Advances in Social Science, Education and Humanities Research, volume 240

2nd International Scientific Conference on New Industrialization: Global, National, Regional Dimension (SICNI 2018)

Concept of the cryptoruble market formation in Russia

Michail Loginov
Ural state University of Economics
Yekaterinburg, Russian Federation
e-mail: port-all@mail.ru

Vasily Tatyannikov
Ural state University of Economics
Yekaterinburg, Russian Federation
e-mail: vat55@mail.ru

Nadezhda Sobina
Ural state University of Economics
Yekaterinburg, Russian Federation
e-mail: pozdnyakova0610@yandex.ru

Abstract – **The subject of this study is the economic relations arising during the cryptocurrency market formation on the basis of the national banking network. The purpose of the study is to analyze the use of various cryptocurrency technologies, identify problems and develop proposals for the organization of the cryptoruble market in Russia.The methodological basis of this study consists of such methods of scientific research as analysis and synthesis, induction and deduction, grouping and comparison, detailing and generalization, systematization and classification Main results: 1. The author's classification of crypto-money, which allows to systematize the approaches to the formation of cryptocurrency markets, has been carried out. 2. The technologies underlying cryptocurrency functioning were studied. Various payment methods using cryptoruble are proposed such as personal identification, e-wallet, electronic deposit (cryptodeposit) using a unique number and a password to use. 3. A typology of cryptocurrency emissions is presented. 4. Steps to create a national crypto network were proposed; 5. The author's approach to the formation of a crypto-ruble market in Russia is developed. The peculiarities of the proposed monetary system is a cryptoruble provided by the government of the Russian Federation with energy resources of the country, each cryptoruble unit has its own unique account number using the blockchain technology, which allows to control the movement of crypto money. The institutional support of the cryptoruble market includes the central bank, commercial or crypto-banks, a crypto-exchange, the federal tax service, data centers, various users. Key findings of the study: 1. Cryptocurrency management approachesare systematized 2. An algorithm for creating a cryptoruble market based on a central bank hybrid network has been proposed.**

Keywords –cryptocurrency, blockchain, bitcoin, cryptoruble, cryptoshares, cryptomoney

I.INTRODUCTION

The topic of cryptocurrencies was one of the most relevant in 2016 – early 2018 among foreign and domestic economists.

Central banks, commercial banks and various financial institutions have been active attempts to introduce the technology of the blockchain, they also considered the possibility of issue ofstate electronic money on the basis of the blockchain with the transfer of the emission of cryptocurrencies (mining) tospecialized IT-companies. However, closer to the end of 2018, the topic of cryptocurrencies becomes less relevant, which is associated both with a decrease in the marketing promotion of cryptocurrencies, and the general decline in interest in their technological component. However, the potential of crypto money remains quite high and is not fully disclosed in the scientific literature.

The purpose of this article is to present the fundamentals of establishing a cryptomoneymarket based on blockchain technology and to develop proposals on formation of thecryptoruble market in Russia.

II. LITERATURE REVIEW

In the scientific literature, a significant amount of works is devoted to the study of the system`s formation. [1-10]

III. RESEARCH METHODOLOGY

First, we propose to consider the existing technology of organization of the system in which the movement of cryptocurrency takes place.

The basis of the cryptosystem isthe technology of computer asymmetric encryption, which has already become standard. This technology is based on two keys (ciphers) – open and closed. The public key is available to everyone, and the private key is at the sender. When sending a message (transaction), the text is encrypted by the computer program using the private key; in the future the text can only be decrypted using the public key. The decryption of the message using the public key is a confirmation of the sender's identification (verification). To send a message to the sender, the text encrypted with his or her public key is sentvia Internet, this text can only be decrypted with the sender`s private key.

The basis of security of the cryptosystem is its availability, safety and originality of public keys. In the cryptosystem, the problem of originality is solved through the creation of "electronic wallets" to which both keys are tied, while the private key is the password for access to the electronic wallet.

When passing transactions between wallets, both parties confirm the transaction with their private keys. Since the e-wallet is in fact an identifier in the cryptosystem, the number of monetary units located in it is registered in the registry, and when a transaction is passed between wallets in the registry, the number of monetary units of the parties to the transaction changes. The register contains details of user transactions and account balances (electronic wallets).

