy ineffective in terms of its stimulating effect on economic activity[62] due to hoarding of all cash resources by entities.

Transactional demand unrelated to uncertainty and the resulting precautionary and speculative demand co-create the so-called liquidity preference, which means the tendency of entities to keep their assets in the most liquid form. This means that the aggregate demand for money is a function of the nominal national income (*P2Y*) and the interest rate (*r*)[63]. It is worth mentioning that it was J.M. Keynes who introduced to the theory of money the concept of (speculative) sensitivity of the demand for money to changes in interest rates[64]. Because the speculative part of demand for money is considered highly unstable, the total demand is never completely stable in Keynesian terms.

Keynesian theory of demand for money was subject to many modifications over the years. These included the views by W.J. Baumol and J. Tobin, who pointed out the difficulties in empirical determining the distribution of reasons for demand for money[65]. In addition, they recognized the impact of the interest rate on both transactional and precautionary demand. This made it possible to formulate the equation:

$$MT = \sqrt{\frac{bY}{2i}},$$

where:

MT — Transactional demand for money of a given economic entity.

---

[60] See: A. Kaźmierczak, *Polityka pieniężna*..., p. 89.

[61] See: ibid.

[62] See: S. Owsiak, op. cit., p. 95; A. Kaźmierczak, *Polityka pieniężna*..., p. 93.

[63] See: R. Milewski, E. Kwiatkowski, op. cit., p. 351.

[64] See: A. Kaźmierczak, *Polityka pieniężna*..., p. 89.

[65] See: S. Owsiak, op. cit., p. 98.

b — Brokerage fee for the transfer of funds from a savings account

Y — Income in nominal terms

i — Interest rate on deposit.

The following relationships result from the formula :

— Both the increase in income and transaction fees determines the growth of the transactional resource

— Increase in the market interest rate will contribute to reducing the size of this phenomenon[66].

In the presented concept, W.J. Baumol and J. Tobin introduced the assumption about the impact of changes in market interest rates on the transactional demand, arguing that the current revenue can be successfully invested in values which are alternatives to deposits, and then gradually released along the maturity of subsequent commitments. Thus, the continuity of the expenses of the entity will be maintained, and the cost of lost opportunities limited[67].

In contrast, precautionary demand is almost identical with the speculative on by both authors. Taking into account the impact of the interest rate on the entire maintained money resources enabled the consideration of types of demand as a whole. Furthermore, the elimination of speculative reason made the total demand for money stable, which in economic practice has been confirmed by the stability of relationships between the demand for money and the size of the national income[68].

J. Tobin also studied the inclination of entities to diversify assets, which, as he believed, was a natural phenomenon. Therefore, changes in demand for a given type of assets result from changes in the profitability of both the assets in question (proportional relationship) and their substitutes (inverse relationship). This means that the demand for money depends on more than one interest rate. In the portfolio theory, the definition of money substitutes was therefore extended to short-term securities. In this situation, the choice between short-term (liquid) and long-term (illiquid) securities determines the size of speculative demand[69]. In this way, the theory of demand for money has been transformed into a theory of demand for assets.

A monetarist theory, derived from the quantity theory, is important in the context of explaining the demand for money in that it is based on the belief in the dependence of prices on the money supply. Therefore, M. Friedman emphasized that "inflation is a monetary phenomenon caused by greater increase in the quantity of money than production"[70].

According to the assumptions by the monetary school, the factors determining the demand for money are:

---

66 See: *Makroekonomia…*, p. 78.

67 See: A. Kaźmierczak, *Polityka pieniężna…*, p. 95.

68 S. Owsiak, op. cit., p. 98.

69 See: A. Kaźmierczak, *Polityka pieniężna…*, p. 96.

70 M. Friedman, R. Friedman, *Wolny wybór*, Sosnowiec 2006, p. 272.

— Income which is considered permanent (does not fluctuate yearly)
— Price level
— Interest rate[71].

The demand for money increases with the increase in prices and/or the national income, while the demand falls when the interest rate rises. Note that the quantities such as income or interest rate, and consequently the demand for money, are dealt with by monetarists in real terms, in which money allows the purchase of specific goods[72]. The real demand for money is then obtained by referencing the price level ($\frac{M^D}{P}$)[73].

The relationship between the demand for money and the individual variables is expressed in the following equation:

$$M^D = f(W, R^e, P^e \frac{W_h}{W}) P,$$

where:
M^D — The demand for money
W — Wealth
R^e — Expected changes in the level of interest rates
W_h — Wealth in the form of human resources
P — Price level
P^e — Expected changes in the price level.

As follows from the formula, the monetarist concept introduces yet unknown factors determining the demand for money. Considerations herein include wealth, which, as the sum of cash, financial assets, real goods, as well as human capital, sets the upper limit of the demand for money[74]. Another variable exposed by M. Friedman are expectations about yield rates of different forms of assets. The higher the rates, the lower is the demand for money. Note that this approach is in many ways consistent with the views of J. Tobin, especially in terms of choices made by entities between money and the relatively broadly defined assets. Therefore, the demand for money is understood as a demand for assets. The following equation clearly shows the dependence of the demand for money on yield rate of assets:

$$\frac{M^D}{P} = f(R_p \frac{Y}{P}),$$

where:
M^D — Real demand for money
R_p — Yield rate of assets[75]

---

71 S. Owsiak, op. cit., p. 99.
72 R. Milewski, E. Kwiatkowski, op. cit., p. 353.
73 Ibid.
74 S. Owsiak, op. cit., p. 100.
75 Ibid., p. 102.

The demand for money is considered fixed because of the proportional dependence on the national income. Therefore, according to monetarists, this demand can be predicted in advance. M. Friedman also brings attention to the fundamental feature of money, which is its liquidity. In contrast, other types of assets are distinguished by their profitability. Therefore, the reflection of the demand for money will be the structure of assets desirable in the portfolio because of their profitability.

The demand for money was the subject of discussion of many economists over the centuries. It is possible, however, to capture the two trends, which developed in parallel among the many views. These are:

— Monetarist theory of money developed on the basis of the quantity theory

— Verified many times and developed theory of liquidity preference by J.M. Keynes.

However, both concepts cannot be described in isolation due to the interpenetration of some of their elements. The course of development of the theory of money enables to observe the changes taking place in the perception of the reasons for demand for money seen in the economy. On the other hand, the transformation of existing theories relating to the reasons for the demand for money are a kind of binder for successive concepts (Table 1).

Table 2. The reasons for the demand for money

Theory	The reasons for the demand for money
Transactional quantity theory (I. Fisher)	Transactional
Resources quantity theory (Cambridge school)	Transactional, Precautionary
Theory of liquidity preference (J.M. Keynes)	Transactional, Precautionary, Speculative
Postkeynesian monetary theory (J. Tobin)	Transactional, Precautionary, Portfolio

Source: own study based on S. Owsiak, op. cit., pp. 92–106.

Extending the scope of the reasons determining the size of the demand for money resulted in the introduction of further variables (factors) responsible for the shaping the size of the demand. However, the researchers agree that the size of the demand for money depends on the following factors:

— National income

— Interest rate

It follows from both theories that economic entities differentiate the amount of money asset owned, basing their decisions on changes in the market interest rate. It is pointed out, however, that by far the greater importance of the impact of the interest rate on the size of the demand for money was put by J.M. Keynes[76]. In contrast, the monetarists stressed the reaction force of expenditures to changes in

[76] See: *Makroekonomia…*, p. 77.

interest rate. On the other hand, Keynesians acknowledged that the decline in the interest rate is accompanied not by the increase in expenditures, but in savings.

For monetarists, the demand for money proportional to the size of a steady income is a stable value. However, due to the volatility of its speculative part, the demand in Keynesian approach is characterized by instability[77].

The money supply is explained differently. In Keynesian terms, it is not a constant variable, but results from the size of the demand for money. Quantity theories explain the changes in the price level by changes in the money supply. In the model created by J.M. Keynes, such a dependency does not exist. This gives rise to consequences in the recommendations for economic policy. Monetarists suggest a passive monetary policy limited to the control of the money supply. In contrast, Keynesian theory was seen as an excuse for extensive government intervention.

2.3.2. The concept of cryptocurrencies in the light of the Austrian school of economics

Factors determining the demand for money, as seen by the demand theory, are certainly an important theoretical foundation for the analysis of the phenomenon of cryptocurrencies, however, they do not explain all its specific aspects. The concept of virtual currency mainly refers to the views of Austrian school initiated by Carl Menger (1840–1921) and developed by Eugene von Böhma-Bawerk (1851–1914), Ludwig von Mises (1881–1973), Friedrich von Hayek (1899–1992) or today — Murray Rothbard (1926–1995) and Roger Garrison (1944–), Jesús de Soto (1956–)[78].

In broad terms, the representatives of this school assumed that economic processes are characterized by a high degree of uncertainty and constant disturbances in balance. As a result, a free market is the best solution contributing to the development of economic entities. It enables information retrieval, as well as verification and interpretation of decisions taken in the market mainly through the price mechanism. For this to happen, the basic requirement is the freedom of price formation, which in turn depends on free competition. According to the representatives of the Austrian school of economics, state institutions are not able to replace the free market as a mechanism for the optimal allocation of goods, because they have too little information resources, and thus cannot effectively or control, or even intervene in the area of economic phenomena and processes.

The theory of the Austrian school is treated as a heterodox trend in economics, i.e. different in terms of research methods and the object of analysis in relation to the mainstream economy. Heterodox trends do not take into account many or all of the assumptions made within the mainstream. Therefore, in contrast to the

[77] A. Kaźmierczak, *Polityka pieniężna*..., pp. 107–108.

[78] C. Menger, *Principles of Economics*, Auburn, Ala 2007; L. Mises, *Teoria pieniądza i kredytu*, trans. K. Śledziński, Warszawa 2012; F.A. Hayek, *Denationalisation of Money*, London 1976.

orthodox view, these concepts are often characterized by a specific "lack of legitimacy"[79]. However, the global financial crisis increases the current involvement in alternative ideas and concepts, because it revealed shortcomings and inadequacies of economic theory towards reality and requirements of sustainable development and balance in socio-economic systems. All the more heterodox economists analyze economic phenomena in a broad context, reiterating the need for a holistic consideration of economic phenomena, and not putting them in formal models, which have little to do with the actual conditions of economic life, as so often happens in the mainstream. Such an approach is particularly valuable in relation to money[80].

The origin, properties and role of money in the economy are of special interest to the Austrian school.

The main assumption is that money is a commodity, but has some important distinctive features when compared to other goods[81]:

a) The value of money results from the function of a means of exchange, and thus money is a specific commodity, as opposed to others, it can be exchanged into any other commodity in any situation

b) In contrast to all other commodities, the increase of its amount does not directly increase the well-being of society This applies in particular to fiduciary money, which has no other use than the monetary function.

One of the main representatives of the mainstream of the Austrian school of economics — Ludwig von Mises — believed that money is neither an abstract symbol nor standard for values or prices. It is an economic good and as such is subject to valuation and pricing, which is based on its specific virtues, that is, it takes into account the benefits that the holder of cash expects. People hold money only because they expect changes whose nature and scope cannot be accurately predicted. The existence of money is only possible in a changing economy, but it is a part of the further changes[82].

L. von Mises classified money in a broader and narrower sense[83]:

— Money in the broader sense includes money in a narrower sense and its substitutes, meant as a perfectly secure and immediately payable claim to money. Money substitutes include cash equivalents (i.e., money substitutes, which have full coverage, e.g. in gold) and fiduciaries (or substitutes that do not have such a coverage). Fiduciaries can be divided into banknotes and deposits, as well as

[79] H. Landreth, D. Colander, *Historia myśli ekonomicznej*, Warszawa 2005, pp. 344–345.

[80] P. Marszałek, "Pieniądz w teoriach szkoły austriackiej", *Ruch Prawniczy, Ekonomiczny i Socjologiczny* LXXIII, 2011, z. 4, p. 131.

[81] L. von Mises, *The Theory of Money and Credit* („The Foundation for Economic Education"), New York 1971; E. Dolan, *The Foundations of Modern Austrian Economics*, Kansas City 1976, pp. 160–184.

[82] R. Goryszewski, "Wokół poglądów na rolę pieniądza w gospodarce w historii i teorii ekonomii", *Rocznik Naukowy Wydziału Zarządzania w Ciechanowie* 1–4, 2011, No. V, p. 31.

[83] A. Sieroń, "Czym jest Bitcoin", *Ekonomia — Wroclaw Economic Review* 19, 2013, No. 4, pp. 39–40.

perfunctory coins in the extent to which their value as a means of exchange exceeds the value of ore, from which they were made.

— Money in the narrower sense, including commodity money (i.e. money, which is a commodity at the same time) and empty money (*fiat*), which is neither a commodity nor a claim to it.

Regardless of such a classification, L. von Mises also took credit money into consideration in his deliberations — as an interest-free claim, which is not payable on demand because of the suspension of the possibility of buyout[84].

The main achievement of von Mises was the inclusion of the theory of marginal utility, not only in the explanation for the demand and market prices, but also for the origin of the money (i.e. regression theorem). According to von Mises, people derive utility from holding cash and intend to have it in their wallets as long as the marginal utility of cash balances does not equal the usefulness of other assets. Hence, the marginal utility becomes the quantity which explains the demand for money. This however, along with the amount of money determines its value, or purchasing power[85]. The demand for money and usability attributed to monetary units in a given period (t) results from the fact that they attributed such value in the previous period (t–1), in which money also had a certain value. Deducing retrospectively, the value in the period t–1 is a consequence of the value assigned in the period t–2. Carrying on, we can track this chain of links between moments in time up to the moment in which the commodity has become money. This means, however, that it had to have some value in the previously existing barter system (otherwise there would be no value in the first period, in which it began to function as money). For example, precious metals, primarily gold, have been used as money for most of human history. However, gold could become money only for the reason that it had a fixed value earlier (because it was used in jewelry). In consequence, this argument can be concluded that it is impossible to assume that money can arise spontaneously as a result of e.g. government decree or "social contract". If the goods are to be money, they must have had exchange value before. The same applies to modern monetary systems of fiduciary money. All currencies, even those newly created (e.g. in emerging new countries or as the result of them issuing their own money), have value only by reference to the existing monetary system[86].

In this context, the book by Friedrich Hayek[87], in which he advocates the liquidation of the monopoly of states on the issue of money, is an important contribution to the theory of money in relation to the cryptocurrencies. The notion of denationalization of money thus introduced to the language of economics meant the issue of stable currencies by private entities in a competitive environment. Accord-

[84] Ibid.

[85] P. Marszałek, op. cit., p. 134.

[86] B. Cioch, *Austriacka teoria pieniądza*, http://mfiles.pl/pl/index.php/Austriacka_teoria_pieniądza.

[87] F.A. Hayek, *Denationalisation of Money*, London 2007, pp. 23–24.

ing to Hayek, commercial banks as private entities should have the right to issue interest-free certificates, based on their own commercial brands. These certificates would be subject to competition and offered at variable rates. Certificates of stable rates would supplant weaker, less stable certificates from circulation.

This could result in an effective system, in which only stable currencies (certificates — as meant by Hayek) would operate[88]. This view is closely related to the later idea of the creation of cryptocurrencies, which implements the concept of "parallel currencies" by Hayek (1976), which advocated the abolition of the status of "legal tender" enjoyed by state money and the idea that everybody can issue their own currency[89]. Note that the concept of cryptocurrencies goes further than the denationalization of money proposed by the Nobel Prize winner of 1974, because he assumed top-down reform, i.e. the abolition of regulations on the legal means of payment by the government, while in the case cryptocurrencies changes occur entirely bottom-up, and possible repercussions from the state are difficult because of the decentralized issuing of this means of exchange[90].

This trend also includes the deliberations of contemporary followers of the Austrian school of economics. Jesús de Soto has introduced the concept of the so-called. *free banking*, promoting free trade and freedom in financial services. A total freedom of choice of money and its privatization is an end to intervening by the state and the central banks in its issuance and control of value. This concept includes a proposal to replace paper money with gold, introduce a free-banking system and the abolish the central bank. In addition, de Soto proposes the use of one-hundred-percent reserve on demand deposits[91].

In summary, the views of economists of the Austrian school on the theory of money lead to several important conclusions. First of all, it should be noted that the proper functioning of money is of great importance to the entire economy, as well as for the economic success of individual entities. However, there is another side to the coin. With a big importance and role of money there is inherent danger that its erroneous functioning can cause enormous losses and disorganize the economy[92]. In particular, excessive credit expansion caused a partial provision and creation of money in the banking system increases the money supply and artificially lowers interest rates. This is a signal for businesses making decisions that are often inconsistent with the preferences of consumers, which leads to crisis[93]. The representatives of the Austrian school of economics postulated the abandonment of the partial reserve in the banking system and a return to the gold standard, which they saw as a response to the possibility of manipulation of money by monetary

[88] E. Chrabonszczewska, op. cit., p. 52.
[89] F.A. Hayek, op. cit.
[90] A. Sieroń, op. cit., p. 43.
[91] E. Chrabonszczewska, op. cit., p. 52.
[92] P. Marszałek, op. cit.
[93] E. Chrabonszczewska, op. cit., p. 52.

authorities[94]. As a result, the views of the Austrian school of economics on the money meant:

a) Independence from the current decisions of governments and other public authorities based on the tide of the market

b) Reliance of money on the intrinsic value

c) Moving away from the mechanism of money creation in the banking system.

Therefore, in the opinion of representatives of the Austrian school of economics a stable currency, which is independent of government and current interventions, should be the foundation of the economy and consequently lead to easing tidal cycles.

These proposals are reflected in the idea of the cryptocurrency. They can be regarded as a starting point for the liquidation of the monopoly of central banks in terms of issuing money, and the creation of money outside the banking system, based on a partial reserve. The fact that cryptocurrencies, as stipulated by the Austrian school of economics, have no intrinsic value (they exist as a contractual provision on a virtual wallet of the user) may raise some doubts. However, you will notice that by reference to the old gold standard[95], cryptocurrencies include a deflation mechanism embedded in their creation caused by a limited number of units put into circulation, which is intended to increase the value of the cryptocurrency while keeping its rarity within the market mechanism.

2.4. Types and structure of the cryptocurrency market

2.4.1. General information

Cryptocurrencies are still a new phenomenon and basically not described previously in the literature. Available publications tend to focus on technological and cryptographic or legal aspects[96], and they miss a broader analysis of the eco-

[94] Ibid.

[95] However, there are ideas to introduce a cryptocurrency based on gold. In 2015, Anthem Blanchard, president of Anthem Vault company which sells gold, announced the launch of a new cryptocurrency called "Hayek". Its price will be at any time pegged to the current price of one gram of gold. Like other cryptocurrencies, Hayek is meant as an alternative to a payment system based on currencies endorsed by central banks. Anthem Blanchard said that he saw no obstacles to launch similar currencies based on other metals in future. Physical delivery of uranium or plutonium is of course impossible, but ownership of portions of these metals may be subject to exchange, http://rynek-zlota24.pl/zlotometale-szlachetne/0302-cyfrowe-waluty-oparte-o-zloto/ (access: February 2, 2016).

[96] D. Ron, A. Shamir, *Quantitative Analysis of the Full Bitcoin Transaction Graph*, Springer 2013; R. Grinberg, "Bitcoin: An Innovative Alternative Digital Currency", *Hastings Science & Technology Law Journal* 2011, No. 4(1), in: M. Polasik, A. Piotrowska, R. Kotkowski, op. cit., p. 131.

nomic aspects of the cryptocurrency trade and the impact of this phenomenon on the economy. The analysis requires first to characterize individual cryptocurrencies and market environment, which will constitute a starting point for the statistical analysis of data aimed at explaining the market volatility of cryptocurrencies in relation to traditional currencies and financial instruments.

Bitcoin is the first and still the most common cryptocurrency, which has already been in circulation since 2009. On the wave of popularity and largely due to the fact that software of the underlying BTC protocol is made available under free licenses, alternative coins — the so-called *altcoins* — began to emerge very quickly. As the result, currently several hundred different cryptocurrencies are traded in parallel and new ones are created on an ongoing basis. Table 3 shows the basic characteristics of the most famous cryptocurrencies.

The table shows that there are significant differences in the capitalization, market price and the average number of concluded transactions even among the major cryptocurrencies. There are some technical differences between cryptocurrencies, e.g. litecoin differs slightly from bitcoin in the method of encryption, sometimes creation of new units and a projected maximum number of units planned to be put in circulation (84 million compared with 21 million in the case of bitcoin). Nevertheless, the nature and effects of the cryptocurrencies shown below are now very close in economic terms. The basic common features of cryptocurrencies include:

— Cryptocurrencies are fully "virtualized" and, in contrast to traditional currencies, they have no equivalent in the form of banknotes or coins

— Total decentralization of the issuing and putting units in circulation, which is a consequence of the lack of a central server and operation in a P2P network

— Issuance of a cryptocurrency is implemented by users within P2P networks by solving complex mathematical equations

— Independence from governments and financial institutions, which is reflected in the lack of supervision of state bodies over the process of issuance of cryptocurrency and its use in trade

— Workings of cryptocurrency are based on the principles of cryptography and trust — on the cryptographic proof to a large extent

— The lack of intermediaries in the transactions using cryptocurrency

— Workings of cryptocurrency are based on *open source* applications, the purpose of which is to provide transparency of the process of creating a cryptocurrency

— Anonymity, which is related to the fact that opening an account (cryptocurrency wallet) no personal data or identification are required. This means that information on cryptocurrency holders are entirely non-personal

— Transactions are irreversible — the solution to the problem of double spending of available funds.

Of course, in addition to the common characteristics, each cryptocurrency has its specifics, which is reflected in the terms of trading and the extent of use.

Table 3. Main types of cryptocurrencies as of December 31, 2015

	Creation date	Number of units in circulation	Current price (USD)	Capitalization (USD)	Average daily number of transactions
Bitcoin	01/09/2009	15,014,432	422.7	6,346,566,995	168,107
Litecoin	10/08/2011	43,839,673	3.4	150,934,901	4,199
Darkcoin (Dash)	01/19/2014	6,100,519	3.2	19,811,776	1,698
Dogecoin	12/08/2013	102,416,625,952	0.00016	16,205,369	22,426
Peercoin	08/19/2012	22,871,733	0.42	9,588,277	494
Namecoin	04/19/2011	11,795,982	0.43	5,036,101	860
Blackcoin	02/24/2014	75,176,756	0.03	2,239,393	2,026
Novacoin	02/09/2013	1,366,662	0.9	1,225,691	245
Vericoin	05/10/2014	27,396,471	0.028	768,222	2,062
Paycoin	12/12/2014	16,299,471	0.039	639,939	26
Quarkcoin	07/21/2013	249,649,483	0.0027	664,929	449
Worldcoin	05/14/2013	95,326,308	0.006	585,924	480
Megacoin	06/01/2013	31,589,825	0.017	545,949	102
Auroracoin	01/24/2014	12,937,513	0.037	4,731,599	70
Reddcoin	01/26/2014	27,919,912,354	0.000017	470,329	2,619
Vertcoin	01/10/2014	21,472,750	0.021	456,435	712

Source: own study based on data available on the website https://bitinfocharts.com/ (access: January 15, 2016).

Therefore, let us explain in detail the economic essence of five largest cryptocurrencies in terms of capitalization.

2.4.2. Bitcoin

Bitcoin (BTC) was first described in 2008 by a person or a group of persons acting under the pseudonym Satoshi Nakamoto, establishing the system for its creation and workings. As shown in the first chapter, bitcoin is a decentralized system of electronic payments via a *peer-to-peer* network that enables transactions between the parties based on mutual trust.

Bitcoin is the first virtual money, which is totally decentralized. The network is created by the users themselves — neither the bank nor the official payment procedure is present between BTC users[97]. This decentralization is the basis for security and freedom, which, being the sociological idea, was one of the essential

[97] E. Chrabonszczewska, op. cit., p. 55.

building blocks for the cryptocurrency phenomenon attracting people ideologically separate from the mainstream economy and expressing public discontent with the current rules of the economy.

The creation of Bitcoin was a kind of phenomenon in the economic aspect, taking into account the traditional solutions used in the monetary system. There is no issuing bank for bitcoin, and it operates without a top-down government oversight. The supply of the currency is increased by the so-called miners. There is software running on miners' computers seeking solutions to a mathematical function, which is the basis for the algorithm of the bitcoin protocol. After finding the solution, a block is generated, which includes bitcoin transactions from the moment of mining the previous block. The maximum supply of BTC has an upper limit resulting from the algorithm and will not exceed 21 million units. Given the current rate of growth of computing power in the network, it is forecast that this figure will be reached around the year 2110.

Of course, the limited supply of units to be issued into the system will cause a deflationary pressure on bitcoin. Due to the design of the system, no person or organization can increase the number of bitcoins, which will function in the system. The limited supply and the assumed increasing demand shall lead to a systematic increase in the value of bitcoin. To prevent the loss of liquidity, system designers decided that 1 BTC is divided into 100 million smaller units, customarily called *satoshi*[98].

Considering the international and anonymous nature of bitcoin, it is very difficult to estimate the number of people using this cryptocurrency[99]. There is no official data on the global number of users. One can try to define it based on the active bitcoin addresses and statistics published on the websites which aggregate information on the trade in cryptocurrencies. The basic statistics on bitcoin studied over the years are shown in Table 4.

Initially, the interest in Bitcoin was very limited. However, bitcoin was used as a means of exchange in the initial period, although to a large extent to carry out transactions in the grey market, or even in illegal trade. Since February 2011, the Silk Road portal has existed in the Tor network, which was the auction service where one could purchase a wide range of goods and services using bitcoin. Estimated turnover of Silk Road exceeded 9 million bitcoins. However, the main trade was in prohibited goods, especially drugs. For this reason, on December 20, 2013 the portal was closed, and its administrators arrested. In 2012, the popularity of virtual currency began to increase. The dynamic growth of bitcoin was initiated in 2013, when the cumulative number of bitcoin client downloads increased from 1.9 million to over 4.2 million. Growing interest in the cryptocurrency resulted in a significant increase in the value of bitcoin in relation to traditional currencies.

[98] Ł. Dopierała, A. Borodo, op. cit., p. 3.

[99] B. Segendorf, "Have Virtual Currencies Affected the Retail Payments Market?", *Economic Commentaries* 2014, No. 3, from: A. Piotrowska, "Czynniki oceny opłacalności inwestycji w kryptowalutę bitcoin", *Zeszyty Naukowe Uniwersytetu Szczecińskiego 862. Finanse, Rynki Finansowe, Ubezpieczenia* 2015, No. 75, p. 372.

Table 4. Basic data about bitcoin in 2010–2015 (end-of-year)

Specification	2010	2011	2012	2013	2014	2015
Number of units in circulation (in thousands)	5,051.5	8,063.9	10,621.2	12,215.2	13,674.7	15,031.4
Capitalization (in millions USD)	1.5	35.9	142.3	9,031.5	4,241.3	6,490.0
The average number of transactions per day (in thousands).	0.5	4.9	45.3	43.9	89.2	176.9
Active bitcoin addresses (in thousands)	1.1	10.5	43.1	119.1	191.2	329.5
Estimated total bitcoin addresses (in thousands)	24.2	947.3	1,908.7	4,202.5	5,534.7	7,242.3

Source: own study based on https://bitinfocharts.com/ (access: January 15, 2016).

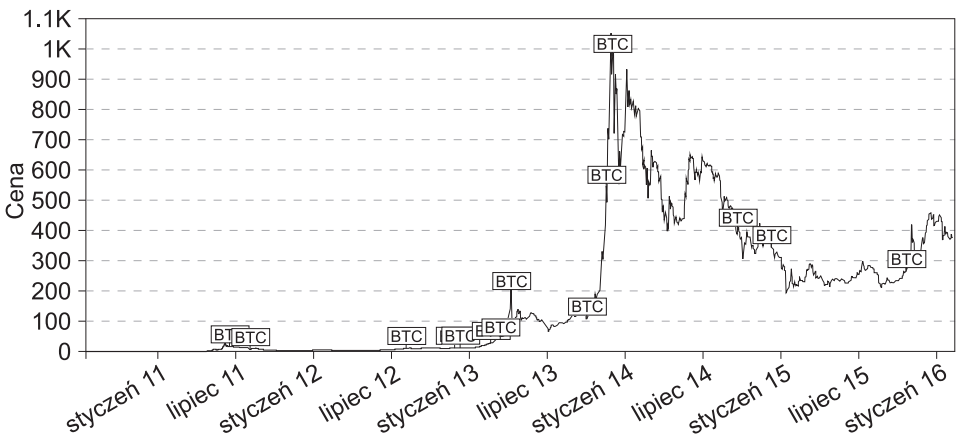

Figure 7. Bitcoin to dollar exchange rate quotations in 2010–2015

Source: data from the bitstamp exchange https://bitinfocharts.com/pl/comparison/price-btc.html (access: January 15, 2016).

In 2013, a growing number of users and the increased interest in Bitcoin generated demand, which contributed to the increase in the price from approx. $15 at the beginning of the year to more than $1,000 at the end of 2013. Historical maximum price of bitcoin in relation to dollar reached the level of 1.1 thousand dollars in December 2013. However, 2014 was critical from the point of view of stability of trading, and especially the beginning of that year, in which panic ensued in the market, which caused a sudden collapse in prices by 60% within three months, at first as the result of the suspension of trading, and then closing the most important bitcoin exchange platform at that time — Mt. Gox. The downward trend observed since that time has very high volatility, which attracts many users with a strong speculative attitude. There are many examples which show the sensitivity of the

price of Bitcoin. One of these situations took place in February 2014, when the value of BTC dropped by 80% as a result of the sell order of 6 thousand bitcoin (which accounted for only 0.05% units being in circulation) worth about $3.8 million at the then exchange rate. The price, which at the time the order was placed stood at $630, fell briefly to $102. Finally, the price returned to baseline levels, but what happened within a few minutes, shows the sensitive nature of BTC[100].

However, this does not prevent steady growth of the number of institutions from different countries accepting the settlements in bitcoin, including such large international corporations as Microsoft, Paypal, Ebay or NewEgg.

The structure of the portfolio value of users having units in bitcoin is an interesting issue from the perspective of stability of bitcoin quotations.

Table 5. Distribution of the number of addresses and values to the condition of the portfolio (as of December 31, 2015)

Condition of the portfolio	Number of addresses	Total value of the portfolios (in BTC)
0–0.001	3,827,552	612
0.001–0.01	1,135,171	4,070
0.01–0.1	1,212,948	37,484
0.1–1	622,708	211,809
1–10	345,953	976,441
10–100	122,698	4,122,374
100–1000	15,364	3,507,744
1000–10.000	1,679	3,361,758
10.000–100.000	106	2,726,771
100.000–1.000.000	2	320,228

Source: own study based on https://bitinfocharts.com/ (access: January 15, 2016).

This distribution indicates a clear disproportion between the users — because of the value of bitcoins they own. More than 50% of addresses have collected value which is almost irrelevant from the point of view of the market and does not exceed a total of 2 thousand dollars. Of particular interest is the fact that for nearly 2% of the addresses account for more than 90% of the value of units in circulation. Given that one user can have more than one address, there is a risk that very narrow group of users has a definite economic advantage over others. This may increase the risk of speculative activities by this group, which inevitably involves concerns about the stability associated with the use of bitcoin and its prevalence in transactions.

[100] http://independenttrader.pl/krach-na-bitcoin-o-80-w-kilka-minut.html (access: January 17, 2016).

