Practices of Using Blockchain Technology in ICT under the Digitalization of the World Economy

Nataliia Kraus [1] [0000-0001-8610-3980], Nataliia Andrusiak [2] [0000-0001-8939-7750], Alina Savchenko [3] [0000-0001-8205-8852], and Maksim Iavich [4] [0000-0002-3109-7971]

[1] Borys Grinchenko Kyiv University, Kyiv, Ukraine, kubg@kubg.edu.ua

[2] Bohdan Khmelnytsky National University of Cherkasy, Cherkasy, Ukraine, cic@cdu.edu.ua

[3] National Aviation University, Kyiv, Ukraine alina@inet.ua

[4] Scientific Cyber Security Association, Tbilisi, Georgia m.iavich@scsa.ge

Abstract. Pursuing the purpose of effective functioning in today's conditions, the business is forced to transform rapidly, to modernize at all levels. The world is changing, erasing the limits of its certainty. Companies need quality transformations and strategies that are effective in the face of rapid change towards "deep" digitization. Massive corporate management systems increasingly need the flexibility to keep pace with change. And companies with an innovative culture are more in need of creative tasks than implementing detailed regulations.
In the post-industrial time of digital economy, issues related to the development of the information sphere, the media and communications, the usage of modern information systems to develop the economy and stabilize social development as a whole, come first. The basic principles of practical application of Blockchain are investigated in the work. The stages of development of Blockchain technology, the stages of development of Blockchain technologies by time, the application of distributed registry technology in Blockchain applications, the principles of construction and operation of Blockchain have been specified. The benefits of using NEM for business are substantiated and the components of Proxima X technology, protocols and service layers, on-line and off-line protocols, decentralized applications are exposed.

Keywords: information and communications technologies (ICT), blockchain technology, E-commerce models.

1 Introduction

The formation and development of the digital economy depends on the implementation of such advanced technologies as nanotechnology, biotechnology, technology of complex energy systems, quantum technologies. At the same time, it is difficult to further development of the digital economy without the widespread adoption of in-

formation and communications (ICT) technologies, including cloud computing, big data, mobile technology, Internet of things technologies, geolocation technologies, distribution networking, etc. [1; 2].

In addition, digital technologies are evolving at an exponential rate, radically changing the essence of business, dematerializing, demonetizing and democratizing every industry. Due to modern technologies in Ukraine, successful businesses like Augmented Pixels (known for developing augmented reality technologies and applications) are born of a simple idea; Paymentwall (provides over 120 payment methods worldwide); Kwambio (3D Design Online Store) [3].

2 Related papers

The latest Blockchain technology (Fig. 1), which focuses on financial asset trading, is potentially the most interesting for both the transactional banking and payment domain, and for processes within and between organizations. But, in fact, the needs of the market have led to new terms. For example, the term “Value Web” for Blockchain technologies was coined to Fintech by Chris Skinner, but the idea is also known as “Internet values” for other applications. It is worth saying that "Internet Values" refers to the next mass evolution of the Internet, which is expected to be characterized by a combination of different technologies, and Blockchain will be the key. The “world of finance” is expected to be different [4].