The cryptosystem registry can be either centralized, which is a database stored on a server or in the cloud at the system administrator, and decentralized, which is a document stored at each member of the system. In the case of a centralized registry, the administrator of the cryptosystem has the ability to adjust the registry data, in the case of a decentralized registry, the adjustment is possible only with the consent of all participants in the system.

Asymmetric cryptography is used in WiFi, Bluetooth, secure sites where data is encrypted to prevent interception of messages or transactions.

IV. PRACTICAL SIGNIFICANCE, SUGGESTIONS AND RESULTS OF INTRODUCTIONS, RESULTS OF EXPERIMENTAL RESEARCHES

Existing cryptocurrencies are similar to non-cash funds, their turnover is based on changes in the registry entries, respectively, and each monetary unit cannot be identified.

One of the main issues of the organization of a cryptosystem is the determination of the order of receipt of money in circulation or their emission. Several types are possible:

- Type 1– the number of currency notes in the cryptosystem is limited (for example, bitcoin, its derivatives and analogues). The organization of the cryptosystem is set to the maximum number of coins, which is not subject to reduction. These cryptocurrencies by their nature represent the shares or tokens of the cryptosystem that issued them. Types of emission:

a) currency notes are entered all at the same time when creating a cryptosystem and distributed among existing e-wallets, from which they are subsequently transferred to newly created wallets;

b) currencynotes are introduced in portions, which is tied to any special conditions of issue (mining) or bonuses of the system.

Type 2– the number of currency notes in the system is not limited. The emission is performed by exchanging currency to cryptocurrencies via "contact point": banks, exchange offices, stock exchanges, terminals, etc. The number of units in them isn`t constant, due to input-output of the funds of the cryptosystem. These cryptocurrencies are electronic money or cryptomoney and are tied to the current money. SuchcryptomoneyincludesYandex.Money, QIWI, PayPalandothers.

The main advantage and problem of the blockchain is a decentralized network, which allows ensuring transparency of the cryptosystem registry, but does not allow to control and to make changes to the software and registry without the consent of all users.

In essence, the existing cryptocurrency does not depend on central banks and is a "private money game", supported by the speculative interest of the participants of the cryptosystem. Therefore, we can predict that the type 1 cryptocurrency indicated above will remain a “game” form of private money, far from the real economy. Table 1 presents the author’s classification of cryptomoney (cryptocurrency).

TABLE I. CRYPTOMONEY (CRYPTOCURRENCY) CLASSIFICATION.

№№	Indicator	Indicator value
1. Content		
1.1	Approaches to determining the content of cryptomoney (cryptocurrency)	- analogue of cash (USA, Japan); -electronic payment system (Spain); - unit of account (Germany); - private money; - a type of digital (virtual) currency (France) or currency (Sweden); - money surrogate as an object of property rights used as a means of payment and (or) exchange for money; - single-purpose vouchers (England before 2014) ; - electronic bill; - property, object of property (the USA, China); - goods, virtual goods (China); - investment asset (instrument); -financial instrument; - digital goods (Spain); - barter transactions, barter exchange (Australia, Singapore) [11]; - legal tender; - medium of exchange; - unit of account; - cost saving facility; - digitized securities.
1.2	Legal tender	Yes No Partially (under the condition) Yes with taxation
1.3	Type of government regulation	Full regulation Partial regulation No regulation
1.4	Cryptocurrencies hierarchy	World, interstate, national, private
2. Technologies		

