

Beyond – Cryptocurrencies: Preparing for the next wave of challenges in Distributed Ledger Technology

Abstract: Blockchain is not just a cryptocurrency – it is one of the examples of chain-based Distributed Ledger Technology (DLT) where another graph-based mechanism is equally important depending on the use case and application. With this ideology in view, this tutorial is planned to cover the introduction of DLTs and then move into the practical space of blockchain, followed by quantum and post-quantum security, malware analysis with smart contracts and practical applications such as supply chain management, digital asset management, multi-layer security in future networks, convergence of quantum with DLTs and other broader challenges and research problems. The tutorial has content that would suit the audience with a prior interest in DLT, even without any workable experience. Two interactive demos will be shared with the audience to allow them to understand how blockchains can facilitate several real-world applications.

Objectives: The tutorial on *Beyond – Cryptocurrencies* at IEEE ICBC is designed to achieve multifaceted objectives. The primary focus is on understanding of DLT from use cases and applications with a focus on adversarial modelling, quantum and post-quantum security, malware analysis and practical usability with real-world examples. We are aiming at three main objectives via this tutorial:

1. *Technical understanding and challenges:* With this tutorial, we aim to help expand on the current understanding of the DLT for use cases that are beyond cryptocurrencies such as supply chain management, digital asset management and networking (future networks).
2. *Education and Research:* This tutorial will have several learning and research aspects with a detailed focus on the quantum and post-quantum landscape that has huge implications on the use case of chain based DLTs, such as blockchain. Here, a specific dimension of blockchain's migration based on secure algorithms will be covered from education and research points of view.
3. *Collaboration and best practices:* We expect that this tutorial will give certain visibility to the team and allow others to network during the session. We have an ideology of collaborating for future research and coming together to examine the best practices for policymaking and regulations on DLTs.

Motivation: As DLT researchers and enthusiasts and being involved in the practical development of blockchain, there is a gap in the understanding of this technology from both implementation and application points of view. We aim to address this challenge by bringing together people with complementary skills on the DLTs and helping the audience expand their understanding of DLTs beyond cryptocurrencies. There are several critical use cases of the traceability features and decentralised mechanisms where DLT can revolutionise specific digital industries, such as supply chains or application-specific security in future networks. We aim to expand this experience of working with real-world solutions on blockchain to broader audiences for wider adoption of this technology.

Timeline and intended audience: This tutorial is planned for 2 hours. There will be two demo sessions in this tutorial allowing users a broader understanding of how blockchain can be used for real-world applications. The first fifteen minutes for Vishal and Trung to cover the introductions, use cases and adversarial modelling for the security of the chain based DLTs.

The next forty-five minutes will be for Teik and Zengpeng to cover quantum and postquantum modelling and its impact including first demo. The next fifteen minutes will be for Oluwafemi on the malware analysis and utilisation of DLT for traceability of threats. And another forty-five minutes for a demo on supply chain management with blockchain as a backbone delivered by Vishal and his research team, followed by questions and other practical work on network usage and data sharing with incentives via DLT. Each subsection will allow five minutes for Q&A and the audience can also ask questions on the go. Our tutorial is planned for an audience of intermediaries towards experts. We will touch on the basics to let the introduction drive the interest in the tutorial followed by advancement in the DLT and more challenges and innovations expected in the future. Thus, the tutorial is intended towards:

1. *Students and Researchers*: Those interested in understanding the current landscape of DLT from a post-quantum point of view and future challenges to tackle for implementation and utilisation of chain-based and graph-based DLT.
2. *DLT enthusiasts*: Those interested in the use cases of the DLTs beyond cryptocurrencies and implementation of applications, such as supply chain management and malware traceability.
3. *DLT programmers*: Those interested in secure coding, smart contract development, quantum, and post-quantum security and beyond ECDSA aspects.
4. *Regulatory Experts*: Those interested in compliance issues and government policies for future investment and planning of commissions for controlling assets relying on DLTs.
5. *Startups and Innovators*: Those interested in utilising DLT for supporting their current ideas or looking for other verticals in their current use case relying on the chain-based and graph-based DLT and other support for networking and asset management.

Name, affiliation, and a short biography of each tutorial speaker:

Vishal Sharma (SMIEEE) is an Associate Professor in the School of Electronics, Electrical Engineering and Computer Science (EECS) at the Queen's University Belfast (QUB), UK. At QUB, he serves as the director of the Innovation-by Design Lab and the Chair of the Computer Science Programme Review Working Group. He is the Co-Investigator for the Northern Ireland Advanced Research and Engineering Centre (ARC) aimed at commercialising research and a Fellow of the QUB's Centre for Secure Information Technologies (CSIT). He has a PhD in Computer Science and Engineering from Thapar University, India. He has over 130 research publications with seven best paper awards. He has been awarded £11.8M in research funding at QUB in Distributed Ledger Technology, cyber defence, and digital twins. He is leading the research project on blockchain-based supply chain development for the PwC-UK as a part of ARC and has been a consultant for Praefere, a blockchain-based privacy management startup, and the scientific advisor for Quantum-NFT, Singapore.