2.4.3. Litecoin

Litecoin is a currency based on a system and algorithm which is very similar to bitcoin. There are two key differences between these cryptocurrencies. Litecoin network generates new blocks containing monetary units every 2.5 minutes as opposed to 10 minutes in the network bitcoin. According to its authors, this is to provide faster flow of transactions and even more resistance to double spending, or spending the same "coins" twice (virtual currency can also be falsified by copying files). Due to the lack of central regulatory organization, *peer-to-peer* networks themselves have to verify transactions to avoid this type of fraud. The faster they are able to carry out validations, the greater their efficiency and effectiveness. In addition, the maximum limit of litecoin network supply is 84 million litecoins, which is four times more than for bitcoin. This is to ensure a greater supply and make it easier to popularize the currency.

Table 6. Basic data about litecoin in 2010–2015 (end-of-year)

Specification	2012	2013	2014	2015
Number of units in circulation (in thousands)	12,857	22,270	35,407	43,960
Capitalization (in millions USD)	0.9	527.8	95.6	152.1
The average number of transactions per day (in thousands).	0.6	9.4	2.8	2.9
Active addresses (in thousands)	2.3	30.4	8.9	7.6
Estimated total number of addresses (in thousands)	82.5	399.4	412.5	437.7

Source: own study based on https://bitinfocharts.com/ (access: January 17, 2016).

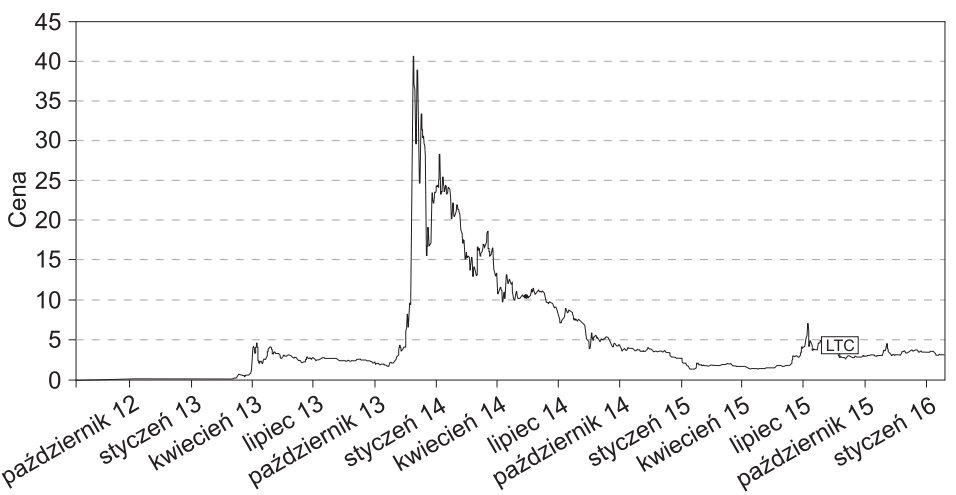

Figure 8. Litecoin to dollar exchange rate quotations in 2010–2015

Source: own study based on https://bitinfocharts.com/ (access: January 17, 2016).

The stages of development of litecoin in terms of these parameters are very similar to the behavior observed in the case of bitcoin. The systematic increase in the number of units put into circulation is associated with high volatility over the years studied.

One can easily see that the quotations chart of litecoin in relation to the dollar is almost a copy of the behavior of bitcoin. The significant increase in 2013, combined with dynamic declines in 2014, resulting from Mt. Gox exchange bankruptcy, as in the case of bitcoin. What is interesting, though, is a distinctive decrease in the number of active user portfolios after the period of litecoin panic as opposed to bitcoin. This does not mean, however, that the speculative demand decreased. During certain days in 2015, the market trading of litecoin was even greater than in the case of bitcoin.

Table 7. Distribution of the number of addresses and values to the condition of the portfolio (as of December 31, 2015)

Condition of the portfolio	Number of addresses	Total value of the portfolios
0–0.001	31,692	6
0.001–0.01	100,808	341
0.01–0.1	108,763	3,399
0.1–1	62,938	24,884
1–10	66,930	229,133
10–100	48,262	1,633,318
100–1000	15,175	4,365,302
1000–10.000	2,703	7,026,920
10.000–100.000	341	8,083,755
100.000–1.000.000	102	12,416,802
1.000.000–10.000.000	4	10,119,696

Source: own study based on https://bitinfocharts.com/ (access: January 17, 2016).

However, the primary objective of putting cryptocurrency in circulation, which was to be the use of litecoin in making payments in the exchange of goods and services, basically disappears with the persistent speculative reason.

The distribution of litecoin value is almost similar to bitcoin. The imbalance in this situation may be even a bit more emphatic, as 4% of addresses own more than 96% of litecoin capitalization. In-depth analysis over the studied years does not indicate the trends that would equalize these relationships, which is a factor increasing the uncertainty with respect to the stabilization of cryptocurrency quotations in the future, and is similar as in the case of bitcoin.

2.4.4. Dogecoin

The popularity of the phenomenon and a flood of various types of altcoins creates situations in which some cryptocurrencies initially come out as a kind

of social joke, but are still functioning today. A good example is dogecoin. It all started with an innocent Internet picture of a Shiba dog with all sorts of humorous texts added. The global popularity of images that were originally to work as the so-called demotivators, well-known on the Web, was picked up by Jackson Palmer, the employee at Adobe. He joked on Twitter that he was going to invest in dogecoin. He received replies inviting him to take this step. Finally, he decided to buy DogeCoin.com domain and launched the project. Billy Markus, who considered creating his own cryptocurrency, stumbled upon the website. The two men agreed and launched dogecoin. The idea appealed to users of the Reddit service, where dogecoin is now very popular as a form of making small payments[101]. The site already includes DogeMarket, where people offer real items in exchange for dogecoin.

Table 8. Basic data about dogecoin in 2010–2015 (end-of-year)

Specification	2013	2014	2015
Number of units in circulation (in millions)	16,429	97,222	102,501
Capitalization (in millions USD)	6.9	17.5	16.7
The average number of transactions per day (in thousands).	110.5	15.5	16.5
Active addresses (in thousands)	35.3	32.3	23.7
Estimated total number of addresses (in thousands)	870.4	1,428.4	1,621.7

Source: own study based on https://bitinfocharts.com/ (access: January 17, 2016).

Data shown in the table indicate that a joke not only caught on, but it turned into quite a sizable cryptocurrency. The capitalization amounting to several million dollars and a significant share of a transactional reason when using dogecoin to make small payments has consolidated the position of the cryptocurrency among many other altcoins. Its little weakness is a very low exchange rate in relation to the dollar ($0.00016/dogecoin at the end of 2015), which somewhat hinders calculations and doing commercial transactions. However, some see this as a potential advantage because this unit can be used to handle micropayments on the Web (and in fact now it mainly carries out this function).

A relatively large number of addresses, i.e. almost 300 thousand (18%) owning microscopic amounts of dogecoins is a kind of specificity of this cryptocurrency. This does not change anything in the imbalance recorded in the previously described cryptocurrencies, because about 2% of addresses control over 95% of the value of traded units.

[101] http://www.businessinsider.com/what-is-dogecoin-2013-12?op=1 (access: January 17, 2016).

Table 9. Distribution of the number of addresses and values to the condition of the portfolio (as of December 31, 2015)

Condition of the portfolio	Number of addresses	Total value of the portfolios
0–0.001	290,803	1.7
0.001–0.01	3,354	16.1
0.01–0.1	19,844	617.2
0.1–1	24,228	9,395
1–10	632,520	1,341,539
10–100	194,729	6,488,672
100–1000	180,294	64,742,040
1000–10.000	146,675	489,080,814
10.000–100.000	86,431	2,858,799,466
100.000–1.000.000	34,337	10,273,277,531
1.000.000–10.000.000	7,452	19,364,317,990
10.000.000–100.000.000	889	22,686,983,234
100.000.000–1.000.000.000	99	2,101,786,665
1.000.000.000–10.000.000.000	3	7,885,577,293
10.000.000.000–100.000.000.000	1	17,850,000,469

Source: own study based on https://bitinfocharts.com/ (access: January 17, 2016).

2.4.5. Dashcoin

Dashcoin was originally founded on January 18, 2014 as darkcoin. However, on March 25, 2015 the name of the cryptocurrency was changed by the authors to dashcoin which means digital cash. The current dash is a currency based on *open source* solutions and built on bitcoin software. In technological terms, the difference in the case of dashcoin is a two-layer network, which significantly increases the anonymity of the transactions and leaves very little information. In contrast to the bitcoin, which publishes and archives all transactions in a blockchain, dashcoin enables to preserve anonymity due to the lack of transaction history and preventing the validation of the portfolio status publicly.

Similar to bitcoin, this protocol is designed to create a maximum of 22 million coins with a decrease in the number of coins mined by 7% annually.

Comparing to the previously described cryptocurrencies, dashcoin is the youngest altcoin, created just after the high volatility caused by panic after the collapse of Mt. Gox exchange. It does not change the fact, however, that the main reason for use is speculative demand also in this case, which is reflected in a growing capitalization while decreasing the average number of transactions using the cryptocurrency.

Table 10. Basic data about dashcoin in 2010–2015 (end-of-year)

Specification	2014	2015
Number of units in circulation (in millions)	4.9	6.2
Capitalization (in millions USD)	9.6	20.5
The average number of transactions per day (in thousands).	4.7	1.3
Active addresses (in thousands)	3.2	5.8
Estimated total number of addresses (in thousands)	98.3	117.5

Source: own study based on https://bitinfocharts.com/ (access: January 17, 2016).

2.4.6. Peercoin

In fact, most virtual currencies basically reproduce the idea of bitcoin and its key features. However, one can see a number of important differences in the case of peercoin. It is cryptocurrency, which was launched on August 19, 2012. Its creators introduced it some interesting innovations — both technological and those having economic effects. First of all, a system is used in the case of peercoin that combines *proof-of-stake* and *proof-of-work* solutions discussed in the first part. Similar to other cryptocurrencies, coins can be mined, but the main part of the network is maintained by the holders of the currency, which derive additional benefits — same as miners in the case of bitcoin. However, the target number of coins for peercoin has not been determined and currently is not a closed range.

Table 11. Basic data about peercoin in 2013–2015 (end-of-year)

Specification	2013	2014	2015
Number of units in circulation (in millions)	20.5	21.2	22.9
Capitalization (in millions USD)	145.9	12.6	10.2
The average number of transactions per day (in thousands).	1.8	0.5	0.4
Active addresses (in thousands)	1.7	0.8	1.5
Estimated total number of addresses (in thousands)	30.3	32.3	36.0

Source: own study based on https://bitinfocharts.com/ (access: January 17, 2016).

As proved in the foregoing statistics, although peercoin is still among the largest cryptocurrencies in terms of capitalization, its significance becomes smaller and smaller. After a dynamic growth and spectacular collapse, as in the case of other cryptocurrencies over the years 2013–2014, the number of transactions has significantly reduced and the capitalization is steadily decreasing. Similarly to the other cryptocurrencies, a clear disparity in the distribution of portfolios is observed. Over 50% currently created units are accumulated to 28 addresses.

2.4.7. Features of the cryptocurrency market

Primary and secondary putting cryptocurrency in circulation is an important issue. Contractual primary market refers to issuing cryptocurrencies, which is inextricably linked to the need to "mine" units using appropriate software. However, most current users of cryptocurrencies acquire their units in the secondary market, i.e. through purchase on the cryptocurrency exchange, at the exchange office, in the virtual stores, or directly from the person who owns them.

The organization of the secondary market, in which it is possible to buy and sell cryptocurrency, is a very interesting issue. First of all, it should be emphasized that a fundamental feature of cryptocurrency, which is the lack of material form and the lack of legal grounds, has significant economic and legal consequences. Transactions between traditional and virtual money have no uniform legal regulation, and the control of money is in the hands of issuers and depends on supply and demand and many existing exchange platforms[102].

Just like in the classic perspective relating to the use of traditional means of payment, the notion of "exchange office" and "cryptocurrency exchange" is very often mistaken in the everyday perception. The main difference between these is that the price is known at the exchange office before the transaction (there is a price list, the transaction occurs at that price), and the cryptocurrency exchange one places an order with a fixed price (the price is determined by the user, the transaction occurs when another exchange user agrees to this price).

Exchange offices specialized in trading cryptocurrencies are in fact entities operating exclusively in the Internet and using an extensive website. Usually, little is known about their organizational structure and ownership. Often, the only information publicly available about them is the place of registration of their business. Lack of explicit information on the operation of exchange offices on one hand fits the idea of anonymity of cryptocurrency very well, on the other hand, it increases the risk of breach of trust in connection with the use of the services provided by such entities.

The technical side of exchange of cryptocurrencies at exchange offices requires setting up a user account at the office. The transaction itself comes down to a fairly simple operation of exchange of owned units for traditional currency (the current structure of trade is dominated by the exchange of dollar and yuan, and, to a lesser extent, euro and other currencies). Following the exchange, cryptocurrency is posted on the purchaser's account, while e.g. dollars or yuans are posted on the seller's account. Exchange offices usually charge a commission on the transaction, which is their primary source of income from its operations. The commission usually differs according to the average monthly turnover for a given user account.

[102] E. Chrabonszczewska, op. cit., p. 55.

The exchange office does not take over the control over the funds, the user can withdraw them from their account at any time, which of course applies to both cryptocurrencies and traditional currencies. Of course, exchanging at the exchange office is not the only possible form of purchase of cryptocurrencies for traditional means. Less formal transactions are also used to this end, such as exchange between users: through direct relationships established on the Web (e.g. discussion forums) or indirectly, using trusted *escrow* mechanisms (hedging transactions between the seller and the buyer with the use of third parties) . Also, the network of ATMs is expanding (though now chiefly limited to major cryptocurrencies, mainly bitcoin).

Table 12. Example table of commissions at cryptocurrency exchange offices

Monthly turnover in BTC	Commission [%]
<20	0.35
<50	0.30
<100	0.25
<200	0.20
>200	0.15

Source: based on commissions charged by Gatecoin exchange office, https://gatecoin.com/public/feeschedule (access: January 30, 2016).

Another issue is transactions using cryptocurrencies via the exchanges functioning of the Internet. Of course, cryptocurrency exchanges have nothing to do with stock exchanges, which we know from the traditional economics. Actually, they are specialized exchange platforms established by private entities to enable the purchase and sale of cryptocurrencies. Just as in the case of exchange offices, the ownership of exchanges is veiled in mystery, to put it mildly.

Transactions at cryptocurrency exchanges include two basic ways of buying of units:

— Direct purchase from the exchange, without the involvement of third parties in the transaction. Traditional currency is transferred from the buyer's bank account and exchanged for cryptocurrency according to the current market pricing directly from the owners of the exchange. Of course, this form of transaction makes cryptocurrency exchanges similar in the principles of operation to exchange offices (many platforms operate in both forms).

— The use of the exchange as an intermediary platform enabling buyers and sellers to meet and implementing exchange transactions between them.

For a long period, namely from 2010 to the turn of years 2013/2014, the most popular place for bitcoin trading between investors was Mt. Gox trading platform. Then, after the bankruptcy of its operator, Bitstamp has become the main trading platform for a few months. Recently, Asian markets, specifically China begin to

dominate in cryptocurrency exchanges, e.g. BTC China and BTC-e. Increasingly popular are also Polish cryptocurrency exchanges, such as Bitcurex, Bitmarket.pl, and Bitbay.

In summary, cryptocurrency market can be divided into two major segments:

— Investment, in which users acquire a given cryptocurrency for speculative purposes in order to obtain benefits from its exchange rate, usually in relation to traditional currencies[103].

— Transactions, where users can use cryptocurrencies in trade transactions, purchasing and selling goods and services.

Despite the growing popularity of cryptocurrencies, their main feature — a means for trade — is minimally used. What discourages both merchants and retailers, are considerable price fluctuations and uncertainty as to keeping the value, even in weekly periods. They are inherently unstable; payment systems operating in the virtual world are exposed to noise, and uncertainty about the legal status of cryptocurrencies may give rise to unforeseen consequences.

2.5. The analysis of market volatility of cryptocurrencies in relation to traditional currencies and selected financial instruments

As mentioned in previous subsections, high volatility in trading of cryptocurrencies in relation to traditional currencies calls for an in-depth analysis. A comparison of variability in relation to both currencies, and the most common financial instruments may be of particular interest in the assessment of the scale of this phenomenon. The dynamic increase in the number of cryptocurrencies in circulation does not change the fact that reference to the most prevalent currency — bitcoin — is the most conclusive from the point of view of the economic analysis of the use of cryptocurrencies.

BTC convertibility is not limited, which means that there is freedom of making international payments. The study compares the exchange rates of BTC in relation to other currencies such as USD, EUR, and PLN. The results were confronted with other traditional financial instruments such as S&P index, EUR/USD, and gold (XAU/USD) or oil quotations (CL.F/USD). The study has taken into account the maximum time series taking into account the rate quotations for BTC from 2010 until the end of 2015.

[103] With the growing popularity of cryptocurrencies, financial market institutions are beginning to increasingly take into account the possibility of speculative investment in this form. For example, more and more FOREX platforms add cryptocurrency contracts to their range, allowing to do transactions on currency pairs such as the BTC/LTC, BTC/USD, etc.

The analysis clearly shows significantly greater volatility of BTC compared to other financial instruments. This is evidenced not only by the spread between the minimum and maximum daily or monthly rate of return, but above all the higher standard deviation, indicating a higher investment risk of BTC. It should be emphasized that there are no clearly formulated principles when it comes to determining the rules and regulations of BTC exchange rates. The rate is set on market-driven exchange platforms without the interference of any supervisory authority.

Table 13. Statistical analysis of daily BTC exchange rate quotations in relation to traditional currencies and selected financial instruments

08/01/2015–09/30/2015									
	BTC/ USD	BTC/ EUR	BTC/ PLN	EUR/ USD	EUR/ PLN	USD/ PLN/	WIG	S&P 500	XAU/ USD
Mean	0.62%	0.63%	0.63%	0.01%	0.00%	0.02%	0.01%	0.04%	0.00%
Deviation	7.00%	7.04%	7.08%	0.60%	0.49%	0.86%	1.02%	0.97%	1.08%
Min.	-44.33%	-43.61%	-42.22%	-2.54%	-3.11%	-4.55%	-6.24%	-6.90%	-9.24%
Max.	54.04%	53.55%	53.55%	2.16%	2.06%	3.86%	4.10%	4.63%	3.97%
Spread	98.36%	97.55%	95.77%	4.69%	5.17%	8.41%	10.35%	11.53%	13.21%

Source: own work.

Table 14. The matrix of correlation of daily returns in the years 2010–2015

Correlation	BTC USD	BTC EUR	EUR USD	S&P Index	XAU/USD	CI.F/USD
BTC USD	1					
BTC EUR	0.996	1				
EUR USD	0.069	0.000	1			
S&P Index	0.071	0.046	0.411	1		
XAU/USD	0.023	0.002	0.246	0.044	1	
CI.F/USD	0.056	0.035	0.316	0.411	0.241	1

Source: own work.

There is also no mechanism to limit the exchange rate risk and prevent currency speculation. In comparison with large shallowness of the market resulting from relatively low volume as compared to other instruments, this leads to high volatility. High volatility of cryptocurrency exchange rates may be a factor limiting the confidence in use of this means of payment, especially in the medium and long term.

Increased volatility of BTC implies the need to check the relationships between the rates of return obtained by the financial instruments studied. The analysis was carried out with the use of daily changes as well.

The results show very low dependencies between quotations of bitcoin and changes in rates of return of other financial instruments (or rather the lack of them).

On the other hand, the correlation between the currency pairs taking BTC into account is very high. The same phenomenon applies to other cryptocurrencies not shown in this subsection whose correlation with the BTC exchange rate is very high. This shows that cryptocurrencies are not currently regarded by the market as independent financial instruments, but a common basket of interrelated currencies. Therefore, these observations reinforce the conviction that despite the fact that cryptocurrencies were created with the intention of implementing payment functions, the current reality shows that they are considered mainly as investment assets. This may be the subject of separate studies, especially given that the specificity of the bitcoin cryptocurrency narrows the types of tools used and limits the amount of analyzed data, and hence reduces the effectiveness of individual methods of analysis of investment profitability.

2.6. Cryptocurrencies and a pyramid scheme

One of the most intriguing subjects related to the creation and workings of cryptocurrencies is a possible similarity of the mechanism of development of cryptocurrencies to the phenomenon of a pyramid scheme. Full virtualization of the cryptocurrency, anonymity of authors, high volatility in relation to traditional currencies, as well as repercussions of controversy associated with market abuses constitute a serious ground for reflection on this subject. Quite often these fears are raised by popular economic thinkers such as Nouriel Roubini, who used harsh words when referring to the most popular currency, which is bitcoin: "Bitcoin isn't a currency. It is by the way a Ponzi game and a conduit for criminal/illegal activities. And it isn't safe given hacking of it"[104]. Naturally, many of these statements are subjective in nature, unsupported by solid arguments. However, from an economic point of view, some doubts in this respect remain, and it certainly worth taking a look on them in this section.

The so-called network effect is one of the basic characteristics of the cryptocurrency market. This effect increases the economic utility for both groups of participants with connecting new entities to the platform[105]. This puts the first holders of units of a given cryptocurrency in a privileged position in relation to other users. The more that creating cryptocurrencies is profitable for their makers due to the fact that they arise *ex nihilo*[106]. The increase in the number of users

[104] *Bitcoin to piramida finansowa* (2014), www.pb.pl/3592126,35620,bitcoin-to-piramida-finansowa (access: 03/28/2014).

[105] G. Gowrisankaran, J. Stavins, "Network Externalities and Technology Adoption: Lessons from Electronic Payments", *RAND Journal of Economics* 2004, No. 35(2), from: M. Polasik, A. Piotrowska, R. Kotkowski, op. cit., p. 131.

[106] A. Sieroń, op. cit., p. 37.

translates into greater popularity of a cryptocurrency, which in turn increases the potential, market value, and, above all, the opportunity to exchange their units to the traditional currency and real goods or services. Rapid increase in the number of new cryptocurrencies (altcoins), whose development and market behavior are surprisingly similar, particularly raises concerns about whether cryptocurrencies are or become pyramid schemes. In the initial phase, a new cryptocurrency is met with great interest, craftily fueled by promotion, followed by quite a dynamic increase in the number of users and values in relation to traditional currencies. Often, the collapse of the market comes soon, resulting from the sale of a large number of units of a given cryptocurrency, which brings quotations in relation to traditional currencies to zero. In such a situation, there is suspicion that the originator of the cryptocurrency, who by definition has an advantage over the rest because of the capability of mining units at minimum cost in the initial phase, is responsible for the promotion, speculative growth, and subsequent breakdown. Of course, anonymity o cryptocurrencies does not allow to confirm or refute this suspicion (it is not known who personally buys or sells a particular cryptocurrency), however, these behaviors should be traced from the perspective of the similarities to the phenomenon of a pyramid scheme.

Theoretically, a pyramid scheme comes down to the structure, in which the profit of a person depends on the contributions of those who are below. Therefore, a pyramid scheme operations consist in promising profits to participants, and above all recruiting new people to participate in the structure — rather than the provision of real investment services[107]. In classical view, the principle of the pyramid scheme is very simple — profits for the initial participants are paid from contributions made by the next users. The pyramid scheme usually lasts as long as new cash inflows exceed the sum of outflows, which takes place until the loss of confidence by users[108]. Mainly people on top of the pyramid, or those who joined early, derive profits from it. In contrast, the likelihood of gaining benefits by other users is negligible, and in any case depends directly on the decisions made by the operators at the top of the pyramid.

The pyramid in the financial market is a special type of a pyramid. In this structure, people are attracted by the prospect of profit that successful investment transactions, mostly in financial instruments or real estate, are to generate. In fact, profits demonstrated by the organizer of the pyramid are "paper" — shown only on statements submitted to customers (customers' funds are not invested or are invested inefficiently and result in loss), and the source of these "paper" profits — which can actually be paid at the initial stage of operation of the pyramid — are payments from other customers[109]. The reason for the payout of profits at the

[107] M. Pachucki, "Piramidy i inne oszustwa na rynku finansowym", [in:] *Komisja Nadzoru Finansowego*, Warszawa 2013, p. 5.

[108] P. Masiukiewicz, *Piramidy finansowe, teoria, regulacje, praktyka*, Warszawa 2015.

[109] M. Pachucki, op. cit., p. 7.

initial stage of the pyramid is obviously maintaining the operations of the pyramid for a certain period in order to attract more new customers and actually gather the largest financial pool possible from current and future participants unaware of the real nature of the project. The profits for customers, which the organizers of the pyramids on the financial market promise, do not depend on the number of new clients "attracted" by existing participants. Admittedly, the organizers of the pyramids can encourage their customers with additional financial bonuses for registering new participants, but most often they seek to attract customers (directly or through the employees). The operations of the pyramid on the financial markets results in much greater damage incurred by its unaware participants than in the case of a classical pyramid, i.e. the one in which it is known from the very beginning that any profits are derived from deposits obtained from new clients. This is due to the fact that the value of funds entrusted per customer in a pyramid on the financial market is much larger than in the classical pyramids. What's more, customers attracted by the profits indicated in statements transaction receipts pay further funds[110].

In light of the presented essence of the pyramid schemes, some differences, but also similarities between them and cryptocurrencies can be noted.

Table 15. Differences and similarities between cryptocurrency system and a pyramid scheme

Similarities	Differences
— The so-called network effect, whose economic utility for both groups of participants increases with connecting new entities to the platform. — The advantage for participants (the originators of the cryptocurrency) who joined at the beginning over the rest of users, resulting from obtaining a significant number of units of a given cryptocurrency cheap and easily. — Recruiting new users by bonuses in the form of new units mined in exchange for providing computing power. — Users transmit officially accepted, traditional currencies they own to the system through the exchange offices or cryptocurrency exchanges in exchange for virtual units having no intrinsic value, thereby supplying the whole system.	— Cryptocurrencies are based on a distributed network, noone has complete control over them or interferes directly in the mechanism of their creation. — Cryptocurrency holders cannot be directly deprived of their property, they are secured in the wallets of individual users. — The benefits are not directly dependent on attracting new users. — No administrative fees are charged for the operation of the cryptocurrency system, which is often the case in a pyramid scheme as the actual profits for its creators.

Source: own work.

Therefore, it is hard to regard the mechanism of creation and operations of cryptocurrencies itself as a financial pyramid in the strict sense. Note that cryptocurrencies are neither a security nor any other document embodying property rights. In addition, there is no promise of high profits from the possession or use

[110] Ibid.

of cryptocurrency, which is an inherent feature of any pyramid scheme[111]. However, the characteristics of cryptocurrencies make them a pyramid scheme with entirely new features and course. The main argument for this is a significant imbalance in terms of the distribution of values of its units in each of the described cryptocurrency (see Tables 2, 4, 6, 8). A small number of users, around 2% in the case of bitcoin, effectively controls more than 90% of the total market. This may therefore directly result in a situation where a small group of users benefits at the expense of the vast majority. In addition, the reasons of this small group of users who currently hold a major value of cryptocurrencies are the risk factor associated with cryptocurrencies, which is difficult or even impossible to estimate. Estimating this risk is virtually impossible, if only because of the main feature of the cryptocurrency system, which is anonymity. In fact, it is totally unknown at this point what people or organized entities have dominant shares in each cryptocurrency. The results of studies carried out on the basis of bitcoin, indicating that more than half of bitcoins are only accumulated on the accounts and not used today for the purpose of trading, are interesting in this context[112]. The specifics of the development of cryptocurrencies suggest that these are individuals who were active users already in the initial period of the cryptocurrency. However, it is now impossible to personalize these people, and thus to determine their intentions and purposes.

The lack of common and explicit knowledge of the subject generates a strong information asymmetry when it comes to forecasting the volatility of cryptocurrencies in relation to traditional currencies and financial instruments. One decision of a user holding 30% of the market share, for example, to exchange the cryptocurrency for the US dollar, can also cause a total collapse of the market. This brings us to the specific socio-economic paradox. On one hand, the prevalence of cryptocurrencies and their capabilities as alternative money depends on the growth of confidence. On the other hand — that increase of confidence and the resulting wider use of cryptocurrencies in payment transactions will bring the greatest benefit to the primary holders of a given cryptocurrency, who have the largest market share. This fact will become a temptation for them to use this to cash in the value of their assets by exchanging for the traditional currency, which could cause the collapse of the market of this cryptocurrency. Therefore, we arrive at a vicious circle, in which a possible increase in the use of the cryptocurrency can be the biggest risk factor for its further development. The occurrence of these two contradictory factors raises serious concerns whether cryptocurrencies can become a stable means of payment which is alternative to traditional currencies.

---

[111] A. Sieroń, op. cit., p. 37.

[112] D. Ron, A. Shamir, "Quantitative Analysis of the Full Bitcoin Transaction Graph", [in:] *Financial Cryptography and Data Security — 17th International Conference, FC 2013, Okinawa, Japan, April 1–5 2013* (Lecture Notes in Computer Science 7859), Springer 2013; R. Grinberg, op. cit., from: M. Polasik, A. Piotrowska, R. Kotkowski, op. cit., p. 131.

2.7. The development of cryptocurrencies and the implications for the economy and financial system

2.7.1. Prospects for the development of cryptocurrencies in the context of acting as money

Referring to the considerations in Section 2.2, the essence of money is determined by its functions. Naturally, the recognition of a given means as money is a very conventional thing and differs significantly depending on whether we adopt the economic or legal point of view. In economic terms, the perception of this issue is quite broad and flexible, and what really decides here is a widespread acceptability, which suggests that all means of payment which fulfill the function of money must be regarded as money by definition[113]. This assumption implies the need to consider the essence of cryptocurrencies with respect to their current and potential capability to act as a measure of value, means of exchange, means of payment or means of hoarding.

With regard to the previous considerations, the function of a measure of value is identified as the capability to determine the value of the goods in cash in the form of a price. In this sense cryptocurrencies in their general establishment clearly meet this function; after all, it is possible to use them to express, and thus compare, the value of goods and commodities operating in trade. However, one can consider whether it is a quasi-measure of value. The current cryptocurrency values are shaped not by their purchasing power, as in the case of traditional currencies, but largely by the rate of exchange for traditional currencies. Certainly, it is now hard to recognize cryptocurrencies as a common measure of value in the sense of the capability of determining the value of all goods and services traded on the market. For most goods, cryptocurrencies carry out this function indirectly at most, exactly through traditional currencies, due to the limited capabilities for exchange. For example, the price of a barrel of oil at $50 a piece can be expressed as 0.17 BTC (the contractually agreed conversion rate of $300/BTC), however, the value of the goods is determined by the conversion rate only. The possibility of direct determination of the price expressed in cryptocurrency is very limited if not impossible (transactions in this commodity are not currently accounted for in this way, but of course can potentially be in the future). As a result, although cryptocurrencies generally carry out the function of a measure of value, its implementation, at least for now, is similar to the various types of assets traded in the secondary market

[113] P. Schaal, op. cit., p. 23.

(such as financial instruments in the stock exchange) rather than money in the traditional meaning in economy[114].

Money playing the role of a means of exchange is very closely associated with the function of a measure of value. This property is related to the general equivalence of cash in the transactions of buying and selling goods and services. Money in this function becomes an intermediary in the exchange, which historically enabled to depart from a barter by the contractual "detachment" of purchase transactions from sale transactions. Thus the exchange of goods for money creates the opportunity for the seller to purchase goods or services which meet the specific needs without having to make a direct exchange. Cryptocurrencies also have this property, and it is one of these functions that they perhaps meet the most. However, one shall emphasize that currently this function is not universal because of the lack of common acceptance of cryptocurrencies in transactions. However, with the possible prevalence, the potential use of cryptocurrencies for exchange is not particularly debatable.