2.1	Networktype	Centralized, decentralized (distributed, peer-to-peer), hybrid (centralized, peer-to-peer)[12]
2.2	Applied technology	Blockchain, DAG-confirmation by transactions, DLT - distributed registry technology, etc.
2.3	Code type	Open, closed, partially open
2.4	Individualization of monetary units based on the blockchain protocol	- general (no individualization); - group individualization; -individual protocol for each currency unit
2.5	Cryptomoney providing	- secured - unsecured
2.6	Number of keys used	- single -multi-signature (multi-key)
2.7	Transactions	- reverse -non-return - non-negotiable with a contract
2.8	Principles of adding a new block to the block chain (mining)	- Proof-of-work; - Proof-of-stake; - Proof-of-space; -Proof-of-movement; - Proof-of-importance;
2.9	Blockchain vulnerabilities (threats)	- Block size limit - low bandwidth - “The majority attack” or 51 percent - the owner of 51% or more mining capacity becomes the owner of the blockchain branches and the manager of transactions in the network - Errors in smart contracts lead to a decrease in network security. -Denial of service (blocking the system by an excessive number of requests - DDOS-attack) -Loss of the private key to the wallet leads to the loss of coins in the account -Hard fork - protocol division into two conflicting networks -Partial or total network blocking
	3.Emission	
3.1.	Type of issue (from the site ru.wikipedia.org)	-mining-a series of calculations with the search parameters to find the hash with the given properties. - forging - the creation of new units based on the confirmation of ownership interest with the opportunity to be rewarded -ICO–form of attracting investments by sailing to investors a fixed number of new units of cryptocurrencies received by a single issue
3.2	Cryptocurrency issuers	Central bank Financial institution Digital platform Private person
3.3	Type of crypto money emission	- one-time (accelerated) or emission of the entire money supply - phased, determined by the system conditions - programmable emission - free transfer of cryptomoney to wallets (grants, sponsorship, etc.) - transfer (paid or free) of fiat money to crypto money through gates (gateways) - banks, payment systems, clearing organizations, trading floors, financial companies, etc. - demission-mandatory destruction of a fixed amount in each transaction
3.4	Emission size	- fixed, the number of coins (monetary units) is limited; - no restrictions, tying crypto money to the volume of sales or time of emission
3.5	Emission limits	Emission criteria Arrangements of the parties Amount of security Entered individually (number of coins, amount of security, no limits)

However, bitcoin has already contributed to the change in the technological structure of the economy and entered the history of the global financial system, primarily through the formation of the cryptocurrencies global market, its promotion and the creation of demand.

In the face of increasing business and government interest in electronic money, the state that offers its people and the global community cryptomoney backed by assets with clear emission technology will be able to take both the bitcoin-created cryptocurrency market and create the world currency among electronic money.

By cryptomoney, the authors understand the central bank's monetary obligations, expressed in cryptorubles, which are the national currency of Russia in digital form, which is created using cryptographic methods.

The authors propose the following hierarchy of cryptomoney (cryptocurrency):

1. World cryptomoney, decentralized or centralized, without trust (security), is issued by the nation state, or by a union of states.

2.Interstate cryptomoney is non-numerical, centralized, without trust (not secured, secured). Interstate settlements are carried out according to the principle of SDR; binding to a specific commodity market is possible - oil, gas, metal, coal, electricity.

Sub-level is possible - regional cryptomoney - centralized, on trust (secured), issued within the framework of interstate institutions - EU, CIS, BRICS, ASEAN.

3. National cryptomoney is centralized, on trust (secured), issued by states.

4. Private cryptocurrencies or tokens-decentralized, untrusted, non-numbered, regulated or unregulated by state authorities

Stages of development of the national crypto network:

Stage 1. The issuer, the cryptoruble registry holder is the central bank. A single-level cryptoruble system is being formed, where the central bank is the issuer and all other are its clients.

The main points of the central bank registry include: the number of the cryptoruble, the address of the owner (location) or the number of his electronic wallet, who made changes to the registry; the cryptoruble registry - its number, addresses and transaction structure, the requirements of the transaction under the condition.

Stage 2. The issuer is the central bank, market participants are crypto banks, crypto companies,crypto-exchange. A two-tier cryptoruble system is formed, where at the first level the central bank is the issuer, the main registrar of the cryptoruble, at the second level, under the license of the central bank, there are crypto banks which open accounts (e-wallets), offer services, loans. When issuing loans, there is no requirement of the central bank for regulatory reservations, crypto banks are not eligible to issue cryptomoney. The outcome of the stage is the creation of a digital business field or cryptoeconomy, as a segment of the digital economy; There is a possibility of paying taxes by cryptomoney.