Trung Q. Duong (Fellow of IEEE and Fellow of AAIA) is a Canada Excellence Research Chair (CERC) and a Full Professor at Memorial University of Newfoundland, Canada. He is also an adjunct Chair Professor in Telecommunications at Queen's University Belfast, UK with a strong record in the areas of wireless communications and machine learning (500+ publications, Google Scholar: 18,500+ citations, h-index of 73). He is the only UK-based researcher who received two prestigious awards from the Royal Academy of Engineering (RAEng): i) the RAEng Research Fellowship (2015–2020) and ii) the RAEng Research Chair (2020-2025). He has been awarded more than £25M research grants as PI/Co-I. He is a Canada Excellence Research Chair laureate from the Canadian government and a Newton Prize winner from the UK government.

Oluwafemi Olukoya is an Assistant Professor in EEECS and CSIT at QUB and leads research in systems security, semantic analysis, cybercrime, and privacy, evidenced by publications in reputable cybersecurity journals and conferences. He is the current module owner of the penetration testing and ethical hacking on the Masters in Applied Cyber Security program, which caters to full-time and part-time students. With a PhD focused on mobile systems security from the University of Glasgow and a postdoc in cybercrime investigation from the University College Dublin, he has a breadth and depth of specialist knowledge.

Teik Guan Tan is the CEO of pQCee, Singapore and works in the niche area of cryptographic security design and integration, having implemented numerous successful projects for banks, government agencies and enterprises. He led a multi-factor authentication solutions provider, DS3, for over a decade through organic growth to Series A to eventually being acquired by an MNC. Teik Guan work is focused on providing post-quantum readiness solutions. He holds a BSc and MSc from NUS and a PhD from SUTD.

Zengpeng Li is currently an Associate Professor at Shandong University (SDU), China, supported by SDU Young Scholar's Future Plan. Before joining SDU, he was a postdoctoral research fellow at the Singapore University of Technology and Design, Singapore, and a postdoctoral research associate at Lancaster University, UK, from Spring 2018 to Fall 2020. He received his Ph.D. degree from Harbin Engineering University (HEU), China, in Spring 2018. He was a research assistant with the University of Auckland, NZ, and Virginia Commonwealth University, USA, respectively, during his doctoral program, from Fall 2015 to Fall 2017. His primary research interests are in cryptographic protocol and secure distributed computing. His research efforts focus on the secure computing on encrypted data, verifiable computation, blockchain consensus protocol, and password-based cryptography. His works appear in ACM CCS, ACM ACSAC, NDSS, IEEE TDSC, IEEE TSC, IEEE TIFS, IEEE TCC, etc. He has served TPC members for IEEE Globecom, ACM BCSI, IEEE Edge, EAI SPNCE, etc.

***An outline of the tutorial content:** Below is the 2 hours timeline-based content of the tutorial:*

Part –I (10 minutes + 5 minutes Q&A) – Vishal and Trung (15 minutes)

Introduction to chain based DLT, its use cases and associated threats and adversaries.

1. Introduction to Chain-based DLT
2. DLT use cases and current market trends
3. Threat Models and Adversaries in DLT

Part – II (40 minutes + 5 minutes Q&A) – Teik and Zengpeng (45 minutes)

(Demo-1) Quantum and postquantum modelling with user impact and applications

1. Threats from Quantum Computers and blockchain migration
2. Live App with blockchain-based quantum NFT
3. Post-quantum security and protocols

Part – III (10 minutes + 5 minutes Q&A) – Oluwafemi (15 minutes)

DLT for cyber security applications

1. Forensic analysis with DLT
2. Decentralised threat intelligence
3. Traceability and code security

Part – IV (40 minutes + 5 minutes Q&A) – Vishal (45 minutes)

(Demo-2) DLT interactions with use cases and future challenges

1. Supply chain management using Hyperledger Fabric and smart contracts
2. Secure networking applications towards Open Radio Access Networks
3. Consumer data management with incentives via DLT
4. Future Research and road map towards adoption of DLT

A description of any previous tutorial experience of the speaker(s), and past versions of the tutorial: Most recently, Trung and Vishal were involved in a tutorial session on Digital Twins for 6G Communications and Networking at [IEEE Globecom 2023](#). Trung has delivered four successful tutorials as follows:

1. IEEE Wireless Communications and Networking Conference, March 2023, Glasgow, Scotland, UK
2. IEEE International Conference on Communications May 2023, Rome, Italy
3. IEEE ATC 2013 - Cognitive Cooperative Communications: System Design and Performance Analysis
4. IEEE VTC 2017 - Physical Layer Security

Apart from these, Vishal has successfully delivered presentations, hands-on experiences, and demos as an Invited Speaker at

1. Blockchain, AI and the Fight for Business Data Authenticity - Frontier Stage: Harnessing Academic Research to Drive Product Development, Belfast, UK (June 2023)
2. Securing Smart Computing Devices - 3rd Emergent Converging Technologies and Biomedical Systems, Solan, India (May 2023)
3. Innovating Future Smart Cities - William J Clinton Leadership Institute, Belfast (March 2023)
4. Intelligent, connected, and secure smart cities)- Belfast City Council Workshop, Belfast (February 2023).

State if a similar tutorial has been offered in other conferences (last two years) and how your tutorial differs: This tutorial is compiled with the complementary expertise of five researchers from four different countries (UK, Canada, Singapore, and China) and has never been offered in other conferences in any form. The contents of this tutorial are unique and address the current and future landscape towards the usability of distributed ledger technology. The tutorial is planned with live demos/examples of the technology developed by the UK Team and how these can be expanded towards other applications.