2020 2nd Blockchain and Internet of Things Conference (BIOTC 2020)

July 8-10, 2020

Supported by

Indexed by

http://www.biotc.net/

Welcome Message from Organizing Committee

It is our great pleasure to invite you to join our international conference - 2020 2nd Blockchain and Internet of Things Conference (BIOTC 2020). This event will provide a unique opportunity for editors and authors to get together and share their latest research findings and results.

We're confident that over the two days you'll get the theoretical grounding, practical knowledge, and personal contacts that will help you build long-term, profitable and sustainable communication among researchers and practitioners working in a wide variety of scientific areas with a common interest in Blockchain and Internet of Things .

On behalf of all the conference committees, we would like to thank all the authors as well as the technical program committee members and reviewers. Their high competence, their enthusiasm, their time and expertise knowledge, enabled us to prepare the high-quality final program and helped to make the conference become a successful event.

We truly hope you'll enjoy the conference and get what you expect from the conference.

Organizing Committee

Conference Introductions

Welcome to 2020 2nd Blockchain and Internet of Things Conference (BIOTC 2020). This conference is organized by ACM Chapter Singapore. The objective of the conference is to provide a platform for researchers, engineers, academicians as well as industrial professionals from all over the world to present their research results and development activities in Blockchain and Internet of Things.

Papers will be published in the following proceeding:

International Conference Proceedings Series by ACM, which will be archived in the ACM Digital Library, and indexed by Ei Compendex, Scopus and submitted to be reviewed by Thomson Reuters Conference Proceedings Citation Index (CPCI).

Conference website and email: http://www.biotc.net/ and biotc.contact@gmail.com

Table of Contents

Keynote Speakers Introductions

Keynote Speaker I

Prof. Qun Jin
Department of Human Informatics and Cognitive Sciences, Faculty of Human Sciences,
Waseda University, Japan

Qun Jin is a professor at the Networked Information Systems Laboratory, Department of Human Informatics and Cognitive Sciences, Faculty of Human Sciences, Waseda University, Japan. He is currently the Dean of Graduate School of Human Sciences, and the Deputy Dean for International Affairs, Faculty of Human Sciences. He has been extensively engaged in research works in the fields of computer science, information systems, and human informatics. His recent research interests cover human-centric ubiquitous computing, behavior and cognitive informatics, big data, personal analytics and individual modeling, intelligence computing, blockchain, cyber security, cyber-enabled applications in healthcare, and computing for well-being. He authored or co-authored several monographs and more than 300 refereed papers published in the world-renowned academic journals, including IEEE and ACM Transactions, and international conference proceedings, among which a few were granted best paper awards. He served as a general chair, program chair, and keynote speaker for numerous IEEE sponsored international conferences. He served as a guest editor in recent years for IEEE Transactions on Industrial Informatics (2019), IEEE/ACM Transactions on Computational Biology and Bioinformatics (2018), IEEE Transactions on Computational Social Systems (2018), IEEE Transactions on Emerging Topics in Computing (2017), IEEE MultiMedia (2017), and IEEE Cloud Computing (2015). He is a foreign member of the Engineering Academy of Japan (EAJ).

Keynote Speaker II

Prof. Chin-Chen Chang
Feng Chia University, Taiwan

Prof. C.C. Chang obtained his Ph.D. degree in computer engineering from National Chiao Tung University. He's first degree is Bachelor of Science in Applied Mathematics and master degree is Master of Science in computer and decision sciences. Both were awarded in National Tsing Hua University. Dr. Chang served in National Chung Cheng University from 1989 to 2005. His current title is Chair Professor in Department of Information Engineering and Computer Science, Feng Chia University, from Feb. 2005.

Prior to joining Feng Chia University, Professor Chang was an associate professor in Chiao Tung University, professor in National Chung Hsing University, chair professor in National Chung Cheng University. He had also been Visiting Researcher and Visiting Scientist to Tokyo University and Kyoto University, Japan. During his service in Chung Cheng, Professor Chang served as Chairman of the Institute of Computer Science and Information Engineering, Dean of College of Engineering, Provost and then Acting President of Chung Cheng University and Director of Advisory Office in Ministry of Education, Taiwan.

Professor Chang's specialties include, but not limited to, data engineering, database systems, computer cryptography and information security. A researcher of acclaimed and distinguished services and contributions to his country and advancing human knowledge in the field of information science, Professor Chang has won many research awards and honorary positions by and in prestigious organizations both nationally and internationally. He is currently a Fellow of IEEE and a Fellow of IEE, UK. On numerous occasions, he was invited to serve as Visiting Professor, Chair Professor, Honorary Professor, Honorary Director, Honorary Chairman, Distinguished Alumnus, Distinguished Researcher, Research Fellow by universities and research institutes. He also published over 1,100 papers in Information Sciences. In the meantime, he participates actively in international academic organizations and performs advisory work to government agencies and academic organizations.

