Blockchain and Its Security: Ignore or Insert into Academic Training?

Natalia Miloslavskaya, Alexander Tolstoy

Blockchain and its Security: Ignore or Insert into Academic Training?

Natalia Miloslavskaya[0000-0002-1231-1805] and Alexander Tolstoy[0000-0001-9265-1510]

The National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), 31 Kashirskoye shosse, Moscow, Russia

{NGMiloslavskaya, AITolstoj}@mephi.ru

Abstract. At present, the blockchain technologies (BCT) cause a serious burst of interest of young people in the first place. Not to meet the rising demand and not to pay attention to the BCT during the training means not to be modern. Any educational institution, which doesn't offer courses in the BCT, is going to be left behind as a non-competitive. The paper analyzes a state of the current training in the BCT worldwide, paying special attention to security issues. It also lists standards and books, which can support this training. On these bases, the desired competencies after mastering a full-time BCT course and an exemplary structure of this course are proposed.

Keywords: blockchain technologies, security, academic training, competencies, standards, survey, educational course structure

1 INTRODUCTION

Starting from 2009 with Bitcoin, there are countless publications advertising the "magic" of blockchain (BC) technologies (BCT) and supporting a high level of "hype" around their usage [1]. The BCT for creating verifiable digital records have shown notable success not only in digital currencies but also in financial application domains (like online payments, currency exchanges, money services and transfers, soft and hard wallets, trade finance, markets, microtransactions, investments, brokerage, insurance, etc.), as well in non-financial domains (like digital identity management, authentication and authorization, digital content storage and delivery systems, smart contracts, certification validation systems, application development, real estate, election voting, patient medical records management, distributing the workload for communication system, computer systems that must comply with legal agreements without human intervention, etc.).

If someone will use the "blockchain" word as a search criterion in the IEEE digital library as well as in Scopus and WebofKnowledge databases, many titles will be returned in the reply. For example, the search for 2018 returned 1427 from Scopus, 418 items from WebofKnowledge and 605 from the IEEE digital library (access date 06.11.2018)! But in 10 years the BCT is not well understood as yet, and no single

agreed definition of this technology has appeared. Some of the most known BC definitions are quoted below:

- UK Government, 2016: “A distributed ledger technology” [2];
- PriceWaterhouseCoopers, 2016: “A decentralized ledger of all transactions across a peer-to-peer network, where participants can confirm transactions without the need for a certifying authority” [3];
- OpenBlockchain, 2017: “A technology that enables the secure and resilient management of distributed data in combination with data analytics techniques that add scale and flexibility” [4];
- Wilson, 2017: “It is not a "trust machine". By the blockchain protocol, it only reaches consensus about one specific technicality – the order of entries in the ledger, free of bias” [5];
- Nielson, 2017: “A distributed file system that keeps files copies of the participants who agree on the changes by mutual consensus, where the file consists of blocks and every block has a cryptographic signature of the last block, making an immutable record” [6];
- Primechaintech, 2018: “A peer-to-peer network which timestamps records by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work” [7].

We define a BC as a secure distributed data structure (database, DB) that maintains without centralized administration and data storage a constantly expanding list of non-editable time-stamped blocks (records) and sets rules about transactions which are tied to these blocks [8].

So far as the BCT cause such a serious burst of interest to them of young people in the first place, not to meet the rising demand and not to pay attention to the BC during the training means not to be modern. Speaking easier, any educational institution, which doesn’t offer courses in the BC, is going to be left behind as a non-competitive. That is why the goal of the paper is to analyze a state of the current training in the BCT and to work out on this basis some recommendations for conducting it for security professionals, paying special attention to security issues. To achieve this goal the paper is organized as follows. Survey of the BCT training worldwide is given in Section 2. Standards as the basis for the BCT training are discussed in Section 3. Section 4 is devoted to books, which can support the BCT training. The desired competencies after mastering a full-time BC course are formulated in Section 5. An exemplary structure of the course in the BCT is proposed in Section 6.

2 Survey of the BCT training worldwide

The efforts to develop individual disciplines (courses) in the BC started a few years ago. The Coinbase Company reviewed BC course catalogs at the top 50 universities [9]. Their study was focused on classes available to undergraduate-level students in the fall 2018 semester or the most recent semester, for which information was available online. We used it to begin our search on the BCT courses worldwide. It was

found that 42 % of the top 50 universities offer at least one class on BC or cryptocurrency, and 22 % offer more than one. These courses are most prominent in the U.S. Only 5 of the 18 international universities on the list (27 %) offer at least one class. And only two—Swiss Federal Institute of Technology Zurich and National University of Singapore—offer more than one.

