International Journal of Civil Engineering and Technology (IJCIET)
Volume 10, Issue 02, February 2019, pp. 1121–1131, Article ID: IJCIET_10_02_108
Available online at http://www.iaeme.com/ijciet/issues.asp?JType=IJCIET&VType=10&IType=2
ISSN Print: 0976-6308 and ISSN Online: 0976-6316

©IAEME Publication **Scopus** Indexed

SMART SOLUTIONS: RISK MANAGEMENT OF CRYPTO-ASSETS AND BLOCKCHAIN TECHNOLOGY

Iryna Bashynska
Department of Accounting, Analysis and Audit, Odessa National Polytechnic University, Shevchenko av. 1, Odesa, Ukraine

Marina Malanchuk
Department of Economics and Financial Support, National University of Defense of Ukraine named after Ivan Chernyakhovsky, Povitroflotsky av. 28, Kyiv, Ukraine

Olena Zhuravel
Organizations Management Department, Odessa Regional Institute for Public Administration of the National Academy for Public Administration under the President of Ukraine, Genuezskaya str. 22, Odesa, Ukraine

Kateryna Olinichenko
Department of Marketing and Commercial Activities, Kharkiv State University of Food Technology and Trade, Klochkivskaya str. 333, Kharkiv, Ukraine

ABSTRACT

In a digital economy, the phenomenon of crypto-assets recently received considerable attention. The article describes in more detail the features of the functioning of crypto-assets and blockchain technology, identify their inherent risks and propose a mechanism for managing these risks by incorporating crypto-asset risk management units in the culture of risk management.

Key words: bitcoin, blockchain technology, crypto-assets, cryptocurrency, risk management, smart contract, stablecoin, token.

Cite this Article: Iryna Bashynska, Marina Malanchuk, Olena Zhuravel, Kateryna Olinichenko, Smart Solutions: Risk Management of Crypto-Assets and Blockchain Technology, *International Journal of Civil Engineering and Technology (IJCIET)* 10(2), 2019, pp. 1121–1131.
http://www.iaeme.com/IJCIET/issues.asp?JType=IJCIET&VType=10&IType=2

1. INTRODUCTION

In the previous works of the authors [1-5], much attention was paid to risk management, however, not all aspects of this process were covered in full. Due to the rapid development of the field of financial innovation and information technology, world space is transformed into a global business system [6; 7].

Dynamic changes in world processes, especially in the virtual economy, create problems for the national security system, including the financial and economic security of the enterprise. Crypto-assets are a recent phenomenon that gets a lot of attention. However, their specific risks, as well as the risks of the blockchain technology, have not yet been studied in detail.

2. CRYPTO-ASSETS

In a digital economy, the phenomenon of crypto-assets recently received considerable attention. Until now there is no established definition of crypto-assets and they are often called crypto-currencies. Crypto-assets potentials can be described as digital units that are created and transmitted by users using cryptography. Cryptographic assets are digital assets written in a distributed ledger. They get their name from cryptographic security mechanisms that are used in public, unchanged distributed logs.

Represent the classification of crypto-assets in Figure 1.