Stage 3.Cryptosharesare denominated in cryptocurrency. At this stage, the digital stock market is formed. The cryptoshare technology allows any company to issue its own shares in the form of cryptoshares or to convert its traditional shares into it. After that, the company can publicly trade them in a crypto-exchange. In this case, there is no need for the company to submit documents to the Securities and Exchange Commission (SEC) in order to obtain approval from the regulator.

This technology reduces the path from company to investor to two steps:

- release of own cryptoshares;
- putting them on the trading floor – crypto-exchange.

This stage development is carried out in parallel with the previous ones.

The authors propose the following approach to the formation of a cryptomoney market in Russia:

1. The cryptosystem in Russia should be based on a partially decentralized or hybrid network owned by the Bank of Russia and this is one of the main differences from the fully decentralized blockchain network.

A hybrid network based on the servers available at the Central Bank of the Russian Federation will help to coordinate the work, search and provide information about existing network machines and their status. Hybrid networks combine the speed of centralized networks and the reliability of decentralized ones thanks to hybrid schemes with independent indexing servers that synchronize information with each other. When one or more servers fail, the network continues to function.

2. The emission of cryptomoney is carried out by exchanging bank notes for a cryptocurrency through points of contact (emission type 2 indicated above).

3. Each cryptocurrency unit - a cryptoruble has its own unique number, which will make it possible to escape from the impersonality of electronic money and will enable the Central Bank to exercise control over countering terrorism and money laundering.

4. When creating a cryptoruble, the blockchain technology is used, so each coin has its own centralized journal of records — an individual register maintained using the blockchain technology [7, p. 22], where the Central Bank or crypto banks enter all transactions with this cryptoruble.

During a transaction, when cryptomoney is transferred from one e-wallet to another, each cryptoruble from the transaction is recorded by completing its registry with information about the transaction.

5. The cryptosystem provides three options for working with cryptomoney:

- personal identification, when specific cryptorubles belonging to a user in a cryptosystemare reserved for him (as a physical or a legal entity); for their use a personal identification by the central bank or a crypto bank established by the central bank is necessary, which allows the client to be protected from unauthorized access to cryptomoney;
- an electronic -wallet with a unique number is assigned to the user in the system, and the cryptomoney belonging to him with specific individual numbers is reserved for the number in the cryptosystem. Transactions in the wallet are carried out using one or several private keys;
- electronic deposit (cryptodeposit) - a certain number of cryptorubles owned by the user are reserved in the cryptosystem. An electronic deposit is drawn up from cryptorubles with their identification numbers, which is assigned a unique number and password for use.

To use crypto money, a user needs to log in to the cryptosystem, enter the electronic deposit number and password. Cryptodeposite is not tied to a specific user and e-wallet, it can be any user. The electronic deposit number and password can be forwarded between users by email or in any other way. It is possible to withdraw funds from an electronic deposit through credit cards and ATMs.

6. The cryptosystem includes the following elements:

- The Central Bank of the Russian Federation performs cryptoruble emission, operations with crypto-money, including input-output of money from the cryptosystem, develops and controls software, monitors the cryptosystem, licenses and controls the activity of crypto banks and crypto-counter in the cryptosystem, provides individuals and legal entities with electronic wallets for work cryptosystem;
- cryptobank is an independent member of the system, which operates under a central bank license, can be a structural unit of a commercial bank, provides e-wallets, deposits money from a cryptosystem, provides various types of banking services (loans, forfeiting, etc.) ;
- e-wallet holders –physical or legal entities, for which identification in the network is strictly required. For physical entities, identification can be done through the public services portal. For legal entities, it is also mandatory to have a multi-signature for an electronic wallet.
- crypto-exchange - carries out exchange trading in crypto money, crypto shares, etc. on the basis of a license of the central bank. These functions can be performed by the structural division of the current stock exchange - Moscow Exchange PJSC.
- Federal Tax Service monitors the activities of legal entities. If legal entities and individual entrepreneurs do not have settlement accounts in commercial banks (there is only an electronic wallet in the cryptosystem), the obligation of quarterly reporting is removed from these legal entities. The compilation and verification of the statements of these persons is carried out by the functional units of the FTS.
- -data centers maintain and monitor cryptosystems by using artificial intelligence technologies.