The existence of money as a means of payment is the development of the function as a means of exchange, which is reflected in the capability to settle all financial liabilities, in particular, taxes, wages, and borrowing and repayments of loans[115]. Cryptocurrencies in this case can hardly be regarded as a measure implementing this function. In the current unregulated legal conditions and the absence of a parallel acceptance from national monetary authorities of the use of cryptocurrencies, the capability to settle liabilities such as taxes, is automatically excluded. One can seriously doubt whether cryptocurrencies have the potential to carry out this function in the long term because of their features. After all, an independence from the current decisions of governments and other public authorities is one of the inherent features of cryptocurrencies. This causes a natural contradiction, which limits the capabilities of the traditional financial system based on cryptocurrencies, in particular, in the basic link which is the tax system. Basically, prevalence of cryptocurrencies in the role of money would require a complete reorientation of economic relations, in particular with regard to the current role of the state and organization of the public finance system[116].

An interesting question is the capability of cryptocurrencies to carry out the functions of a means of hoarding. On one hand, immaterial form of cryptocurrencies and the resulting lack of intrinsic value inherently limits the tendency to hold the purchasing power in this form. The more that the lack of supervision and state guarantees inevitably increases uncertainty as to the security of the accumulated savings. On the other hand, note that the essence of creating a cryptocurrency includes an inherent hoarding element with the main aspect being the algorithm

[114] M. Franków, T. Kopyściański, "Analiza perspektyw rozwoju bitcoina w kontekście możliwości pełnienia funkcji pieniądza", *WSB University Research Journal* 16, No. 2, Wrocław 2016, p. 161.

[115] See: *Makroekonomia…*, p. 76.

[116] M. Franków, T. Kopyściański, op. cit., pp. 156–158.

limiting the number of generated units (fixed at 21 million in the case of bitcoin). The limited supply, strengthening its rarity, following the market mechanism can foster the appreciation of a cryptocurrency in the long run. Therefore, this may increase the propensity of keeping the cryptocurrency to store value. However, the lack of other use than in clearing and payments (as opposed to, e.g. gold or other commodities[117]) may the weakness of cryptocurrencies with regard to the hoarding function. In addition, a determinant in the tendency to accumulate savings in this form is undoubtedly the stability of the purchasing power of money, and this, as already shown, is now quite uncertain.

It should be emphasized that the separation of semantic content of each function of money is extremely conventional[118]. Means playing the role of money fulfill these roles simultaneously, and having one function determines the fulfillment of another. For example, doing transactions (money as a medium of exchange) would be virtually impossible in isolation from the function of the measure of value which identifies the quantity of goods that can be purchased for a monetary unit, which also is a necessary condition for transaction settlement[119]. For money to be a means of hoarding, it is necessary to have a purchasing power, inherent in the capability of exchange of currency for certain goods or services, which can meet the future needs of people accumulating savings in the form of cash. Mutual relationships between the functions, complementary in this case, are an important element in the discussion on the possibility of cryptocurrency playing the role of money. Undoubtedly, modern forms of money, both cash and non-cash, have such a property. Whereas, in the case of cryptocurrencies, one can indeed notice the presence of these functions with varying intensity, but it is difficult, at least in the current state of their use in the economy, to conclude that they carry out all of these functions to the same extent and are complementary in the fulfillment of these functions. In addition, there are serious doubts about to what extent, if at all, cryptocurrencies can carry out some functions, primary as a means of payment. The result is that cryptocurrencies are now closer to a financial instrument than money in economic terms. However, the acceptability and social trust will still determine the prospects for the development of cryptocurrencies and any possibility of their use as a universal currency.

[117] In the case of gold, even if hypothetically it is no longer considered precious, it will still be used in jewelry, although decorations made of it would no longer be considered prestigious (see: R. Faszyński, *Jeśli bitcoin jest pieniądzem, to transferowym*, http:// www.obserwatorfinansowy.pl/tematyka/rynki-finansowe/jesli-bitcoin-jest-pieniadzem-to-transferowym/). (access: January 19, 2016).

[118] See: S. Owsiak, op. cit., p. 108.

[119] M. Franków, T. Kopyściański, op. cit., p. 162.

2.7.2. The use of cryptocurrencies and the benefits and risks for individual users

Summing up the role and significance of cryptocurrencies in the economic aspect, we should take a particular look at the undoubted benefits, but also risk factors involved in the spread of use of cryptocurrencies by individual users now and in the future.

Undoubtedly, cryptocurrencies have many essential features, the use of which in transactions or even the wider use as an alternative to traditional money may be attractive from the point of view of their holders. The most important include:

a) The speed of transactions
b) Reducing the cost of transactions
c) Solution to the problem of *double spending*
d) Anonymity
e) Diversification
f) Capability to generate new units.

The speed of transactions is an undoubted advantage of cryptocurrencies. Even the electronic interbank clearing system cannot provide such fast circulation of funds. Bank transfers within the current clearing system depend on the times of incoming and outgoing session at the bank. Time differences in the fulfillment of transactions and non-cash transfers in the banking system are even greater in the case of international transfers. Meanwhile, in the case of cryptocurrency transactions, the execution time it is incomparably faster and, most importantly, takes place regardless of the geographical scope of the transaction. In this perspective, cryptocurrency can be safely regarded as a global means of payment, as the operations and transfers are executed immediately, if they do not require confirmation by a blockchain (in case there is the need to confirm, the time extends depending on the type of cryptocurrency from a few to a dozen or so minutes, and so it is a much better result than in the case of interbank transfers).

The use of cryptocurrencies may constitute innovation which contributes not only to increasing the speed of transactions, but also to reduce the cost of their conclusion, both from the perspective of the individual user as well as the functioning of the entire settlement system. Transaction fees are inherent to the settlements made within the banking system. Meanwhile, in the case of transactions using cryptocurrencies, fees are minimal, and in many cases non-existent.

An important aspect of the use of cryptocurrencies, which is positive from the perspective of the individual user, is the solution to the double spending problem, or double issue of the same funds. Double spending occurs when a dishonest person tries to spend the same monetary units in two different places. Double spending is the classic problem when using non-cash money, especially electronic one, manifesting itself in scams and fraud related to payments, which often take place e.g. in the case of ordinary credit cards. With regard to cryptocurrencies, the problem

is limited due to the fact that once the units are sent, they are lost, and the sender cannot retrieve them without the consent of the recipient.

One of the most original features regarding the trading in cryptocurrencies is anonymity, which enables to keep the privacy of transactions. In a globalized world, surrounded by the network of exchange of information and recording of all sorts of activities by banks or companies for the purpose of sales and marketing, almost every transaction is monitored so as to keep track of the personal data of the person who does it. Yet cryptocurrencies do not require entering any private information. For this reason they are sometimes called confidential currencies, because noone knows who owns the portfolio of cryptocurrencies from which the payment is made.

In the case of cryptocurrencies, the feature which strongly excites the imagination is the capability to individually create new units and put them in circulation. In the case of traditional money emitted by the state or created in the banking system, the individual user does not have the slightest possibility of creating their own funds, and thus participate in a seigniorage, which is the traditional monopoly of the state. Participation in the cryptocurrency system and the activity in "mining" of new units provides the opportunity to raise funds as if *ex nihilo*, by having a computer with sufficient computing power. Of course, in practice, this possibility is often hypothetical with the development of cryptocurrencies, because the more difficult it is to mine new units in the mature phases of the cryptocurrency, the costs of such activities appear to outweigh the benefits of the newly acquired units.

However, the benefits associated with the use of cryptocurrencies are at the same time related to multiple risk factors. These include:

a) Irreversibility of transactions
b) Responsibility of the user for the security of collected funds
c) The risk of losing control over the funds owned
d) The risk of abuse of trust by the entities engaged in trading of cryptocurrencies
e) Market volatility of cryptocurrencies
f) The dependence of using cryptocurrencies on computer and Internet access.

The risks associated with the use of cryptocurrencies in transactions include the irreversibility as a kind of a side effect of the immanent feature of cryptocurrencies, which is the inability to withdraw the concluded transaction. Such a situation can be described as very positive for the payment recipient, but risky for the payer. This results in a significantly greater risk of breach of trust compared to traditional means of payment. For every mistake when transferring the cryptocurrency units to the wrong address or, worse, loss of control over the wallet means in practice the irreversible loss of transferred or accumulated funds.

Unlike traditional money, the full responsibility for the security of the funds in a cryptocurrency rests basically on their owner. Security of collected funds depends on many factors, including the type of a wallet, the way to store private

keys, the frequency of creation and backup retention policies, and general level of knowledge on the principles of cryptocurrencies. Each of these factors depends only on the individual behavior of each user, and failure to observe them could result in loss of stored funds. Therefore, in contrast to the funds deposited in the banking system, the user has no institutional, formal or even technological support providing the security of transactions.

The risk of losing control over the funds owned is related to the loss of the private key. Of course, in the traditional means of payment, in particular the use of online bank accounts, this risk also exists. However, it is much larger in case of cryptocurrencies, and certainly has greater impact. The loss of passwords to the bank account does not result in the loss of ownership to the funds in the account because the data can be reproduced, while in the case of cryptocurrencies, the loss of individual data providing access to the wallet and the capability of doing transactions results in an irreversible loss of accumulated funds.

Breach of security, not only individual, but also global, especially in the context of secondary trading in cryptocurrencies, is also an important threat. Exchange offices and cryptocurrency exchanges are still entities with very unclear organizational and ownership structure and with unregulated, or at least non-standard principles of conducting business. These factors inevitably erode the confidence in the use cryptocurrencies and these concerns are systematically fueled by loud scandals related to their use. The suspension of trading and bankruptcy of Mt. Gox is the most famous example of abuse in an immature market of cryptocurrencies. however, much more minor situations of this type are reported almost every month. An example is cryptodouble.com, a platform operating like an ordinary pyramid scheme, which promised contributors that it will double the transferred funds after every one hundred hours of the investment. Of course, payments were made for some time using contributions from subsequent users, but at some point the platform was closed without a refund to the payers' account. With the previously described irreversibility and anonymity of transactions, there is basically no possibility of recovery for the victims.

One of the principal risk factors associated with the use of cryptocurrencies from the perspective of an individual user is their instability, translating into the risk of losing purchasing power. As shown in previous sections, the cryptocurrency market still has very little stability, and each currency is exposed to large price fluctuations. This is due to the fact that speculative reason is still one of the main factors increasing interest in cryptocurrencies. Of course, this may change in the future if bitcoin and other currencies will be increasingly used in trade settlements between businesses and customers. For now, however, the speculative reason for the use cryptocurrencies supersedes the transactional reason, and the consequence is that with turbulence in the cryptocurrency market some companies announce that they accept payments in cryptocurrencies, while others withdraw from the market.

The use of cryptocurrencies is inextricably associated with the subjection of the capability of doing transactions on the computer and access to the Internet. In contrast to the traditional means of payment, cryptocurrencies are entirely dependent on the computer, they do not exist in reality. There is no alternative, such as cash, which would allow transactions during system failure, which can always happen. In the case of cryptocurrencies, even a simple power cut, failure of the local Internet or computer failure can result in a complete cutting off the user from the possibility of buying anything.

2.7.3. The stability of the economy and the financial system and the functioning and development of cryptocurrencies

The use and possible prevalence of cryptocurrencies can not only give rise to significant effects from the perspective of individual users, but also have a greater impact on the conditions of the economy, both in real and financial aspect. Therefore, it is worthwhile to trace the possible implications from the perspective of key aspects, in particular the impact on the banking system, the functioning of public finances and macroeconomic effects.

Referring to subjects presented in previous chapters, it is worth recalling that the development of cryptocurrencies is stimulated by uncertainty, lack of confidence or sometimes even ideological aversion of users towards the traditional banking system. It is no wonder that financial institutions, in particular those representing the banking sector, expressed at least extreme caution, and often outright objections referred to the functioning of cryptocurrencies. Cryptocurrencies are seen from the banks' perspective primarily as a competition for the traditional creation of non-cash money in the banking system. Using cryptocurrency wallets is a natural alternative to the use of bank accounts and other products, such as credit cards. Cryptocurrencies can therefore be seen as a natural substitute for bank offers relating primarily to making payments. Consequently, the relations between cryptocurrency and traditional banking is now reduced to entrenching on two opposite sides. But still, technological solutions applied in cryptocurrencies create the potential for their use and eventual adaptation by banks to create new products which are more efficient from the perspective of a customer.

The use of cryptocurrencies is also often discussed in relation to the impact on public finances. Two main threats emerge in this regard:

a) Risk associated with money laundering; the speed of transactions, facilitating circulation of funds between many unidentified entities and their ultimate exchange for the traditional currency through cryptocurrency exchanges is a potentially convenient source of putting large sums derived from illegal sources into legal business trade or even financing illegal activities.

b) The growth of tax grey market; the use of cryptocurrencies can significantly expand the scale of the phenomenon, creating the possibility of conducting unregistered business, in which payments are settled in cryptocurrencies; anonymity of transactions makes it difficult to control this type of phenomena.

In either case, as the result of these threats, users avoid complying with their tax obligations, thereby impairing the level of income generated within the public finance sector. The anonymity of users, limiting the capabilities of effective control by tax authorities is a main factor that causes these threats. The possible prevalence of cryptocurrencies in their current form and theoretically replacing the traditional currencies with them would have to involve an outright revolutionary change of the system of public finances.

Analyzing this in somewhat futuristic terms, different from the current reality, it is worthwhile to note that it is not entirely impossible to link a particular person to a particular account . All transactions are recorded in the network, and at the time of making a standard exchange transaction (e.g. exchanging funds for a traditional currency and transferring them to a private bank account of the user), there is the possibility of "recourse" of personal details of entities involved in the transactions. There are even specialized companies which track transactions[120]. In any case, this indicates a quite interesting potential prospect in which the model of cryptocurrencies with immanent explicit registration of transactions while finding solutions to identify users, could provide an ideal mechanism for conducting tax inspections and detection of fraud. Although the collapse of anonymity is significantly at odds with the idea of cryptocurrencies, actions are already taken to introduce this type of a hybrid. An example is the initiative of the People's Bank of China (PBOC), which considers the introduction of their own cryptocurrency aimed to increase the transparency of economic activities and to curb money laundering and tax evasion[121].

A separate, though equally debatable issue is the potential impact of cryptocurrencies on the economy in a macroeconomic perspective.

The following problems emerge in this regard:

a) Deflationary nature of cryptocurrencies

b) the capability to use commercial transactions in the conditions of economic growth, the risk of excessive fragmentation of payment units.

Limited supply of units that can be introduced into circulation is an essential feature of the vast majority cryptocurrencies, including first and foremost the most important ones, such as bitcoin or litecoin. This automatically brings a lot of controversial issues in economic terms. On one hand, the limited supply and lack of capability to print more coins than the maximum number is undoubted-

[120] M. Muszyński, http://biznes.pl/magazyny/finanse/bitcoin-niewykorzystana-polska-specjalnosc/s92gwp (access: January 12, 2016).

[121] http://comparic.pl/chinski-bank-ludowy-chce-wprowadzic-wlasna-kryptowalute/ (access: January 20, 2016).

ly a factor in stabilizing the macroeconomic situation by reducing the risk of inflation phenomena, on the other — this results in that cryptocurrencies in the long run can cause a permanent deflation, which, with the possible prevalence of cryptocurrencies in circulation could permanently inhibit economic development, as pointed out by proponents of theories derived from mainstream economics. This is because if the size of the issue is limited at the very beginning, it means that there will be relatively less cryptocurrencies in relation to the growing mass of goods and services on the market in future. They will become too rare, which can enhance the hoarding function, but with the simultaneous loss of liquidity. In any case, this is strongly related to economic uncertainties, in that to what extent the fixed number of units assumed in cryptocurrencies would be able to sustain the function of a medium of exchange. Assuming hypothetically widespread use of cryptocurrencies and driving out of traditional currencies, there is a risk that, in the absence of monetary emission proportional to the economic growth, deep recession would occur, leading to a strong drop in demand.

A factor that could also pose a potential threat with the assumed — purely visionary — driving out the traditional currencies from circulation by cryptocurrencies, there is the risk of excessive dispersal of existing units in circulation. A huge number of already existing altcoins with the simultaneous unlimited opportunities of their further creation could cause chaos hampering both the conduct of monetary policy (if it is possible at all in the case of cryptocurrencies, given a fixed number of units and the lack of state supervision) and settlements in business transactions between companies. In addition, creating cryptocurrencies outside the formal financial system deprives the monetary authorities of this part of the seigniorage, which becomes the property of issue groups or individuals. Monetary authorities also lose control over the amount of money in circulation and cannot increase or reduce its supply[122].

Of course, it should be emphasized that many of these threats are purely potential. Currently the cryptocurrencies, with their small prevalence on a global scale, have a marginal impact on the economy and its individual segments, the more so that they do not currently exist on many levels. For example, the cryptocurrency system, by excluding intermediaries, limits the development of institutions whose functioning is useful for the economy, like banks and other financial institutions enabling the transfer of capital. In addition, the gradual increase in popularity of cryptocurrencies for payments (which is, of course, not comparable with the speculative reason for the use of the currency) factors such as the use of cryptocurrencies by companies for e.g. payment of wages do not appear yet so fundamental to the prevalence of the currency.

Lack of confidence in central banks and governments controlling the conditions in the financial markets has become a source of bottom-up initiatives, as

[122] E. Chrabonszczewska, op. cit., p. 60.

evidenced by the establishment of cryptocurrencies. Their prevalence would result in a completely new approach to the concept of money and its existing functions, particularly related to the official circulation. The conclusion from the study is that cryptocurrencies, with a specific example being the most widespread bitcoin, are not a way to avoid various risks related to trading in cash. Volatility of the exchange rate and the risk associated with the legal use of the new currency are difficult to avoid. At the same time, we should take into account the fact that the innovative character of creating cryptocurrencies, and the idea of separation of control over their trade from the state, is gaining ground, which has to be considered not only as a social phenomenon, but also as a process which, together with its prevalence, may cause significant economic effects.

Cryptocurrencies as electronic means of payment without the issuer, 2016

Chapter 3

Legal aspects of cryptocurrencies

3.1. Legal nature of cryptocurrencies

3.1.1. The concept of electronic means of payment without the issuer

The concept of electronic means of payment without the issuer has no legal definition. Three essential elements analyzed in close relation to each other determine the nature of the legal means of payment:

— The concept of means of payment
— Electronic form
— Lack of an issuer.

We must first divide them into legal tender and other means of payment. Legal tender is always clearly indicated by the legislator, so that there is no doubt as to whether a given means of payment is or is not a legal tender. Banknotes and coins issued by the central bank of the country concerned are legal tender all over the world.

Legal tender are distinguished in that they have the power to write off the commitments given to it by a given state. Creditor under the public authority of a country may not refuse to accept a legal tender from the debtor, and the debt of the debtor expires with its acceptance (or the creditor's claim ceases). This universal power of writing off commitments is indisputable for cash (banknotes and coins), while theoretically in doubt if the payment using a bank account (and now also a payment one in the European Union). In practice, the validity of the transfer made by the debtor to fulfill his or her obligations is widely accepted.

There no legal definition of means of payment in the Polish law, but one can identify areas of legislation where the concept of means of payment is used by the legislator. This includes regulations on central banking, foreign exchange and criminal law[123].

[123] More about the concept of means of payment in Polish law, see: W. Srokosz, "Prawo a rozwój elektronicznych środków płatniczych w XXI wieku", [in:] *XXV lat przeobrażeń w prawie*

Cryptocurrencies as electronic means of payment without the issuer, 2016

In turn, according The European System of Accounts, also known as ESA 2010[124], the concept of means of payment includes monetary gold, special drawing rights, currency and transferable deposits. However, this is not in legal, but in accounting terms. More legal approach is included in the PSD Directive[125], which, however, does not use the term "means of payment", but the term "funds" and according to Art. 4 Section 15 "funds" mean banknotes and coins, scriptural money and electronic money as defined in Article 1 par. 3 b) of the Directive 2000/46/EC. This definition was literally (only the Directive 2000/46/EC changed to the current Directive 2009/110/EC) repeated in Art. 4 Section 25 PSD 2[126], which repeals PSD Directive with effect from January 13, 2018.

Due to the lack of the definition of a legal tender, we cannot provide a full objective catalog of the means of payment. Each such a catalog will be more or less subjective. Based on the law, doctrine and case law, we can indicate at most some kind of an unambiguous catalog of means of payment, as well as generally state that the means of payment function as payment — are used to make payments for purchased goods and services[127]. The means of payment undoubtedly include:

— Cash money (banknotes and coins), which is legal tender (e.g. Euro, US Dollar, Polish Zloty)

— Non-cash money (scripture in the meaning of Art. 4 Section 15 of PSD Directive and Art. 4 Section 24 of PSD 2), expressed in monetary units of legal means of payment (e.g. Euro, US Dollar, Polish Zloty)

— Electronic money (which meets the definition in Art. 2, Section 2 of Directive 2009/110/EC[128])

— Cheque, promissory note

— Gold, silver.

---

finansowym i prawie podatkowym: ocena dokonań i wnioski na przyszłość, ed. Z. Ofiarski, Szczecin 2014, pp. 841–849.

[124] Regulation (EU) No 549/2013 of the European Parliament and of the Council of May 21, 2013 on the European system of national and regional accounts in the European Union (OJ. EU L 174 of 06/26/2013).

[125] Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC (OJ. EU L 319 of 12/05/2007, as amended; hereinafter: PSD).

[126] Directive 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market amending Directives 2002/65/EC, 2009/110/EC, 2013/36/EU and Regulation (EU) No. 1093/2010 and repealing Directive 2007/64/EC (OJ. EU L of 12/23/2015; hereinafter: PSD 2).

[127] See also: W. Srokosz, op. cit., p. 842.

[128] Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC EU L 267 of 10/10/2009 as amended).

Moreover, the law indicates that securities and other documents serving as a means of payment issued in certain currencies are also means of payment in addition to these currencies (i.e. legal tender)[129].

In principle, one cannot regard payment instruments within the meaning of PSD and PSD 2 as means of payment (in Polish law — as set forth in Art. 2 Section 10 of the Law on Payment Services[130], hereinafter: LPS). However, this trend is dominant in the case law of the Polish criminal courts and in the doctrine of Polish criminal law, in which the concept of a payment instrument also includes credit cards[131]. Furthermore, the doctrine of criminal law stipulates that the concept of means of payment consequently includes the instrument of electronic money[132]. Such an approach should be limited to the area of criminal law only, and it should be regarded only as a temporary solution there. Payment instrument as set forth in PSD and PSD 2 is a device or a set of procedures, and therefore only allows the access and disposition of the means of payment — in practice, often in cash, scriptural money and possibly electronic money.

Until the days of the IT revolution that occurred in the late twentieth century, the means of payment have taken a material form — of a banknote, coin or paper document, such as a promissory note or a cheque. From a legal perspective, means of payment moved to electronic form in two ways. The first is the replacement of a paper document, which was the carrier of certain rights, with an electronic document by using the electronic signature and the related legal regulation (e.g. The Act on trust services and electronic identification in Poland[133], and the Regulation of the European Parliament and of the Council (EU) No 910/2014 at the level of the European Union[134]). It is a path taken by electronic promissory note or electronic cheque. However, this way of transition to the electronic form has not been accepted generally in relation to stocks and bonds, which by definition

[129] See the Polish Act of July 27, 2002 — Foreign Exchange Law (Journal of Laws of 2012 item. 826 as amended) for the definition of national and foreign currencies.

[130] The law of August 19, 2011 On payment services (Journal of Laws of 2014, item 873 as amended).

[131] See e.g. the judgement of the Court of Appeal in Gdansk of June 19, 2013. (II AKa 473/12), published in LEX No. 1353695; the judgement of the Court of Appeal in Warsaw on December 11, 2012 (II AKa 293/12), published in LEX No. 1246938; the judgement of the Court of Appeal in Wrocław on November 29, 2010 (II AKa 325/10), published in LEX No. 677942; J. Skorupka, "The concept of means of payment w art. 310 k.k.", *Prokuratura i Prawo* 2002, No. 11, p. 43.

[132] J. Skorupka, "Jeszcze o pojęciu pieniądza w przestępstwie z art. 310 k.k.", *Prokuratura i Prawo* 2009, No. 2, p. 5.

[133] The Act on trust services and electronic identification of September 5, 2016 (Journal of Laws of 2016, item 1579).

[134] Regulation of the European Parliament and of the Council (EU) No 910/2014 of July 23, 2014 on electronic identification and trust services in relation to electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ. UE L 257 of 08/28/2014 as amended). With effect from July 1, 2016 the Regulation repealed Directive 1999/93/EC on a Community framework for electronic signatures.

do not perform the payment function — only exceptionally. In the case of stock and bonds, the electronic signature has been superseded by the simpler and more practical solution, which is the dematerialization of securities.

The second way of transition of means of payment to electronic form is the adoption of an electronic form without the use of electronic documents signed with electronic signatures, which takes place primarily in the case of electronic money. The EU legal regulation of e-money is so extensive that the use of the regulations on electronic signatures is not necessary for the effective use of electronic money. But it is not ruled out due to the high technological neutrality of legislation on electronic money.

Money which is legal tender must have the issuer by its nature. The power of legal tender comes from the issuer, which is a sovereign state, acting usually through the central bank. The issuer exists also in the case of means of payment, which take the form of securities, which is also their inherent feature.

Interestingly, the first means of payment used by a man — copper, gold, silver — had no issuer. They occur naturally in nature. Electronic means of payment without the issuer are their equivalents, except that they exist in cyberspace, do not have the material substrate — the environment created by modern computers connected to the Internet is enough for their existence. Gold, silver and other ores themselves do not become the means of trade. It is man who extracts them from earth and puts in circulation by paying for goods and services. Similarly, human action is required in the case of electronic means of payment without the issuer to prepare specialized software and then use it to create units of the electronic means of payment without the issuer. In this sense, a man "mines" such means of payment, for example cryptocurrencies like bitcoin or litecoin. A person who has a computer connected to the Internet with an installed special software (a client in the case of the so-called cryptocurrency) can "extract" or "mine" cryptocurrency. As already described in detail in the first chapter, the cryptocurrency unit is created by software running on computers that communicate with each other using the Internet. It is difficult, in a legal sense, to call a person, who possesses one of these computers and "mines" cryptocurrency using this computer, its issuer. The technological solution, which is the basis for the cryptocurrency system, primarily P2P technology, results in the inability to identify a legal or a natural person, or even a person without legal personality — who has the status of the issuer of a single unit of cryptocurrency. This is a typical feature of any electronic means of payment without the issuer. This feature must have an impact on the legal nature of such means. Lack of issuer means there is no person responsible for the market value of the means of payment. The central bank is responsible in the case of a legal tender. In the case of electronic money, the issuer is obliged to redeem the electronic money they issued for such a nominal amount of legal tender, for which electronic money has been issued[135]. However, for

[135] See e.g. Art. 11 Par. 2 of the Directive 2009/110/EC.

electronic means of payment without the issuer, primarily cryptocurrencies, there is no entity responsible for caring for the exchange rate of these means in relation to legal tender, and above all there is no person liable for their redemption.

Electronic means of payment without the issuer, just as all means of payment which are not legal tender, have the power to write off the commitments only if the parties agree so in the binding agreement. Therefore, it is not a feature which distinguishes them from other means of payment which are not legal tender. There is similar situation with the electronic form. However, as already mentioned, the combination of the three characteristics, i.e. electronic form, the lack of the issuer and functional capability of payment, makes it a completely new quality.

In practice, currently there is only one technological solution that can qualify as an electronic means of payment without the issuer, and these are called cryptocurrencies.

3.1.2. Legal essence of cryptocurrencies

The idea of cryptocurrencies refers to the idea of money as large stones (called Rai) lying on the paradise island of Yap. The natives made individual characters on these stones (i.e., signed them), thereby marking "their" stones. Payments were made by blurring the signature of one native and placing another signature there[136].

A transaction using cryptocurrency is similar, except that users use the same signatures, and they are electronic signatures (private and public).

This creates a "chain of electronic signatures", which is the equivalent of signatures on a stone. However, as described in the first chapter, the cryptocurrency system contains the modified idea of the system of Rai stones resulting from of encryption solutions aimed at counteracting the multiple use of the same unit of cryptocurrency (bitcoin unit in the bitcoin system). Thus, a specific register of completed transactions is the essence of the cryptocurrency system. Therefore, there is nothing in the cryptocurrency system (e.g. bitcoin) that corresponds to the money mark, which is a feature of cash[137]. There is only a record of the operations. Only information (links) on where in individual blocks a confirmation of the transaction is stored in "wallets" of system users. From a legal point of view, cryptocurrency is close to all kinds of registers, including — using a remote analogy and a strong simplification — payment accounts.

In the case of so-called mining of cryptocurrency (e.g. bitcoins), system assigns a certain amount of cryptocurrency (bitcoins) to users according to certain rules — but this is just a "declaration of the system" written in the chain of

[136] Due to the small number of islanders, sometimes they even gave up signing of stones, because all residents knew who owned the stone.

[137] In contrast, in the case of regulated e-money one can trace the equivalent of a money mark — an electronic money mark — see more in: W. Srokosz, "Istota prawna pieniądza elektronicznego", *Prawo Bankowe* 2002, No. 12, p. 71.

digital signatures. A simplification — the system states that the person signing with a specific signature has a certain amount of private cryptocurrency (e.g. bitcoins). Further so-called transactions are only changes in this chain. Nothing is "transferred" from the so-called wallet of one "holder" of bitcoin (and any other cryptocurrency) to the so-called wallet of the next "holder" — only links (indicators of locations in blocks) change. It is therefore difficult to talk about a "money mark" even digital or electronic, and what is more — there is no medium of value, because the bitcoin unit is only a record in the registry, which is *blockchain*. A bit confusing from this point of view is the use of the term "electronic coin" by Satoshi Nakamoto, although he also links this "electronic coin" closely with a blockchain perceived as a chain of electronic signatures[138].

Thus, bitcoins (and any other cryptocurrency, for example. litecoins or dogecoins), in the meaning of units (e.g. 1 BTC), and not as a system, are only records in the registry, which is a *blockchain*.

These records represent a subjective value. For convenience, one can apply the concept of a monetary unit, understood as an abstract measure of value and used by the doctrine[139] in relation to legal tender, to such records. At the same time, the fact that the regulation of public law and criminal law does not prohibit the use of cryptocurrencies, opens the opportunity to use them based on the principle of freedom of contract. For example, as has already been stated in the literature[140], cryptocurrencies can be seen on the ground of Art. 358^1 § 2 of Polish Civil Code[141] (hereinafter: CC) in Poland as the "measure of value other than money", if the parties stipulated in the agreement that the amount of benefit will be determined according to the measure of value, which is a given cryptocurrency. A similar opportunity exists in the legal systems of other countries[142]. This approach corresponds with the perception of cryptocurrency as an abstract measure of value, or a monetary unit.

---

[138] Satoshi Nakamoto states: "we define an electronic coin as a chain of digital signatures", see: S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, https://bitcoin.org/bitcoin.pdf (access: October 6, 2016).

[139] See: T. Dybowski, A. Pyrzyńska, *System prawa prywatnego*, vol. 5, ed. E. Łętowska, Warszawa 2013, Nb 86 ff. However, the monetary unit of a cryptocurrency is not prescriptive, unless it is accepted that the parties of the contract give it such a nature.

[140] K. Zacharzewski, "Bitcoin jako przedmiot stosunków prawa prywatnego", *Monitor Prawniczy*" 2014, No. 21, p. 1132.

[141] The Civil Code of April 23, 1964 (Journal of Laws of 2014, item 121 as amended).