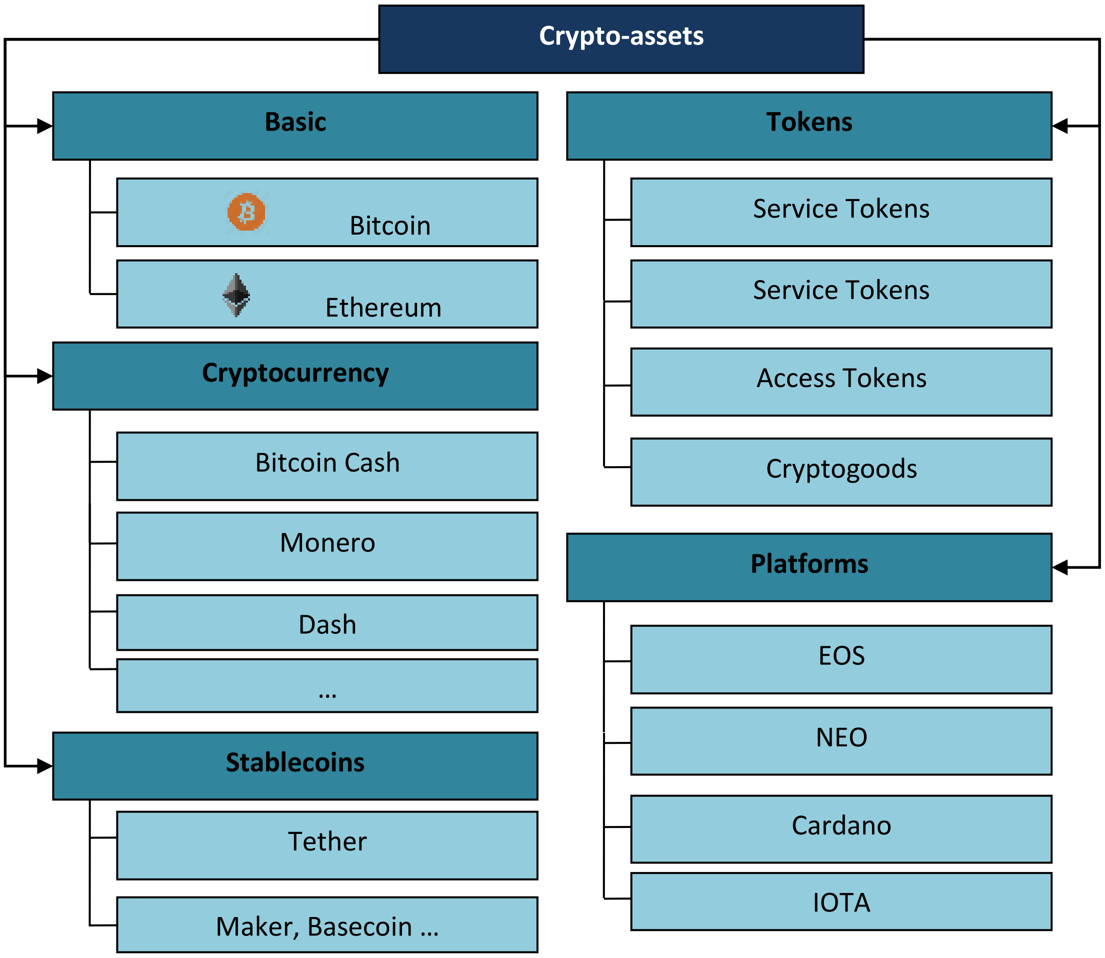

Figure 1 Classification of enterprise crypto-assets

The fundamental aspect consider the allocation of basic crypto-assets – Bitcoin and Ethereum. By many features, the Etherium should lead the list of platforms, but its presence in this class is due to the fact that it still has special properties. Ultimately, investors should convert almost any crypto currency into bitcoins or ether to then buy other coins. While Bitcoins and Ethereum differ in many ways, they combine high quality. There are many convincing arguments in favor of the fact that “bitcoins are the core”, and bitcoins should have their own class, but we believe that these two cryptographic assets combine a special dynamic in the market.

Stablecoins. This type of asset exists to ensure stable cost savings. Currently in this class there is one big player – Tether. However, everything may change soon. Already there are several projects aimed at applying different methods to achieve the stability of the price of the coin. This is a new and growing asset class.

Token is a unit of accounting that is not a cryptographic currency intended to represent a digital balance in some asset, in other words, serves as a "substitute for securities" in the digital world. Tokens are records in a register distributed in a block cache chain. We offer such distribution of tokens by signs:

- Service tokens perform some useful function and serve as a means of calculating and interacting in any application. From platforms, service tokens often differ in that they are on a third-party block and depend on it. The value of service tokens depends on their usefulness, as well as on how much a person uses a program or application to ensure the operation of which service tokens are used. The greater the need for tokens, the higher their price.
- Investment tokens are tokens that are provided with a tangible asset. These tokens are similar to stocks of enterprises. Their value is provided with material assets of the company and for this company is constantly undergoing an independent audit. These markers fall under the law "On Securities".
- Crypto-goods are tokens that are provided with goods or services of their issuer. For example, computing power, if the company is engaged in mining. Usually tokens related to crypto products are on a separate blockade. Their cost depends on the price of the goods or services they provide. From investment tokens they are distinguished by the fact that cryptic goods do not pass mandatory audit as investment tokens, their price is rather conditional and is determined by the market. They also do not fall under the law "On Securities".
- Application Tokens are tokens that serve to organize the work of a particular application. From service tokens, they differ in a more narrow direction. Service tokens can work as part of multiple application interactions, application tokens only work on one application. Their cost depends on the usefulness of this application and how much people use it.