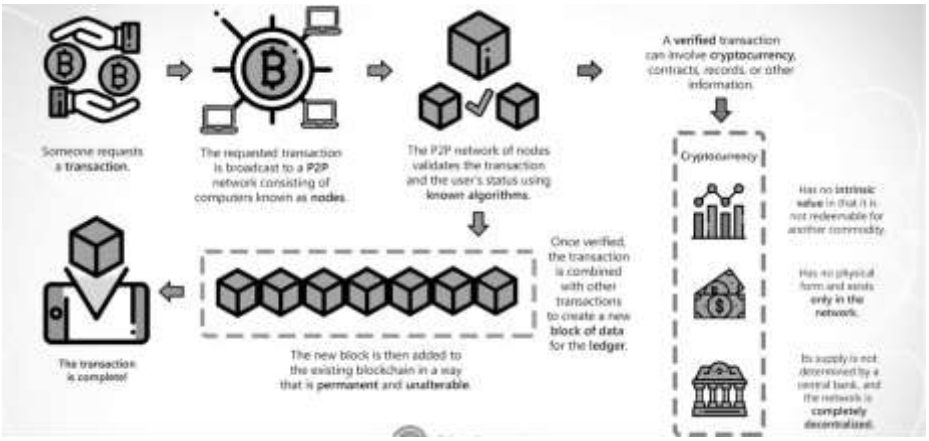

Fig. 1. Step-by-step scheme of Blockchain technology

To give an example from FINTECH, we add that the advent of Blockchain and financial record sharing technologies, which offer new opportunities for decentralized identity systems, may be beyond the control of any company or government, ultimately relying on massively used devices. FINTECH 2.0 is already considering a product design focused on the support of the following solutions, which is highly dependent on personal requests of users.

Blockchain is able to transform the payments ecosystem by improving the efficiency of financial transactions around the world. Banks and other financial institutions

have the opportunity to improve operational efficiencies in cross-border transfers in real time, but as transactions grow, Blockchain algorithms will be exposed to multiple participants, which increase the risk. In the future, the realization of the potential will require significant investment from participants to ensure the security and transparency of all agreements [5].

3 Outline of the main material of the research with full justification of scientific results

Blockchain's innovative technology will determine the trend of the 21st century's global economy, according to expert estimates, Blockchain will completely or partially change the industries that generate a fifth of GDP of USA (about $ 3.6 trillion) [6].

Table 1. Stages of Blockchain technologies development in the context of time.

Number of stage	Time period	Contents of the stage of development Blockchain technologies
Stage 1	2014–2016	Analysis of Blockchain implementation opportunities for the financial services industry.
Stage 2	2017–2018	Review of concepts that can influence business and Blockchain decisions to secure the activities of financial institutions. Today, experts identify seven promising areas of implementation of Blockchain technologies, namely: documentary transactions, syndicated borrowings, clearing and mutual settlement, digital personal identity, lending, contracts.
Stage 3	2019–2020	The appearance of shared infrastructure, APIs and interfaces to extend the scope of Blockchain
Stage 4	2021–2025	Active development of Blockchain networks, completion of formation and approval of standards of interoperability and communication channels.

In essence, Blockchain technology provides a close link between the financial, logistical and commercial components of trade and economic transactions with the ability to unify the payments and delivery.

Blockchain algorithm is called the sequence of operations by which the information content of multiple data structures in distributed peer systems is consistent with each other like the system of democratic voting [7].

There is also a separate subtype of P2P systems that is "centralized peering systems", which have a central node that facilitates interaction between system members, maintains directories describing the services provided by system nodes, or searches and identifies system nodes [8].

Blockchain is a multifunctional and multilevel information and communication technology that aims to make the accounting of various assets reliable and instantly accessible. Reliable storage technology for keeping records of all transactions that have been taken place. Blockchain is a chain of data blocks that is steadily increasing by adding new blocks with recent transaction records. It is a chronological database,

that is, a database in which the time when the record was made is inextricably linked to the data itself, making it non-commutative [9].

Data is represented by a sequence of records that can be supplemented. The records together with the supporting information are stored in blocks. The blocks are stored as a single list. Each participant is represented by a node (node), which stores all the actual array of data and communicates with other nodes. Nodes can add new entries at the end of the list, and notify each other of changes to the list.

Each member of the network, upon registration in it and installed the necessary software, receives a set of two cryptographic keys to the workstation: the closed one - for encryption of the transaction, and the open one - for verification of the transaction. Each regular participant, sending the transaction to the next one, signs the hash of the previous transaction and the public key of the next and adds this information at the end of the transaction. In this way, the recipient can check the entire transaction chain by checking all signatures of previous participants in the transaction.