[142] See e.g. the judgement of the civil court in the Netherlands (Rechtbank Overijssel) of May 14, 2014 (C/08/140456/HA ZA 13-255), http://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBOVE:2014:2667 (access: October 6, 2016), in which the Court stated that bitcoin can be considered as a medium of exchange, and therefore it is acceptable as a form of payment in the Netherlands. Discussion of this judgement, see: W. Zeldin, *Netherlands: Local Court Ruling on Bitcoin Transaction*, 4 czerwca 2014, http://www.loc.gov/law/foreign-news/article/netherlands-local-court-ruling-on-bitcoin-transaction/ (access: October 6, 2016).

While agreeing with the view expressed in the literature[143] that "bitcoin is undoubtedly the property right" and that "it is a type of property (Art. 44 CC)" in the light of Polish law — cryptocurrency (including bitcoin) is also seen this way in other countries[144], we should note how it is represented as a property right — it is a record in the registry, which is *blockchain*.

Recognition of a cryptocurrency as the property right opens up the opportunity to apply a number of institutions of civil law to cryptocurrency (e.g. cryptocurrency can be included in the estate and be subject to inheritance)[145].

It is because of the abstract measure of value, or monetary unit, among others (and perhaps above all) that in the opinion of society, and contrary to legal regulations, the cryptocurrency (e.g. 1 BTC) is considered a kind of currency. Such a monetary unit is the common element with a legal tender (e.g. 1 PLN, 1 USD), centralized virtual currencies (e.g. 1 Linden), local money [146] (e.g. Brixton pound[147], Bristol pound[148]), and the regulated electronic money (or electronic money within the meaning of the Directive of the European Parliament and Council 2009/110/EC). Cryptocurrencies undoubtedly are private money and they belong to the broad category of social money (community currency) along with local money and centralized virtual currencies[149].

Cryptocurrency should not be considered a kind of virtual currency, because there are too many differences between them. In particular, in contrast to the virtual currency, cryptocurrency has no issuer. In practice, however, very often the concept of virtual currency includes cryptocurrency. This is how European Banking Authority (EBA)[150], The European Central Bank[151], The Financial Action Task

[143] K. Zacharzewski, "Bitcoin jako przedmiot stosunków…", p. 1132.

[144] See section 3.1.3., in particular the footnote 158.

[145] See more: K. Zacharzewski, "Praktyczne znaczenie bitcoina w wybranych obszarach prawa prywatnego", *Monitor Prawniczy* 2015, No. 5, pp. 186 ff.

[146] Currently, the term "local money" or "local currency" is used in many cases to denote money in functional economic terms, having four functions: measure of value, means of circulation, means of accumulation, and the means of payment, however, not having the generally accepted character of legal tender. In addition, importantly, the use of such money is geographically limited to a relatively small area, and its use is expected to bring all sorts of benefits to local community living in that area within the extended ideology. More about local money, see: W. Srokosz, "Pieniądz lokalny", [in:] *Finanse samorządowe po 25 latach samorządności. Diagnoza i perspektywy*, ed. W. Miemiec, Warszawa 2015, pp. 496–505.

[147] http://brixtonpound.org (access: October 6, 2016).

[148] http://bristolpound.org/ (access: October 6, 2016).

[149] Some authors suggest the use of a collective term „*complementary currencies* — CCs" for such currencies — such as in J. Blanc, M. Fare, "Understanding the Role of Governments and Administrations in the Implementation of Community and Complementary Currencies", *Annals of Public and Cooperative Economics* 84, 2013, No. 1, p. 64.

[150] See e.g. the document from the European Central Bank titled *Virtual Currency Schemes*, October 2012.

[151] See the warning issued by the EBA on December 12, 2013 entitled. *Warning to Consumers on Virtual Currencies* and the opinion of EBA of July 4, 2014 (EBA/Op/2014/08) titled *EBA Opinion on "Virtual Currencies"*.

Force (FATF)[152] or Bank for International Settlements (BIS)[153] use of the concept of virtual currency. Putting such considerations. Bitcoin and linden dollars or e-gold on the same level can lead to far-reaching simplifications, even if they are divided into centralized and decentralized virtual currencies (the division proposed by EBA, FATF, and BIS).

Although as yet there is no legal definition of a cryptocurrency in any country in the world (i.e. there is no state that has defined cryptocurrencies in their generally applicable law), a legal definition of virtual currency, including cryptocurrency, appeared in the middle of 2015. This definition is contained in a separate legal regulation announced by the state of New York on June 24, 2015 concerning economic activity in the area of virtual currencies, including mainly cryptocurrencies[154]. This definition clearly states that virtual currency (including cryptocurrency) is a "digital unit", which can be used as a medium of exchange, or as a form of digitally stored value. Legal definition of virtual currencies, with its scope extended to cryptocurrencies, is also included in the draft directive amending Directive 2015/849[155].

3.1.3. Cryptocurrencies as financial instruments

The concept of financial instruments is legally regulated and as a rule, their legal definition exists in the relevant legal regulations of each country, usually referring to the appropriate catalogs where financial instruments are enumerated. EU law includes this directory in Section C of Annex I to Directive 2004/39/EC of the European Parliament and of the Council of April 21, 2004 on markets in financial instruments[156]. This Directive will be repealed effective from January 3, 2017 by the Directive of the European Parliament and of the Council 2014/65/EU of May 15, 2014 on markets in financial instruments and amending Directive

[152] See FATF report titled *Virtual Currencies: Key Definitions and Potential AML/CFT Risks* from June 2014, p. 4, http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf (access: October 6, 2016).

[153] See BIS report titled *Non-Banks in Retail Payments*, wrzesień 2014, p. 16, http://www.bis.org/cpmi/publ/d118.pdf (access: October 6, 2016).

[154] N.Y. COMP. CODES R. & REGS. tit. 23, § 200 (2015), zob. http://www.dfs.ny.gov/legal/regulations/bitlicense_reg_framework.htm; http://www.dfs.ny.gov/legal/regulations/adoptions/dfsp200t.pdf (access: October 6, 2016).

[155] The application of July 5, 2016 — Directive of the European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for money laundering or terrorist financing and amending Directive 2009/101/EC, COM/2016/0450 final — 2016/0208 (COD).

[156] Directive 2004/39/EC of the European Parliament and of the Council of 21 April 2004 on markets in financial instruments amending Council Directives 85/611/EEC and 93/6/EEC and Directive 2000/12/EC of the European Parliament and of the Council and repealing Council Directive 93/22/EEC (OJ. UE L 145 of 04/30/2004 as amended).

2002/92/EC and Directive 2011/61/EU[157]. The catalog of financial instruments in the new Directive 2014/65/EU is also included in Section C of Annex I of the Directive and has changed rather little in relation to the directory contained in Directive 2004/39/EC. The definition of financial instruments in both Directives is equal — the concept of financial instruments should be understood as "instruments specified in Section C of Annex I […] (Art. 4 Section 17 of Directive 2004/39/EC and Art. 4 Section 15 of Directive 2014/65/UE)".

Cryptocurrencies cannot be classified as financial instruments from the legal point of view, because, as already demonstrated in this paper, they neither have an issuer nor are created by virtue of a contract. Financial instruments either have the issuer (e.g. shares), or a created by virtue of a contract (e.g. derivatives).

The subject of eligibility of bitcoin as a financial instrument in US law has been already discussed in American doctrine in 2011 with negative results. First of all, it was found that bitcoin is not a bill of exchange or promissory note, a share, or in broader meaning — a security (stock), or an investment contract[158].

As it has already been brought up, due to the fact that cryptocurrencies do not have the issuer, they may not be securities (transferable securities are financial instruments according to point 1 of Section C). It is therefore difficult to agree with the position of the German financial supervisory authority BaFin, which qualifies bitcoin as a financial instrument in the form of settlement units in accordance with Section 1 (11) sentence 1 of German Banking Law (Kreditwesengesetz — KWG)[159]. At the same time, BaFin says that these units are similar to foreign currencies and do not constitute a legal means of payment, which in the light of previous findings made in the present study seems to be the right approach. However, undoubtedly valuable observation made by the BaFin was to recognize bitcoins as settlement units — this approach is close to the assumption proposed in this chapter that the concept of a monetary unit can be applied to bitcoins.

Stating that cryptocurrencies can not be legally considered financial instruments, does not exclude the possibility of using them to construct financial instruments, e.g. cryptocurrencies may be the primary instrument for derivatives (derivative contracts). Derivatives based on cryptocurrencies are covered by US supervision performed by Commodity Futures Trading Commission (CFTC), in accordance with the provisions of the Commodity Exchange Act (CEA). For the

[157] (OJ. EU L 173 of 06/12/2014.

[158] R. Grinberg, op. cit., pp. 194–199 and references cited therein.

[159] J. Münzer, *Bitcoins: Supervisory Assessment and Risks to Users*, February 17, 2014, http://www. bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2014/fa_bj_1401_bitcoins_en.html (access: October 6, 2016). According to section 1 (11), point 1 of KGW "Financial instruments within the meaning of subsections (1) to (3) and (17) as well as within the meaning of section 2 (1) and (6) are […] foreign exchange or units of account".

purpose of application of these regulations, CFTC qualifies cryptocurrencies as a commodity[160].

However, due to the fact that cryptocurrencies are part of property without a doubt (they are property in the legal sense), first of all they may be the subject of investing[161]. One can purchase cryptocurrencies on one's own behalf and on one's own account, hoping for profitable resale in the future. There is also the possibility of conducting business of buying and then reselling cryptocurrencies to third parties. In practice, there is such a business — for example, an American company Bitcoin Savings and Trust, which accepted only bitcoins from their customers (it did not operate legal tender) for further investment. According to the Federal Court this company, even though it did not accept legal tender, conducted investment business and was subject to U.S. legal regulations, including those on financial instruments. As the case concerned fraud by organizing a pyramid scheme by Bitcoin Savings and Trust and its owner, it has been discussed in more detail in Section 3.2.2.

3.1.4. Cryptocurrencies and barter

Cryptocurrencies are very similar to settlement units used by the multilateral barter platforms. From the system point of view, the cryptocurrency system features similarities to a multilateral barter system. In such a comparison, *blockchain* would be equivalent to the accounts of participants of the barter system, where settlement units of private money used in the barter system are inventoried. However, an important difference is that the entity organizing the barter system runs the relevant accounts, but there is no entity organizing the system in the case of cryptocurrencies.

The natural development of a multilateral barter system is moving away from running a separate account for the settlement units of a certain private community currency used for each of the participants. This would further bring cryptocurrencies closer to such currencies. An obstacle in our analogy is that cryptocurrencies do not have an issuer. But even more important is the feature of openness and universality of cryptocurrencies, which allows paying anyone and for any goods

[160] See more: H.B. Shadab, *Regulating Bitcoin and Block Chain Derivatives*, October 9, 2014, http://www.cftc.gov/idc/groups/public/@aboutcftc/documents/file/gmac_100914_bitcoin.pdf (access: October 6, 2016); see also T.I. Kiviat, "Beyond Bitcoin: Issues in Regulating Blockchain Transactions", *Duke Law Journal* 65, 2015, No. 3, pp. 594 ff.

[161] This has been observed e.g. by one of the UK supervisors — Financial Conduct Authority (FCA), which recognizes cryptocurrencies, including bitcoin, as "investment assets" — see: Annual Report 2013/2014 — FCA. Markets Pactitioner Panel, p. 17, https://www.fca.org.uk/your -fca/documents/markets-practitioner-panel-annual-report-2013-14 (access: October 6, 2016). Investment assets include stocks in a broader sense, bonds, commodities, and currencies; see also U.S. Securities and Exchange Commission, Investor Alert: *Ponzi Schemes Using Virtual Currencies*, SEC Pub. No. 153 (7/13), https://www.sec.gov/investor/alerts/ia_virtualcurrencies.pdf (access: October 6, 2016).

and services, including for legal tender (which means the exchange of cryptocurrencies for legal tender). Barter systems, by definition, do not have this feature. Community money is secondary to the system in barter systems — i.e., first you need to join a barter system, and then you can make payments in the internal currency. Cryptocurrencies operate in the opposite way — first you become a member of the cryptocurrency system by installing and using an applicable software, and only then you can make payments for goods and services within this system. Cryptocurrencies provide the opportunity to create "open barter systems", i.e. those, which theoretically could, if developed without hindrance, cover all goods and services throughout the world.

However, from a legal point of view, payments using cryptocurrency cannot be considered exactly the same as payments using private currency carried out under a barter system. The difference is that in the latter case, the parties to the transaction belong to the same barter system and, therefore, certain rights and obligations relating to the payment and resulting from membership in the system are incumbent on them. When using cryptocurrency, parties must each time define mutual rights and obligations before making payment, or at least agree between themselves that the payment will be in the cryptocurrency.

3.2. Lawfulness of cryptocurrencies

3.2.1. Prohibition on the use of cryptocurrencies

By the end of 2015, no country in the world has decided to formally, directly and totally ban the use of cryptocurrencies[162]. The possibility of using bitcoin has been strongly restricted in China, but this was done not at the level of statutory regulations, but the recommendation issued by the People's Bank of China, Ministry of Industry and Information Technology and committees involved in the supervision of the Chinese banking, capital and insurance market[163].

This recommendation is addressed to financial institutions (including those dealing with payment settlements) and includes such a broad catalog of activities, which cannot be performed using bitcoin, that it actually rules out the use of bitcoin. Other entities, in particular, natural persons can use bitcoin and they are

[162] See e.g. *Regulation of Bitcoin in Selected Jurisdictions*, The Law Library January of Congress, Global Legal Research Center, styczeń 2014, http://www.loc.gov/law/help/bitcoin-survey/ (access: October 6, 2016). This report is updated on an ongoing basis.

[163] *People's Bank of China, Ministry of Industry and Information Technology of China, China Securities Regulatory Commission, China Banking Regulatory Commission and the China Insurance Regulatory Commission Notice on the Prevention of Risks Associated with Bitcoin* (Bank Notice [2013] No. 289) — unofficial translation into English is available at https://exchange.btcc.com/page/bocnotice2013 (access: October 6, 2016).

only warned of the risks involved. On the other hand, websites that serve as "bitcoin trading platforms", that is — as it seems — cryptocurrency exchanges should be entered in the relevant register kept by the Chinese Telecommunication Office in accordance with the applicable regulations. So, e.g., bitcoin and litecoin exchange still operates legally in China[164].

There are countries which plan to introduce restrictions on the use of cryptocurrencies. For example, a project of penalty of imprisonment (up to 4 years) for the exchange of cryptocurrency into rubles has been introduced in Russia (this penalty would not apply to "mining" a cryptocurrency, using it to pay for goods and services, as well as exchange for other cryptocurrencies)[165]. It is also planned to introduce a penalty for the "use" of cryptocurrencies and their "distribution" in Russia. The penalty would range from 5,000 to 50,000 rubles ($77–770) for natural persons and from half a million to one million rubles ($7,700–15,400) for legal persons[166].

The prohibition on the use of cryptocurrencies only makes sense while establishing sanctions. In turn, such a sanction would be effective, i.e. the state would have to effectively enforce the ban by the actual application of sanctions. The specificity of cryptocurrencies, which guarantee a considerable degree of anonymity to their users, raises doubts as to the effectiveness of the enforcement of the ban on their use. Undoubtedly, such a ban would greatly restrict the development of individual cryptocurrency systems, at least because professional traders who take care of the legality of their activities would not accept payments for goods and services in cryptocurrencies. As a consequence of the ban on the use of cryptocurrencies (or the excessive restriction of their use by the state), cryptocurrency payment systems would undoubtedly go "underground" and therefore would function without any possibility of controlling them in the fight against money laundering and terrorist financing[167]. Ironically, this will facilitate the use of cryptocurrencies to hide income before tax authorities[168]. It seems that the most reasonable limitation of the cryptocurrency system is licensing (authorization, introducing the requirement to obtain authorization) of business carried out by the so-called cryptocurrency exchanges and exchange offices in the exchange of cryptocurrencies to legal tender and pen-

[164] https://www.btcc.com/ (access: October 6, 2016).

[165] See: Y.B. Perez, *Russian Minister Confirms Plans to Ban Bitcoin-to-Fiat Conversions*, http://www.coindesk.com/russian-minister-confirms-plans-to-ban-bitcoin-to-fiat-conversions/ (access: October 6, 2016).

[166] A. Bazenkova, "Russian Firm Plans Local Version of Bitcoin Digital Currency", *The Moscow Times*, September 17, 2015, http://www.themoscowtimes.com/business/article/russian-firm-plans-local-version-of-bitcoin-digital-currency/531300.html (access: October 6, 2016). Until mid-2016, such restrictions have not become law in Russia.

[167] See paragraph 28 of the guidelines FATF titled *Guidance for a Risk-Based Approach to Virtual Currencies* June 2015, p. 9, http://www.fatf-gafi.org/publications/fatfgeneral/documents/guidance-rba-virtual-currencies.html (access: October 6, 2016); see also subsection 3.6.

[168] See more in subsection 3.7.3.

alties for conducting such a business without an appropriate authorization. Such a solution can bring many benefits, both in terms of measures to counter money laundering and terrorist financing[169], and preventing tax evasion and tax fraud[170].

Although, as already mentioned, no state has decided to formally ban the use of cryptocurrencies (and so far there are only such plans, and only in Russia), the competent authorities and institutions responsible for financial supervision (including banking) and the financial system, in particular the banking system, are not neutral towards cryptocurrencies. Basically, their position is critical and focuses on pointing out many dangers associated with the use of cryptocurrencies to potential users (mainly, but not limited to consumers). It is about documents published by the European Central Bank[171] and followed by the national central banks of the European System of Central Banks[172]; warnings announced by the European Banking Authority (EBA)[173] and Reserve Bank of India[174], Central Bank of Indonesia[175], Central Bank of the Russian Federation[176], and Monetary Authority of Singapore[177].

3.2.2. Legal consequences of qualifying the cryptocurrency system as a pyramid scheme

The definition of the pyramid scheme system in the European Union law is included in the paragraph 14 of Annex I to Directive 2005/29/EC of the European

[169] FATF recommends establishing regulations concerning the prevention of money laundering and terrorist financing for platforms of exchange between virtual currencies and legal tender, and thus subject cryptocurrency exchanges and exchange offices to such regulations. The recommendations also mention the possibility of introducing the obligation to register/obtain a license/permit for such platforms (and thus the cryptocurrency exchanges and exchange offices) — see FATF guidelines titled *Guidance for a Risk-Based Approach to Virtual Currencies*, pp. 9–10 (in particular, see section 37 and 38 of the guidelines); BIS takes a similar position — see *Non-Banks in Retail Payments*, p. 16.

[170] See more in subsection 3.7.3.

[171] The document from the European Central Bank titled *Virtual Currency Schemes.*

[172] E.g. warnings issued by the Central Bank of Cyprus, http://www.centralbank.gov.cy/nqcontent.cfm?a_id=13239&tt=article&lang=en (access: October 6, 2016); Central Bank of the Netherlands, http://www.dnb.nl/en/news/news-and-archive/nieuws-2013/dnb300672.jsp (access: October 6, 2016).

[173] Warning issued by the EBA, *Warning to Consumers on Virtual Currencies*, see also *EBA Opinion on "Virtual Currencies"*.

[174] https://rbi.org.in/scripts/BS_PressReleaseDisplay.aspx?prid=30247 (access: October 6, 2016).

[175] http://www.bi.go.id/en/ruang-media/siaran-pers/Pages/SP_160614.aspx (access: October 6, 2016).

[176] http://www.cbr.ru/press/PR.aspx?file=27012014_1825052.htm, omówienie zob. http://www.loc. gov/law/foreign-news/article/russia-bitcoin-exchanges-can-be-penalized/ (access: October 6, 2016).

[177] http://www.moneysense.gov.sg/understanding-financial-products/investments/consumer-alerts/virtual-currencies.aspx (access: October 6, 2016).

Parliament and of the Council of May 11, 2005[178]. This Annex lists "commercial practices considered unfair in all circumstances", and the paragraph 14 defines such a practice as "establishing, operating or promoting 'pyramid' type promotional systems in which a consumer gives consideration in exchange for the opportunity to receive compensation, which depends primarily on the introduction of other consumers into the scheme rather than from the sale or consumption of products." The provisions of Directive 2005/29/EC, including paragraph 14 of Annex I, do not apply to the "classic" cryptocurrency system because of the scope of the directive specified in its Article 3. Directive 2005/29/EC applies to unfair commercial practices in the meaning of Art. 5 (wherein in accordance with Art. 5, paragraph 5 Annex I contains a list of commercial practices which are considered unfair in all circumstances), used by businesses towards consumers before concluding a commercial transaction relating to the product, during the transaction and after its conclusion. The cryptocurrency system is decentralized by design, so there is no "organizer", or an entity that could legally be responsible for its organization. There is no entity in the cryptocurrency system that could be designated as a business using unfair commercial practices towards a consumer. Certainly, there is a natural person, or group of such persons, which created the cryptocurrency system. However, this person is not necessarily an entrepreneur, and besides, this person remains anonymous in the case of the largest cryptocurrency systems. It is so e.g. in the case of the creator of bitcoin system (but e.g. the creator of the litecoin system is widely known). However, if the cryptocurrency system was organized by an entrepreneur acting explicitly and would include consumers within the meaning of Directive 2005/29/EC[179], then it should be considered whether its activity shows all features of an unfair commercial practice as set forth in paragraph 14 of the Annex to the Directive 2005/29/EC.

The participants of the cryptocurrency system "mine" cryptocurrency or use it in order to acquire goods or services, or exchange it for legal tender. The benefit, which the consumer who uses the cryptocurrency may receive, is either receiving cryptocurrency due to its "mining", or selling it for a price higher than the purchase price. In either case, there may exist the element of the introduction of other consumers into the scheme, although it is not so clear, and therefore may be questionable. In the case of "mining" of cryptocurrency, the introduction to the

[178] Directive 2005/29/EC of the European Parliament and of the Council of May 11, 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council (OJ. EU L 149 of 06/11/2005), pp. 22–39.

[179] There are already instances of the declaration of intention to create such systems by enterprises (legal persons). An example would be the Russian company Qiwi, which is about to create a cryptocurrency system to be called bitruble — see A. Bazenkova, op. cit.; E. Lace, *BitRuble? First Russian Cryptocurrency Announced by Qiwi*, http://cointelegraph.com/news/115281/bitruble-first-russian-cryptocurrency-announced-by-qiwi (access: October 6, 2016).

system would consist in the consumer providing computing power necessary to carry out transactions, through which new consumers could receive cryptocurrency. Obtaining cryptocurrency is related to the use of specialized software and in general — joining the system. Also, the exchange of cryptocurrency for legal tender means that the buyer of cryptocurrency must be a member of the system. This line of reasoning may, however, be considered controversial, it is not as clear and transparent pyramid scheme as e.g. Madoff's pyramid scheme, MMM financial pyramid by Sergei Mavrodi in Russia or World Trading System pyramid in Germany.

If one considered that the organization of the financial pyramid system, such as a cryptocurrency system, is a fraud within the meaning of criminal law (e.g. Art. 286 § 1 of the Polish Criminal Code[180]; hereinafter: CC), then one would have to identify a natural person who commits fraud by organizing such a system or a natural person representing a legal person organizing such a system. Usually, a natural person organizing the hitherto financial pyramid was determined after the collapse of the pyramid, who then bore criminal responsibility. However, the creator of the most popular cryptocurrency system — Bitcoin — remains anonymous. Perhaps the fear of legal responsibility is one of the reasons he keeps his anonymity. Besides, criminal responsibility of the creator of a cryptocurrency system would be quite controversial, even assuming that such a system meets the conditions of the financial pyramid. Criminal law rigorously constructs criminal responsibility, requiring the determination of guilt or causality. The behavior of such a person would have to show all features of an offense, e.g. as set forth in Article 286 § 1 of the Penal Code in Poland, which means that one should have proven that such a person brought another person (i.e. the cryptocurrency user) to the negative disposal of his or her own or someone else's property by misrepresentation, exploit of a mistake or inability to properly understand the performed action in order to gain material benefits.

In contrast, the so-called bitcoin system developers, i.e. those developing the system and taking care of its proper functioning, are widely known. Similarly with the developers of other cryptocurrency systems. As a fraud is a universal crime ("everyone" can do it), therefore the activity of cryptocurrency developers can be assessed from this perspective. However, construing the criminal responsibility of developers in the context of the crime of fraud is even more difficult and more controversial than constructing such a responsibility of persons organizing the cryptocurrency system. First of all, developers declare *non-profit* activity, and what's more — this activity has such a nature that it is difficult to identify a material benefit resulting from it.

There is also the question of whether cryptocurrency can be used for organizing a pyramid scheme and whether law in the respective country aimed at

[180] Penal Code of June 6, 1997 (Journal of Laws of 1997, No. 88, item 553 as amended).

preventing the creation of pyramid schemes and punishment for their organization will be applicable in such a case. This question should be answered affirmatively, as pointed out by Securities and Exchange Commission (SEC) in a warning for investors[181]. This even follows from the fact that cryptocurrencies have a certain value and can be, as it has already been raised, classified as property. Moreover, one can easily determine the entity organizing the financial pyramid in such a situation. However, such considerations are by no means purely theoretical. There was Bitcoin Savings and Trust company run by Trendon T. Shavers in the US, whose activities consisted of taking bitcoins on a percentage (they promised a 1% return per day!). Bitcoins were to be properly invested, but in fact they served the repayment of people, who have entrusted their funds to the company. According to Securities and Exchange Commission (SEC), this was a pyramid scheme, which violated the provisions of American Securities Act of 1933 and Exchange Act of 1934, currently included in Title 15 of U.S. Code. Federal Court (United States District Court for the Eastern District of Texas, Sherman Division) acknowledged in its judgement of August 26, 2014, containing partial recognition and partial rejection of the request for reconsideration of the case (*case number* 4:13-cv-00416), that the legal responsibility arising out of these regulations does not exclude the circumstances of organizing a pyramid scheme in bitcoins only[182]. The court has not ruled on how to legally qualify bitcoins, but found that no doubt bitcoins have a specified value ("[…] the Court is easily able to determine that bitcoin constitutes something of value […]"). In a final judgement in the proceedings in this case[183], The Federal Court found a violation of section 10(b) of Securities Exchange Act of 1934 (15 U.S.C.§ 78j(b)] and Rule 10b-5 promulgated thereunder 17 C.F.R. § 240.10b-5), sections 17(a) of the Securities Act of 1933 (15 U.S.C. § 77q(a)), sections 5 of the Securities Act (15 U.S.C. § 77e) and based on 15 U.S.C. §§ 77t(d) and 78u(d)(3) sentenced Shavers to a fine of $150,000, and also sentenced Bitcoin Savings and Trust company to $150,000.

It does not seem likely that such a decision was possible on the basis of national regulations implementing Directive 2005/29/EC. The system organized by Bitcoin Savings and Trust run by Trendon T. Shavers rather did not meet the definition of a pyramid scheme indicated in paragraph 14 of the Annex to Directive 2005/29/EC. There is a legal loophole here. What remains are other national provisions allowing for combat Ponzi schemes or possibly punish (with the use of criminal

[181] U.S. Securities and Exchange Commission, Investor Alert: *Ponzi Schemes Using Virtual Currencies*, SEC Pub. No. 153 (7/13), https://www.sec.gov/investor/alerts/ia_virtualcurrencies.pdf (access: October 6, 2016).

[182] Securities and Exchange Commission v. Trendon T. Shavers and Bitcoin Savings and Trust, case number 4:13-cv-00416, https://www.manatt.com/uploadedFiles/Content/4_News_and_Events/Newsletters/BankingLaw@manatt/SEC%20v.%20Shavers.pdf (access: October 6, 2016).

[183] http://www.davispolk.com/sites/default/files/gov_uscourts_txed_146063_88_0.pdf (access: October 6, 2016).

or administrative sanctions) for carrying out investment activities without an appropriate authorization. First of all, it should be noted that Shevers bore criminal responsibility partly for having run the investment business in the name and on behalf of third parties without the relevant permit. SEC takes a clear position that any investment is covered by its jurisdiction, regardless of whether they are denominated in dollars, or in virtual currencies — particularly individuals selling investments are covered by federal and state licensing requirements[184].

3.3. Legal aspects of cryptocurrency creation

Creation of a unit of cryptocurrency (e.g. 1 BTC) in fact involves making the appropriate entry in the registry, which is a blockchain. As already shown, a computer program makes such an entry in accordance with a specified algorithm (for details, see Chapter 1). However, a computer program has no legal personality in the current state of the law, it cannot make commitments and cannot be a subject of rights and obligations[185]. The program runs according to an algorithm written by a man or a group of people, and the authors of computer programs, who have moral rights to these programs, are usually known to users. In addition, there are usually people who have economic copyrights to the program. However, cryptocurrencies, including bitcoin, are by their nature developed based on the ideology of free software.

Thus, there is no one who can have the moral rights and economic copyright to the bitcoin system software. The same is the case with most cryptocurrencies, although one can not exclude a situation where the copyright to the software of a specific cryptocurrency system will be reserved for a specific person. In principle, such action, although contrary to the ideological foundations of cryptocurrencies, creates new, interesting opportunities for the development of cryptocurrencies. In practice, despite the absence of the owner of the copyright to a specific cryptocurrency software, there is a group of people who deal with the development and updating of cryptocurrency software[186]. This group works on a voluntary basis and is not formally responsible for the operations of the system.

---

[184] U.S. Securities and Exchange Commission, Investor Alert: *Ponzi Schemes Using Virtual Currencies*, SEC Pub. No. 153 (7/13).

[185] The declarations of will by means of computer programs, and more broadly — the legal personality of artificial intelligence — is becoming increasingly important — see e.g. G. Sartor, "Cognitive Automata and the Law: Electronic Contracting and the Intentionality of Software Agents", *Artificial Intelligence and Law* 17, 2009, No. 4, pp. 253–290; F. Andrade et al., "Contracting Agents: Legal Personality and Representation", *Artificial Intelligence and Law* 15, 2007, No. 4, pp. 357–373. It is possible that this issue will soon become important for the legal considerations concerning systems of electronic means of payment without the issuer.

[186] In the case of bitcoin, see https://bitcoin.org/en/development (access: October 6, 2016).

To sum up, there is no natural or legal person, who can be attributed with the creation of cryptocurrency units.

However, according to the actual state, one can assume that computer programs (clients) included in the cryptocurrency system (or, taking another point of view — one computer program reproduced in multiple copies) record certain cryptocurrency units in a blockchain (e.g. 1 BTC). This entry, seen from the perspective of the cryptocurrency system, is obviously realistic in the sense that anyone can state its existence — simply by checking the blockchain code, which is publicly available. Due to the existence of so-called cryptocurrency exchanges, the cryptocurrency unit (monetary unit) stored in the blockchain may have a value expressed in legal tender (and other cryptocurrencies at the same time). This means that it has a certain value expressed in legal monetary units (e.g. the exchange rate of 1 BTC on a particular stock market and on a particular day may be a certain number of U.S. dollars).

Undoubtedly, a cryptocurrency unit (monetary unit) can be owned by someone. Such a possibility is inherent feature of the cryptocurrency system. When mining cryptocurrency, the system combines a certain amount of cryptocurrency with a specific, unique, private signature, over which control is exercised by a particular natural person. Through this combination a property right — the right to non-material interest, which is a record of a certain number of cryptocurrency units in the registry, or in the blockchain — is created.