Platforms at their base implement smart contracts and support them. Due to this, on the platform you can create various projects and programs that allow you to use the created smart contracts for various purposes. Smart contracts are required to transfer and store any information, including information about financial transactions. In this case, smart contracts can be used as a payment system or other financial instrument. This may be information about various transactions and contracts concluded – registries, such as the copyright register, the registry of property rights or the register of public services provided. Smart contracts are transparent. Information stored in smart contracts is easy to track, it can not be removed, changed or falsified.

Cryptoctives are sometimes referred to as crypto currencies because Bitcoin's cryptographic currency appeared first and for some time was the only cryptographic asset. The first, still the largest and one of the most famous crypt-assets is Bitcoin. Bitcoin was created in early 2009 by an unknown person or group hiding under the nickname Satoshi Nakamoto. The reason, as noted, is dissatisfaction with the dominant financial system after the financial crisis of 2007-2008. Technically, the concept was based on previous innovations that were already known to computer scientists and cryptographers.

After Bitcoin was introduced, new crypto assets were created in accordance with similar principles, such as Ethereum and Litecoin. Over the past year, the number of crypt assets has grown rapidly and now exceeds 1,500 units.

It is worth noting that the proposed classification is not final and may and should change with the development of the market of cryptographic assets: to supplement, expand categories, exclude them, etc.

3. BLOCKCHAIN TECHNOLOGY

Cryptocysts are usually based on what is known as blockchain technology. Blockchain is composed, as the name implies, from a chain of different blocks, each block consists of several verified transactions. Blockchain can thus be called a digital system that stores all previous transactions. Because there are many different Blockchain crypto assets, there are also many technological variations, but Bitcoin is the oldest and still the largest cryptographic asset, and so we decided to illustrate the work of the block circuit based on this asset. Most other crypto-assets operate on the same lines, even if there are some exceptions. For clarity, we will show the Blockchain technology on a practical example (Fig. 2).

Blockchain technology is easier to describe through the implementation of financial transactions with Bitcoin. Bitcoin is a decentralized system where users make nodes on the network. Payments are made and new crypto-asset units are created by interaction between the users themselves. The system operates according to a number of rules, the so-called Bitcoin protocol.

Each user and owner of Bitcoins has a couple of public and private keys, which is generated randomly. The network verifies whether the subject has money (bitcoins) and verifies the transaction through a public key. Transactions form a consistent system, and the very mechanism of merging transactions into blocks is called "blockchain " (literally – "chain of blocks").

In the blockchain algorithm there is a mathematical hash function, which takes 10 minutes to calculate, and a fraction of a second for verification. For calculations involved the power of many computers around the world: who first calculates, receives a reward of 12 Bitcoins. To validate a transaction, it is necessary to collect 6 confirmations of the correct function calculation, after which the transaction record falls into the distributed registry.

In practice, the world of crypto-assets has a hundred innovations each month, with new products that combine various features of cryptographic technologies and distributed logs (something like a book in electronic form). Nevertheless, we believe that it is possible to roughly classify the world of crypt assets in those representing the institutions or assets most prominent in currencies (cybercurrencies) and those networks for future services or payments (ICO). Finally, there are cryptographic service providers, through which crypto assets can exchange against each other and against real currencies, and suppliers of purses that offer brokerage services and simple services, such as cryptographic keys. This distinction has significant implications for risk management, regulation and supervision.