The hash in this scheme is a data array transformed with the hash function. In the case of crypto currency, this is transaction information; in more complicated systems is information about smart contracts and the current status of Blockchain code. As a result of the transformation, we get a virtually unique, except in the case of hash collisions, alphanumeric string that characterizes the initial element, but cannot be converted in the opposite direction. Cryptographic hash functions have the following properties: rapid calculation of hash values for any data type, determinism, pseudo-randomness, irreversibility, resistance to contradictions [10].

The combination of public and private keys together with hashes gives Blockchain technology a high level of data security [8]. A summary of the principles of Blockchain construction and operation is presented in Table 2.

Table 2. Principles of Blockchain construction and operation (compiled on the basis of sources [11; 12])

Principle	Content of the principle of Blockchain construction and operation
Network integrity	The purpose of having confidence within the system is pursued and, in essence, the participants' consensus, their equality, is mentioned.
Intensity partition	Energy costs are distributed throughout the peering network.
Value as an incentive	The system aligns the incentives of all stakeholders, means that participants are interested in developing technology and maintaining its stability.
Principle	Content of the principle of Blockchain construction and operation
Privacy and protection of rights	One of the principles of Blockchain is trust. Having this principle eliminates the need to identify others to interact with them.
Security	In addition to the fact that each member of the network must use encryption, security measures are built into the network and provide privacy and authentication of the print. Each user also has two keys: one for encryption, the other for decryption.

One of the major benefits of Blockchain technology comes from the ability to speed up processes and reduce transaction complexity and risk. New benefits will appear as this technology can be integrated with outdated IT, legal laws and existing assets such as currencies, stocks, bonds. For this reason, existing financial services can be strengthened by blockchain systems, enabling financial institutions to enter into potentially lower costs, better products and accelerate time to appear in the market [4].

Researcher and founder of the Blockchain Research Institute, Melanie Swan, identifies three conventional areas of application of this technology:

- Blockchain 1.0 is currency (crypto currency is used in various applications related to financial transactions, such as wire transfers and digital payments);
- Blockchain 2.0 is the contracts (applications in the fields of economics, markets and finance that deal with different types of instruments: stocks, bonds, futures, mortgages, legal documents, assets and contracts);
- Blockchain 3.0 is applications whose scope extends beyond financial transactions and markets (extending to branches of government, health, science, education, etc.) [13];
- Blockchain 4.0 is so-called industry infrastructure based Blockchain ecosystem.

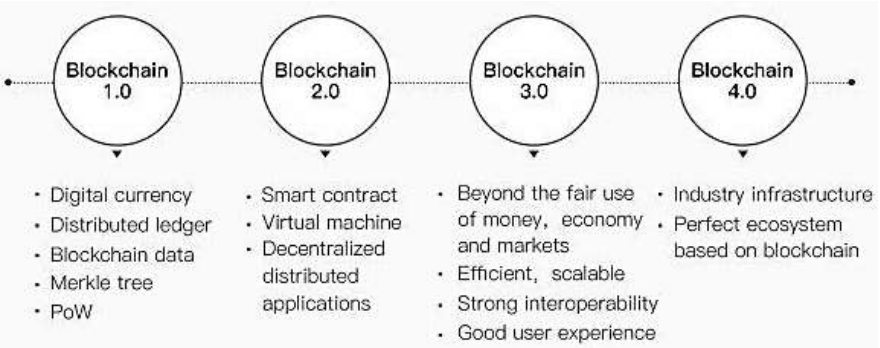

Fig. 2. Evolution of Blockchain

The main advantage of Blockchain technologies from an economic point of view is that it is a transparent, fast, cheap and secure way of conducting transactions with electronic money. E-commerce models (e-commerce, e-trade), which use Blockchain technology in particular, are gaining popularity not only in the world but also in Ukraine, presented in Table 3 and Fig. 3. E-commerce or electronic commerce is an intangible business platform which enables the individuals, business entities and companies to sell their products or services and carry out various commercial activities, through an electronic network (Fig. 4).