A record of a specific value of cryptocurrency for a specific user, carried out by the system (the so-called mining cryptocurrency), is made mostly without user intervention (that is, the person who controls the private key). However, a certain activity on the user's part is necessary — to acquire cryptocurrency from mining, the user must take many conventional steps, which have been described in Chapter 1. It can be assumed that their execution means the user agrees that the system assigns a certain amount of cryptocurrency (a number of monetary units of cryptocurrency). Measures aimed at "mining" cryptocurrency can give the total effect of a declaration of will[187]. What's more — the theory of civil law states that the declaration of will also means a manifestation of will, whose purpose is not to inform another person of a will, and an example is given of taking a self-contained possession of a nobody's thing (Art. 180 of the Civil Code)[188]. In the process of "mining" cryptocurrencies, the action of a person intending to mine cryptocurrency has no recipient, and taking into account the views of this doctrine, one can analyze the acquisition of cryptocurrency units by analogy to taking a self-contained possession of a nobody's thing[189].

[187] According to Art. 60 of Polish Civil Code, the will of the person doing the legal action can be expressed by any behavior of this person, which reveals his or her will in a sufficient manner, including the disclosure of the will in electronic form.

[188] A. Wolter, *Prawo cywilne. Zarys części ogólnej*, Warszawa 1982, pp. 246–247.

[189] This approach can be extended to all electronic means of payment without the issuer — not only to cryptocurrencies.

Of course, only a remote analogy is possible here, because certainly cryptocurrency units are not things in the meaning of civil law. An intuitive comparison of allocating bitcoins by the system to mining for gold is accurate in this perspective.

One may also consider whether due to the fact that the user takes up a lot of conventional actions, waiting for a random result (the granting of a certain amount of cryptocurrency by the system), one should rather seek an analogy to the legal qualification of cryptocurrency mining in the regulations relating to games of chance in the broad sense (gambling). The difference is that the user has no claims against the entity, which allocates cryptocurrency, for the simple reason that there is no such entity. Therefore, the accession to the game and meeting certain requirements (i.e. buying a lottery ticket) in games of chance in a broad sense means the acquisition of a claim to the winning payment, whereas when mining cryptocurrency, a person providing the resources of his or her computer to the cryptocurrency system does not claim an entry of a specified quantity of cryptocurrency, because the system is decentralized. Decentralization of the cryptocurrency system prevents the use the rules on gambling by analogy, because there is no entity which could be classified as a lottery organizer. The situation changes when the cryptocurrency system is controlled by a natural or legal person despite technical decentralization, especially when that person assumes the responsibility for the operation of the system. In such a situation, an entity exists, towards which the user mining a cryptocurrency may have a claim. There are also no problems with constructing the appropriate legal framework using civil law. But the point is that in most civilized countries, the games of chance (gambling) in a broad sense are subject to state control and a separate legal regulation defining the terms of their organization and doing business by entities which organize them. The primary purpose of the state control and at the same time the relevant legal regulations is to counteract the negative effects arising from gambling, the fiscal issue is also of great importance.

In case the cryptocurrency system was led by a specifically defined entity, then one may consider the qualification of cryptocurrency mining as slot machines within the meaning of Art. 2 paragraph 3 of Polish Act of November 19, 2009 on gambling[190]. According to this regulation, slot machine games are games on mechanical, electromechanical and electronic equipment, including computers, with winnings in cash or things, in which the game contains an element of randomness. The application of this regulation to cryptocurrency mining can raise a lot of important questions — first of all, devices for cryptocurrency mining remain, in principle, the cryptocurrency users' ownership and it does not seem that the provisions of the Act take into account this circumstance. Obviously, a lot depends on the particular factual status and one can make a reasonable interpretation of the

[190] Journal of Laws of 2015, item 612. The Act uses the collective term "gambling", which includes games of chance, betting, and slot machines.

law only in relation to a particular cryptocurrency system controlled by a specified entity. However, neither the Polish law, or the law of any other country concerning gambling was created or amended with the intention of including the creation of cryptocurrencies in its provisions. It seems that it is quite an important argument in the debate on whether the creation of cryptocurrencies should be legally qualified as gambling. One cannot exclude that in case the cryptocurrencies (or any other similar means of payment without the issuer) prevail, the legislative action will be taken in order to extend the scope of the regulations on gambling to the creation of cryptocurrency (or any other similar means of payment without the issuer). This is undoubtedly one of the directions of possible intervention by the legislator in the process of creating cryptocurrencies, and more broadly — electronic means of payment without the issuer.

In passing, it is necessary to note the possibility to distinguish the person controlling the IT device (PC, server, etc.), on which *blockchain* is installed, from the cryptocurrency user. There is coincidence in the classical model of cryptocurrency, but there are wallets in trade that do not require installation of a blockchain. However, such a solution prevents the user, or a person controlling the private key, from "mining" the cryptocurrency.

Consistent application of the principle that the person who controls the private key is the cryptocurrency user results in the so-called. miner working in a mine (a person who works with others in mining of cryptocurrency using specialized software which provides the computing power of hits person's computer to the community which mines cryptocurrency — see Chapter 1) cannot be qualified as a person acquiring the right to a newly created cryptocurrency unit.

Such a right will always be entitled to the one who controls the private signature used for creating this unit by the system. On the other hand, the "miner" claims to submit a certain amount of cryptocurrency to him or her under a contract with the person organizing the mining system (the "mine"). This not necessarily has to be the person controlling the private signature associated with a new record of a specified number of cryptocurrency units — a lot depends on the organizational structure of the mine and the content of the contracts concluded between individuals in the community involved in mining cryptocurrency within a given mine.

Sometimes a specific person (natural, legal) in no way takes part in the process of "mining" cryptocurrency, and above all does not provide computing power of the controlled hardware, but only acquires rights to cryptocurrencies, which are mined by others who control both the private key for mining the cryptocurrency and hardware used in its mining (i.e. the acquisition of shares in computing power, "mining in the cloud"). In this case the one who controls the private key and hardware mines the cryptocurrency. The person who acquired the rights to cryptocurrency has a claim towards the person who mined the cryptocurrency, and the content of the claim results from the previously concluded contract.

Cryptocurrencies as electronic means of payment without the issuer, 2016

In addition, there are drastic situations when the person controlling the IT device is not aware that it is used as a "mine". It is mostly the result of a hack using sophisticated Trojans (or other "worms"). Then the person controlling the private signature, or the hacker, is the user of the newly mined cryptocurrency. This person becomes the owner of so insidiously mined cryptocurrency.

3.4. Legal aspects of making payments using cryptocurrencies

3.4.1. Sources of law

Currently, there is no specific EU legislation on payments using electronic means of payment without the issuer, including primarily cryptocurrency. Basically, as of now — in mid-2016 — there is no will to regulate virtual currencies at the EU level in the European Parliament; at most, they see such a need in the fight against money laundering and terrorist financing[191].

So far there is also no national legislation concerning the payment in cryptocurrencies (and more broadly — in virtual currencies) in any of the Member States of the European Union. Other countries in the world also do not have such special law — this applies even to the U.S. federal law, where cryptocurrencies are the most popular. However, proposals for such regulations are notified[192], and if cryptocurrencies become more common, it seems that the intervention of the legislators will be necessary.

The state of New York stands out, which announced a separate, specific legislation for economic activity in the area of virtual currencies, including mainly cryptocurrencies, by introducing the so-called *BitLicense* (hereinafter: NY regulation) on June 24, 2015[193]. This regulation does not concern payments using cryptocurrencies as much as it is focused on defining terms and conditions for licensing of economic activity with the use of virtual currencies, items of capital requirements and defining public responsibilities in the fight against money laun-

[191] See European Parliament resolution of May 26, 2016 on virtual currencies (2016/2007(INI)), published http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+20160526+ITEMS+DOC+XML+V0//PL&language=PL (access: October 6, 2016).

[192] France intends to introduce relevant regulations — see http://www.economie.gouv. fr/files/regulatingvirtualcurrencies.pdf (access: 10/06/2016) and Japan — see http://pl.scribd. com/doc/289131216/Japan-Ministry-of-Economy-Trade-and-Industry-FinTech-Group-Second-Meeting; http://www.newsbtc.com/2015/11/22/japanese-government-to-draft-regulatory-billfor-bitcoin-by-early-2016/ (access: October 6, 2016).

[193] N.Y. COMP. CODES R. & REGS. tit. 23, § 200 (2015), see http://www.dfs.ny.gov/legal/regulations/bitlicense_reg_framework.htm (access: October 6, 2016); http://www.dfs.ny.gov/legal/regulations/adoptions/dfsp200t.pdf (access: October 6, 2016); see also I. Kiviat, op. cit., pp. 597 ff.

dering and terrorist financing, consumer protection, as well as — as a significant new regulation — in the field of cybersecurity of licensed entities.

The lack of regulations regarding payments using cryptocurrencies obviously means the lack of detailed legal regulations for the protection of consumers using cryptocurrencies. Certainly, the use of cryptocurrencies involves a specific risk for the consumer, resulting largely from the lack of an entity responsible for the correct execution of transactions in a decentralized cryptocurrency system. The legislation of the State of New York regarding business carried out with the use of virtual currencies show the direction of regulations for the protection of consumers using cryptocurrencies. As is usually the case with rules intended to protect consumers, it is about obligations regarding information. The NY regulation imposes these obligations on the entity, which received "bitlicence", and places it under obligation to inform the consumer that:

— Cryptocurrency is not legal tender

— Changes in legislative and regulatory or actions on the state, federal, or international level may adversely affect the use, transfer, exchange, and value of cryptocurrency

— Transactions made using cryptocurrency may be irreversible, and therefore the amount lost due to fraudulent or random transactions may not be recoverable

— Transactions in cryptocurrency are recognized at the time of making an entry in the public register (*blockchain*[194] in the case cryptocurrencies), which does not necessarily coincide with the moment of the initiation of the transaction by the consumer.

However, the risks, which are not related to the specifics of payments in cryptocurrency, but refer to payments on the Internet and acquiring goods and services "remotely" in general, are covered by existing consumer regulations, which in the case of acquisition of goods and services through cryptocurrency can be used after a proper interpretation (for example, of Art. 385^1 of the Civil Code specifying the prohibited provisions of contracts with consumers, as well as the regulations in specific laws (e.g. the law on consumer rights[195]) or, more broadly — consumer directives, such as Directive on consumer rights[196]).

Due to the lack of the issuer, one cannot apply specific provisions on electronic money to cryptocurrencies (and more broadly, to electronic means of payment

[194] The legislature of New York tries to be technologically neutral, and uses a broader concept of "public ledger" instead of the term "blockchain".

[195] The Act of May 30, 2014 on Consumer Rights (Journal of Laws of 2014 item 827). It must first be determined in the specific case whether there are grounds for exemption from its application specified in Articles 3 and 4.

[196] Directive 2004/39/EC of the European Parliament and of the Council of 25 April 2011 on markets in financial instruments amending Council Directives 85/611/EEC and 93/6/EEC and Directive 2000/12/EC of the European Parliament and of the Council and repealing Council Directive 93/22/EEC (OJ. EU L 304 of 11/22/2011).

without the issuer). In the European Union, this applies to Directive 2009/110/EC and national regulations that implement it (e.g. the provisions of Polish LPS regarding electronic money or the rules of English Electronic Money Regulations 2011[197] or German Gesetz über die Beaufsichtigung von Zahlungsdiensten (Zahlungsdiensteaufsichtsgesetz — ZAG)[198].

Transactions executed using cryptocurrencies are not included in the scope of PSD and the PSD 2 directives, because cryptocurrencies are neither legal means of payment nor electronic money. Thus, national provisions implementing PSD Directive do not apply to cryptocurrencies. Any legal regulation of transactions using cryptocurrencies should be made by an amendment to the PSD 2 directive, and it certainly will not be a simple procedure.

A significant exception concerns Brazil, where a legal document regulating the provision of payment services and the operation of payment institutions is in effect — LEI Nş 12.865, de 9 de outubro de 2013[199]. The scope of this act includes, as it seems, payments made by cryptocurrencies, which mainly results from the definition of electronic currency (*moeda eletrônica*) contained in Art. 6 VI of this act. According to this definition, an electronic currency means resources stored in the memory of a device or electronic system that allow the user to make a payment transaction ("recursos armazenados em dispositivo ou sistema eletrônico que permitem ao usuário final efetuar transação de pagamento")[200].

The lack of a specific legal regulation does not mean the lack of legal regulation in general. First of all, national civil law (e.g. Civil Code in Poland) is applicable to transactions using cryptocurrencies. As already indicated, specific rules on consumer protection can also apply to transactions using cryptocurrencies, although so far these provisions do not apply directly to such transactions.

It may be necessary to reach for the rules of private international law in the case of cross-border transactions using cryptocurrencies. Due to the high degree of anonymity of payments using cryptocurrencies and the scatter of information in physical space, specific to the Internet (physical locations of the user, computer,

[197] Her Majesty's Stationery Office (HMSO) 2011 No. 99; http://www.legislation.gov.uk/uksi/2011/99/made (access: October 6, 2016).

[198] Zahlungsdiensteaufsichtsgesetz vom 25. Juni 2009 (BGBl. I S. 1506), das zuletzt durch Artikel 23 des Gesetzes vom 20. November 2015 (BGBl. I S. 2029) — http://www.gesetze-im-internet.de/zag/index.html (access: October 6, 2016), see also the version in English: https://www.bafin.de/SharedDocs/Downloads/EN/Aufsichtsrecht/dl_zag_en.pdf?__blob=publicationFile (access: October 6, 2016).

[199] Lei No. 12.865, de 9 de Outubro de 2013 [Law No. 12,865 of October 9, 2013], http://www.receita.fazenda.gov.br/Legislacao/leis/2013/lei12865.htm (access: 6.10.2016); see also http://legislacao.planalto.gov.br/legisla/legislacao.nsf/Viw_Identificacao/lei%2012.865-2013?OpenDocument (access: October 6, 2016).

[200] Translated into English: "»Electronic currency« is defined as resources stored on a device or electronic system that allow the end user to perform a payment transaction" — see http://www.loc.gov/law/help/bitcoin-survey/#_ftnref14 (access: October 6, 2016).

and server may differ, not to mention the possibilities provided by the information processing in the so-called clouds), the determination of a proper national law and application of the relevant international regulations may be troublesome to a large extent. In extreme cases, especially in the event of keeping maximum anonymity by cryptocurrency users (e.g. using the TOR network), problems with determining the applicable law may prove to be insurmountable.

3.4.2. Payment using cryptocurrency as a change of entry in the registry, which is a blockchain

One can use the concept of the payer and the recipient for the purposes of legal analysis of payments using cryptocurrencies. These are concepts defined by the PSD Directive and used in its legislation, as well as the concept of a payment transaction. As already indicated, PSD and the PSD 2 directives do not apply to payments made in cryptocurrencies, however, it does not seem to prevent using some terms and concepts used in the directive. Of course, both the payer and the recipient must be users of the cryptocurrency system, i.e. control the private key. They may, but need not have installed a blockchain on computer hardware controlled by themselves. In practice, controlling the private key amounts to controlling the so-called wallet (see Chapter 1).

In the case of payments by cryptocurrencies, there is no "payment service provider" in the sense of PSD and PSD 2, and as a consequence, there is also no "payment order" within the meaning of the Directive (payment order is an instruction from a payer or payee to its service provider requesting the execution of a payment transaction). Instead, there is a payment system, but it is decentralized. Decentralization is possible through the use of blockchain technology. Due to this technology, in case of cryptocurrencies it is difficult to talk about "payment transaction" within the meaning of the PSD. The action initiated by the payer (the recipient cannot yet initiate a payment in the cryptocurrency system) does not "deposit", "transfer" or "withdraw" the funds, because there is only one register, in which entries are made — blockchain. For example, executing a transfer via the payment service provider means the "transfer" of funds in the form of a scripture (scriptural money) between two accounts held by the payment service provider of the payer and the payee, and it essentially consists in the relevant changes to the entries on these accounts[201]. There are no various payment service providers in the cryptocurrency system, there are no various accounts, therefore, there is no "transfer of funds". There is also no "depositing" and "withdrawal" of funds, because the system does not provide other units of cryptocurrency (e.g. 1 BTC), than an entry in the blockchain. From the "technical" point of view, there is no "transfer" of cryptocurrency in the

[201] From this point of view, "blockchain" differs from the payment accounts in that it is the only one (but it occurs in a large number of copies).

cryptocurrency system — there is only a change in the location and content of this entry within the blockchain. However, from a legal point of view, the payment in cryptocurrency clearly and indisputably leads to the transfer of property rights (property within the meaning of the civil law) from the assets of one cryptocurrency system user (payer) to the assets of another cryptocurrency user.

The question is, in the light of the current legal status, that is, in the absence of detailed legal regulation on payments using cryptocurrencies, whether a payment order consisting in the making of specific conventional activities in the so-called wallet (that is, entering the recipient's public key, indicating the amount in cryptocurrency [e.g. 0.01 BTC], and "clicking" the specific button to complete the transaction [e.g. the "send" button]) can qualify as a declaration of will. Certainly it is a manifestation of will, which sufficiently expresses the intent to cause the legal effect of establishing, changing or removing a legal relationship. In this particular case it is about a remittance of an obligation by a payment or transfer of ownership to a certain number of cryptocurrency units to another person. Undoubtedly, the will of the payer is thus disclosed in a sufficient way.

As already indicated, these activities do not necessarily have to have the recipient to be classified as a declaration of will of the payer. While a payment order governed by the PSD Directive has a recipient — it is the payment service provider — the payment order in the cryptocurrency system is not directed to an entity, which could be compared to the payment service provider even by analogy. The cryptocurrency system, as this paper has repeatedly stated, is decentralized. Therefore, although the behavior of the payer aimed at initiating the payment using cryptocurrency is not made available to another person (legal, natural), but is only performed in a decentralized cryptocurrency system, it may be classified as a statement of will from a legal perspective.

3.4.3. The moment of performance of commitment using cryptocurrency

The earliest time from which the recipient may have cryptocurrency, which is the subject of payment, at his or her disposal, is the moment of performance of commitment using cryptocurrency. This is the moment of making the entry in the blockchain system, whereby the amount of the transaction expressed in cryptocurrency is associated with a private key controlled by the recipient.

3.4.4. The responsibility for the validity of the transaction carried out using cryptocurrency

Current payment systems are characterized by the fact that there is always a legal entity responsible for the validity of the payment transaction. At the level of the European Union, this has been specifically addressed in PSD (and PSD 2)

Directive. However, in the case of cryptocurrency, due to the fact that it is a decentralized system, the entire responsibility for the validity of the transaction lies with the payer, unless this responsibility will be regulated differently in the contract with the customer and wholly or partially transferred to the recipient. Thus, in the event of incorrect performance of a payment transaction, there is no one from whom the payer may assert any claims in the standard cryptocurrency system (such as bitcoin). At best, one can construct contract with the recipient so that he or she is liable (in whole or in part) for the validity of the transaction.

We cannot rule out that a third party will take the responsibility for the validity of the transaction in cryptocurrency. This may be the entity organizing the cryptocurrency system, but this way the system would cease to be a decentralized system[202]. We can also reflect on the legal responsibility of entities providing different IT solutions to facilitate the user to use the cryptocurrency system, these include the provider of the so-called wallet.

3.5. Cryptocurrency and the monopoly of the central bank on issuance of money

3.5.1. Cryptocurrencies and other electronic means of payment without the issuer as money — a legal perspective

There is no legal definition of the concept of money, which naturally implies different ways of defining it. Everyone agrees that money being legal tender must be distinguished from money having no such character. From this perspective cryptocurrency, as any private money, is certainly not legal tender.

As commonly accepted in the economic and law literature, money in the economic sense has four main functions[203]:

— Medium of exchange
— Means of payment
— Unit of account — store of value.

In economic terms, something which performs all these functions is considered money regardless of the legal nature. In fact, the actual performance of

[202] It seems that an example of such a system may be the one organized by Ripple Labs Inc — see https://ripple.com/ (access: October 6, 2016).

[203] R.M. Lastra, *International Financial and Monetary Law*, Oxford 2015, p. 12. Sometimes these functions are called differently, e.g. the function of a medium of exchange is called a function of the means of circulation, and the function of the settlement unit is called the function of the measure of value — see e.g. C. Kosikowski, "Pieniądz", [in:] *Encyklopedia prawa bankowego*, ed. W. Pyzioł, Warszawa 2000, pp. 479–480.

these functions is closely and rather inseparable related to the "general acceptance" of a given means of payment. In turn, the element of "general acceptance" enables to apply a sociological (or even psychological) perspective, and certainly, from this perspective, money is what people consider so[204].

In democracy, the power comes from people (society, the people), which is closely related to a nation (society, the people) and is its emanation. The state exercises a sovereign power, and the monetary stability is one of its aspects. States, as part of the monetary sovereignty, issue banknotes and coins, which are legal tender, through central banks. As a rule, only those banknotes and coins are money in the legal sense[205].

In contrast to the economy, in which the concept of money is very broad, money in the legal sense is considered in extremely narrow meaning — as banknotes and coins. However, the rules of the law may apply the concept of money and by way of interpretation, it must be determined whether the term is used in the narrow sense — as banknotes and coins, or more broadly — in economic terms.

Therefore, from a strictly legal perspective, cryptocurrencies are not money, because they are not created by the state as a part of their monetary sovereignty, which is now manifested by the fact that they are not banknotes and coins which are legal tender. In contrast, cryptocurrencies can perform the functions of money in economic terms, which has been recognized by the legislature of the state of New York by pointing out these functions in the definition of virtual currencies (which also include cryptocurrencies).

3.5.2. Cryptocurrency system as a system striving for universality

There are two types of private money systems — those limited by their nature and those seeking universality. The former may not become common by definition, because they are limited either geographically (e.g. local money (currency)), or to a particular game or portal (e.g. virtual money), or legally and functionally (as e.g. a regulated electronic money). In addition, they have a low or even negligible capitalization in relation to the money which is legal tender. The latter aim to strive for universality by their nature, and their creators declare replacing or even eliminating legal tender issued by central banks as a part of a specific ideology (as is the case of cryptocurrencies, bitcoin in particular).

[204] See: J. Górniak, *My i nasze pieniądze. Studium postaw wobec pieniądza*, Kraków 2000, pp. 18 ff.

[205] More about monetary sovereignty, see R.M. Lastra, op. cit., pp. 14 ff. and the references cited.

3.5.3. Cryptocurrency as a threat to the money which is legal tender and monetary sovereignty of the state

Inherently private money systems, limited by their nature, such as local currency or virtual currencies, rather may not be a threat to the monopoly of the central bank and, therefore, in-depth research in this direction is not currently required in their case. In particular, they do not have the impact on monetary stability and on financial market stability, primarily due to low capitalization. However, it is different with cryptocurrencies. The cryptocurrency system is of a global nature (supraterritorial or transnational) and anyone can use it to purchase any goods and services (including virtual or illegal).

Currently (in 2015), cryptocurrencies still are not "public" due to the relatively small capitalization and nobody knows if they ever become such, and it seems that the already mentioned question of trust is the key here. In addition, as detailed in chapter 2, cryptocurrencies have not yet fulfilled all the functions of money[206]. Note, however, that the contemporary socio-economic processes take place very rapidly and a rapid spread of some kind cryptocurrency (at present, bitcoin is still the best candidate here) or any other type of electronic means of payment without the issuer cannot be ruled out. Legal tender would then be displaced by the cryptocurrency (or other type of electronic means of payment without the issuer). This would clearly compromise the monetary sovereignty of the state. This is why extensive research should be already carried out in the field of legal regulation of monetary sovereignty, in particular the monopoly of the central bank to issuing currency in the context of the development of cryptocurrencies, and more broadly — electronic means of payment without the issuer functioning in systems striving for universality.

However, these studies should consider a general global trend, consisting in the gradual erosion of the monetary sovereignty of states. According to some, it is an inevitable phenomenon, because it is a consequence of such processes as globalization and the information revolution and the progressive economic and financial development of states. The erosion takes place at various levels and in various areas — e.g. within the European Union, in particular Economic and Monetary Affairs, as a result of the activity of the International Monetary Fund, or because of the ease of contemporary flow of large capital across borders[207].

Thus cryptocurrencies are one of many factors, which weakens or may weaken the monetary sovereignty of the state. The Constitution of the state concerned

[206] E.g. Central Bank of the Netherlands claims that virtual currencies (also cryptocurrencies, including Bitcoin), can fulfill the functions of money to a very little extent, and they will not become widespread in the near, foreseeable future; see more http://www.dnb.nl/en/news/news-and-archive/dnbulletin-2014/dnb307263.jsp (access: October 6, 2016).

[207] See more: R.M. Lastra, op. cit., pp. 21–27.

is a legal point of reference, whether this effect of cryptocurrencies is positive or negative and should be regarded as a "threat" to the monetary sovereignty.

For example, according to Art. 227 paragraph 1 of the Polish Constitution[208], the National Bank of Poland, which is the central bank of the state, shall have the exclusive right to issue money and to determine and implement monetary policy. From the Act of August 29, 1997 on Polish National Bank[209] follows that this money is Polish Zloty, which takes the form of coins and banknotes and is legal tender on the territory of the Republic of Poland[210]. Note that only the notion of money without clarifying is used the Polish constitution; such clarifying and narrowing of the constitutional concept to coins and notes was made only by law. Similarly, the Constitution of the Russian Federation[211] only indicates in Art. 75 that "Ruble is the monetary unit in the Russian Federation, and only the Central Bank of the Russian Federation issues money". Also in this constitution the form of money is not clearly decided. What's more, the next sentence of this article clearly states that "the introduction and issuance of other money in the Russian Federation is prohibited". In addition, paragraph 2 states that "the protection and ensuring the stability of Ruble is the main function of the Central Bank of the Russian Federation, which it performs fully independently from other bodies of state power". Next, according to Art. 137 of the Constitution of Romania[212], "national currency is Leu, and its hundredth part is Ban", without specifying the form in which it exists, or without using the concept of money. A special case is undoubtedly the Constitution of the Czech Republic[213], which indicates Czech National Bank as a country Central Bank in Art. 98, defines its main objective, which is to care for price stability, indicates that its activities can be interfered with only according to law, and leaves the determination of the position of the central bank, its powers and other details to the Act. Thus, money in the Czech Republic are regulated by law.

[208] Constitution of the Polish Republic of April 2, 1997 (Journal of Laws No. 78, item 483 as amended).

[209] Journal of Laws of 2013, item 908 as amended.

[210] According to Art. 4 of the Act, NBP has the exclusive right to issue the currency of the Republic of Poland. On the other hand, in accordance with Art. 31, banknotes and coins with indicated amounts in zlotys and grosz are the currency in Poland, and in accordance with Art. 32, monetary units issued by NBP are legal tender in the Republic of Poland.

[211] The Constitution of the Russian Federation adopted in a national referendum on December 12, 1993, for Polish language version see: http://libr.sejm.gov.pl/tek01/txt/konst/rosja.html (access: October 6, 2016).

[212] The Constitution of Romania of November 21, 1991, for Polish language version see http://libr.sejm.gov.pl/tek01/txt/konst/rumunia2011.html#mozTocId165972 (access: October 6, 2016); for English version see http://www.cdep.ro/pls/dic/site2015.page?id=339&idl=2 (access: October 6, 2016).

[213] The Constitution of the Czech Republic of December 16, 1992, for Polish language version see http://biblioteka.sejm.gov.pl/wp-content/uploads/2015/07/Czechy_pol_010811.pdf (access: October 6, 2016); for English version see http://www.usoud.cz/en/constitution-of-the-czech-republic/ (access: October 6, 2016).

However, Western constitutions clearly refer to money as banknotes and coins (or just coins) at the constitutional level. For example, according to Art. 99 paragraph 1 and 2 of the Federal Constitution of the Swiss Confederation "the competence of the Federation includes the system of monetary and currency relations; it has the sole right to mint coins and issue banknotes" (paragraph 1), and "Swiss National Bank, as an independent central bank conducts monetary and currency policy, which serves the general interest of the country; it is managed with the cooperation and supervision of the Federation"[214]. According to paragraph 1 Section 8 of the Constitution of the United States, only Congress has the right to mint coins and determine the value of money, including foreign one[215]. Currently, the competence of the Congress is performed by the Federal Reserve and its transfer took place by means of an Act. It is clear here that the original right to issue money (in the case of the US — "minting coins and determining the value of money") belongs exclusively to the state. In this regard, the Treaty on the Functioning of the European Union[216] (hereinafter: TFEU) contains a special regulation in relation to the Euro area countries. According to Art. 128, paragraph 1 of TFEU, the European Central Bank has the exclusive right to authorize the issue of euro banknotes within the European Union. European Central Bank and national central banks may issue such banknotes, and the notes issued by the European Central Bank and national central banks shall be the only legal tender within the EU. However, according to Art. 128 paragraph 2 of TFEU, Member States may issue coins subject to approval by the European Central Bank of the volume of the issue. The Council, on a proposal from the Commission and after consulting the European Parliament and the European Central Bank, may adopt measures in order to harmonize the denominations and technical specifications of all coins intended for circulation to the extent necessary to permit their smooth circulation within the EU. As follows from Art. 139 paragraph 2 of TFEU, Art. 128 TFEU does not apply to countries included in a derogation, i.e. those for which the Council has not decided that they fulfill the necessary conditions to adopt the Euro, (just as Art. 127 paragraph 1, 2, 3, and 5 of the TFEU, setting out the objectives and tasks of the ESCB, as well as

[214] The Federal Constitution of the Swiss Confederation of April 18, 1999 trans. by Z. Czeszejko-Sochacki, Warszawa 2000, (access: October 6, 2016).

[215] The Constitution of the United States of America, translation and introduction by A. Pullo, Warsaw 2002, published in http://biblioteka.sejm.gov.pl/konstytucje_swiata/ (access: October 6, 2016).

[216] Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union — the Treaty on European Union (unified version) — the Treaty on the Functioning of the European Union (unified version) — Protocols — Annexes Declarations attached to the Final Act of the intergovernmental conference which adopted the Treaty of Lisbon, signed in on December 13, 2007 — Tables of equivalences (OJ. EU C 326, 26/10/2012 P. 0001–0390.

Art. 132 of the TFEU relating to the acts of the European Central Bank and Art. 133 TFEU establishing measures for the use of the euro, do not apply)[217].

Individual Member States that belong to the Economic and Monetary Union, renounced sovereignty over the issue of money and decide on monetary policy to the European Central Bank in their constitutions. Namely, for example, Art. 88 of the Basic Law of the Federal Republic of Germany states, admittedly, in the first sentence that "the Federation creates Federal Bank as the currency and issue bank", but in the second sentence states that "the tasks and competences may be transferred within the European Union to the European Central Bank which is independent and related to the primary objective, which is to protect price stability"[218].

Basically, the constitutions of most of the countries (mainly Western ones), and in the case of the European Union — the Treaty on the Functioning of the European Union, restrict directly coin minting and issuance of banknotes, and therefore money in the narrow legal sense to the exclusive responsibility of central banks (and the ECB). There are also countries which make such a restriction at the level of an Act only. In contrast, the creation of other types of money in economic terms, i.e. mainly deposit money, but also other private money[219], is not subject to the monopoly of the central bank, and therefore also the state from a legal perspective. So now, taking into account the provisions of constitutions and in some cases the provisions of the laws, one cannot regard cryptocurrency as a threat to banknotes and coins, which are legal tender in the legal terms. However, as already indicated, in economic terms, such a threat may occur in the future. Thus, there is a clear mismatch between legal regulation and socio-economic phenomena. This mismatch becomes even more pronounced if one takes into account that although the issue monopoly of the central bank (and more broadly — the monetary sovereignty[220]) does not include the very creation of bank (deposit) money, however,

[217] See also Art. 42 of Protocol No. 4 on the Statute of the European System of Central Banks and of the European Central Bank, which is annexed to the TFEU.

[218] The Basic Law of the Federal Republic of Germany of May 23, 1949; translation by B. Banaszak, A. Malick, [in:] *Konstytucje państw Unii Europejskiej*, Warszawa 2011, http://biblioteka.sejm.gov.pl/konstytucje_swiata/ (access: October 6, 2016).