Keynote Speaker III

Prof. Liyanage C De Silva
Universiti Brunei Darussalam, Brunei Darussalam

Prof. Liyanage C De Silva received BSc Eng(Hons) degree from the University of Moratuwa Sri Lanka in 1985, MPhil degree from The Open University of Sri Lanka in 1989, MEng and PhD degrees from the University of Tokyo, Japan in 1992 and 1995 respectively. He was with the University of Tokyo, Japan, from 1989 to 1995. From April 1995 to March 1997 he has pursued his postdoctoral research as a researcher at ATR (Advanced Telecommunication Research) Laboratories, Kyoto, Japan. In March 1997 he has joined The National University of Singapore as a Lecturer where he was an Assistant Professor till June 2003. He was with the Massey University, New Zealand from 2003 to 2007. Currently he is a Professor of Engineering and the Dean of the Faculty of Integrated Technologies (FIT) at the Universiti Brunei Darussalam (UBD).

Liyanage's current research interests are Internet of Things (IoT) Neural Network Applications, Image and Speech Signal Processing (in particular multi modal emotion recognition and speech emotion analysis), Digital Communication (CDMA, OFDMA etc.), Information theory (source coding), Pattern recognition and understanding (biometric identification), Multimedia signal processing, and Smart Sensors (Smart environments for security, eldercare and energy efficiency).

Liyanage has published over 180 technical papers in these areas in international conferences, journals and Japanese national conventions and jointly holds three US, one Brunei and one Japanese national patent. The Japanese national patent was successfully sold to Sony Corporation Japan for commercial utilization. Liyanage's works have been cited as one of the pioneering works in the bimodal (audio and video signal based) emotion recognition by many researchers. His papers so far have been cited by more than 3400 times (according to scholar.google.com) with an h-index of 23.

Keynote Speaker IV

Prof. Maode Ma
School of Electrical and Electronic Engineering,
Nanyang Technological University, Singapore

Dr. Maode Ma, a Fellow of IET, received his Ph.D. degree in Department of Computer Science from Hong Kong University of Science and Technology in 1999. Now, Dr. Ma is a tenured Associate Professor in the School of Electrical and Electronic Engineering at Nanyang Technological University in Singapore. He has extensive research interests including network security and wireless networking. He has led 25 research projects funded by government, industry, military and universities in various countries. He has supervised over 20 research students to get their Ph. D degree. He has been a conference chair, technical symposium chair, tutorial chair, publication chair, publicity chair and session chair for over 100 international conferences. He has been a member of the technical program committees for more than 200 international conferences. Dr. Ma has more than 430 international academic publications including over 210 journal papers and more than 220 conference papers. His publication has received about 6000 citations in Google Scholar. He currently serves as the Editor-in-Chief of International Journal of Computer and Communication Engineering, Journal of Communications and International Journal of Electronic Transport. He also serves as a Senior Editor for IEEE Communications Surveys and Tutorials, and an Associate Editor for International Journal of Security and Communication Networks, International Journal of Wireless Communications and Mobile Computing and International Journal of Communication Systems. He had been an Associate Editor for IEEE Communications Letters from 2003 to 2011. Dr. Ma is a senior member of IEEE Communication Society and IEEE Education Society, and a member of ACM. He is now the Secretary of the IEEE Singapore Section and the Chair of the ACM, Singapore Chapter. Dr. Ma has been invited to be an IEEE Communication Society Distinguished Lecturer from 2013 to 2016.