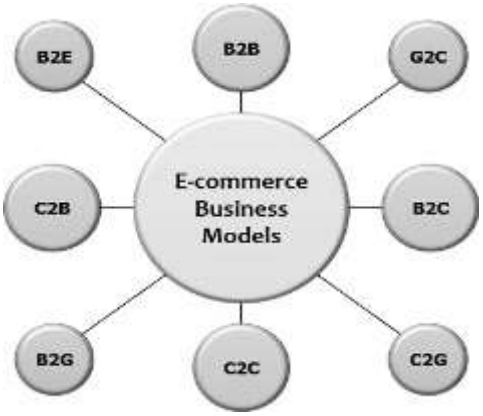

Fig. 3. E-commerce models

The B2B model is the typical basis for the creation of a digital platform that provides the opportunity to buy goods, services and works online from one business to another. Another example of using this model is digital platforms that provide logistics, for example, for the optimization of marine transport using "smart ships".

The B2C model is most often embodied in digital platforms that follow the logic of an online store. The most well-known and capitalized digital venues of this type are Amazon and Alibaba Group.

Fig. 4. E-commerce models

The B2G model implements digital procurement platforms.

The C2B model is about creating customer value for business. One example of this model could be contextual advertising on consumer blogs and online resources (such as Google AdSense). However, households are a provider of workforce resources for businesses, and accordingly digital platforms that aggregate jobseekers 'and employers' registers can be seen as embodying a model of reconciling business and household needs.

Fig. 5. E-commerce today challenges

Table 3. E-Commerce models (E-commerce, E-trade) using Blockchain technologyv

The subject (manufacturer of goods and services)	The object (consumers of goods and services)		
	Business	Consumers (households)	Government
Business	Business-to-business (B2B) model. Electronic government procurement	Business-to-customer (B2C) model. Online Stores (ex: Alibaba, Amazon)	Business-to-Government (B2G) model. Electronic government procurement
Consumers (households)	Model Customers to Business (Customer-to-business: C2B). Contextual Business Advertising and Electronic Job Exchanges (ex: Google AdSense; Work.ua)	Model Customer to Customers (Customer-to-Customer: C2C). Digital sharing platforms (for example: blablacar; Airbnb; eBay).	Model Customer to Government (Customer-to-Government: C2G). Digital petition platforms).
Government	Model Government to Business (Government-to-Business: G2B). Public services for business.	Model Government to Customers (Government-to-Customer: G2C). Government services for citizens.	Model Government to Government (Government-to-Government: G2G). E-government.

The C2C model is represented by digital sharing platforms (such as Airbnb) as well as customers' sales to one another (eg, eBay37).

The C2G model involves the interaction of households with public authorities, for example, to get information on attitudes to particular initiatives (eg, e-petition platforms).

The G2B model is implemented through digital public service delivery platforms for business (tax collection, permitting and miscellaneous information, etc.).

The G2C model involves the interaction of households with public authorities, for example, to pay taxes online or to obtain information in the form of certificates (extracts) from state registers.

The G2G model involves communication between government agencies and is often implemented in the context of e-government. In this case, the positive effect on the national economy is due to the reduction of public spending on public administration.

Conclusions

Information and communication technologies transform all subsystems of society and the state, affecting the growth of all sectors of the economy. To determine the current stage of development of society and economy should use a system of categories: information society, digital economy.

The basic components of the digital economy that are evolving through its digitalization today are infrastructure, e-business and e-commerce. The digital economy is the result of the transformational effects of new general-purpose technologies in information and communication. Digital technologies are rapidly transforming society, business relationships, and are an integral part of an innovative, nationally oriented economy of the future. In the "old" economy, or the so-called "traditional economy," the flow of information was physical: cash, checks, invoices, way bills, reports, face-to-face meetings, phone calls, in the new one - information in all its forms is reduced to bits [14].

In the digital economy, e-products/services, produced by e-business and e-commerce, dominate. Payments for services/products in the digital economy are most often due to the use of electronic money.