[219] In passing, one should state that the logical consequence of the division of money into banknotes and coins, which are money in the legal sense, and into the remaining money in broad economic terms, with the simultaneous use of the concept of private money as money issued by other parties than the central bank (broadly — the state), is the recognition that the so-called banking (deposit) money created by the banks when lending is private money.

[220] According to R.M. Lastra, op. cit., p. 19, monetary stability of the state is expressed in having the authority by the state in the scope of:

1) Issuing coins and banknotes, which is usually reserved only for the central bank of the country concerned (this is a classic issue monopoly)

2) Legal regulation of money, the banking system and the clearing and settlement system

3) Monetary policy i.e. in the control of money supply and interest rates, which is also assigned mostly to the central bank

the amount in circulation is controlled by the central bank as a part of formulating and implementing the monetary policy, which falls within the scope of monetary sovereignty of the state and for which the legitimacy for the central bank is included in the constitution itself. Of course, no central bank in the world (nor any government) is currently authorized to regulate the amount of cryptocurrency.

3.5.4. Cryptocurrencies and legal protection of the monetary sovereignty of the state

As already mentioned, in case of popularization of cryptocurrencies (or other electronic means of payment without the issuer), there is no situation of breaking the monopoly of the central bank to issue banknotes and coins which are legal tender in the present state of the law. However, this monopoly can have two levels of legitimacy — the constitution (e.g. in Switzerland or the United States in the case of coins) or the constitution and the treaty, such as in eurozone. Therefore, changing this state of affairs requires intervention in the highest legal act. In countries where the concept of money has not been further specified in the constitution (e.g. in Poland) or where this issue is not addressed at constitutional level at all (e.g. in the Czech Republic), there is a greater ease in modifying the monopoly of the central bank, because changing the law is enough. In addition, if the constitution generally addresses the issuance of "money", for example in the Constitution of Poland, in the case of popularization of a cryptocurrency (or other electronic means of payment without the issuer), which would begin to perform the functions of money, one may wonder whether or not the constitutional monopoly of NBP on the issuance of money has been violated in the broad economic sense. Similarly, the Constitution of the Russian Federation, where Art. 75 clearly states that "the introduction and issuance of other money in the Russian Federation is prohibited", and the general concept of "money" is used that can be interpreted in a broader economic sense[221].

The possibility to prohibit and prosecute "the introduction and issuance of cryptocurrency in the Russian Federation" is highly legitimate, because it is included in the Constitution of the Russian Federation. Russian authorities seem to realize

4) Exchange rate policy, i.e. in the control of exchange rates and determining the exchange regime, usually performed by the central bank

5) The power to impose exchange and capital controls.

[221] Of course, the authors of the Constitution of the Russian Federation have not thought about cryptocurrencies nor, it seems, even private money — this radical provision was to counteract the issuance of money by local authorities. Such situations have occurred immediately after the fall of the Soviet Union — as stated by Ł. Szul, *Omówienie Konstytucji Rosji z 1993 r.*, http://www.rosjapl.info/historia-rosji-ukrainy-zsrr/historia-i-polityka-wspolczesnej-rosji/omowienie-konstytucji-rosji-z-1993.html (access: October 6, 2016).

this[222]. And they make use of this opportunity, planning restrictions mentioned in subsection 3.2.1. In contrast, under Polish law, even in the event of a positive response to the question about the possibility of a breach (in case of popularization of cryptocurrency) of NBP monopoly, there is another, equally important question of how prevent such a breach in accordance with the applicable law. Unfortunately, there are no regulations applicable in this situation in the current Polish law. Therefore, the intervention of the legislature would be needed here, if they consider it necessary. The same is true for other countries, particularly those in which constitutions only provide for banknotes and coins (or even just coins, as in the US). Such a decision would have been, however, more political and would have to provide an answer to the question of to what extent the state may agree to restrict its monetary sovereignty by cryptocurrencies (and even other means of payment without the issuer).

3.6. Legal regulation concerning the prevention of money laundering and terrorist financing in relation to the payments using cryptocurrencies

In practice, cryptocurrencies are extensively used for money laundering, because, among others, they provide a significant anonymity (but not a full anonymity), especially when used with the TOR system, have a global reach, are easy to store, and they are very difficult to access by unauthorized persons (e.g. law enforcement) due to the capability to employ sophisticated encryption methods of the so-called wallets. Cryptocurrencies, in particular bitcoins, are a favorite means of payment for hackers[223], and criminals use them to make payments in the so-called Deep Web (Darknet), which is an online black market, where individuals pay for things such as drugs, pornography, counterfeit documents, weapons and ammunition[224].

[222] See the speeches by the Deputy Finance Minister of Russia — S. Higgins, *Russian Official: Payment Giant Qiwi's Digital Currency Idea 'Illegal'*, http://www.coindesk.com/russian-official--qiwi-digital-currency-illegal/ (access: October 6, 2016); A. Bazenkova, op. cit.

[223] See e.g. M. Romney, "Tax Returns Hacked? Alleged Ransom Asks For $1 Million In Bitcoins", *International Business Times*, September 5, 2012.

[224] See e.g. M.C. Van Hout, T. Bingham, "'Silk Road', the Virtual Drug Marketplace: A Single Case Study of User Experiences", *International Journal of Drug Policy* 24, 2013, No. 5, pp. 385–391, http://www.ijdp.org/article/S0955-3959(13)00006-6/pdf (access: October 6, 2016); Commission report of November 27, 2015 on progress in the implementation of the EU Drugs Strategy for 2013–2020 and the EU Action Plan in the field of drugs for 2013–2016, p. 11, COM(2015) 584 final; report by HM Treasury titled *UK National Risk Assessment of Money Laundering and Terrorist Financing*, October 2015, pp. 12, 82–84, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/468210/UK_NRA_October_2015_final_web.pdf (access: October 2016).

Currently, cryptocurrencies are an essential element of cybercrime[225]. To a lesser extent, they serve the financing of terrorism, which probably results from the fact that they are not yet sufficiently widespread (and after all, financing of terrorism is less frequent than money laundering)[226].

3.6.1. Recommendations and guidelines by FATF

The growing importance of cryptocurrencies in money laundering and terrorist financing has already been identified by the FATF (Financial Action Task Force)[227], which dedicated a lot of attention to it in two reports on virtual currencies — *Virtual Currencies: Key Definitions and Potential AML/CFT Risks*[228] from June 2014, and *Guidance for a Risk-Based Approach to Virtual Currencies*[229] from June 2015 (hereinafter: the guidelines of June 2015). In the first of these reports, which is a kind of a "conceptual basis (definitions)" for the second report, cryptocurrencies have been classified by FATF in the category of decentralized virtual currencies and to the category of convertible (or open) virtual currencies, i.e. those that have a value equivalent to legal tender (real currency) and can be exchanged for legal tender[230].

FATF guidelines of June 2015 addressed to legislators are of particular value, because they set the directions of interference of states in the functioning of cryptocurrency in order to counter money laundering and terrorist financing. These guidelines refer to FATF recommendations of February 2012[231] and explain how

[225] Thus, for example. INTERPOL's Cyber Research Lab (Interpol's agency) has set up its own "private" Darknet, their own "private" cryptocurrency and simulates its own marketplace in order to create a virtual "underground" criminal environment as a specific training tool in support for police investigations — see http://www.interpol.int/News-and-media/News/2016/N2016-010 (access: October 6, 2016).

[226] E.g. according to the report by Europol, terrorists of the Islamic State so far have not used bitcoins to finance their activities — see the document issued by Europol titled *Changes in modus operandi of Islamic State terrorist attacks. Review held by experts from Member States and Europol on 29 November and 1 December 2015*, The Hague, 18 stycznia 2016, p. 7, https://www.europol.europa.eu/sites/default/files/publications/changes_in_modus_operandi_of_is_in_terrorist_attacks.pdf (access: October 6, 2016).

[227] FATF (Financial Action Task Force) is an independent intergovernmental team, which develops and promotes policies to protect the global financial system and combat money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction — see more at http://www.fatf-gafi.org (access: October 6, 2016).

[228] http://www.fatf-gafi.org/publications/methodsandtrends/documents/virtual-currency-definitions-aml-cft-risk.html (access: October 6, 2016).

[229] http://www.fatf-gafi.org/publications/fatfgeneral/documents/guidance-rba-virtual-currencies.html (access: 6 października 2016).

[230] See the report titled *Virtual Currencies: Key Definitions and Potential AML/CFT Risks*, pp. 4–5. FATF uses their own definition of virtual currencies, which is given in this report.

[231] International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. The FATF Recommendations, February 2012, http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html (access: October 6, 2016).

they should be interpreted, especially in relation to the convertible virtual currencies, including cryptocurrencies (the guidelines use the notion of virtual currency payment products and services — VCPPS). The general idea promoted by FATF (expressed in paragraph 14 of the guidelines of June 2015) is such that the control of activities involving convertible virtual currencies (and therefore including cryptocurrencies) aimed at money laundering and terrorism financing was primarily directed at the so-called convertible VC nodes, and therefore the cryptocurrency "nodes", i.e. the points of intersection (crossing) of the system of virtual currencies (including cryptocurrency systems) and the regulated financial system, which constitute a kind of gateways to the regulated financial system. Whereas the users of cryptocurrencies (broadly — virtual convertible currencies), who use cryptocurrencies (convertible virtual currencies) to purchase goods and services remain outside such a control and the legal regulation concerning the prevention of money laundering and terrorist financing. In the case of cryptocurrencies, such nodes or points of intersection of the cryptocurrency systems and the regulated financial system are primarily cryptocurrency exchanges and exchange offices covered by the term *VC exchangers* — "virtual currencies exchangers" used by FATF. FATF stipulates that this kind of entities (*VC exchangers*) are covered by the regulations compatible with the FATF recommendations (i.e., FATF recommendations of 2012 construed in accordance with *Guidance for a Risk-Based Approach to Virtual Currencies* of June 2015). Moreover, FATF suggests that the states should consider extending the legal regulation aimed at preventing money laundering and terrorist financing also to entities, which only deal with sending, receiving, and storing of virtual currencies (and thus cryptocurrencies) and do not provide services of exchange to legal means of payment — this would concern both the entities defined by FATF as financial institutions and entities "designated non-financial business and profession" — DNFBPs as called by FATF. However, this kind of regulation remains outside the scope of the guidelines of June 2015, and so far FATF has not responded in detail to this suggestion. It seems that DNFBPs can include entities running websites which enable various types of gambling using cryptocurrencies. Usually participants of such games are not able to exchange cryptocurrencies to legal means of payment — thus, the entities running such games can not be regarded as "virtual currencies exchangers".

Note also that the definition of financial institution[232] used by FATF is so comprehensive that it also includes entities which provide all kinds of financial

[232] See paragraph 17 of the guidelines of June 2015. According to this, "The FATF defines a »financial institution« as any natural or legal person who conducts as a business one or more of several specified activities for or on behalf of a customer. The categories potentially most relevant to currently available VCPPS include persons that conduct as a business: Money or value transfer services (MVTS); acceptance of deposits and other repayable funds from the public; issuing and managing means of payment; and trading in foreign exchange, or transferable securities. Depending on their particular activities, decentralised VC exchangers, wallet providers, and payments

services based solely on cryptocurrencies and do not come into contact with the legal means of payment (e.g. the entities receiving contributions in cryptocurrencies or granting "loans" in cryptocurrencies). At the same time, the concept of a financial institution used by FATF also includes *VC exchangers*, and thus the cryptocurrency exchanges and exchange offices.

Although the FATF guidelines of June 2015 do not directly concern cryptocurrencies, but virtual currencies, in particular convertible virtual currencies, which, according to FATF, shall include the cryptocurrencies, one can determine the position of FATF in terms of how to interpret the FATF guidelines of 2012 in relation to particular areas of the cryptocurrencies (in particular, the operations of cryptocurrency exchanges and other financial institutions providing services using cryptocurrencies) based on the content of these guidelines. In Section III of guidelines of June 2015, FATF specifically explains how the specific FATF recommendations regarding VCPPS should be applied by individual countries and the competent authorities, and in this section FATF focuses on identifying and reducing risks associated with convertible virtual currencies (thus, the cryptocurrencies), use of licenses (permits, authorizations)/registrations, the implementation of effective supervision, ensuring effective and dissuasive sanctions and facilitation of international and national cooperation. It is about the FATF recommendation No. 1 (Assessing risks and applying a risk-based approach)[233], No. 2 (National cooperation and coordination)[234], No. 14 (Money or value transfer services), No. 15 (New technologies), No. 16 (Wire transfers), No. 26 (Regulation and supervision of financial institutions), No. 35 (Sanctions), No. 37 (Mutual legal assistance), No. 38 (Mutual legal assistance: freezing and confiscation), No. 39 (Extradition), No. 40 (Other forms of international cooperation).

In turn, FATF explains in Section IV the use of recommendations to the cryptocurrency exchanges and exchange offices (which fall under the term convertible

processors/senders, as well as other possible VC business models, may fall within one or more of these categories".

[233] E.g. in accordance with the FATF recommendation No. 1, states should require financial institutions and DNFBPs to identify, assess and take effective measures to reduce the risk of money laundering and terrorist financing related to services and products based on cryptocurrencies. Moreover, even if the state does not decide to regulate cryptocurrencies with respect to risks other than those relating to money laundering and terrorist financing, such as the risk applicable to consumer protection, prudential security and network security, the state should take action to identify and evaluate and apply the risk-based approach (RBA) to mitigate the risk related to money laundering and terrorist financing associated with cryptocurrency on the basis of the relevant FATF recommendations. Moreover, after having assessed the risk of money laundering and terrorist financing, the state must decide whether to regulate cryptocurrency exchanges and exchange offices in this respect.

[234] E.g. the application of the recommendation No. 2 (National cooperation and coordination) to cryptocurrencies means, according to FATF, establishing the appropriate international cooperation by the states (e.g. by creating appropriate interagency working groups), as well as to make their own efforts to assess and control risk of money laundering and terrorist financing using cryptocurrencies (details are included in paragraphs 29–31 of the guidelines).

VC exchangers) and other types of entities acting as nodes, where the activity based on convertible virtual currencies (and thus cryptocurrencies) intersects with the regulated financial system. It is about the use of the following recommendations: No. 1 (Assessing risks & applying a risk-based approach), No. 10 (Customer due diligence (CDD)), No. 11 (Record-keeping), No. 14 (Money or value transfer services — in the scope of legal regulation of actions applicable to MVTS[235]), No. 15 (New technologies — in the scope of identification and reduction of the risks associated with new technologies), No. 18 (Internal controls and foreign branches and subsidiaries — in terms of AML/CFT program requirements), No. 20 (Reporting of suspicious transactions — in respect of the obligation to report suspicious transactions).

3.6.2. Prevention of money laundering and terrorist financing in relation to the payments using cryptocurrencies in the law of European Union, Poland and U.S.

Despite the FATF suggestions and demands made by some Member States[236], the European Union has not formally imposed obligations related to the prevention of money laundering and terrorist financing on cryptocurrency exchanges and exchange offices, however, it must be emphasized that the relevant legislative work has already begun[237]. This issue has not been clearly resolved in Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on prevention of the use of the financial system for money laundering and terrorist financing[238] (also known as the Third Directive), which is understandable, considering that cryptocurrencies are a relatively new way of payment. However, it is surprising that in the new directive of the European Parliament and of the Council

[235] MVTS — *Money value transfer service*.

[236] E.g. French authorities stipulate the harmonization of legal regulations relating to the exchange of virtual currencies in the European Union, as well as at the international level — see the report titled *Regulating Virtual Currencies. Recommendations to prevent virtual currencies from being used for fraudulent purposes and money laundering*, czerwiec 2014, http://www.economie.gouv.fr/files/regulatingvirtualcurrencies.pdf (access: October 6, 2016). This report has been prepared by Virtual Currencies Working Group set up by Tracfin (the French Financial Intelligence Unit).

[237] The application of July 5, 2016 — Directive of the European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for money laundering or terrorist financing and amending Directive 2009/101/EC, COM/2016/0450 final — 2016/0208 (COD).

[238] (OJ. EU L 309 of 11/25/2005, as amended. Implementing measures of the Directive have been laid down by the Commission Directive 2006/70/EC of August 1, 2006 regarding the definition of a politically exposed person and the technical criteria for simplified rules for due diligence towards the customer, as well as exclusions due to a financial activity conducted on an occasional or very limited basis (OJ. EU L 214 of 08/04/2006, as amended).

2015/849/EU of 20 May 2015 on prevention of the use of the financial system for money laundering or terrorist financing[239] (the so-called Fourth Directive), the EU legislator has not included clear provisions in this regard. One can, however, make an appropriate interpretation of the provisions of the Fourth Directive, taking into account the recommendations and guidelines of FATF. However, a literal interpretation (the wording) limits such an interpretation, carried out according to the FATF guidelines. Namely, according to Art. 3 paragraph 2 letter a) of Directive 2015/849/EU, the "financial institution" means: an undertaking other than a credit institution which carries out one of the activities listed in paragraphs 2–12 and in paragraphs 14 and 15 of Annex I to the Directive of the European Parliament and of the Council 2013/36/EU, including the activities of currency exchange offices (the wording is much like Art. 3 paragraph 2 a) of the Third Directive. There is no doubt that the activities listed in Annex I to Directive 2013/36/EU are carried out in legal means of payment (the annex is an integral part of Directive 2013/36/EU); besides, the very concept of "currency exchange" refers to an entity which carries out the exchange of one kind of legal tender for other legal means of payment. Hence, the definition of a financial institution in Art. 3 paragraph 2 a) of both Third and Fourth Directives shall not apply to cryptocurrency exchanges and exchange offices. Basically, this definition has a much narrower scope than the definition of a financial institution stipulated by FATF in paragraph 17 of the guidelines of June 2015 and does not include entities which provide services in cryptocurrencies, even if these services are similar to the activities listed in Annex I to Directive 2013/36/EU. Therefore the intervention of the legislature is necessary in order to clearly include cryptocurrency exchanges in the catalog of obligated entities.

On the other hand, Directive 2015/849/EU undoubtedly applies to entities running Websites which allow gambling using cryptocurrencies. According to Article 2 paragraph 1 point 3 f), this Directive is applicable to such an obligated entity, as a service provider in the field of gambling, and it seems that the Member States, pursuant to paragraph 2 of this article may exclude such entities, in whole or in part, from the scope of national measures transposing the Directive 2015/849/EU based on the disclosed low risk posed by nature and, where applicable, the scale of the operation of such services[240].

[239] Directive of the European Parliament and of the Council 2015/849/EU of May 20, 2015 on prevention of the use of the financial system for money laundering or terrorist financing, amending the Regulation of the European Parliament and of the Council No. 648/2012/EC and repealing the Directive of the European Parliament and of the Council 2005/60/EC and Directive 2006/70/EC (OJ. EU L 141 of 06/05/2015). Directive 2015/849 repeals Directives 2005/60/EC and 2006/70/EC with effect from 26 June 2017.

[240] According to Art. 3 paragraph 10 of Directive 2015/849/EU, "gambling services" means services related to placing a stake with monetary value in games of chance, including those where specific skills are important, such as lotteries, casino games, poker games and mutual betting, provided locally or in any way remotely, using electronic means or any other technology to facilitate communication and at the individual request of the recipient of services. Therefore, undoubtedly,

In Poland cryptocurrencies have already been recognized by the General Inspector of Financial Information[241]. However, there is still no legislation specifically relating to the use of cryptocurrencies for money laundering and terrorist financing. In particular, cryptocurrency exchanges and exchange offices are not classified as obligated institutions within the meaning of Art. 2 paragraph 1 of the Act of November 16, 2000 on counteracting money laundering and financing of terrorism[242] (hereinafter: CMLFT). It is true that, in accordance with Article 2 paragraph 1 p) of CMLFT, entities operating in the field of currency exchange are the obligated institution, but cryptocurrencies are not currencies neither within the meaning of the Foreign Exchange Act, nor any other Polish Act. Such an interpretation is consistent with EU law, because, as already mentioned, also on the basis of Directives 2006/50/EC and 2015/849/EU, cryptocurrency exchanges and the exchange offices are not obligated institutions (although currency exchange offices, or more broadly — financial institutions, are the obligated entities). However, taking into account the FATF guidelines, it should be postulated to appropriately amend both the EU regulation, and in consequence, the Polish on, so that cryptocurrency exchanges and exchange offices are formally recognized as obliged entities. This postulate has a high probability of implementation, because now (i.e. in October 2016), as already mentioned there is the legislative process taking place on a draft directive amending Directive 2015/849. It is expected that this project will include cryptocurrency exchanges and exchange offices, as well as suppliers of virtual currency accounts in the directory of obligated entities.

Until the introduction of the appropriate regulation, there is nothing to prevent the cryptocurrency exchanges and exchange offices to voluntarily impose obligations of the obligated entity on themselves. In addition, it should be noted that each cryptocurrency user (including natural persons who do not do business, and use cryptocurrencies to purchase goods and services) may incur criminal liability provided for in Article 299 § 1 of the Criminal Code regulating the crime of money laundering. This is a consequence of the recognition of cryptocurrencies as property rights. This regulation is more applicable if we accept that cryptocurrency are means of payment in the light of the provisions of the Criminal Code.

---

these services can be provided over the Internet, web pages and using cryptocurrencies. Directive 2005/60/EC contains neither definition nor the concept of gambling services, and although it uses the term casino (which is applied in accordance with Art. 2 paragraph 1 point 3 f), taking into consideration Art. 10 of Directive 2005/60/EC, one can reasonably doubt whether it applies to entities which organize gambling on the web paid only through cryptocurrency.

[241] See the report of the General Inspector of Financial Information on the implementation of the Act of November 16, 2000 on counteracting money laundering and financing of terrorism in 2014, Warsaw, March 2015, p. 20, http://www.mf.gov.pl/documents/764034/1223641/20150414_sprawozdanie+z+dzialalnosci+GIIF+2014.pdf (access: October 6, 2016).

[242] Journal of Laws of 2010, No. 46, item 276 as amended. These obligations can be divided into three basic groups — registration, information, and the obligation to suspend a transaction and block the account.

Federal and state regulations for payment transactions in the U.S. focus on counteracting financial crime and consumer protection (federal and state "Money Transmission Laws"[243]), as well as bank secrecy and counteracting money laundering (Bank Secrecy Act[244] — BSA). Of particular importance is the definition contained in the federal law, in § 1960 Title 18 U.S. Code[245] of the term "money transmitting", which includes the transfer of funds to the public, by anyone and any means, including without limitation domestic or foreign transfers, carried via wire, check, draft, fax or courier[246]. Clearly, this definition applies to payments made using cryptocurrencies, so this approach is much broader than that which can be observed in the legislation of the European Union. Federal authorities involved in counteracting money laundering and terrorist financing — Financial Crimes Enforcement Network (FinCEN)[247] — issued a special "guidance"[248], which refers to the application of FinCEN regulation to persons administering virtual currencies, persons exchanging virtual currencies and the users of virtual currencies. FinCEN adopts such a broad definition of virtual currencies[249], that it also includes cryptocurrencies, however, the guidance applies only to convertible virtual currency that is, according to FinCEN, such a kind of virtual currency, which either has an

[243] For example: http://www.dbo.ca.gov/Licensees/money_transmitters/ (access: October 6, 2016), http://www.dbcf.state.ms.us/documents/cons_finance/7515MoneyTranAct2011.pdf (access: 10/06/2016); see also http://www.communitycurrencieslaw.org/financial-and-banking-laws/#State_Money_Transmission_Laws (access: October 6, 2016).

[244] https://www.fincen.gov/resources/statutes-regulations/fincens-mandate-congress (access: October 6, 2016).

[245] http://uscode.house.gov/browse.xhtml (access: 6 października).

[246] „The term »money transmitting« includes transferring funds on behalf of the public by any and all means including but not limited to transfers within this country or to locations abroad by wire, check, draft, facsimile, or courier" — zob. https://www.law.cornell.edu/uscode/text/18/1960 (access: October 6, 2016).

[247] FinCEN is the Office of the US Treasury Department. FinCEN Director is appointed by the Secretary of the Treasury and reports to the undersecretary of the treasury for terrorism and financial intelligence. The mission of FinCEN is to protect the financial system, counteract money laundering and promote national security by conducting financial intelligence and coordinating the activities of financial authorities.

[248] Guidance by FinCEN titled *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies* of March 18, 2013 (FIN-2013-G001). FinCEN is serious about its recommendations and monitors the cryptocurrency market, also taking into account the latest innovations similar to cryptocurrencies, where the system is not fully decentralized — for example, FinCEN punished the company Ripple Labs Inc, because "Ripple Labs willfully violated several requirements of the Bank Secrecy Act (BSA) by acting as a money services business (MSB) and selling its virtual currency, known as XRP, without registering with FinCEN, and by failing to implement and maintain an adequate anti-money laundering (AML) program designed to protect its products from use by money launderers or terrorist financiers" — see https://www.fincen.gov/news_room/nr/pdf/20150505.pdf (access: October 6, 2016).

[249] "In contrast to real currency, »virtual« currency is a medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency. In particular, virtual currency does not have legal tender status in any jurisdiction".

equivalent value in real currency[250], or is a substitute for real currency. FATF uses the term "convertible virtual currency" in a similar sense in its recommendations. FinCEN guidelines refer to one of the types of convertible virtual currencies — decentralized convertible virtual currency, which clearly includes cryptocurrencies, and states that the person who creates the units of such currencies (and therefore the units of cryptocurrencies) and uses them subsequently to acquire real or virtual goods and services, is a user of convertible virtual currencies and is not a money transmitter under U.S. law[251]. Therefore, the regulations aimed at counteracting money laundering and financing of terrorism contained in the Bank Secrecy Act do not apply to such a person. A year later, in the next document[252], FinCEN already explains simply — a user who "mines" bitcoins *and uses bitcoin solely for [...] own purposes*, and not for the benefit of others, does not run *money services business — MSB* and FinCEN regulation, and, therefore, the provisions on counteracting money laundering and terrorist financing do not apply[253]. Of course, such regulations do not apply to a person who obtains cryptocurrencies in another way (e.g. buying them) and then purchases goods and services in his or her own name (this is the user). FinCEN opinion is that when the user purchases goods or services for mined cryptocurrency (bitcoins), paid to a third party, acting on behalf of the seller or creditor, there may constitute the situation of "money transmission" and the rules designed to counteract money laundering and terrorist financing may apply. Similarly, according to FinCEN, "money transmission" occurs when the person who creates the units of decentralized virtual currency sells it to another person for the "real currency" or its equivalent, and is engaged in the transmission to another location — thus becomes the money transmitter. The person who accepts cryptocurrency from someone and transmits a virtual currency is a "money transmitter" and the entity named the "exchanger" by FinCEN[254].

FinCEN makes its position more detailed in explanations, stating that the "miner", who uses mined bitcoins for his or her own purposes, benefit and not for the benefit of others, will not be subject to FinCEN regulations, because these bitcoin transactions will not be the transmission of funds in terms of the regulations used by FinCEN. It is about the purchase of goods and services on account of the miner, repayment of miner's obligations or transfer of bitcoins to shareholders if the

[250] "Real currency" according to FinCEN are coins or banknotes being the money of the United States or any other country, recognized as legal tender, being in circulation and those which are used and accepted as a medium of exchange in the issuing country.

[251] FinCEN guidance titled *Application of FinCEN's Regulations*..., p. 5. According to Bank Secrecy Act, "money transmitter" is "a person that provides money transmission services, or any other person engaged in the transfer of funds".

[252] Explanations by FinCEN titled *Application of FinCEN's Regulations to Virtual Currency Mining Operations* of January 30, 2014 (FIN-2014-R001).

[253] It is about purchasing goods and services in someone's own name, repaying the obligations, and if the user is a company, it is also about the transfer of "mined" cryptocurrency to shareholders.

[254] Guidance titled *Aplication of FinCEN's Regulations*..., p. 5.

miner is a company. This also applies to the exchange of cryptocurrency to legal means of payment by the miner, if the miner makes such an exchange for his or her own purposes, benefit and not for the provision of services for another person[255]. According to FinCEN, any transfers to third parties on behalf of sellers, creditors, owners and contractors involved in these transactions should be examined, because they can be a money transmission and thus can require the application of regulations aimed at preventing money laundering and terrorist financing[256].

FinCEN states that the virtual currency can not be regarded as a "currency" within the meaning of the Bank Secrecy Act, because it is not legal tender. This means that the person who accepts real currency for virtual currency and *vice versa*, cannot be regarded as a "dealer in foreign exchange" (the equivalent of a currency exchange office) as set forth in the rules applied by FinCEN[257]. Thus, the cryptocurrency exchanges and exchange offices will not be regarded a "dealer in foreign exchange" by FinCEN and from this perspective, there are no differences in the regulations in the U.S. and Europe. Also on the basis of Third and Fourth Directives, cryptocurrency exchanges and exchange offices are not currency exchange offices and thus are not obligated entities as set forth in these directives. However, the use of the broad definition of the concept of money transmission in the U.S. regulation causes the cryptocurrency exchanges and exchange offices may have obligations to properly record and report transactions (as well as the obligation to register) resulting from the need to counteract money laundering and terrorist financing. Although the cryptocurrency exchanges and exchange offices are not categorized as "dealers in foreign exchange" according to the provisions of the Bank Secrecy Act, FinCEN will consider them a so-called "exchanger".

According to the guidance, the "exchanger" is a person running a business in the exchange of virtual currency for real currency, funds or other virtual currencies. According to FinCEN, the entity called the "exchanger", which receives and transmits convertible virtual currency, or buys and sells, is a money transmitter and subject to FinCEN regulations (including those aimed at counteracting money laundering and financing of terrorism) unless the relevant exclusion applies (the regulation 31 CFR § 1010.100(ff)(5)(ii)(a)–(F) provides for six situations in which an entity, despite the transfer of currency, funds or the value replacing the currency is not considered a money transmitter)[258].

Thus, the cryptocurrency exchanges and the exchange offices undoubtedly perform "money transmitting" and their activities will be "money services business — MSB" and they will be considered the "exchanger", and thus be subject to

[255] Explanations by FinCEN titled *Application of FinCEN's Regulations to Virtual Currency Mining Operations*, p. 3.

[256] Ibid.

[257] Guidance titled *Aplication of FinCEN's Regulations*..., p. 5.

[258] Ibid., p. 3.

FinCEN regulations, if the foregoing exclusions do not apply to them[259]. This is a fundamental difference in relation to the legal regulation in the European Union, which currently (i.e. in mid-2016) does not create the possibility of extending the regulation concerning the counteracting money laundering and terrorist financing to cryptocurrency exchanges. Undoubtedly, U.S. law is closer to the FATF guidelines with regard to cryptocurrency exchanges and exchange offices.

3.7. Taxation of cryptocurrencies and other electronic means of payment without the issuer

3.7.1. Income taxes

From the perspective of the cryptocurrency system and the opportunities of its use, we should distinguish between income earned in cryptocurrency and the income derived from cryptocurrency exchange for legal tender. It seems that no state legislation explicitly indicates this kind of source of income, but as a rule, the catalog of these sources is open (as this is the case in e.g. Polish law) or, as in the case of *common law* systems, one can make the appropriate interpretation of judgements[260].