Our analysis shows that at present the training proposed can be divided into two groups: the first one is designed for distance learning only and the second one for face-to-face full-time (not online) training. The first group is represented by the following universities and companies, providing training in the BCT by means of online, usually paid open courses (on successful completion of these courses, students earn certificates) and even master's degree programmes (like the last item in the list):

On Coursera [https://www.coursera.org]:

- State University of New York and University of Buffalo (USA): the "Blockchain" course covers basics, smart contracts, decentralized applications, and platforms. It includes projects for practicing. Potential students can get a free 7-days trial before deciding to pay for the course. Duration: 4 weeks (w), 3.5 hours per week (hpw);
- University of Buffalo: the "Blockchain Basics" course provides a broad overview of the essential BCT concepts – by initially exploring the Bitcoin protocol followed by the Ethereum protocol – to lay the foundation necessary for developing applications and programming (4w-3.5hpw);
- Princeton University (USA): the "Bitcoin and Cryptocurrency Technology" course teaches the basic technical foundations of how the BC works and archives decentralization, dispelling misconceptions and pointing to the future of the BCT. (11 w);
- The "IBM Blockchain Foundation for Developers" course teaches software developers with a little or no experience concepts and strategies on building private BC networks for IBM Bluemix. Students can learn how to add code for smart contracts using the chaincode interface from the Hyperledger Project's Fabric. The course includes a lab demo of how assets are transferred to several roles across a network (6w-2hpw);
- ConsenSys Academy: the "Blockchain: Foundations and Use Cases" course consists of several modules, introducing the BCT, Ethereum and different business use cases (5w-2hpw);

On edX [https://www.edx.org]*:*

- University of California at Berkeley (USA): the "Blockchain Technology" course provides the ideal foundation required to comprehend the BCT. Among other things, it covers distributed systems, alternative consensus mechanisms, fundamental applications and implementations of the BCT (like JP Morgan's Quorum, Ripple, Tendermint, HyperLedger). It is good for both beginners and those at the intermediate level (6w-3-5hpw);
- University of California at Berkeley: the "Bitcoin and Cryptocurrencies" course learns, for example, the basics of smart contracts, the Ethereum platform and how to build decentralized applications (6w-3-5hpw);

- Linux Foundation: the “Blockchain for Business – An Introduction to Hyperledger Technologies” course covers key features of the BCT and the differentiators between various types of Hyperledger projects (10w-3-4hpw);
- Linux Foundation: the “Blockchain: Understanding Its Uses and Implications” course analyzes the concept of transparent ledgers, both public and permissioned, and focuses on using cryptography to achieve consensus, immutability, and governance of transactions (5w-3-4hpw);
- University of Hong Kong: the “Blockchain and FinTech: Basics, Applications, and Limitations” course discusses the BCT, the differences of the various existing BC platforms, applications best fit the BCT, as well as limitations and the downside of the BC with respect to the protection of criminal activities (6w-3-4hpw);

On Udemy [https://www.udemy.com] (only the first 7 courses with the best scores are represented here)*:*

- The “Blockchain and Bitcoin Fundamentals” course by G.Levy (2.5 hours of video, 37 lectures (l), 2 articles(a)) learns all about the fundamentals, including how miners and block hashes work;
- The “The Basics of Blockchain: Ethereum, Bitcoin, & More” course by T.Serres, B.Warburg, Dr.Bull (3.5h-51l-4a) gives fundamentals of the BCT;
- The “Blockchain for Business 2018: The New Industrial Revolution” course (6h-60l-3a) develops solid fundamental understanding of the inner workings of BC with detailed explanations of mining, decentralized consensus, cryptography, smart contracts and many other important concepts;
- The “Blockchain A-Z™: Learn How To Build Your First Blockchain” course by H. de Ponteves (14.5h-94l-9a) learns how to build a BC, create a cryptocurrency and smart contracts;
- The “Ethereum & Solidity: The Complete Developer’s Guide” course by S.Grider (24h-246l-13a) teaches how to use Ergereum, Solidity and secure Smart Contracts to build applications based on the BC and to use the latest version of Ethereum development tools;
- The “Become a Blockchain Developer with Ethereum & Solidity” course by S.Agrobast (15h-86l-4a) learns from the very basics to advanced levels how to develop a distributed application, to unit test them and create a user interface for them, and to use the Truffle build/testing framework;
- The “Build a Blockchain and a Cryptocurrency from Scratch” course by D.J.Katz (6.5h-71l-5a) discusses the implementation of the BC, gives understanding of the main concepts like Proof-of-Work, mining, peer-to-peer connections, etc. and how to build your own BC, create a NodeJS application with real-time websocket connections and build an API with NodeJS and Express;