Due to Blockchain technology [15-24], if used comprehensively, it can lead to the transition to a digital person (personality), which will be the result from all transactions involving the individual from the beginning of their birth recorded in the Blockchain type [25-28].

Digitalization is a significant factor in technological evolution that will help manufacturers to overcome territorial constraints, reduce transaction costs of decision-making transactions and formation of contracts, develop new business models based on network effects, engage the customer in the process of creating benefits.

References

1. Efimushkin V. A., Ledovskih T. V., Sherbakova E. N.: Infokommunikacionnoe tehnologicheskoe prostranstvo cifrovoj ekonomiki. T-Comm: Telekommunikacii i transport 11(5), 15–20 (2017).
2. Kraus N., Kraus K.: Cifrovizaciya v umovah institucijnoyi transformaciyi ekonomiki: bazovi skladovi ta instrumenti cifrovih tehnologij. Naukovij ekonomichnij zhurnal. Intelekt XXI stolittya (1), 211–214 (2018).
3. Nova era cifrovoyi transformaciyi. Centralna ta Shidna Yevropa, https://www2.deloitte.com/content/dam/Deloitte/ua/Documents/research/c500/CETop500_2016_ua.pdf, last accessed 2019/11/13.
4. Kupriyanovskij V. P., Sinyagov S. S., Klimov A. A., Petrov A. V., Namiot D. E.: Cifrovye cepi postavok i tehnologii na baze blokchejn v sovmestnoj ekonomike. International Journal of Open Information Technologies 5(8), 80-95 (2017).
5. Pogosyan A. M.: Innovacionnye platezhnye instrumenty v cifrovoj ekonomike. Nauchnye zapiski molodyh issledovatelej (3), 63-67 (2017).
6. Shin L.: Razrushiteli bankov. Forbes (2), 86-91 (2016).
7. Drescher D.: Blockchain basis: a non-technical introduction in 25 steps. 1st edn. Apress, Frankfurt am Main (2017).
8. Tanenbaum A.S., van Steen M.: Distributed systems: principles and paradigms. 2nd edn. Pearson Prentice Hall, Upper Saddle River, NJ (2007).
9. Pryanikov M. M., Chugunov A. V.: Blokchejn kak kommunikacionnaya osnova formirovaniya cifrovoj ekonomiki: preimushestva i problemy. International Journal of Open Information Technologies 5 (6), 49-55 (2017).
10. Rogaway Ph., Shrimpton T.: Cryptographic hash-function basics: definitions, implications, and separations for preimage resistance, second-preimage resistance, and collision resistance. In: Roy B., Meier W. (eds.). Fast Software Encryption (FSE) 2004. Lecture Notes in Computer Science, vol. 3017, pp. 371-388. Springer, Berlin, Heidelberg (2004).
11. Tapscott D., Tapscott A.: The Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World. Penguin Books, New York, NY (2016).
12. Kraus N. M., Shevchenko O. M.: Innovacijna diyalnist ta venchurnij kapital v sistemnij modernizaciyi nacionalnoyi ekonomiki: monografiya. Divosvit, Poltava (2013).
13. Svon M.: Blokchejn: Shema novoj ekonomiki. Olimp-biznes, Moskva (2017).
14. Tapscott D.: Digital Economy. Promise and Peril in the Age of Networked Intelligence. 1st edn. McGraw-Hill, New York (1995).
15. Gnatyuk S., Kinzeryavyy V., Kyrychenko K., Yubuzova Kh., Aleksander M., Odarchenko R. Secure Hash Function Constructing for Future Communication Systems and Networks, Advances in Intelligent Systems and Computing, Vol. 902, pp. 561-569, 2020.
16. Kalimoldayev M., Tynymbayev S., Gnatyuk S., Khokhlov S., Magzom M., Kozhagulov Y. Matrix multiplier of polynomials modulo analysis starting with the lower order digits of the multiplier, News of the National Academy of Sciences of the Republic of Kazakhstan, Series of Geology and Technical Sciences, №4 (436), pp. 181-187, 2019.
17. Iavich M., Gagnidze A., Iashvili G., Gnatyuk S., Vialkova V. Lattice based Merkle, CEUR Workshop Proceedings, Vol. 2470, pp. 13-16, 2019.
18. Tynymbayev, E. Aitkhozhayeva, R. Berdibayev, S. Gnatyuk, T. Okhrimenko and T. Namazbayev, Development of Modular Reduction Based on the Divider by Blocking Negative Remainders for Critical Cryptographic Applications, Proceedings of 2019 IEEE 2nd