Invited Speakers Introductions

Invited Speaker I

Prof. Zhi Zheng

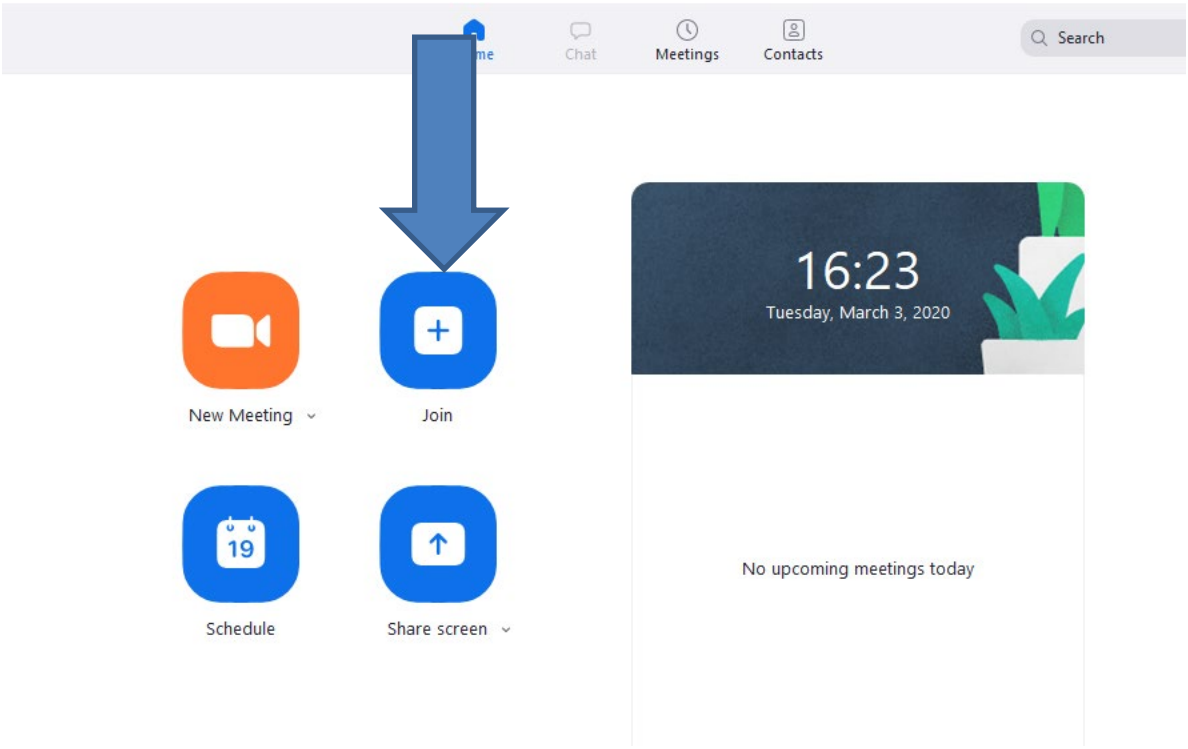
University of Electronic Science and Technology of China, China

Prof. Zhi Zheng received the M.S. and Ph.D. degrees in electronic engineering and information & communication engineering from the University of Electronic Science and Technology of China (UESTC), Chengdu, China, in 2007 and 2011, respectively. From 2014 to 2015, he was an Academic Visitor with the Department of Electrical and Electronic Engineering, Imperial College London, U.K. Since 2011, he has been with the School of Information and Communication Engineering, UESTC, where he is currently an Associate Professor. His research interests lie in the areas of statistical and array signal processing, including direction finding, source localization, target tracking, sparse array design, robust adaptive beamforming, jammer suppression, compressive sensing, machine learning, and convex optimization, with applications to radar, sonar, navigation, wireless communications, wireless sensor networks, etc.

Instructions for the Online Tool “ZOOM”

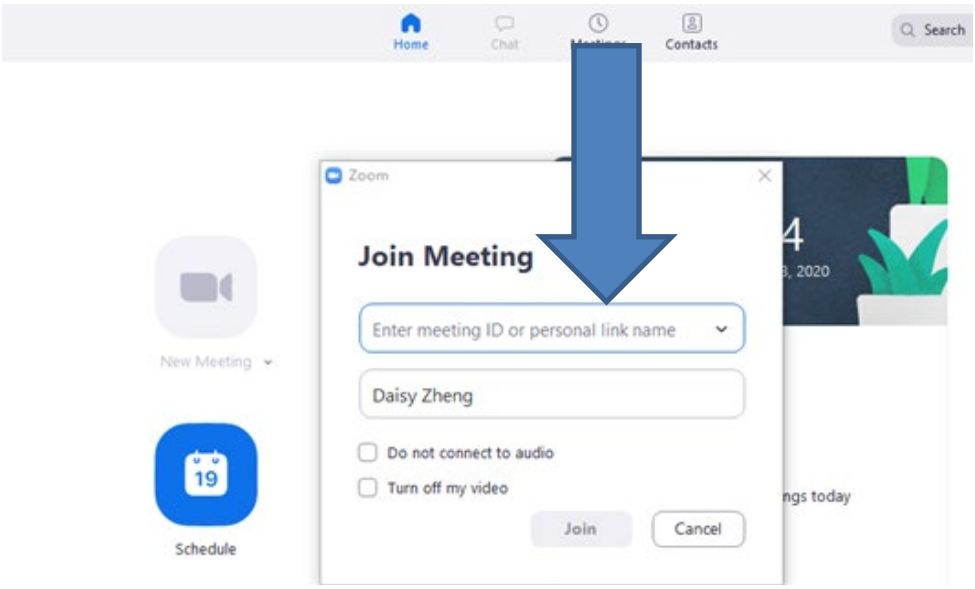
1. You can download the software “Zoom” from this URL:
http://www.zoom.us/