Miscellaneous:

- Royal Melbourne Institute of Technology (Australia): the 8-week, fully online short course in the BCT [https://www.rmit.edu.au/news/all-news/2018/feb/blockchain-strategy-course-students-jobs-future] is designed in partnership with the Accenture company and Stone and Chalk Fintech hub;

- The “Blockchain Developer” two 3-month terms Nanodegree programme [https://www.udacity.com/course/blockchain-developer-nanodegree--nd1309] teaches to work with the Bitcoin and Ethereum protocols, as well as to build smart contracts and projects for real-world application;
- B9Lab ACADEMY [https://academy.b9lab.com], an independent firm in London and Hamburg working in collaboration with private industry and higher education, provides several online courses in the BCT, consults with businesses who want to make use of it, and performs crucial research on the BCT developments and applications. Students have access to experienced tutors via a dedicated slack channel. Students who complete their studies successfully receive a certificate in the BC, backed up by the Ethereum network;
- University of Nicosia (Cyprus): the first full, 3-semester long Master’s degree programme in digital currency offered through distance learning [https://digitalcurrency.unic.ac.cy/about-the-program]. The majority of the courses consist of lectures delivered by the faculty, but in some cases by guest lecturers with academic and business background related to topics covered in courses. Practical exercises, individual and group projects, simulations and case study analyses form an integral part of the programme. One additional note: the UNIC is the first university to accept Bitcoin as payment for tuition.

The second group of face-to-face full-time (not online) courses in represented mostly by American universities having specialized research centers in their structures supporting training in the BCT. They are appeared in the list in alphabetical order, not in any scientific or statistical ranking:

- Cornell University with the support from Cornell’s IC3 (Initiative for Cryptocurrencies and Contracts) research organization has created in 2017 the Cornell Blockchain project [https://cornellblockchain.org] to provide education, certification, and application of the BCT for students and corporate clients. Unfortunately, the content of this web site is available only to its members;
- Duke University’s Blockchain Lab [http://www.dukeblockchainlab.com] is a specialized, student-led research center designed to bring students and faculty alike up to speed on the newest developments in the BCT through lectures, interest groups, and workshops. On the web site, there are some links to the selected resources for further learning, research, news, etc.;
- Center for Financial Markets and Policy of the Georgetown University’ McDonough School of Business [https://finpolicy.georgetown.edu/about] is one of the most notable academic studies in the BC, sponsoring an annual international BC Summit and seminars and publishing white papers and analysis of BC’s impact on finance and investment;
- Massachusetts Institute of Technology is one of the world’s authorities on the BCT through the Media Lab’s Digital Currency Initiative [https://dci.mit.edu], which is working to push the BC development with research projects, papers, and groups while raising awareness of its risks and potential;
- New York University’s Stern School of Business has the BCT as an integral part in the FinTech MBA program [http://www.stern.nyu.edu/programs-

admissions/full-time-mba/academics/areas-interest/fintech] focused on technology's impact on finance, including analytics, artificial intelligence, and the BC. They offer the "Digital Currencies, Blockchains, and the Financial Services Industry" course in the BC. The first course was offered in 2014;