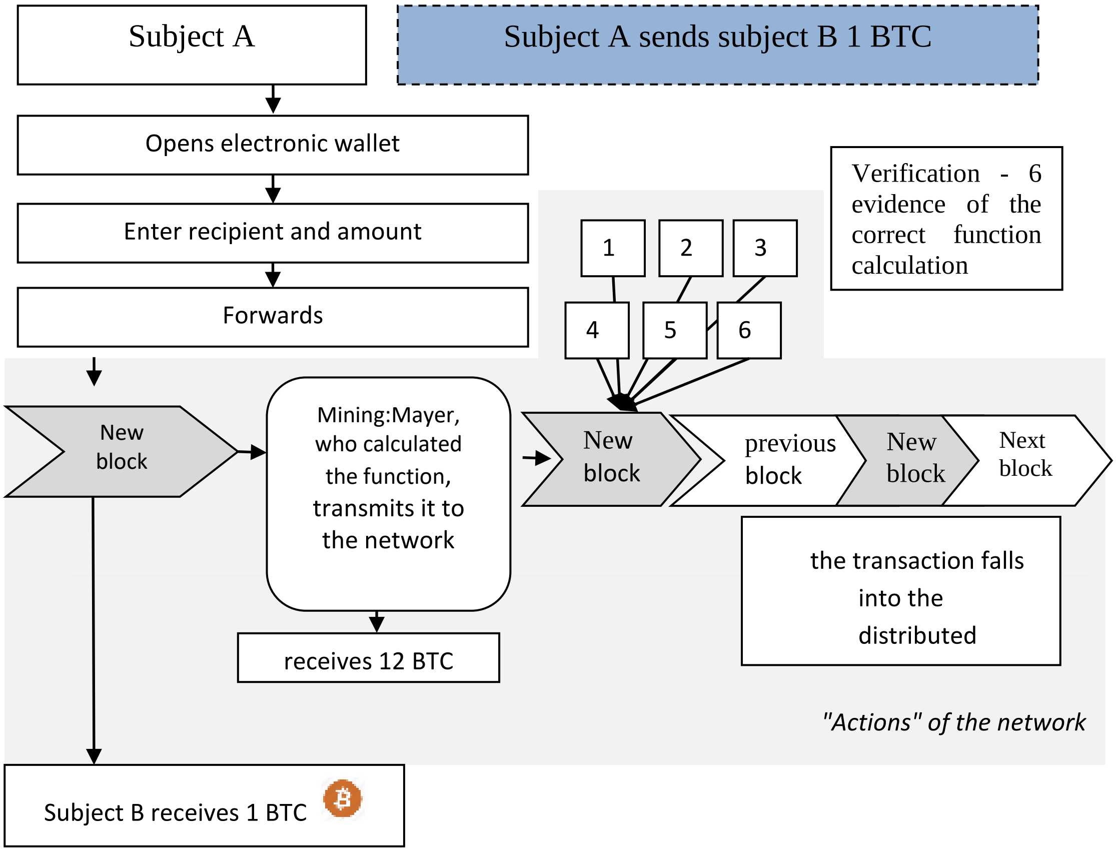
Subject A
Subject A sends subject B 1 BTC
Opens electronic wallet
Enter recipient and amount
Forwards
Verification - 6 evidence of the correct function calculation
1
2
3
4
5
6
New block
Mining:Mayer, who calculated the function, transmits it to the network
New block
previous block
New block
Next block
receives 12 BTC
the transaction falls into the distributed
"Actions" of the network
Subject B receives 1 BTC

Figure 1 Blockchain technology

3.1. Mathematical Foundations of Blockchain

The fundamental part of Blockchain are cryptographic algorithms. In particular, the ECDSA algorithm is an Elliptic Curve Digital Signature Algorithm, which uses elliptic curves and finite fields to sign data so that a third party can confirm the authenticity of the signature by eliminating the possibility of falsification. ECDSA uses different procedures for signing and verification, consisting of several arithmetic operations.

The elliptic curve over the field K is a cubic curve over the algebraic closure of the field K, defined by a third-degree equation with coefficients from the field K and a "point at infinity". One form of elliptic curves are Weierstrass curves:

For coefficients a = 0 and b = 7 (used in Bitcoin), the graph of the function takes the following form (Fig. 2) [8].

$$y^2 = x^3 + ax + b$$

Elliptic curves have several interesting properties, for example, a non-vertical line intersecting two non-tangent points on a curve will cross a third point on a curve. The sum of two points on the P + Q curve is called the R point, which is a reflection of the -R point (constructed by continuing the straight line (P; Q) to the intersection with the curve) relative to the X axis (Fig. 3) [9].

