

Blockchain and IT Security

Raimundas Matulevičius
Mubashar Iqbal

https://infosec.cs.ut.ee/

BlockChain Network Online Education for interdisciplinary European Competence Transfer (BlockNet) Multiplier Event, 3rd December, 2020



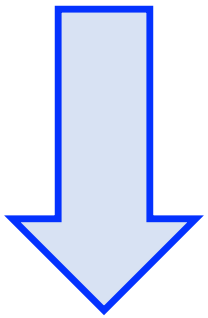
Blockchain and IT Security

KA2 - Cooperation for Innovation and the Exchange of Good Practice Strategic Partnerships for higher Education 2018, no. 2018-1-LT01-KA203-047044
Disclaimer: The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, the Commission and the NA DAAD cannot be held responsible for any use which may be made of the information contained therein.

Is Blockchain a Security?

*"If you think **technology** can solve your **security problems**, then you don't understand the **problems** and you don't understand the **technology**"*

Bruce Schneier



If you think **blockchain** is a **security**, then you don't understand the **security** and you don't understand the **blockchain**

Lecture Topics

- Security Design for Distributed Information Systems
- Cryptographic Methods in Blockchains
- Blockchain Components and Security Methods
- Secure Platforms, Tools and Enterprise Models



Lecture Topics

- Security Design for Distributed Information Systems
- Cryptographic Methods in Blockchains
- Blockchain Components and Security Methods
- Secure Platforms, Tools and Enterprise Models



Security Design for Distributed Information Systems

- Why security is important?
- What is principles of security in Blockchains?
- What is role of cryptography in Blockchains?
- What are Blockchain platforms and applications?



BlockNet

Cryptographic Methods in Blockchains





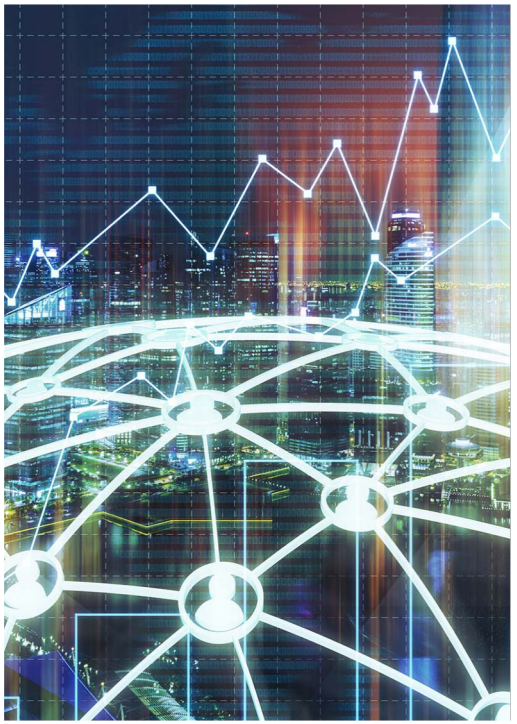


- How are transactions performed?
- What is Blockchain ecosystem?
- How is identity managed?
- How is access control implemented?
- How is privacy managed?

Erasmus+

Blockchain Components and Security Methods

- What are domains where blockchain technology is used?
- What are the security risks that are mitigated by the blockchain technology?
- What are the security risks that are found in the blockchain technology?
- What are contermeasures to mitigate these risks?



Secure Platforms, Tools and Enterprise Models

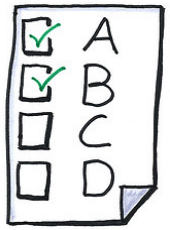


Solve Blockchain security challenges in a hands-on case analysis

Blockchain and IT Security

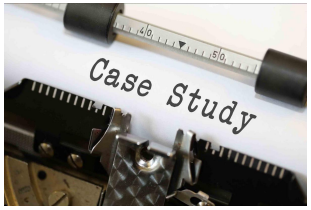
170
lecture slides

33
recommended external videos for self-studying



30
Multi-choice questions

1
Hands-on case analysis



110
minutes of voice-over narration

2 ECTS
52 hours of studying



Erasmus+

Research and Publications

- **Iqbal, M., Matulevičius, R.** (2020) *Corda Security Ontology: Example of Post-Trade Matching and Confirmation*, Baltic Journal of Modern Computing, Vol. 8, pp. 638-674
- **Iqbal, M., Matulevičius, R.** (2020) *Managing Security Risks in Post-Trade Matching and Confirmation Using CorDapp*. In: Robal T., Haav HM., Penjam J., Matulevičius R. (eds) Databases and Information Systems. DB&IS 2020. Communications in Computer and Information Science, vol 1243. Springer, Cham. *https://doi.org/10.1007/978-3-030-57672-1_24.*
- **Mammadzada K., Iqbal M., Milani F., García-Bañuelos L., Matulevičius R.** (2020) *Blockchain Oracles: A Framework for Blockchain-Based Applications*. In: Asatiani A. et al. (eds) Business Process Management: Blockchain and Robotic Process Automation Forum. BPM 2020. Lecture Notes in Business Information Processing, vol 393. Springer, Cham. *https://doi.org/10.1007/978-3-030-58779-6_2*
- **Iqbal, M.** (2020). *A Reference Model for Security Risk Management of the Blockchain-based Applications*, CAiSE 2020 Doctoral Consortium, pp. 44-52 *http://ceur-ws.org/Vol-2613/paper5.pdf*
- **Iqbal, M., Matulevičius, R.** (2019) *Comparison of Blockchain-Based Solutions to Mitigate Data Tampering Security Risk*. In: Di Ciccio C. et al. (eds) Business Process Management: Blockchain and Central and Eastern Europe Forum. BPM 2019. Lecture Notes in Business Information Processing, vol 361. Springer, Cham. URL: *https://link.springer.com/chapter/10.1007/978-3-030-30429-4_2*
- **Iqbal, M., Matulevičius, R.** (2019) *Blockchain-Based Application Security Risks: A Systematic Literature Review*. In: Proper H., Stirna J. (eds) Advanced Information Systems Engineering Workshops. CAiSE 2019. Lecture Notes in Business Information Processing, vol 349. Springer, Cham *https://link.springer.com/chapter/10.1007/978-3-030-20948-3_16*

UNIVERSITY OF TARTU
Institute of Computer Science

Blockchain Skills for ICT Professionals

http://bliss-project.eu

BLISS project

L1. Blockchain essentials
L2. Blockchain platforms
L3. Business merits, challenges and implications of blockchain technology
L4. Practical design and development of blockchain applications

ONLINE COURSE

BONNE PRATIQUE

ENG: https://www.openlearning.com/courses/bliss-mooc/
EST: https://www.openlearning.com/courses/bliss-vooc-ee-version-/

UNIVERSITY OF TARTU
Institute of Computer Science

Projects

CHAISE - A Blueprint for Sectoral Cooperation on Blockchain Skill Development

01.11.2020-31.10.2024

Erasmus+, Sector Skills Alliances

More info at: **https://www.cs.ut.ee/en/news/university-tartu-launches-chaise-design-europes-strategy-blockchain-skills**

CyberPhish - Safeguarding against Phishing in the age of 4 Industrial Revolution

02.11.2020-1.11.2022

Erasmus+ Strategic Partnership

UNIVERSITY OF TARTU
Institute of Computer Science

Thank you!



BLOCKNET

UNIVERSITY OF COPENHAGEN

technische universität dortmund