- Blockchain at Berkeley at the University of California at Berkeley [https://blockchain.berkeley.edu] is a student-led organization, uniting students, alumni, and community members to offer education, research, and consulting in the BCT and their future uses via workshops, lectures, seminars, and meetings. They offer the 1-semester "Blockchain Fundamentals" course with 1 hour of lecture per week and 1 hour of interactive discussion. Among their workshops are the following: "What is Blockchain (Introduction to the BC)", "Bitcoin (How a Bitcoin transaction works)", "Ethereum (Introduction to Ethereum)", "Consensus Algorithms (Algorithms, data structures and scripting)", "Smart Contract Security (Programming smart contracts with Ethereum)", "How to Consult (Lessons learnt from the BC)", "Blockchain vs Database (What makes the BC unique)", "Smart Contracts and Business (What makes the BC unique)", and "EVM (Ethereum Virtual Machine)";
- Decentralized Systems Lab of the University of Illinois at Urbana-Champaign [http://decentralize.ece.illinois.edu] is a multidisciplinary research center for educating and extending the academic conversation with research projects and papers, as well as creating the BCT. In 2018, they offered the half-semester "Smart Contracts and Blockchain Security" course (2 credits, slides are available at http://soc1024.ece.illinois.edu/teaching/ece398sc/spring2018/);
- National University of Singapore: the "Blockchain: Embarking on the Journey" [https://academy.smu.edu.sg/blockchain-embarking-journey-1136] is a 1-day course targeted at professionals seeking to gain an understanding of the BCT and their applications in the business world;
- Swiss Federal Institute of Technology Zurich: the "Blockchain and Internet of Things" [http://www.vvz.ethz.ch/lerneinheitPre.do?semkez=2018S&lerneinheitId=122368&lang=en] 1-semester course provides opportunities to gain fundamental understanding of promising new technologies as well as develop creative decentralized solutions for societal challenges using these technologies. During the hackathon, students work in mixed teams on concrete challenges (like climate change, financial instability, energy, or mass migration, etc.) and develop decentralized approaches towards a sustainable, sharing circular economy using BC and Internet of Things (IoT) technologies;
- Financial University under the Government of the Russian Federation: the only one in the world full-time face-to-face Master's degree "Blockchain Technologies and Cryptocurrency" programme (2 years, 120 credits) in the framework of the "Applied Mathematics and Computer Science" direction [http://www.fa.ru/en/admissions/Pages/Master-programs.aspx] started in 2018. Graduates are preparing to use the BCT in various fields of activity, technological support for the secure usage of cryptocurrencies, ensuring cybersecurity in the field of finance using BC and cryptocurrency technologies.

In Russia, PwC Academy conducts the “First touch to Blockchain. Features and application of blockchain technology" 4-hours face-to-face master class [https://training.pwc.ru/seminars/workshop-blockchain], introducing the use of the BCT in the financial sector, its purpose, open and closed types, and distinctive advantages. Cryptoacademy [https://cryptocademy.ru] offers several 6-hours intensive courses in the BCT. Blockchain Academy [https://block.academy/ru/edu/] has several 1-2-days face-to-face programmes for banks, developers, and investors. The “Blockchain Basics” online course from the Skillbox Company consisting of 10 seminars and 5 assignments is available at [https://skillbox.ru/blockchain]. Luxoft Training [https://www.luxoft-training.ru/kurs/blokcheyn_i_kriptovalyuty.html] teaches the “Blockchain and Cryptocurrencies” 6-hours course.

This list can be continued more and more, but from our perspective, it is enough information to define main competencies for those who will master a course in the BCT.

3 Standards as the basis for the BCT training

In 2016, the ISO/TC 307 “Blockchain and distributed ledger technologies” has been created for standardization of the BCT and distributed ledger technologies (DLT). This technical committee combines several specialized and working groups, namely “Blockchain and distributed ledger technologies and IT Security techniques”, "Foundations”, “Use cases”, “Security, privacy and identity”, “Smart contracts and their applications”, “Governance of blockchain and distributed ledger technology system” and “Interoperability of blockchain and distributed ledger technology systems”. At present, they just started 10 standards, technical specifications and reports in the BCT and DLT, the majority of which are at the preparatory stage: ISO 22739 Terminology (the first draft is registered – for January 2019); ISO 23244 Overview of privacy and personally identifiable information (PII) protection; ISO 23245 Security risks and vulnerabilities (the first draft is registered – for November 2018); ISO 23246 Overview of identity management using BCT and DLT; ISO 23257 Reference architecture; ISO 23258 Taxonomy and Ontology; ISO 23259 Legally binding smart contracts; ISO 23455 Overview of and interactions between smart contracts in BCT and DLT systems; ISO 23576 Security of digital asset custodians; and ISO 23578 Discovery issues related to interoperability.