Ukraine Conference on Electrical and Computer Engineering (UKRCON), Lviv, Ukraine, 2019, pp. 809-812.
19. M. Iavich, S. Gnatyuk, E. Jintcharadze, Y. Polishchuk, A. Fesenko and A. Abisheva, Comparison and Hybrid Implementation of Blowfish, Twofish and RSA Cryptosystems, Proceedings of 2019 IEEE 2nd Ukraine Conference on Electrical and Computer Engineering (UKRCON), Lviv, Ukraine, 2019, pp. 970-974.
20. Tynymbayev S., Gnatyuk S.A., Aitkhozhayeva Y.Z., Berdibayev R.S., Namazbayev T.A. Modular reduction based on the divider by blocking negative remainders, News of the National Academy of Sciences of the Republic of Kazakhstan, Series of Geology and Technical Sciences, №2 (434), pp. 238-248, 2019.
21. Kalimoldayev M., Tynymbayev S., Gnatyuk S., Ibraimov M., Magzom M. The device for multiplying polynomials modulo an irreducible polynomial, News of the National Academy of Sciences of the Republic of Kazakhstan, Series of Geology and Technical Sciences, №2 (434), pp. 199-205, 2019.
22. Hu Z., Gnatyuk S., Kovtun M., Seilova N. Method of searching birationally equivalent Edwards curves over binary fields, Advances in Intelligent Systems and Computing, Vol. 754, pp. 309-319, 2019.
23. S. Gnatyuk, V. Kinzeryavyy, M. Iavich, D. Prysiazhnyi, Kh. Yubuzova, High-Performance Reliable Block Encryption Algorithms Secured against Linear and Differential Cryptanalytic Attacks, CEUR Workshop Proceedings, Vol. 2104, pp. 657-668, 2018.
24. S. Gnatyuk, A. Okhrimenko, M. Kovtun, T. Gancarczyk, V. Karpinskyi, Method of Algorithm Building for Modular Reducing by Irreducible Polynomial, Proceedings of the 16th International Conference on Control, Automation and Systems, Oct. 16-19, Gyeongju, Korea, 2016, pp. 1476-1479.
25. O. Kuznetsov, M. Lutsenko and D. Ivanenko, "Strumok stream cipher: Specification and basic properties," *2016 Third International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T)*, Kharkiv, 2016, pp. 59-62. DOI: 10.1109/INFOCOMMST.2016.7905335
26. I. Gorbenko, A. Kuznetsov, M. Lutsenko and D. Ivanenko, "The research of modern stream ciphers," *2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)*, Kharkov, 2017, pp. 207-210. DOI: 10.1109/INFOCOMMST.2017.8246381
27. Moskovchenko, I., Kuznetsov, A., Kavun, S., Akhmetov, B., Bilozertsev, I., Smirnov, S. Heuristic Methods for the Design of Cryptographic Boolean Functions. International Journal of Computing, 18(3), 265-277. http://computingonline.net/computing/article/view/1519
28. Kuznetsov, A., Potii, O., Poluyanenko, N., Ihnatenko, S., Stelnyk, I., Mialkovsky, D. Opportunities to Minimize Hardware and Software Costs for Implementing Boolean Functions in Stream Ciphers. International Journal of Computing, 18(4), 443-452. http://computingonline.net/computing/article/view/1614