The user can obtain legal profits in cryptocurrency in two ways — either legally receiving cryptocurrency from another user, or "mining" it. In both cases, the value of the property is increased by the value of cryptocurrency, which should be treated as property also for tax purposes[261]. In terms of the income tax, as a tax on the increment of pure wealth, it should, at least theoretically, give rise to revenue, and therefore the tax liability. There is no other possibility than determining this income in a legal means of payment, accepted by the tax authorities of a particular country. Therefore, there is the problem of the conversion of cryptocurrency value on a given day. It seems logical that it should be the market value of cryptocurrency, however, its determination may not be easy due to the lack of a single

[259] See also the content of FinCEN explanations titled *Application of FinCEN's Regulations to Virtual Currency Software Development and Certain Investment Activity* of January 30, 2014. (FIN2014-R002), p. 4.

[260] See: T. Slattery, "Taking a Bit Out of Crime: Bitcoin and Cross-Order Tax Evasion", *Brooklyn Journal of International Law* 39:2, 2014, pp. 846 ff.

[261] Such an approach prevails in the U.S. law — see e.g. T.R. Koski, "Bitcoin — Tax Planning in the Uncertain World of Virtual Currency", *Practical Tax Strategies* December 2014, pp. 256 ff.; according to Internal Revenue Service (IRS), "For federal tax purposes, virtual currency is treated as property" — see also IRC document titled *Publication 525 — Introductory Material*, https://www.irs.gov/publications/p525/ar01.html (access: October 6, 2016).

official exchange rate, a large number of cryptocurrency exchanges and globality of cryptocurrency systems[262].

Cryptocurrencies are not financial instruments, and most of all, they are not securities and, therefore, the revenue gained by the user from the sale of cryptocurrencies for the price higher than its cost should not be treated as income from the sale of securities[263].

Cryptocurrency is to serve primarily the payment function — this is a means of payment which is alternative to legal tender. Its receipt should therefore be considered equally to the receipt of legal tender under the law governing income tax. As already indicated, the moment of "receipt" of cryptocurrency is the moment to save the transaction by the system in blockchain. For example, according to the Art. 11 paragraph 1 of Polish law on income tax from natural persons[264] revenues include the monetary value received or made available to the taxpayer in the calendar year. However, according to Art. 12 paragraph 1 point 1 of Law on income tax from legal persons[265] revenues include the monetary value received. As indicated in the doctrine, the concept of money value is not defined by the legislators, but it can be assumed that "It is a kind of financial assets that can be used to regulate the monetary obligations as a substitute for money, even though they are not money. Monetary values express the existence of the property right of a certain value. The use of monetary values instead of money requires the consent of the creditor"[266]. The undersecretary of state at the Ministry of Finance gave a similar answer of October 27, 1999 to a parliamentary question no. 1093 on the clarification of the notion of "monetary value", used in the laws on income tax from individuals and legal entities[267]. Thus it seems that the term "monetary value" used in the Polish laws on income tax from natural and legal persons can include cryptocurrencies. However, the Directors of Tax Chambers assume that the revenue from the sale of

[262] According to the IRS, this is about the market value of cryptocurrency on the date of receipt by the user — see Internal Revenue Bulletin: 2014-16, April 14, 2014, https://www.irs.gov/irb/201416_IRB/ar12.html (access: October 6, 2016) IRS gives more detail on its position in another document, writing about "The fair market value of virtual currency (such as Bitcoin)" — see *Publication 525 — Introductory Material*, https://www.irs.gov/publications/p525/ar01.html (access: October 6, 2016).

[263] See the comments provided in subsection 3.1.3.

[264] Personal Income Tax of July 26, 1991 (Journal of Laws of 2012, item 361 as amended).

[265] Corporate Income Tax Act of February 15, 1992 (Journal of Laws of 2014, item 851 as amended).

[266] J. Marciniuk, "Komentarz do art. 11 u.p.d.o.f.", [in:] *Podatek dochodowy od osób fizycznych. Komentarz*, Warszawa 2015. The author gives examples of monetary values: bills of exchange, checks, other securities entitling to receive certain amounts of money and vouchers. Cryptocurrencies belong to the same group of means of payment, only that these electronic means of payment and do not have the issuer.

[267] http://orka2.sejm.gov.pl/IZ3.nsf/main/6B25E0FB (access: October 6, 2016).

previously purchased bitcoins is income from property rights as set forth in Art. 18 of the Law on income tax from natural persons[268].

An important challenge for the tax authorities of the country concerned is to establish a consistent means of interpreting laws regulating income taxes, so that taxpayers have confidence that the provisions used by the tax authority apply in the event of revenue in cryptocurrency. The problem is to determine:

— The source of income

— The moment of inception of revenue

— The types of costs of revenue that can be deducted from income

— The method of determining the amount of income in a legal means of payment.

Perhaps the intervention of the legislators is necessary in this regard. The lack of clarity about the correct way to interpret the law may further hinder, or even prevent the tax authorities to effectively determine whether tax fraud or actions aimed at tax evasion took place in a given case.

3.7.2. Value added tax (VAT)

In the case of VAT, there are doubts related to such fundamental issue as fiscal and legal qualification of transmitting the cryptocurrency to the other party. Such action can be considered the provision of services, or making payments using other means of payment than legal tender. Certainly it will not be a supply of goods, because cryptocurrency is not a commodity within the meaning of VAT. According to Art. 14 paragraph 1 of Directive 2006/112/EC of November 28, 2006 on the common system of value added tax[269], the „supply of goods" means the transfer of the right to control property as owner, and cryptocurrency is not a thing in accordance with the provisions of the civil law (also, it is not electricity, gas, thermal or cooling energy nor is it alike; is also not a share in the real estate or a property right — see Art. 15 of Directive 2006/112/WE). The first approach, according to which the transfer of cryptocurrency is the provision of services, is closer to the linguistic interpretation. According to Art. 24 paragraph 1 Directive 2006/112/EC "provision of services" shall mean any transaction which does not constitute a supply of goods. Therefore, if the transmission of cryptocurrencies is not a supply of goods, it is a provision of services — and usually, such was also

[268] Director of Tax Chamber in Poznań in individual interpretation of October 2, 2014 (ILPB2/415-741/14-2/TR), largely duplicating the contents of individual interpretation of June 26, 2014, issued by the Director of the Tax Chamber in Warsaw (IPPB1/415276/14-4/EC), states that "for tax purposes, revenue derived from the sale of previously purchased bitcoin currency is income from property rights as set forth in Art. 18 of the Law on income tax from natural persons".

[269] (OJ. EU L 347 of 12/11/2006 as amended.

the position of the tax authorities[270] adopted before the judgement of the Court of Justice of the European Union of October 22, 2015 in Case C-264/14 Skatteverket vs. David Hedqvist (the verdict is described later in this paper). Except that second approach, consisting of the recognition of the transmission of cryptocurrency as the payment using a different means of payment than legal tender, better reflects the function and the point to use cryptocurrency. All the more, the parties usually agree in the contract that payment using cryptocurrency leads to the cancellation of debt, and therefore has the same effect as using a legal tender. It is very important for the taxpayer that by adopting such an approach, debt cancellation to contractors, as well as the settlement of obligations by one of the parties using cryptocurrency (e.g. bitcoins) will not bring about consequences for the payer (debtor) for the purposes of VAT, as it does not constitute a supply of goods or provision of services and will not belong to the catalog of activities subject to VAT referred to in Art. 5 paragraph 1 of the Act on tax on goods and services[271] (or, from the EU perspective, referred to in Article 2 paragraph 1 of Directive 2006/112/WE)[272].

It is worth quoting the position took by Advocate General Kokott in her opinion of October 24, 2013 in the case Granton Advertising BV vs. Inspecteur van de Belastingdienst Haaglanden/kantoor Den Haag (C-461/12). It did not concern cryptocurrencies, but the special discount cards. Advocate General stated in grounds 41: "In my opinion, the point is that the rights, which are treated in a similar way to money in trade, should be regarded in terms of VAT as handing in money itself. Undoubtedly, handing in money is not taxed as such, but it only represents the mutual performance for the taxable provision, either for the reason that it is not about the supply of goods or provision of service as set forth in Art. 2 paragraph 1 of the

[270] See, e.g. the individual interpretation of the Director of the Tax Chamber in Katowice dated June 21 2013 IBPP2/443-258/13/ICz and of July 10, 2014, IPPB5/423-397/14-4/MW. A different position has been taken by the Director of the Tax Chamber in Poznań in the individual interpretation of January 8, 2014, http://interpretacje-podatkowe.org/wierzyciel/ilpp1-443-910-13-2-awa (access: 10/06/2016). The assumption that payment using cryptocurrency is a service leads to the taxation of the purchase of goods and services using cryptocurrency in the same way as a barter — see e.g. the individual interpretation by the Director of the Tax Chamber in Katowice dated June 21, 2013 or the position taken by the Australian Taxation Office in a letter entitled *Tax treatment of crypto--currencies in Australia — specifically bitcoin*, https://www.ato.gov.au/General/Gen/Tax-treatment--of-crypto-currencies -in-Australia---specifically-bitcoin/ (access: 10/06/2016).

[271] The Act of March 11th, 2004 on Goods and Services Tax (Journal of Laws of 2011, No. 177, item 1054 as amended), hereinafter GST.

[272] See the individual interpretation by the Director of the Tax Chamber in Poznań dated January 8, 2014, http://interpretacje-podatkowe.org/wierzyciel/ilpp1-443-910-13-2-awa (access: October 6, 2016), according to which "debt cancellation contractors, as well as the settlement of obligations by the applicant using bitcoin will not bring about consequences to the Company for the purposes of VAT, because it does not constitute a supply of goods or provision of services and will not belong to the catalog of activities subject to VAT referred to in Art. 5 paragraph 1 of the Goods and Services Tax Act. J. Prokurat, "Podatkowe aspekty obrotu wirtualnymi walutami", *Przegląd Podatkowy* 2015, No. 3, pp. 24 ff.

Sixth Directive, or for the reason that it is exempt from taxation under Article 13 Part B paragraph d) of Section 4 of the Directive"[273].

Article 13 Part B point d) paragraphs 3 and 5 of the Sixth Directive 77/388/EEC[274] currently corresponds to Art. 135 paragraphs 1 d)–f) of Directive 2006/112/EU, which states that "Member States shall exempt the following transactions: […] d) transactions, including agency, concerning deposit accounts, current accounts, payments, transfers, debts, checks and other negotiable instruments, excluding debt collection; e) transactions, including agency, concerning currency, banknotes and coins used as legal tender, with the exception of banknotes and coins being collectors' items, which are considered to mean coins made of gold, silver or other metals, as well as banknotes which are not normally used as legal tender or coins of numismatic value only; f) transactions, including agency, but excluding the storage and management of shares, interests in companies or associations, bonds and other securities, excluding documents establishing title to goods, and the rights or securities referred to in Art. 15 paragraph 2 […]". Therefore, it is essential for payments made using cryptocurrency to answer the question of whether such a payment is subject to Art. 135 paragraph 1 d)–f) of Directive 2006/112/EU, or in other words — whether it is exempt from VAT. So far, the European Court of Justice (ECJ) has not answered directly to such a question, but in the judgement of October 22, 2015 in the case C – 264/14 Skatteverket vs. David Hedqvist[275] ruled that under the provisions of Directive 2006/112/EC the exchange of bitcoins for legal tender is the service and subject to an exemption under Article 135 paragraph 1 e) of Directive 2006/112/EC[276]. However, the reasoning of the Court and arguments raised may have wider application and enable to resolve doubts as to the applicability of Article 135 paragraph 1 e) of Directive 2006/112/EC in the case of any

[273] „in my view, such instruments are rights which are regarded in the course of trade as being similar to money and which are to be treated for VAT purposes in the same way as payments of money. Payments of money are admittedly not taxed as such, but are rather simply the consideration for a taxed supply, either because they are neither a supply of goods nor a supply of services within the meaning of Article 2(1) of the Sixth Directive, (21) or because they are non-taxable by virtue of Article 13(B)(d)(4) of the Sixth Directive".

[274] Sixth Council Directive of May 17, 1977 on the harmonization of the laws of the Member States relating to sales taxes — common system of value added tax: uniform basis of assessment (OJ. EU L 145 of 06/13/1977 as amended). This directive is currently no longer in force — it was repealed on December 31, 2006 by the Directive 2006/112/EC.

[275] ECLI:EU:C:2015:718. By mid-January 2016, the judgement has not been published in the Court Reports, but it is available on the website http://curia.europa.eu/ (access: October 6, 2016).

[276] In the conclusion of the judgement, the Court stated that: "1) Art. 2 paragraph 1 c) of the Council Directive 2006/112/WE shall be interpreted as meaning that transactions, such as in the one in the main proceedings, consisting of exchange of traditional currency to the units of virtual currency »bitcoin« and vice versa, made by paying the amount corresponding to the profit margin resulting from the difference between the price at which a trader buys currency, and the price at which a trader sells it to customers, constitute a paid provision of services within the meaning of this regulation.

transaction using cryptocurrency (and not only to the exchange of cryptocurrency for legal tender), and above all in the case of purchase of goods and services for cryptocurrency. Namely, in paragraph 46 of the Explanatory Memorandum to this judgement, the Court observed that "as the Advocate General stated in paragraphs 31–34 of the testimony[277], different language versions of Art. 135 paragraph 1 e) of VAT Directive do not allow to conclude unequivocally whether this regulation applies only to transactions involving traditional currencies, or whether it also concerns transactions relating to another currency". Further, the Court states that "in the event of language differences one cannot determine the scope of the phrase in question solely on the basis of a literal interpretation. This expression has to be interpreted in the context in which it is used, and in the light of the objectives and systematics of the VAT Directive (see judgements: Velvet & Steel Immobilien, C-455/05, EU:C:2007:232, paragraph 20 and case law cited; Commission/Spain, C-189/11, EU:C:2013:587, point 56). As pointed out in paragraphs 36 and 37 of this judgement, the exemptions provided for in Art. 135 paragraph 1 e) of VAT Directive in particular remedy the difficulties associated with determining the tax base and the amount of deductible VAT, which arise in the taxation of financial transactions". Finally, paragraph 49 of the grounds of the Explanatory Memorandum, the Court expressly qualifies the payment in cryptocurrency within the category of "financial transaction", stating that "transactions involving non-traditional currencies, that is, other than money that are legal tender in one or more countries, if the currencies have been accepted by parties to the transaction as an alternative means of payment to the legal means of payment and their only purpose is the function of means of payment, represent financial transactions". In addition, the Court confirmed the approach presented in this paper in paragraph 51, arguing that "it is undisputed in the main proceedings that the only purpose of virtual currency "Bitcoin" is the function of means of payment, and it is for this purpose accepted by some entrepreneurs."

In summary, the ECJ judgment of October 22, 2015. Case C-264/14 Skatteverket vs. David Hedqvist settles the issue of VAT taxation of transactions using cryptocurrencies in the Member States of the European Union. The supply of goods or provision of service for which payment is made in cryptocurrency, will be in principle subject to VAT, while the "transfer" of cryptocurrency, or payment using cryptocurrency, should be treated as payment with a legal tender based on the

[277] Art. 135 paragraph 1 e) of the Directive 2006/112/WE shall be interpreted as meaning that providing services, such as the ones in the main proceedings, consisting of exchange of traditional currency to the units of virtual currency "bitcoin" and vice versa, made by paying the amount corresponding to the profit margin resulting from the difference between the price at which a trader buys currency, and the price at which a trader sells it to customers, are transactions exempt from VAT within the meaning of this regulation. Article 135 paragraph 1 d) and f) of Directive 2006/112 shall be interpreted as meaning that such services are not included within the scope of these regulations".

Directive 2006/112/EC, and thus should be exempt from VAT under the national rules implementing Article 135 paragraph 1 e) of this Directive.

We should also emphasize the position of Advocate General stated in paragraphs 13–15 of the opinion of July 16, 2015, in case C-264/14 and constructed based on the judgment in case First National Bank of Chicago (C-172/96)[278], which judgment also has been referred to by the Court when ruling on case C-264/14. Namely, the Court stated in the judgment that the transfer of currency is neither a supply of goods nor provision of services. According to the Advocate General, the Court had no doubt that the transfer of means of payment as such does not constitute an event giving rise to VAT taxation, "to the contrary, in principle it may be only the mutual performance for the tax benefit, because VAT is a tax on the final consumption of goods." Taking into account the postulate of the Advocate General stated in paragraph 15 of his Opinion, in order to apply what applies to legal means of payment to other means of payment, one should postulate that the payment in cryptocurrency (understood as making w new entry in the blockchain), or simplifying the "transfer" of cryptocurrency for a service or goods, should not give rise to tax liability at all based on VAT regulations. From this perspective, there is no need for the application of the exemption provided for in Art. 135 paragraph 1 e) of Directive 2006/112/EC. Of course, the supply of goods or provision of a service covered by the payment in cryptocurrency may be subject to VAT.

Judgment of the CJEU in case C-264/14 Skatteverket vs. David Hedqvist and the Opinion of Advocate General in that case are therefore groundbreaking and can standardize the taxation of transactions paid in cryptocurrencies not only in the European Union (and EEA) but also on a global scale — worldwide.

3.7.3. The problem of using cryptocurrencies for tax evasion[279]

Tax savings, tax planning, and tax avoidance are generally licit actions (especially concerning the tax law), while tax evasion is always an illegal action, contrary to the tax law, which constitutes a "direct violation of the tax law." There is a particular category of tax evasion — tax fraud, which is generally defined as the intentional tax evasion[280].

[278] The judgment of July 14, 1998 in case C-172/96 Commissioners of Customs & Excise vs. First National Bank of Chicago (EU:C:1998:354), Court Reports 1998 I–04387.

[279] This section is based on the article by W. Srokosz, "The Use of Cryptocurrencies for Tax Evasion and Tax Fraud", [in:] *Tax Law vs Tax Frauds and Tax Evasions. Non-conference Proceedings of Scientific Papers*, ed. V. Babcak, A. Romanowa, I. Vojnikowa, vol. 2, Kosice 2015, pp. 253–263.

[280] P. Pietrasz, *Opodatkowanie dochodów nieujawnionych*, Warszawa 2007, p. 46 and the references cited.

Anonymity of the transaction, decentralization of the system and the ease of hiding the private key undoubtedly predispose cryptocurrencies to hiding income obtained from illegal sources, followed by its introduction into the legal trade. In this case, tax fraud and tax evasion are often associated with money laundering.

It should be emphasized that currently, due to little popularization of cryptocurrencies (compared to other payment methods, such as e.g. credit cards, bank transfers), and also because of still relatively small (or the volume) capitalization of cryptocurrencies, it is difficult to imagine significant tax fraud when using them[281]. However, the cryptocurrency market is growing and one cannot exclude their larger (and even violent) popularization in the coming years, which means that their role in tax evasion, and in particular in tax fraud may increase[282].

Due to the fact that there is no one central entity managing the entire network in the cryptocurrency system, there is no one responsible before state authorities for the possible use of the system for tax fraud and tax evasion. There is no entity, to impose upon an obligation to disclose the transactions made by users using cryptocurrencies to authorities. The exceptions are the cryptocurrency exchanges and exchange offices — analyzing the transactions carried out by them, the tax authorities can obtain information about the exchange transactions made by their customers. However, regulations imposing the obligation on such exchanges and exchange offices to determine the identity of their clients for tax purposes would be necessary here. Currently, there are generally no such regulations, although the regulations counteracting money laundering, already mentioned in section 3.6.2, are of growing importance. The need for such regulation results from the fact that the cryptocurrency system is anonymous to a large extent, though this is not a full (absolute) anonymity — transactions are recorded in a publicly accessible blockchain, and the user can be identified by the so-called. IP. Of course, the anonymity of cryptocurrencies may attract people who do not want the transactions they do to be controlled by tax authorities. Also note that advanced cryptocurrency users can also mask their identities by changing wallets (and thereby nicks), changing public keys (besides, e.g. creators of the bitcoin system recommend changing the public key after each transaction), and finally hiding their real IP, for example using TOR.

It should also be emphasized, because of the importance of the control over the private key and keeping it secret from third parties, that in practice tax inspection authorities will need to know the private key to effectively take control of a certain amount of cryptocurrency (i.e. over the property, which has a certain value). It is hard to imagine something as easy to hide and protect from the tax authorities, as the password to the private key required to use cryptocurrency.

---

[281] See: O. Marian, *Are Cryptocurrencies Super Tax Havens?*, „Michigan Law Review First Impressions" 38, 2013, p. 6, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2305863## (access: October 6, 2016).

[282] See: ibid.

At the same time, the taxpayer, who intends to honestly and loyally settle accounts with the tax authorities, may have practical problems with proving his or her income in cryptocurrencies to tax authorities for the same reasons, arising from the technical aspects of the cryptocurrency system. In addition, such a settlement is made difficult by high volatility cryptocurrency and lack of official exchange rate.

In practice, such problems have already been recognized. It is recommended to create a separate online wallet for each purchase of cryptocurrency[283], but it would be too burdensome. Therefore, it seems that it is enough to just create a different address (public key) for each transaction, which indeed is commonly recommended. But it is necessary to document each transaction using cryptocurrency for tax purposes, preferably including the creation date of the address. This of course seems very unlikely in the case of a normal cryptocurrency user. Interestingly, the solution to this problem is "embedded" in the cryptocurrency system — after all, the details of each transaction are stored in the blockchain and the taxpayer can use these entries as evidence before the tax authorities[284]. Software acting on the basis of the information stored in the blockchain, which helps cryptocurrency users (both individuals and businesses) in determining the amount of tax, bookkeeping, proper documenting and making settlements with tax authorities, has already been created the U.S[285].

In fact, it seems that most of the situations of tax evasion by cryptocurrency users will be intentional. It should be, however, point out one very important exception — it is difficult to speak of intent in a situation when tax evasion is a consequence of the fundamental problems with the interpretation of the tax law, and such problems apply to cryptocurrencies[286].

Two situations should be distinguished here — when payment in cryptocurrencies takes place after the activity which cannot be the subject of a legally effective contract[287], and when the payment is through the unlawful activity, but which may be subject to effective legal agreement. The first takes place e.g. in the

[283] See: T.R. Koski, op. cit., p. 257.

[284] This was pointed out by T.R. Koski — ibid. Note, however, that in principle it is possible to store such entries in the blockchain "forever", they have to be removed after some time, otherwise the blockchain will grow to the size preventing its effective functioning.

[285] http://www.libratax.com/ (access: October 6, 2016).

[286] For example, the crime of tax fraud in Polish law, governed by Art. 56 of the Act of September 10, 1999 — Fiscal Penal Code (Journal of Laws of 2013 item 186 as amended) can be only intentional — see e.g. the decision of the Supreme Court dated February 23, 2006, III KK 267/05, LEX No. 180799; Explanatory Memorandum for the judgment of the Constitutional Court of September 12, 2005, SK 13/05, OTK-A 2005, No. 8, item 91.

[287] Income derived from activity which cannot be the subject of a legally effective contract, is excluded from the scope of the Polish legislation on the taxation of personal and corporate income tax, and thus in general is not taxed. Likewise, the remuneration obtained for the activity which cannot be the subject of a legally effective contract (legal trade) is not within the scope of Directive 2009/112/EC, and thus of the Polish Goods and Services Tax Act (VAT Act).

case of a request made to break into someone else's computer — the increment of wealth obtained in this way by the hacker will not be treated as income, and what's more — the hacker will not be required to indicate that income in the tax return. He will then be able to put the obtained remuneration in the legal trade (buying some goods or services on the legitimate market). With the current development of the market of payments in cryptocurrencies, which, however, does not allow ample opportunity to purchase any legitimate goods and services, it is best for a criminal to exchange cryptocurrency for legal tender, which is why it is so important to place an obligation upon such entities to identify their customers and store information about exchange transactions not only for the counteracting of money laundering and financing of terrorism, but also for inspections by the tax authorities.

The second situation may occur e.g. in the case of activities which may be subject to an effective legal agreement, e.g. the sale of drugs or alcohol without the required permits. Such activities, although violate certain regulations (e.g. pharmaceutical Law), may cause the tax implications in the area of income tax and VAT. If such activity is carried out on a wider scale, it will be difficult for the seller who gets paid in cryptocurrencies to hide the fact of accepting cryptocurrencies from tax authorities. Thus, the tax authorities will be able to attempt to assess the income (revenue) earned by the user.

Popularization of cryptocurrencies will undoubtedly cause an attempt to use the same tax fraud as used when using legal means of payment with respect to VAT (these include the so-called tax carousel (carousel fraud), fraud of non-disclosure of intra-community purchase of goods and the fraud of fictitious intra-community supply of goods). However, it is not a consequence of specific characteristics of cryptocurrencies that distinguish them from other means of payment, but rather another manifestation of their basic payment function, the same as in the case of legal tender.

Chapter 4

Conclusions

The analysis of the cryptocurrency phenomenon from three different points of view, that is, from the perspective of computer science, economics and law, leads to three different groups of conclusions. Particularly noteworthy is that cryptocurrencies arouse the least controversy within computer science, whose representatives mostly confine themselves to only describing the phenomenon. Cryptocurrency is seen from their perspective primarily as an innovative technical solution with not much contribution to the development of computer science. Innovation consists in a clever combination of the existing solutions and ideas (such as e.g. digital money, electronic signature or *peer-to-peer*). Hence, the conclusions are limited to the comparison of cryptocurrency, digital money and credit card, and the understanding of digital money and credit card is specific to information technology and differs significantly from the one adopted in economics or law. The conclusions are mainly about the fact that digital money is issued in exchange for legal tender, and cryptocurrencies are not created in this way (likewise, cards are closely related to the legal tender). This has important legal consequences, causing problems with the of qualification cryptocurrency purchase under civil law as indicated in chapter three, which in turn have consequences in the area of tax law. In addition, this specific way of cryptocurrency creation has economic consequences, primarily being a breeding ground for possible categorization of cryptocurrency as a pyramid scheme. Trading digital money (in terms of information technology proposed in this book) and trading cryptocurrencies, as opposed to card transactions, is anonymous. On the other hand, the registry (as meant by the computer science) of financial transactions made using cards and digital money is "confidential", while the registry in the case of cryptocurrencies (i.e currently *blockchain*) is "pseudoanonymous-explicit". This is especially ˛of legal importance in the area of regulations concerning the access of public entities to information on citizens, especially this is about counteracting money laundering and terrorist financing, as well as the fight against tax evasion.

The activities of public entities may be directed here not so much to get information from the market in cryptocurrency, as to obtain information directly

Cryptocurrencies as electronic means of payment without the issuer, 2016

from the operation registry (blockchain). Anyway, this blockchain feature, i.e. its "overt pseudoanonymity", makes it available to other uses than payments, which further affects the popularization of cryptocurrencies.

Counteracting the use of cryptocurrency exchanges and exchange offices for money laundering and terrorist financing requires appropriate amendments to existing legislation. FATF guidelines and recommendations play the most important role here, and the most important issue is to eliminate the possibility of providing services of anonymous exchange of cryptocurrency to legal tender and respectively the exchange of legal tender to cryptocurrencies by cryptocurrency exchanges and exchange offices (or any other entities). The elimination of anonymity of such an exchange is also important in preventing tax fraud using cryptocurrencies and in preventing tax evasion by their users.

An important finding is raising the fact that in principle the cryptocurrency technology (including bitcoin) is not ecological. Increasing computing power of the entire network of miners results in increased energy consumption and the number of solved blocks approaches 2016 for two weeks. The question arises about the economic sense of such a solution and at the same time it is worth to point out that ecological cryptocurrency systems are created (so-called energy-saving), i.e. whose which do not require large amounts of energy (e.g. ECCoin, MintCoin).

A limitation of technology affecting the popularization of cryptocurrencies is the upper limit for the mining speed of blocks and the size of blocks, which creates a bottleneck related to the number of authorized transactions made per minute. Systems enabling card payments do not have this type of restriction, which currently allow several thousand times more authorized transactions per second than the Bitcoin system. However, technological progress in the area of payments occurs extremely quickly, cryptocurrency systems are modified all the time, the available computing power increases, and therefore it is possible that the said restriction on cryptocurrency systems will soon be eliminated.

It seems that this is not technical solutions where the greatest threat to the development and popularization of cryptocurrencies is, but in their economic nature, which is a consequence of the fundamental principles of cryptocurrency systems. It has been shown in this book that cryptocurrencies constitute fertile ground for the development of pyramid schemes due to their nature, the principles of the creation and popularization. An important feature increasing the likelihood of development of the cryptocurrency system as a pyramid scheme, are significant differences in the cost of acquisition of the first units of cryptocurrency (very low), comparing to the next ones. At the same time, however, the categorization of the cryptocurrency system as a pyramid scheme in economic terms does not automatically mean the same categorization in legal terms. What's more, there are no regulations that would allow effective counteracting the cryptocurrency system as a pyramid scheme. However, law is able to cope with the creation of pyramid schemes using financial instruments constructed based on cryptocurrencies. Sim-

Cryptocurrencies as electronic means of payment without the issuer, 2016

ilarly, there is a legal possibility to counteract cryptocurrency systems having the features of a pyramid scheme, when the cryptocurrency system is organized by an entrepreneur acting openly and the system includes consumers.

Another important economical conclusion is establishing that cryptocurrencies definitely cannot be seen as money due to the fact that they currently do not meet all the functions of money. This is important in the context of the discussion about the possible popularization of cryptocurrencies, and also affects legal considerations. At most, cryptocurrencies can now be seen as a "money substitute" in the economic context due to the fact that they partially implement selected functions of money in economic trade (mainly the medium of exchange). It seems that such economy connotation is not inconsistent with the recognition of cryptocurrencies from the legal perspective as private money (even if there are clear problems in categorization and cryptocurrencies cannot be clearly classified as money, financial instrument or electronic means of payment in the current economic theory). As established in the legal part of the book, cryptocurrencies are entries in the registry, which is a *blockchain*, representing the property rights of the person controlling the private signature and are expressed in monetary units (e.g. 1 BTC). Cryptocurrencies can be used based on the principle of contractual freedom.

From the economic perspective, the current nature of cryptocurrencies (primarily speculative motives of use and high volatility of cryptographic currency exchange rates in relation to traditional currencies) is much closer to a financial instrument (investment alternative?) rather than to money. At the same time, it should be emphasized cryptocurrencies cannot be, from the legal perspective, categorized as financial instruments. Cryptocurrencies can be "invested" in legal tender, and cryptocurrencies themselves can be used to construct various types of financial instruments. In order to protect the purchasers of such financial instruments, one can use the existing regulations (as exemplified by the federal U.S. law) using the appropriate interpretation. It seems necessary to take appropriate legislative initiatives in the long term, with an example being the legislation of the State of New York. However, in the area of consumer protection, the use of cryptocurrencies involves specific risks and threats that force specific actions of the legislators.

From an economic point of view, there are serious doubts whether cryptocurrencies could function as a universal means of payment in the future in the economy, due to:

— High volatility reducing trust in cryptocurrencies

— Lack of state supervision over cryptocurrency systems

— The features of a pyramid scheme are inherent in the cryptocurrency system.

Therefore, countries have the choice — they can take actions that will facilitate the development and popularization of cryptocurrencies, they may not take any action, or they can actively fight cryptocurrencies, primarily using legal means.

Currently, all three of these approaches exist, with most states choosing the passive approach which, taking into account the economic conclusions, rather hinders the development of cryptocurrencies. The activities of the legislature of New York is the example of the first approach, and activities in the Russian Federation — of the third one.

Undoubtedly, the introduction of a public oversight of entities which accept cryptocurrencies from the public under the repayable title, will increase citizens' trust in cryptocurrency and will be an important complement to the gap, which is the lack of (and practical impossibility) supervision by public (state) of the entire cryptocurrency system. Besides, such supervision should extend to other commercial entities using cryptocurrencies, especially cryptocurrency exchanges and exchange offices, intermediaries in making payments using cryptocurrency or those using financial instruments constructed based on cryptocurrencies. Of course, the need for state supervision (public law) and its subjective and objective scope are closely correlated with the degree of cryptocurrency popularization. Introducing such a supervision with little popularization is pointless.