The IEEE P2418.1 standard for the framework of BC use, implementation, and interaction in one particular application – IoT – has started in June 2017 with June 2019 as an expected date of draft submission to the IEEE-SA. This framework will include BC tokens, smart contracts, transaction, credentialed network, permissioned and permissionless IoT BC enable decentralized, autonomous peer-to-peer, consumer-to-machine and machine-to-machine communications without the need for a trusted intermediary and address scalability, interoperability, security and privacy challenges with regard to BC in IoT.

The Draft NISTIR 8202 “Blockchain Technology Overview” [1] discusses how the BC works, especially when applying to electronic currency. It shows the BCT’s

broader applications (banking, supply chain, insurance, healthcare, trusted timestamping, energy industry) and highlights some of their limitations, concerning the BC control, malicious users, no trust, resource usage, transfer of burden of credential storage to users, and Private/Public Key Infrastructure and identity. This draft defines the high-level components of BC system architecture like transactions, blocks, hashes, forks, etc. It describes how new blocks are added to the BC and how consensus models resolve conflicts among miners. Different BC permission models and their use case examples are introduced. The draft also covers smart contracts and BC platforms in use today. Here we rely on this document as the only one is currently publicly available.

We hope that for the beginning of the next educational year some of these standards will be adopted and published, so they could be used as a basis for the training.

4 Books support for the BCT training

As our search has shown, there are a lot of books, which can be taken as the basis for conducting training in the BCT. Here is a list of books published in 2016-2018 and available on the book markets in alphabetic order (with their volumes in pages):

1. Bahga A., Madisetti V. 2017. Blockchain Applications: A Hands-On Approach. 380 p.
2. Bashir I. 2017. Mastering Blockchain: Deeper insights into decentralization, cryptography, Bitcoin, and popular Blockchain frameworks. 542 p.
3. Bashir I. 2018. Mastering Blockchain: Distributed ledger technology, decentralization, and smart contracts explained, 2nd Edition. 658 p.
4. Bishop A. 2018. Blockchain Technology Explained: A Beginner's Guide to Blockchain Technology. 66 p.
5. De Filippi P., Wright A. 2018. Blockchain and the Law: The Rule of Code. 312 p.
6. Drescher D. 2017. Blockchain Basics. 255 p.
7. Ellis R. 2017. Blockchain Maturity: A New Internet. 310 p.
8. Gaur N., Desrosiers L. 2018. Hands-On Blockchain with Hyperledger: Building decentralized applications with Hyperledger Fabric and Composer. 460 p.
9. Hill B., Chopra S. 2018. Blockchain Quick Reference: A guide to exploring decentralized Blockchain application development. 350 p.
10. Kuo Chuen D.L., Deng R.H. 2017. Handbook of Blockchain, Digital Finance, and Inclusion, Volume 2: ChinaTech, Mobile Security, and Distributed Ledger. 514 p.
11. Norman T.A. 2017. Blockchain Technology Explained: The Ultimate Beginner's Guide About Blockchain Wallet, Mining, Bitcoin, Ethereum, Litecoin, Zcash, Monero, Ripple, Dash, IOTA and Smart Contracts. 127 p.
12. Oliver P., Reads C. 2018. Blockchain 101: Distributed Ledger Technology (DLT) (Book 1). 59 p. and Blockchain 101: Forking, Smart Contracts, Scaling, & Permissioned States (Book 2). 47 p.

13. Prusty N. 2018. Blockchain for Enterprise: Build scalable blockchain applications with privacy, interoperability, and permissioned features. 220 p.
14. Richmond T.J. 2017. Blockchain: 2 Books in 1 - The New Ultimate Guide To Understanding and Using Blockchain Technology (Blockchain, Bitcoin, Cryptocurrency). 210 p.
15. Sebastian L. 2018. Blockchain: Two Books - The Complete Edition On The Blockchain Basics, Technology and Its Application in Cryptocurrency and Other Industries That Are Happening Now. 183 p.
16. Vigna P., Casey M.J. 2018. The Truth Machine: The Blockchain and the Future of Everything (2018). 302 p.
17. Xu X., Weber I. 2019. Architecture for Blockchain Applications.

We allocate separately the books devoted to BC and security issues:

1. Gupta R. 2018. Hands-On Cybersecurity with Blockchain: Implement DDoS protection, PKI-based identity, 2FA, and DNS security using Blockchain. 236 p.
2. Karame G., Audroulaki E. 2016. Bitcoin and Blockchain Security. 218 p.
3. Pherr G. 2018. Blockchain and Cybersecurity: How the Blockchain technology can change the face of security in the Internet of Things Era. 30 p.
4. Robinson R.J. 2018. Introduction To Embedded Blockchain Cyber Security. 17 p.
5. Shetty S. and Kamhoua C.A. 2019. Blockchain for Distributed Systems Security.