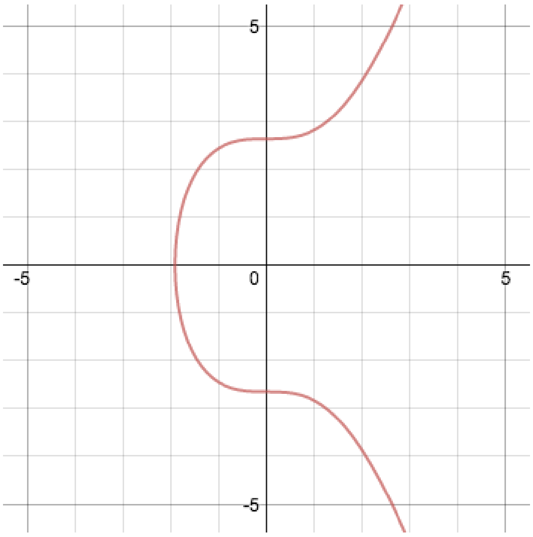

Figure 2 An elliptic curve

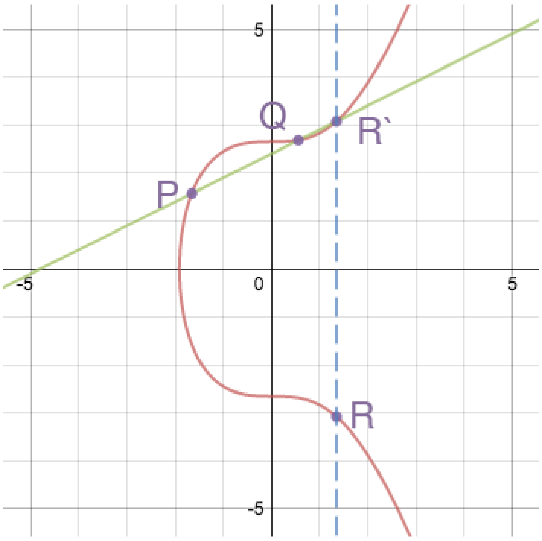

Figure 3 The sum of two points on the curve

If we draw a straight line through two points that have coordinates of the form P (a, b) and Q (a, -b), then it will be parallel to the ordinate axis. In this case there will be no third intersection point. To solve this problem, a so-called point at infinity (point of infinity) is introduced, denoted as O. Therefore, if there is no intersection, the equation takes the following form P + Q = O.

If we want to add the point to itself (double it), then in this case the tangent to the point Q is simply drawn. The resulting intersection point is reflected symmetrically with respect to the X axis (Fig. 4).

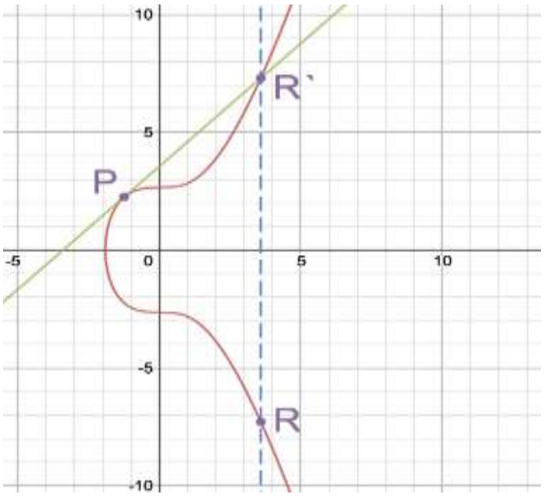

Figure 4 Double point

These operations allow us to carry out the scalar multiplication of the point R = k * P, adding the point P with itself k times. However, note that faster methods are used to work with large numbers.

In elliptical cryptography (ECC), the same curve is used, only considered over some finite field. The final field in the context of the ECC can be represented as a predefined set of positive numbers, which should be the result of each calculation:

$$y^2 = x^3 + ax + b \ (mod\ p)$$

For example, 9 mod 7 = 2. Here we have a finite field from 0 to 6, and all operations modulo 7, no matter how many times they are carried out, will give a result that falls in this range.

All the properties mentioned above (addition, multiplication, point at infinity) for such a function remain in force, although the graph of this curve will not resemble an elliptic curve. The bitcoin elliptic curve, $y^2 = x^3 + 7$, defined on the finite field modulo 67, looks like in Fig. 5.

This is a set of points where all values of x and y are integers between 0 and 66. The straight lines drawn on this graph will now “wrap” around the field as soon as they reach barrier 67 and continue from the other end of it. while maintaining the same slope, but with a shift. For example, the addition of points (2, 22) and (6, 25) in this particular case looks like in Fig. 6 [9].