The main feature of the cryptosystem proposed by the authors is the providing the cryptorublewith assets which are various types of energy [13]. The energy supply may be electricity, gas, oil, coal. It allows the cryptoruble owner, if necessary, to exchange cryptomoney for the state-owned energy carriers. Thecryptoruble providing can be either complete or partial.

Having a unique individual number in a cryptoruble and linking it to specific users allows to ensure the security of the cryptosystem, track hacker attacks, control unlawful actions of users.

V. CONCLUSIONS

In conclusion, the article should note the main features of the cryptosystem proposed by the author - cryptoruble with energy supply, hybrid network, the individualization of cryptoruble based on blockchain technology. The development of the domestic cryptosystem in the future will allow replacing the US dollar in transactions with energy carriers with the use of a cryptoruble with energy supply as the main world currency.

VI. DISCUSSION OF THE RESULTS

A crypto-monetary system will develop if cryptomoney has significant advantages, such as:

1. No deposit (non-cash) emission, high stability and liquidity of the system.

2. Providing cryptomoney on the basis of energy resources.

3. No high bank transaction fees.

4. No cross-national barriers to transactions.

5.High speed of cryptomoney transfer to the account.

6. Unified digital interaction platform.

7. Individualization of a cryptoruble currency.

8. Legal entities are able to maintain accounting in cloud services, simplifying reporting to the tax office.

9. Technological ease of transactions under the condition, the ability to make non-refundable payments.

10. The ability to control the availability of cash (cryptomoney) from the counterparty at the conclusion of the transaction and to lock it for the duration of the transaction.

Crypto-money will help to attract investment in the Russian economy; will provide an opportunity for foreign investors to buy real estate and other assets for cryptorubles. A decrease in real money supply due to an increase in cryptomoney will help to reduce inflation and increase the population investment activity.

References

[1] Friedrich August von Hayek *Denationalisation of Money: An Analysis of the Theory and Practice of Concurrent Currencies*. London: Institute of Economic Affairs, 1976.

[2] Chaum D. Blind Signatures for Untraceable Payments, In: Chaum D., Rivest R.L., Sherman A.T. (eds) *Advances in Cryptology*. Springer, Boston, MA, 1983

[3] Satoshi Nakamoto *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008.

[4] A. Tapscott, D. Tapscott *Blockchain technology is what drives the financial revolution today*, Moscow: Exmo, 2017, 448p.

[5] W. Magyar, V. Buterin *Blockchain for business*, Moscow, Eksmo, 2017, 224p.

[6] D. Karpilovsky *Bitcoin, blockchain and how to make money on cryptocurrencies*, Moscow: AST, 2018, 256p.

[7] M. Swan Blockchain. *Scheme of the new economy*, Olympus-Business, 2015.

[8] P. Vinia, M. Casey *The era of cryptocurrencies. How bitcoin and blockchain are changing the world economic order*, Mann, Ivanov and Ferber, 2018, 432p.

[9] E. D. Butenko Bitcoin. State and prospects of cryptocurrency development, *Finance and credit*, 2014, No. 23, pp. 44-47.

[10] V. Katasonov *Digital Finance. Cryptocurrency and e-economy. Freedom or a concentration camp?*, Moscow: Book world, 2017, 320 p.

[11] Kuznetsov, Yakubov Approaches to international regulation (bitcoin) in certain foreign jurisdictions, *Money and credit*, 2016, №3, pp. 20-29.

[12] M.P.Voronov, V.P.Chasovskih Formation of the concept of marketing 3.0 in the context of globalization and development of social communications, *Discussion*, 2013, № 3 (38), pp. 103-114.

[13] M.P. Loginov Formation of the cryptocurrency market in Russia, *Economic, social and spiritual renewal - the basis of the new industrialization of Russia*, Collection of the Vth Ural scientific readings of professors and doctoral students of social Sciences (Ekaterinburg, February 6, 2018), Publishing house Ural. state Econ. un-ty, 2018.