5 Desired competencies after mastering a full-time BCT course

Based on a detailed analysis of all the previously mentioned courses, the content of standards and some of the books listed above, we are ready to formulate what students who have completed full-time semester training on a BCT-related course will know and be able to do.

Upon successful completion of this training, students should:

- Know and understand what the BC is and the terminology used;
- Know where, how and why the BCT can be used in the modern world;
- Know and get a deep understanding of international standards on the BC;
- Know key BC's theoretical principles and practices and understand how they can be applied within an individual business environment;
- Have a deep understanding of how to build a BC (meaning building a blockchain system from scratch);
- Understand BC's security and know its vulnerabilities and security risks.

Besides this, students should master basic BC handling skills and be able to:

- Identify and analyze the challenges and prospects of the BCT and propose or develop systems and services that address them;
- Develop or participate in developing the BCT itself and the things that interact with the BC (like developing a new BC protocol or improving existing one, understanding and being able to apply cryptography used in BC systems, designing a distributed system architecture, innovative systems, and services that complement and extend the existing BC concept);

- Implement requirements of international standards on the BCT;
- Carry out the synthesis and analysis of design projects on distributed ledgers, smart contracts, and applications for the BCT;
- Analyze and compare different BC platforms, as well as select the right BC platform to be applied within an individual business environment;
- Analyze best practices of the BCT applications, specify business opportunities, and apply the BCT-based innovative solutions to address business problems;
- Conduct a security risk assessment for the BCT and propose a set of measures (rules, procedures, practical methods, guidelines, and tools) to mitigate them.

Of course, the given list of knowledge and skills can be taken only a basis. It does not pretend to completeness as every educational institution training on the BCT can broaden it according to the country and its business specific, for example.

6 Exemplary structure of the course in the BCT

Based on the above-formulated knowledge and skills, it is possible to determine the structure of a typical full-time 1-semester university course in the BCT for a Master's degree programme as it requires some prerequisites as knowledge in cryptography, networks, information security and so on. The following exemplary detailed structure is proposed for a classical course in the BCT.

Section 1. Introduction

Module 1. Blockchain Technologies in Modern Business Environment

- Introduction to the BC and its ecosystem; History of BC's development (to understand its roots); Problems solved by the BCT (to know their implications and to recognize the potential); The areas of the BCT's application (to know their scope and to see the big picture); BC in the different fields of law (transactional, corporate, commercial); BC regulation and regulatory environment

Module 2. Technologies used by the BCT

- Fundamentals of cryptography (including independent, repeated, combined, sequential and hierarchical hashing and asymmetric cryptography) and crypto programming; Fundamentals of data and databases; Private and public networks; Distributed and centralized system architectures; Peer-to-peer systems and their architecture; Ledger and authorities

Section 2. BC foundation

Module 3. Basics of the BCT

- Introduction of a BC concept; BCT terminology (including the following terms: account, actor, agent, altchain, block, chain, consensus, cryplet=runtime, distributed ledger, immutability, forking, hybrid BC, ledger, main chain, middleware, miner, mining mechanism, node, ordering service, peer, permissioned (dedicated, private) ledger, sidechain, shared ledger, smart contracts, transaction, unpermissioned

(permissionless, public) ledger, user, validating mechanism, etc.); BC-related standards (ISO/IEC, NIST, etc.)

Module 4. BC Characteristics and Architecture

- Characteristics of the BC (immutable, append-only, ordered, time-stamped, open, transparent, secure, eventually consistent, interoperable); Architecture of BC networks; Soft and hard forking; Security and privacy protection issues for the BC; Trust and ownership in the BC

Section 3. How the BC works

Module 5. Planning the BC

- Describing and protecting ownership; Storing transaction data; Preparing and distributing ledgers; Adding new transaction; Deciding on trust; BC deployment architecture; Resource management in the BC development

Module 6. BC protocols

- Protocol for transactions; Protocol for peer-to-peer communications; Consensus protocol (proof of work; proof of stake; round robin; ledger conflicts and resolutions); Data storage protocol