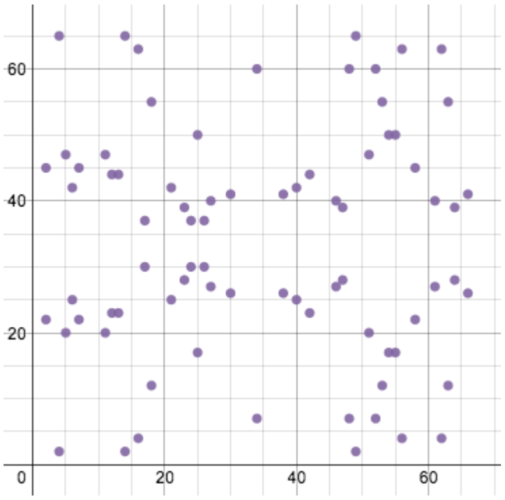

Figure 5 Bitcoin elliptic curve defined on a finite field modulo 67

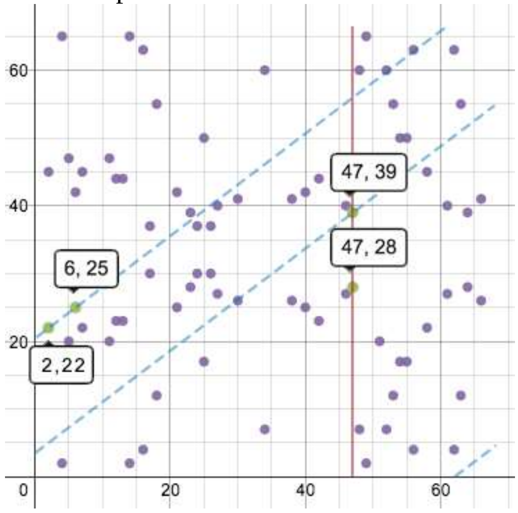

Figure 6 Addition of points (2, 22) and (6, 25)

3.2. ECDSA in bitcoin

The Bitcoin protocol contains a set of parameters for an elliptic curve and its finite field, so that each user uses a well-defined set of equations. Among the recorded parameters, the equation of the curve (equation), the value of the field modulus (prime modulo), the base point on the curve (base point) and the order of the base point (order) are distinguished. This parameter is chosen specifically and is a very large prime number.

In the case of bitcoin, the following values are used:

The equation of an elliptic curve: $y^2 = x^3 + 7$

Simple module: 2^{256}— $2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1 =$ FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE FFFFFC2F

Base point:

04 79BE667E F9DCBBAC 55A06295 CE870B07 029BFCDB 2DCE28D9 59F2815B 16F81798 483ADA77 26A3C465 5DA4FBFC 0E1108A8 FD17B448 A6855419 9C47D08F FB10D4B8

The bold font is the x coordinate in hexadecimal notation. It is immediately followed by the Y coordinate.

Order: FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE BAAEDCE6 AF48A03B BFD25E8C D0364141

This set of parameters for an elliptic curve is known as secp256k1 and is part of the SEC (Standards for Efficient Cryptography) family of standards proposed for use in cryptography. In Bitcoin, the secp256k1 curve is used in conjunction with the ECDSA (elliptic curve digital signature algorithm). In ECDSA, a secret key is a random number between one and an order value. The public key is generated based on the secret: the latter is multiplied by the value of the base point. The equation has the following form:

$$Public\ key\ =\ private\ key\ *\ G$$

This shows that the maximum number of secret keys (therefore bitcoin addresses) is the final and is equal to the order. However, the order is an incredibly large number, so it is unrealistic to accidentally or intentionally pick up another user's secret key.

The public key is calculated using the same doubling and adding points operations. This is a trivial task that an ordinary personal computer or smartphone solves in milliseconds. But the inverse problem (obtaining a secret key publicly) is a problem of discrete logarithmization, which is considered computationally complex (although there is no strict proof of this fact). The best known algorithms for its solution, like Pollard's rho [10], have exponential complexity. For secp256k1, in order to solve the problem, you need about 2^{128} operations, which will require a computation time on a regular computer, comparable to the lifetime of the Universe.

When a private / public key pair is obtained, it can be used to sign data. This data can be of any length. Usually, the first step is to hash the data in order to obtain a unique value with the number of bits equal to the bit order of the curve (256). After hashing, the z data signing algorithm is as follows. Here, G is the base point, n is the order, and d is the secret key.