The development of cryptocurrencies depends not only on the development of a public supervision of entities that operate cryptocurrencies, but above all on finding an effective public law mechanism, which would be able to counteract the negative effects of features of a pyramid scheme, which are inherent to each cryptocurrency system.

Cryptocurrencies as electronic means of payment without the issuer, 2016

References

Literature

Andrade F. et al., "Contracting Agents: Legal Personality and Representation", *Artificial Intelligence and Law* 15, December 2007.

Arystoteles, *Etyka nikomachejska*, Warszawa 1956.

Back A., *Hashcash — a Denial of Service Counter-measure*, www.hashcash.org/papers/hash-cash.pdf.

Barber S. et al., "Bitter to Better — How to Make Bitcoin a Better Currency", [in:] *Financial Cryptography and Data Security*, ed. A.D. Keromytis, Springer, Berlin-Heidelberg 2012.

Bazenkova A., "Russian Firm Plans Local Version of Bitcoin Digital Currency", *The Moscow Times*, September 17, 2015, http://www.themoscowtimes.com/business/article/russian-firmplans-local-version-of-bitcoin-digital-currency/531300.html.

Begg D., *Ekonomia*, PWE, Warszawa 1994.

Blanc J., Fare M., "Understanding the Role of Governments and Administrations in the Implementation of Community and Complementary Currencies", *Annals of Public and Cooperative Economics* 84, 2013, No. 1.

Canard S., Gouget A., "Divisible e-Cash Systems Can Be Truly Anonymous", [in:] *Advances in Cryptology — Proceedings of EUROCRYPT 2007*, Springer, Berlin-Heidelberg 2007.

Chaum D., "Blind Signatures for Untraceable Payments", [in:] *Advances in Cryptology — Proceedings of CRYPT0' 82*, Plenum Press, New York 1983.

Chaum D., Fiat A., Naor M., "Untraceable Electronic Cash", [in:] *Advances in Cryptology — CRYPTO '88*, *8th Annual International Cryptology Conference*, *Santa Barbara*, *California*, *USA*, *August 21–25*, *1988*, *Proceedings*, ed. Sh. Goldwasser ("Lecture Notes in Computer Science" 403) Springer, London UK 1988.

Chrabonszczewska E., "Bitcoin — nowa wirtualna globalna waluta?", *International Journal of Management and Economics* 40, Warszawa 2013.

Czarnecki J., "Nie tylko bitcoin, czyli rodzaje wirtualnych walut", [in:] *Wirtualne waluty*, Wardyńscy i Wspólnicy, Warszawa 2014, http://www.wardynski.com.pl/gfx/wardynski/userfiles/_public/raport_o_wirtualnych_walutach.pdf.

Dai W., *B-Money*, http://www.weidai.com/bmoney.txt.

Dolan E., *The Foundations of Modern Austrian Economics*, Sheed Andrews and McMeel, Kansas City 1976.

Dopierała Ł., Borodo A., "Znaczenie waluty kryptograficznej Bitcoin jako środka wymiany", *Contemporary Economy* 5, 2014, No. 2.

Dybowski T., Pyrzyńska A., [in:] *System prawa prywatnego*, vol. 5, ed. E. Łętowska, C.H. Beck, Warszawa 2013.

Everaere P., Simplot-Ryl I., Traoré I., "Double Spending Protection for e-Cash Based on Risk Management", [in:] *Information Security*, ed. M. Burmester et al., Springer, Berlin-Heidelberg 2011.

Fedorowicz Z., *Teorie pieniądza*, Poltext, Warszawa 1993.

Franco P., "Understanding Bitcoin: Cryptography, Engineering and Economics", *Wiley Finance Series*, 2015.

Franków M., Kopyściański T., "Analiza perspektyw rozwoju bitcoina w kontekście możliwości pełnienia funkcji pieniądza", *WSB University Research Journal* 16, No. 2, Wrocław 2016.
Galbraith J.K., *Money: Whence It Came, Where It Went*, Houghton Mifflin Company Boston 1976.
Goryszewski R., "Wokół poglądów na rolę pieniądza w gospodarce w historii i teorii ekonomii", *Rocznik Naukowy Wydziału Zarządzania w Ciechanowie* 1–4, 2011, No. V.
Gowrisankaran G., Stavins J., "Network Externalities and Technology Adoption: Lessons from Electronic Payments", *RAND Journal of Economics* 2004, No. 35 (2).
Górniak J., *My i nasze pieniądze. Studium postaw wobec pieniądza*, Aureus, Kraków 2000.
Grinberg R., "Bitcoin: An Innovative Alternative Digital Currency", *Hastings Science & Technology Law Journal* 2011, No. 4 (1).
Guzdek S., "Historyczne ujęcie klasyczno-neoklasycznej teorii pieniądza i poglądów", *Zeszyty Naukowe Polskiego Towarzystwa Ekonomicznego* 2010, No. 8.
Hayek F.A., *Denationalisation of Money*, Institute of Economic Affairs, London 2007.
Higgins S., *Russian Official: Payment Giant Qiwi's Digital Currency Idea 'Illegal'*, http://www.coindesk.com/russian-official-qiwi-digital-currency-illegal/.
Kaźmierczak A., *Pieniądz i bank w kapitalizmie*, PWN, Warszawa 1994.
Kaźmierczak A., *Polityka pieniężna w gospodarce otwartej*, PWN, Warszawa 2008.
Kiviat T.I., "Beyond Bitcoin: Issues in Regulating Blockchain Transactions", *Duke Law Journal* 65, December 2015, No. 3.
Kosikowski C., "Pieniądz", [in:] *Encyklopedia prawa bankowego*, ed. W. Pyzioł, Wydawnictwo Prawnicze PWN, Warszawa 2000.
Koski T.R., "Bitcoin — Tax Planning in the Uncertain World of Virtual Currency", *Practical Tax Strategies*, December 2014.
Lace E., *BitRuble? First Russian Cryptocurrency Announced by Qiwi*, http://cointelegraph.com/news/115281/bitruble-first-russian-cryptocurrency-announced-by-qiwi.
Landreth H., Colander D., *Historia myśli ekonomicznej*, PWN, Warszawa 2005.
Lastra R.M., *International Financial and Monetary Law*, Oxford University Press, Oxford 2015.
Lipiński E., *Historia powszechnej myśli ekonomicznej do roku 1870*, PWN, Warszawa 1981.
Makroekonomia ze szczególnym uwzględnieniem polityki pieniężnej, ed. M. Noga, CEDEWU, Warszawa 2012.
Marciniuk J., "Komentarz do art. 11 u.p.d.o.f.", [in:] *Podatek dochodowy od osób fizycznych. Komentarz*, C.H. Beck Warszawa 2015.
Marian O., "Are Cryptocurrencies Super Tax Havens?", *Michigan Law Review First Impressions* 38, 2013.
Marszałek P., "Pieniądz w teoriach szkoły austriackiej", *Ruch Prawniczy, Ekonomiczny i Socjologiczny* LXXIII, 2011, z. 4.
Masiukiewicz P., *Piramidy finansowe, teoria, regulacje, praktyka*, Publ. PWN, Warszawa 2015.
Menger C., *Principles of Economics*, Ludwig von Mises Institute, Auburn, Ala 2007.
Milewski R., Kwiatkowski E., *Podstawy ekonomii*, PWN, Warszawa 2008.
Miller S. et al., *Discovering Bitcoin's Public Topology and Influential Nodes*, https://cs.umd.edu/projects/coinscope/coinscope.pdf.
Mises L., *Teoria pieniądza i kredytu*, Fijorr publishing, Warszawa 2012.
Mises L., *The Theory of Money and Credit*, The Foundation for Economic Education, Irvington-on-Hudson, New York 1971.
Mishkin F.S., *Ekonomika pieniądza, bankowości i rynków finansowych*, PWN, Warszawa 2002.
Münzer J., *Bitcoins: Supervisory Assessment and Risks to Users*, February, 17, 2014, http://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2014/fa_bj_1401_bitcoins_en.html.
Nakamoto S., *Bitcoin: A Peer-to-Per Electronic Cash System*, https://bitcoin.org/bitcoin.pdf.
Okamoto T., "An Efficient Divisible Electronic Cash Scheme", [in:] *Advances in Cryptology — Proceedings of CRYPT0'95*, Springer, Berlin-Heidelberg 1995.

Owsiak S., *Podstawy nauki finansów*, Publ. PWE, Warszawa 2002.
Oyrzanowski B., *Makroekonomia*, Wydawnictwo Profesjonalnej Szkoły Biznesu, Kraków 1997.
Pachucki M., *Piramidy i inne oszustwa na rynku finansowym*, Komisja Nadzoru Finansowego, Warszawa 2013.
Perez Y.B., *Russian Minister Confirms Plans to Ban Bitcoin-to-Fiat Conversions*, http://www.coindesk.com/russian-minister-confirms-plans-to-ban-bitcoin-to-fiat-conversions/.
Piaszczyński W., *Anatomia pieniądza*, SCRIPT, Warszawa 2004.
Pietrasz P., *Opodatkowanie dochodów nieujawnionych*, Wolters Kluwer, Warszawa 2007.
Pietrzak B., Polański Z., Woźniak W., *System finansowy w Polsce*, PWN, Warszawa 2008.
Piotrowska A., "Czynniki oceny opłacalności inwestycji w kryptowalutę bitcoin", *Zeszyty Naukowe Uniwersytetu Szczecińskiego 862. Finanse, Rynki Finansowe, Ubezpieczenia* 2015, No. 75.
Polański Z., *Pieniądz i system finansowy w Polsce*, PWN, Warszawa 1995.
Polasik M., Piotrowska A., Kotkowski R., "Waluta wirtualna Bitcoin z perspektywy oferentów internetowych. Analiza wstępna", *Nauki o Finansach* 4, 2013, No. 17.
Prokurat J., "Podatkowe aspekty obrotu wirtualnymi walutami", *Przegląd Podatkowy* 2015, No. 3.
Ron D., Shamir A., "Quantitative Analysis of the Full Bitcoin Transaction Graph", [in:] *Financial Cryptography and Data Security — 17th International Conference, FC 2013, Okinawa, Japan, April 1–5, 2013* (Lecture Notes in Computer Science 7859), Springer 2013.
Sartor G., "Cognitive Automata and the Law: Electronic Contracting and the Intentionality of Software Agents", *Artificial Intelligence and Law* 17, 2009, No. 4.
Schaal P., *Pieniądz i polityka pieniężna*, Wydawnictwo PWE, Warszawa 1996.
Segendorf B., "Have Virtual Currencies Affected the Retail Payments Market?", *Economic Commentaries* 2014, No. 3.
Shadab H.B., *Regulating Bitcoin and Block Chain Derivatives*, October 9, 2014, http://www.cftc.gov/idc/groups/public/@aboutcftc/documents/file/gmac_100914_bitcoin.pdf.
Sieroń A., "Czym jest Bitcoin", *Ekonomia — Wroclaw Economic Review* 19, 2013, No. 4.
Skorupka J., "Jeszcze o pojęciu pieniądza w przestępstwie z art. 310 k.k.", *Prokuratura i Prawo* 2009, No. 2.
Skorupka J., "Pojęcie środków płatniczych w art. 310 k.k.", *Prokuratura i Prawo* 2002, No. 11.
Slattery T., "Taking a Bit Out of Crime: Bitcoin and Cross-border Tax Evasion", *Brooklyn Journal of International Law* 39:2, 2014.
Srokosz W., "Istota prawna pieniądza elektronicznego", *Prawo Bankowe* 2002, No. 12.
Srokosz W., "Pieniądz lokalny", [in:] *Finanse samorządowe po 25 latach samorządności. Diagnoza i perspektywy*, ed. W. Miemiec, Wolters Kluwer, Warszawa 2015.
Srokosz W., "Prawo a rozwój elektronicznych środków płatniczych w XXI wieku", [in:] *XXV lat przeobrażeń w prawie finansowym i prawie podatkowym: ocena dokonań i wnioski na przyszłość*, ed. Zbigniew Ofiarski, Uniwersytet Szczeciński. Wydział Prawa i Administracji, Szczecin 2014.
Srokosz W., "The Use of Cryptocurrencies for Tax Evasion and Tax Fraud", [in:] *Tax Law vs Tax Frauds and Tax Evasions. Non-conference Proceedings of Scientific Papers*, ed. V. Babcak, A. Romanowa, I. Vojnikowa, vol. 2, Univerzita Pavla Jozefa Šafárika v Košicach. Pravnicka Fakulta, Kosice 2015.
Stankiewicz W., *Historia myśli ekonomicznej*, PWE, Warszawa 1998.
Szul Ł., *Omówienie Konstytucji Rosji z 1993 r.*, http://www.rosjapl.info/historia-rosji-ukrainy-zsrr/historia-i-polityka-wspolczesnej-rosji/omowienie-konstytucji-rosji-z-1993.html.
Wolter A., *Prawo cywilne. Zarys części ogólnej*, PWN, Warszawa 1982.
Van Hout M.C., Bingham T., "'Silk Road', the Virtual Drug Marketplace: A Single Case Study of User Experiences", *International Journal of Drug Policy* 24, 2013, No. 5, http://www.ijdp.org/article/ S0955-3959(13)00006-6/pdf.

Zacharzewski K., "Bitcoin jako przedmiot stosunków prawa prywatnego", *Monitor Prawniczy* 2014, No. 21.
Zacharzewski K., "Praktyczne znaczenie bitcoina w wybranych obszarach prawa prywatnego", *Monitor Prawniczy* 2015, No. 5.

List of legal acts

Bank Secrecy Act, https://www.fincen.gov/statutes_regs/bsa/.
Directive 2004/39/EC of the European Parliament and of the Council of April 21, 2004 on markets in financial instruments amending Council Directives 85/611/EEC and 93/6/EEC and Directive 2000/12/EC of the European Parliament and of the Council and repealing Directive 93/22/EEC (OJ. EU L 145 of 04/30/2004, as amended.
Directive 2005/29/EC of the European Parliament and of the Council of May 11, 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council (OJ. EU L 149 of 06/11/2005).
Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (OJ. EU L 309 of 11/25/2005, as amended.
Commission Directive 2006/70/EC of August 1, 2006 regarding the definition of a politically exposed person and the technical criteria for simplified rules for due diligence towards the customer, as well as exclusions due to a financial activity conducted on an occasional or very limited basis (OJ. EU L 214 of 08/04/2006, as amended).
Council Directive 2006/112/EC of November 28, 2006 on the common system of value added tax (OJ. UE L 347 of 12/11/2006 as amended).
Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC (OJ. EU L 319 of 12/05/2007, as amended.
Directive 1999/93/EC of the European Parliament and of the Council of December 13, 1999 on a Community framework for electronic signatures (OJ. EU L 2000 No. 13, as amended.
Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC (OJ. EU L 267 of 10/10/2009 as amended.
Directive 2011/83/EU of the European Parliament and of the Council of October 25, 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council (OJ. EU L 304 of 11/22/2011.
Directive of the European Parliament and of the Council 2014/65/EU of May 15, 2014 on financial instruments markets and amending Directives 2002/92/EC and 2011/61/EU, OJ. EU L 173 of 06/12/2014.
Directive of the European Parliament and of the Council 2015/849/EU of May 20, 2015 on prevention of the use of the financial system for money laundering or terrorist financing, amending the Regulation of the European Parliament and of the Council No. 648/2012/EC and repealing the Directive of the European Parliament and of the Council 2005/60/EC and Directive 2006/70/EC, OJ. EU L 141 of 06/05/2015.
Directive 2015/2366 of the European Parliament and of the Council of November 25, 2015 on payment services in the internal market amending Directives 2002/65/EC, 2009/110/EC, 2013/36/

EU and Regulation (EU) No. 1093/2010 and repealing Directive 2007/64/EC (OJ. EU L of 12/23/2015).
The Electronic Money Regulations 2011, Her Majesty's Stationery Office (HMSO) 2011 No. 99; http://www.legislation.gov.uk/uksi/2011/99/made.
Gesetz über die Beaufsichtigung von Zahlungsdiensten (Zahlungsdiensteaufsichtsgesetz), Zahlungsdiensteaufsichtsgesetz vom 25. Juni 2009 (BGBl. I S. 1506), das zuletzt durch Artikel 23 des Ge-setzes vom 20. November 2015 (BGBl. I S. 2029) — http://www.gesetze-im-internet. de/zag/index.html ; https://www.bafin.de/SharedDocs/Downloads/EN/Aufsichtsrecht/dl_zag_ en.pdf?__blob=publicationFile.
Penal Code of June 6, 1997 (Journal of Laws of 1997, No. 88, item 553 as amended).
The Constitution of the Russian Federation adopted in a national referendum on December 12, 1993, for Polish language version see: http://libr.sejm.gov.pl/tek01/txt/konst/rosja.html
The Federal Constitution of the Swiss Confederation of April 18, 1999 trans. by Z. Czeszejko-Sochacki, Wydawnictwo Sejmowe, Warszawa 2000, http://biblioteka.sejm.gov.pl/konstytucje_swiata/.
The Constitution of the Czech Republic of December 16, 1992, for Polish language version see: http://biblioteka.sejm.gov.pl/wp-content/uploads/2015/07/Czechy_pol_010811.pdf; for English language version see: http://www.usoud.cz/en/constitution-of-the-czech-republic/.
The Constitution of Romania of November 21, 1991, for Polish language version see: http://libr.sejm.
gov.pl/tek01/txt/konst/rumunia2011.html#mozTocId165972; for English version see: http://www.cdep.ro/pls/dic/site2015.page?id=339&idl=2.
Constitution of the Polish Republic of April 2, 1997 (Journal of Laws No. 78, item 483 as amended).
The Constitution of the United States of America, translation and introduction by A. Pułło, Wydawnictwo Sejmowe, Warszawa 2002, http://biblioteka.sejm.gov.pl/konstytucje_swiata/.
Lei No. 12.865, de 9 de Outubro de 2013 [Law No. 12,865 of October 9, 2013], http://www.receita.
fazenda.gov.br/Legislacao/leis/2013/lei12865.htm; see also http://legislacao.planalto.gov.br/legisla/legislacao.nsf/Viw_Identificacao/lei%2012.865-2013?OpenDocument.
"Money Transmission Laws" — http://www.dbo.ca.gov/Licensees/money_transmitters/, http://www.
dbcf.state.ms.us/documents/cons_finance/7515MoneyTranAct2011.pdf; http://www.community-currencieslaw.org/financial-and-banking-laws/#State_Money_Transmission_Laws.
N.Y. COMP. CODES R. & REGS. tit. 23, § 200 (2015), http://www.dfs.ny.gov/legal/regulations/bitlicense_reg_framework.htm; http://www.dfs.ny.gov/legal/regulations/adoptions/dfsp200t.pdf.
Regulation of the European Parliament and of the Council (EU) No 549/2013 of May 21, 2013 on the European system of national and regional accounts in the European Union (OJ. EU L 174 of 06/26/2013).
Regulation of the European Parliament and of the Council (EU) No 910/2014 of July 23, 2014 on electronic identification and trust services in relation to electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ. UE L 257 of 08/28/2014 as amended).
Sixth Council Directive of May 17, 1977 on the harmonization of the laws of the Member States relating to sales taxes — common system of value added tax: uniform basis of assessment (OJ. EU L 145 of 06/13/1977 as amended).
Treaty on the Functioning of the European Union (OJ. EU C 326 of 10/26/2012). U.S. Code, http://uscode.house.gov/browse.xhtml.
Civil Code of April 23, 1964 (Journal of Laws of 2014 item 121 as amended).
The Basic Law of the Federal Republic of Germany of May 23, 1949; translation by B. Banaszak, A. Malick, [in:] *Konstytucje państw Unii Europejskiej*, Warszawa 2011, http://biblioteka.sejm.gov.pl/konstytucje_swiata/
Personal Income Tax Act of July 26, 1991 (Journal of Laws of 2012, item 361 as amended).

Corporate Income Tax Act of February 15, 1992 (Journal of Laws of 2014, item 851 as amended).
Act of September 10, 1999 — Fiscal Penal Code (Journal of Laws of 2013 item 186 as amended).
The Act of November 16, 2000 on counteracting money laundering and financing of terrorism (Journal of Laws 2010 No. 46, item 276 as amended).
The Act on trust services and electronic identification of September 5, 2016 (Journal of Laws of 2016, item 1579).
The Act of July 27, 2002. Foreign Exchange Law (Journal of Laws of 2012, item 826 as amended).
The Act of March 11th, 2004 on Goods and Services Tax (Journal of Laws of 2011, No. 177, item 1054 as amended).
The Act of November 19, 2009 on gambling, (Journal of Laws of 2015, item 612).
The law of August 19, 2011 On payment services (Journal of Laws of 2014, item 873 as amended).
The Act of May 30, 2014 on Consumer Rights (Journal of Laws of 2014 item 827).

Case law

The decision of the Supreme Court of February 23, 2006, III KK 267/05, LEX No. 180799.
The judgment of ECJ of July 14, 1998 in case C-172/96 Commissioners of Customs & Excise vs. First National Bank of Chicago (EU:C:1998:354), Court Reports 1998 I–04387.
The judgment of the Constitutional Court of September 12, 2005, SK 13/05, OTK-A 2005, No. 8, item 91.
The judgment of ECJ of October 22, 2015 in case C-264/14 Skatteverket vs. David Hedqvist, ECLI:EU:C:2015:718, publ. http://curia.europa.eu/.
The judgement of the Court of Appeal in Wrocław on November 29, 2010 (II AKa 325/10), published in LEX No. 677942.
The judgement of the Court of Appeal in Gdansk of June 19, 2013. (II AKa 473/12), published in LEX No. 1353695.
The judgement of the Court of Appeal in Warsaw on December 11, 2012 (II AKa 293/12), published in LEX No. 1246938.
The judgment of August 26, 2014 of the United States District Court for the Eastern District of Texas, Sherman Division) in case Securities and Exchange Commission vs. Trendon T. Shavers and Bitcoin Savings and Trust on partial recognition and partial rejection of the request for retrial (case number 4:13-cv-00416), opubl. https://www. manatt.com/uploadedFiles/Content/4_News_and_Events/Newsletters/BankingLaw@manatt/ SEC%20v.%20Shavers.pdf.

Websites

https://bitcoin.org/en/development.
http://www.bi.go.id/en/ruang-media/siaran-pers/Pages/SP_160614.aspx.
http://brixtonpound.org.
https://www.btcc.com/.
http://www.businessinsider.com/what-is-dogecoin-2013-12?op=1.
http://curia.europa.eu/.
http://www.fatf-gafi.org.
http://www.libratax.com/.
http://www.moneysense.gov.sg/understanding-financial-products/investments/consumer-alerts/virtual-currencies.aspx.
https://ripple.com/.
http://www.worldometers.info/pl/.

Other materials

Annual Report 2013/2014 — FCA. Markets Pactitioner Panel, https://www.fca.org.uk/your-fca/documents/markets-practitioner-panel-annual-report-2013-14.

Changes in modus operandi of Islamic State terrorist attacks. Review held by experts from Member States and Europol on 29 November and 1 December 2015, The Hague, January 18, 2016, https://www.europol.europa.eu/sites/default/files/publications/changes_in_modus_operandi_of_is_in_terrorist_attacks.pdf

EBA, *EBA Opinion on "Virtual Currencies"*, July 4, 2014 (EBA/Op/2014/08).

EBA, *Warning to Consumers on Virtual Currencies*, December 12, 2013.

European Central Bank, *Virtual Currency Schemes, Eurosystem*, October 2012.

Press release about the hearing in the Committee on Economic and Monetary Affairs (ECON), which was held on January 25, 2016, http://www.europarl.europa.eu/news/pl/newsroom/20160126STO11514/Pos%C5%82owie-dyskutowali-z-ekspertami-o-wyzwaniach -zwi-%C4%85zanym-z-wirtualnymi-walutami.

Internal Revenue Bulletin: 2014–16, April 14, 2014, https://www.irs.gov/irb/2014-16_IRB/ar12.html, http://orka2.sejm.gov.pl/IZ3.nsf/main/6B25E0FB.

International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. The FATF Recommendations, February 2012, http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html.

Individual interpretation by the Director of the Tax Chamber in Katowice dated 21 June 2013 IBPP2/443-258/13/ICz.

Individual interpretation by the Director of the Tax Chamber in Katowice dated 10 June 2014, IPPB5/423-397/14-4/MW.

Individual interpretation of January 8, 2014 by the Director of the Tax Chamber in Poznań, http://inter- pretacje-podatkowe.org/wierzyciel/ilpp1-443-910-13-2-awa.

Mitt Romney Tax Returns Hacked? Alleged Ransom Asks For $1 Million In Bitcoins, "International Business Times", September 5, 2012.

The answer by the Undersecretary of State in the Ministry of Finance of October 27, 1999 to a Parliamentary Question No. 1093 on the clarification of the notion of "monetary value" used in the laws on income tax from natural and legal persons, http://orka2.sejm.gov.pl/ IZ3.nsf/main/6B25E0FB.

The opinion of Advocate General Juliane Kokott of July 16, 2015 in case C-264/14 Skatteverket vs. David Hedqvist (ECLI:EU:C:2015:498), http://curia.europa.eu/.

People's Bank of China, Ministry of Industry and Information Technology of China, China Securities Regulatory Commission, China Banking Regulatory Commission and the China Insurance Regulatory Commission Notice on the Prevention of Risks Associated with Bitcoin, (Bank Notice [2013] No. 289), https://exchange.btcc.com/page/bocnotice2013.

Document of Australian Taxation Office titled *Tax treatment of cryptocurrencies in Australia — specifically bitcoin*, https://www.ato.gov.au/General/Gen/Tax-treatment-of-crypto-currencies-in-Australia-specifically-bitcoin/.

Document of IRC titled *Publication 525 — Introductory Material*, https://www.irs.gov/publications/p525/ar01.html.

FinCEN guidance titled *Application of FinCEN's Regulations to Persons. Administering, Ex-changing, or Using Virtual Currencies*, March 18, 2013 (FIN-2013-G001).

BIS report: *Non-Banks in Retail Payments*, September 2014, p. 16, http://www.bis.org/cpmi/publ/d118.pdf.

FATF report titled *Virtual Currencies: Key Definitions and Potential AML/CFT Risks* of June 2014, http://www.fatf-gafi.org/publications/methodsandtrends/documents/virtual-currency-definitions-aml-cft-risk.html.

Report of HM Treasury titled *UK National Risk Assessment of Money Laundering and Terrorist Financing*, October 2015, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/468210/UK_NRA_October_2015_final_web.pdf.

Report titled *Regulating Virtual Currencies. Recommendations to prevent virtual currencies from being used for fraudulent purposes and money laundering*, June 2014, http://www.economie.gouv.fr/files/regulatingvirtualcurrencies.pdf.

Regulation of Bitcoin in Selected Jurisdictions, The Law Library January of Congress, Global Legal Research Center, January 2014, http://www.loc.gov/law/help/bitcoin-survey/.

The report of the General Inspector of Financial Information on the implementation of the Act of November 16, 2000 on counteracting money laundering and financing of terrorism in 2014, Warsaw, March 2015, http://www.mf.gov.pl/documents/764034/1223641/20150414_sprawozdanie+z+dzialalnosci+GIIF+2014.pdf

Commission report of November 27, 2015 on progress in the implementation of the EU Drugs Strategy for 2013–2020 and the EU Action Plan in the field of drugs for 2013–2016, COM(2015) 584 final.

U.S. Securities and Exchange Commission, Investor Alert: *Ponzi Schemes Using Virtual Currencies*, SEC Pub. No. 153 (7/13), https://www.sec.gov/investor/alerts/ia_virtualcurrencies.pdf.

FATF guidance titled *Guidance for a Risk-Based Approach to Virtual Currencies* of June 2015, http://www.fatf-gafi.org/publications/fatfgeneral/documents/guidance-rba-virtual-currencies.html.

Explanations by FinCEN titled *Application of FinCEN's Regulations to Virtual Currency Mining Operations* of January 30, 2014, (FIN-2014-R001).

http://biznes.pl/magazyny/finanse/bitcoin-niewykorzystana-polska-specjalnosc/s92gwp.

http://www.cbr.ru/press/PR.aspx?file=27012014_1825052.htm.

http://www.communitycurrencieslaw.org/financial-and-banking-laws/#State_Money_Transmission_Laws.

http://comparic.pl/chinski-bank-ludowy-chce-wprowadzic-wlasna-kryptowalute.

https://cs.umd.edu/projects/coinscope/coinscope.pdf. http://www.dbcf.state.ms.us/documents/cons_finance/7515MoneyTranAct2011.pdf. http://www.economie.gouv.fr/files/regulatingvirtualcurrencies.pdf.

https://www.fincen.gov/news_room/nr/pdf/20150505.pdf.

http://independenttrader.pl/krach-na-bitcoin-o-80-w-kilka-minut.html.

http://www.interpol.int/News-and-media/News/2016/N2016-010.

http://www.loc.gov/law/foreign-news/article/russia-bitcoin-exchanges-can-be-penalized/.

http://mises.pl/blog/2012/03/29/machaj-krotki-przewodnik-po-teorii-pieniadza/

http://www.newsbtc.com/2015/11/22/japanese-government-to-draft-regulatory-bill-for-bitcoin-by-early-2016/. http://www.obserwatorfinansowy.pl/tematyka/rynki-finansowe/jesli-bitcoin-jest-pieniadzem-to-transferowym/.

www.pb.pl/3592126,35620,bitcoin-to-piramida-finansowa.

http://pl.scribd.com/doc/289131216/Japan-Ministry-of-Economy-Trade-and-Industry-FinTech-Group-Second-Meeting.

Notes about the authors

***Dr* Sebastian Bala**

Assistant Professor at the University of Opole, he obtained the title of Doctor of mathematical sciences, specialty in the computer science at the University of Wrocław in 2006. Scientifically interested in the theory of automata, computational complexity, cryptography, and computer security. He has been giving lectures on information security for several years.

***Dr* Tomasz Kopyściański, WSB University in Wrocław**

Dean of the Faculty of Finance and Management at WSB University in Wrocław. Lecturer at postgraduate and MBA studies, a member of the Supervisory Board at Logintrade SA, a company listed at Newconnect exchange, court expert in the area of finance and accounting. The main areas of interest include the sources of business financing, corporate finance, monetary policy, public finance.

***Dr hab.* Witold Srokosz, Associate Professor at the University of Wrocław**

Employed in the Department of Financial Law, Faculty of Law, Administration and Economics of the University of Wrocław as the associate professor. Legal advisor in Wrocław, where he runs a lawyer's office. He specializes in banking law and the financial market law. Head of the research project titled "Electronic means of payment without the issuer", financed by the National Science Centre, under which this monograph has been written.

Cryptocurrencies as electronic means of payment without the issuer, 2016

List of figures

Cryptocurrencies as electronic means of payment without the issuer, 2016

List of tables

Cryptocurrencies as electronic means of payment without the issuer, 2016

Orders for the publications of
Wydawnictwo Uniwersytetu Wrocławskiego
should be directed to
Dział Sprzedaży
Wydawnictwa Uniwersytetu Wrocławskiego Sp. z o.o.
50-137 Wrocław, pl. Uniwersytecki 15
tel. +48 71 3752885
e-mail: marketing@wuwr.com.pl
www.wuwr.com.pl

Wydawnictwo Uniwersytetu Wrocławskiego
invites to its bookshops:
• Online bookshop: www.wuwr.com.pl
• Księgarnia Uniwersytecka
50-137 Wrocław, pl. Uniwersytecki 15
tel. + 48 71 3752923

Cryptocurrencies as electronic means of payment without the issuer, 2016