Module 7. Maintaining the history of transactions

- Choosing a transaction history; Storing, using, adding the history of transactions; Ordering the transactions; Integrity of the history; Detecting changes in the history

Module 8. Hashes and cryptography in the BC

- Providing hash values for data in the BC; Detecting changes in data; Asymmetric cryptography in the BC for identifying accounts and authorizing transactions; Merkle tree; Cryptographic Changes and Forks

Module 9. Transactions and data storage in the BC

- Creating a new block for inclusion into the BC; Chaining blocks; Verifying and adding transactions; Distributing the data store among peers

Section 4. BC vulnerabilities and limitations and how to overcome them

Module 10. BC vulnerabilities and limitations

- BC control and hidden centrality; The security model utilizing asymmetric cryptography; No trust; Lack of privacy; Resource usage; Limited scalability; High cost; Critical size; Malicious users; Double spending as a problem of distributed peer-to-peer systems of ledgers and how to solve it; Transfer of burden of credential storage to users; Conflicting BC goals: transparency vs. privacy, security vs. speed; Lack of legal acceptance;

Module 11. How to overcome some BC limitations

- Redactable BC by Accenture

Section 5. Using the BC

Module 12. Specific BC use cases

- Finance, digital identity, notary services, voting, manufacturing, IoT, supply chain, security, etc. BC use cases; Detour to the emergence of

cryptographic currencies; introduction to BC platforms: Bitcoin, Ethereum, Ripple, etc.; Hyperledger project; Multichain platform; Economical, social, cultural and political implications of the BC;

Module 13. BC research and further development

- Research and development in the BCT;
- Further BC development

Section 6. BC Project

Option 1 – Choose a BC topic from the given content for its detailed discussion

Option 2 – Create a BC business plan for the application area selected

Option 3 – Create a BC for the application area selected

7 CONCLUSION

After a detailed study of the issue put at the beginning, for us it is obvious that teaching the BCT and their security is the urgent need of today.

The next steps in preparing a course with the proposed structure for teaching in the MEPhI in the framework of the "Business Continuity and Information Security Maintenance" Master's degree programme since the Autumn 2019 semester will include the development of all educational and methodical materials required for its support, a set of laboratory works to acquire the necessary skills and a web site as a tool for coordinating the educational process and providing a teacher-student interaction during it.

Acknowledgement. This work was supported by the MEPhI Academic Excellence Project (agreement with the Ministry of Education and Science of the Russian Federation of August 27, 2013, project no. 02.a03.21.0005).

8 REFERENCES

1. Yaga D., Mell P., Roby N., Scarfone K. Draft NISTIR 8202 Blockchain Technology Overview. 2018. URL: https://csrc.nist.gov/CSRC/media/Publications/nistir/8202/draft/documents/nistir8202-draft.pdf (accessed: April 15, 2019).
2. PriceWaterhouseCoopers. Making sense of bitcoin, cryptocurrency, and blockchain. 2016. URL: https://www.pwc.com/us/en/financial-services/fintech/bitcoin-blockchain-cryptocurrency.html (accessed: April 15, 2019).
3. UK Government, Office for Science. Distributed Ledger Technology: Beyond Block Chain (Report). 2016. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf (accessed: April 15, 2019).
4. OpenBlockchain. Researching the potential of blockchains. 2017. URL| http://blockchain.open.ac.uk/ (accessed: April 15, 2019).
5. Wilson S. How it works: Blockchain explained in 500 words. 2017. URL: http://www.zdnet.com/article/blockchain-explained-in-500-words/ (accessed: April 15, 2019).

6. Nielson B. Blockchain Solutions for Cyber & Data Security. 2017. URL: https://richtopia.com/emerging-technologies/blockchain-solutions-for-cyber-data-security (accessed: April 15, 2019).
7. Primechaintech. Blockchain Security Controls. 2018. URL: http://www.primechaintech.com/docs/blockchain_security_controls.pdf (accessed: April 15, 2019).
8. Miloslavskaya N. Designing Blockchain-based SIEM 3.0 System. Information and Computer Security (UK). Emerald Publishing. September 2018. Vol. 26, N 4. DOI: 10.1108/ics-10-2017-0075.
9. The rise of crypto in higher education. 2018. URL: https://blog.coinbase.com/the-rise-of-crypto-in-higher-education-81b648c2466f (accessed: April 15, 2019).