After receiving the data and signing it, a third party, knowing the public key, can verify it as follows:

$$\mathrm{uG + vQ = u + vdG = (u + vd)G = (zs^{-1} + rds^{-1})G = (z + rd)\, s^{-1}G = kG}$$

ECDSA security is related to the complexity of the secret key search task described above. In addition, the security of the original scheme depends on the “randomness” of the choice of k when creating a signature. If the same value k is used more than once, then the secret key can be extracted from the signatures. Therefore, modern implementations of ECDSA, including those used in most bitcoin wallets, generate k deterministic based on the secret key and the message to be signed.

4. RISK MANAGEMENT OF CRYPTO-ASSETS

Society believes that it is impossible to stop technology development in our digital age. Thus, enterprises should be far-sighted and think about the use of crypto-asssets in their activities today. First of all, today it is necessary to review the existing risk management culture at the enterprise and integrate it into risk management of cryptographic assets.

Management of most risks represents a culture that consists of certain stages. Rigorously generalizing the risks of crypto-asssets, they can be attributed, first of all, to information risks. In this way, we propose to manage the risks of cryptographic assets as part of the risk management culture in the enterprise's economic security system. That is, it is necessary to incorporate into the culture special blocks that will help manage this type of risk (Fig. 7).

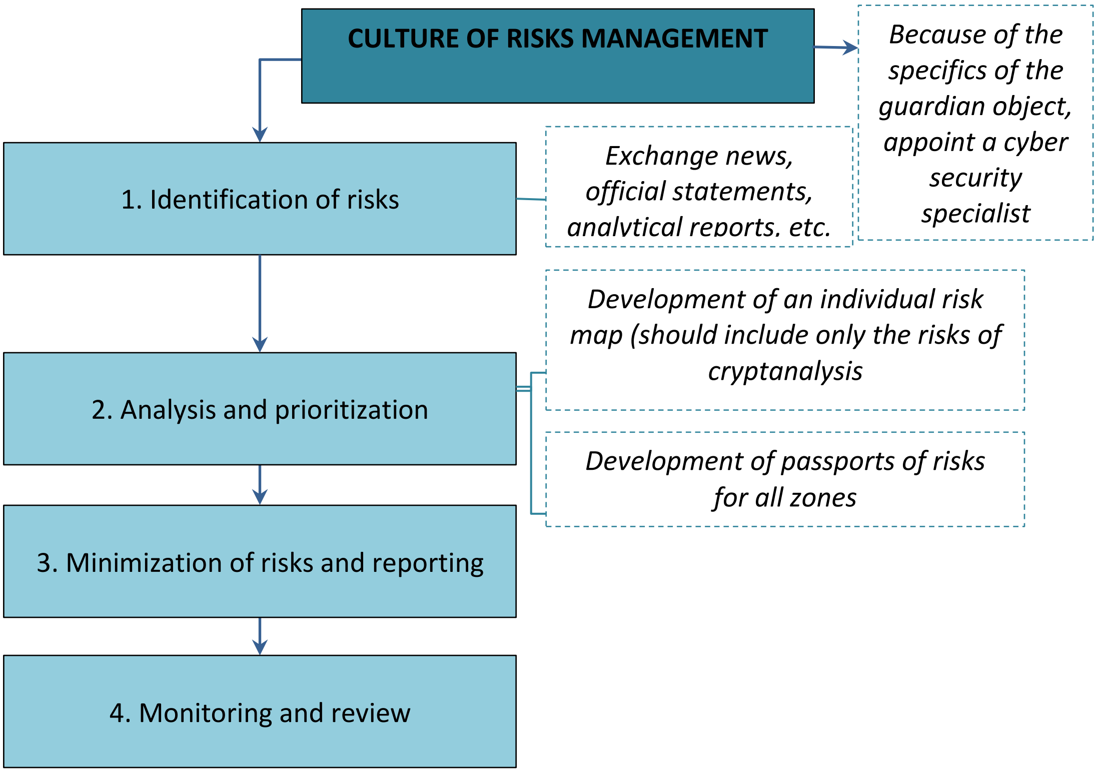
CULTURE OF RISKS MANAGEMENT
Because of the specifics of the guardian object, appoint a cyber security specialist
1. Identification of risks
Exchange news, official statements, analvtical reports, etc.
Development of an individual risk map (should include only the risks of cryptanalysis
2. Analysis and prioritization
Development of passports of risks for all zones
3. Minimization of risks and reporting
4. Monitoring and review

Figure 7 The proposed adjustment of the culture of risk management due to the risks of crypto-assets

As you can see, the specifics of cryptographic assets impose their limits and limits on the culture of enterprise risk management, so we recommend starting with the hiring of a cybersecurity specialist, and in addition, he may be a specialist in risk management.

The cryptocurrency market is unstable, as it is at the stage of formation. It requires special knowledge and skills that are often incomprehensible to beginners. And while high volatility may seem attractive to investment, there are numerous risks in this completely new field.

5. CONCLUSIONS

In practice, the world of crypto-assets has a hundred innovations each month, with new products that combine various features of cryptographic technologies and distributed logs (something like a book in electronic form). Nevertheless, we believe that it is possible to roughly classify the world of crypt assets in those representing the institutions or assets most prominent in currencies (cybercurrencies) and those networks for future services or payments (ICO). Finally, there are cryptographic service providers, through which crypto assets can exchange against each other and against real currencies, and suppliers of purses that offer brokerage services and simple services, such as cryptographic keys. This distinction has significant implications for risk management, regulation and supervision.

The purpose of this study was to describe in more detail the features of the functioning of these technologies, identify their inherent risks and propose a mechanism for managing these risks.

REFERENCES

[1] Iryna Bashynska, Volodymyr Filippov, Nadiia Novak, Smart Solutions: Protection NFC Cards with Shielding Plates, *International Journal of Civil Engineering and Technology* (IJCIET) 9(11), 2018, pp. 1063–1071

[2] Lagodiienko Volodymyr, Malanchuk Marina, Gayvoronska Inna and Sedikov Denys. Selection of criteria for key performance indicators by the matrix method, *International Journal of Mechanical Engineering and Technology*, 10(1), 2019, pp. 1303-1311

[3] Bashynska, A. Dyskina The overview-analytical document of the international experience of building smart city, *Verslas: Teorija Ir Praktika / Business: Theory And Practice*, 2018 19: 228-241 https://doi.org/10.3846/btp.2018.23

[4] Bashynska I.O. Using the method of expert evaluation in economic calculations, *Actual Problems of Economics*, 7 (169): 408-412

[5] Bondarenko Svitlana, Bodenchuk Liliya, Krynytska Oksana and Gayvoronska Inna, Modelling Instruments in Risk Management, *International Journal of Civil Engineering and Technology*, 10(01), 2019, pp. 1561–1568

[6] K. Tanashchuk, K. Kovtunenko, Yu. Kovtunenko, Theoretical and Methodical Principles of Capital Structure Management in the Innovation Activity of Telecommunication Operators, *Journal of Automation and Information Sciences* 50 (3), 2018, pp. 71-84. http://10.1615/JAutomatInfScien.v50.i3.60

[7] Svitlana Bondarenko, Iryna Liganenko, Olga Kalaman and Liubov Niekrasova, Comparison of Methods For Determining The Competitiveness of Enterprises To Determine Market Strategy, *International Journal of Civil Engineering and Technology (IJCIET)* 9(13), 2018, pp. 890–898

[8] Rykwalder E. The Math Behind Bitcoin. Retrieved from:
https://www.coindesk.com/math-behind-bitcoin

[9] Mistry N. An Introduction to Bitcoin, Elliptic Curves and the Mathematics of ECDSA. Retrieved from: https://www.slideshare.net/NikeshMistry1/introduction-to-bitcoin-and-ecdsa?from_action=save

[10] Pollard's rho algorithm for logarithms. Retrieved from:
https://en.wikipedia.org/wiki/Pollard%27s_rho_algorithm_for_logarithms

[11] Manisha Valera, Parth Patel and Shruti Chettiar, an Avant-Garde Approach of Blockchain in Big Data Analytics, *International Journal of Computer Engineering and Technology*, 9(6), 2018, pp. (115)-(120).

[12] Reepu,Blockchain: Social Innovation in Finance & Accounting, *International Journal of Management*, 10(1), 2019, pp. 14-18.

[13] Irina Yakovenko, Lyazzat Kulumbetova, Irina Subbotina, Gaukhar Zhanibekova and Kenzhegul Bizhanova, the Blockchain Technology as a Catalyst for Digital Transformation of Education, *International Journal of Mechanical Engineering and Technology*, 10(01), 2019, pp.886–897