2. How to join online conference in Zoom



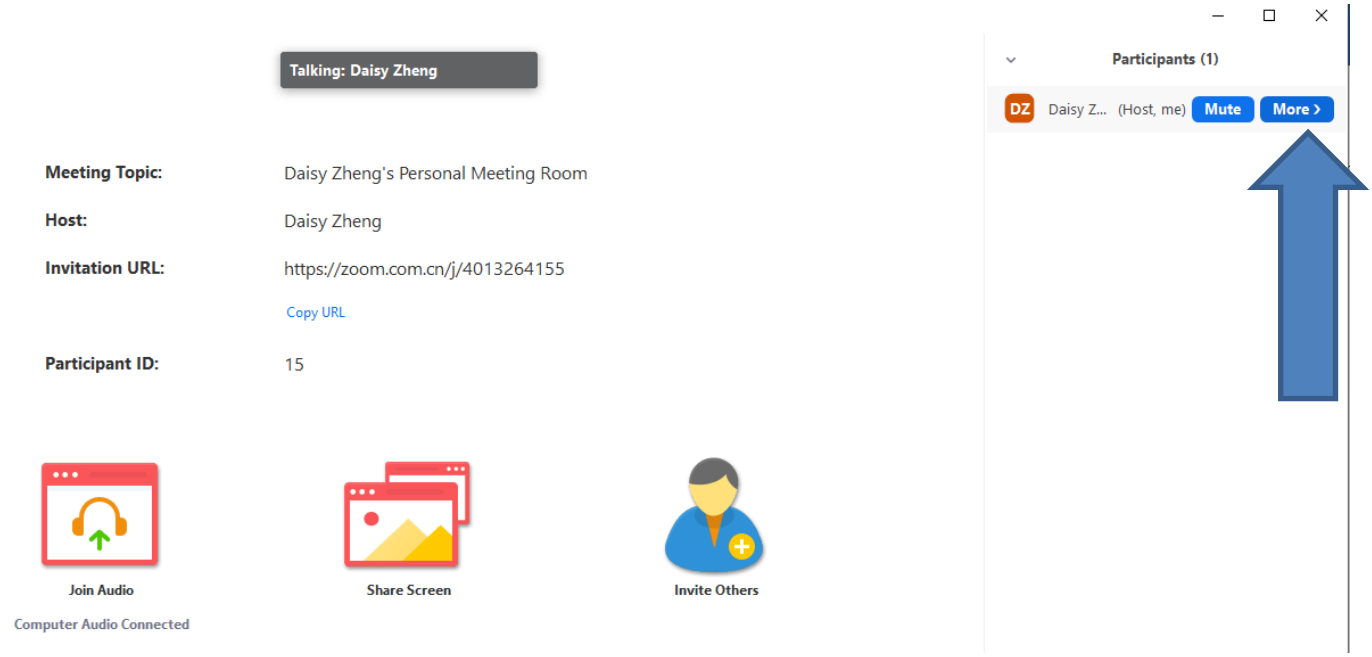
Please click **“join”**

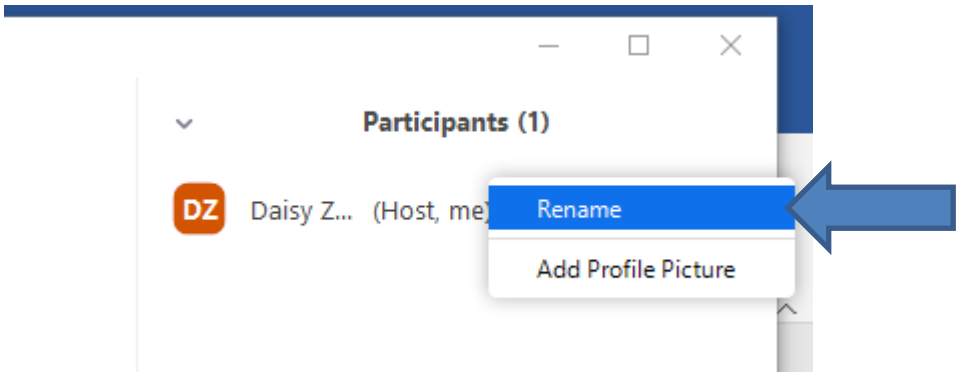
3. Fill in the Conference ID



Please fill in the **Online-Meeting Room ID: 690 6915 5259**and join the online conference

4. How to rename





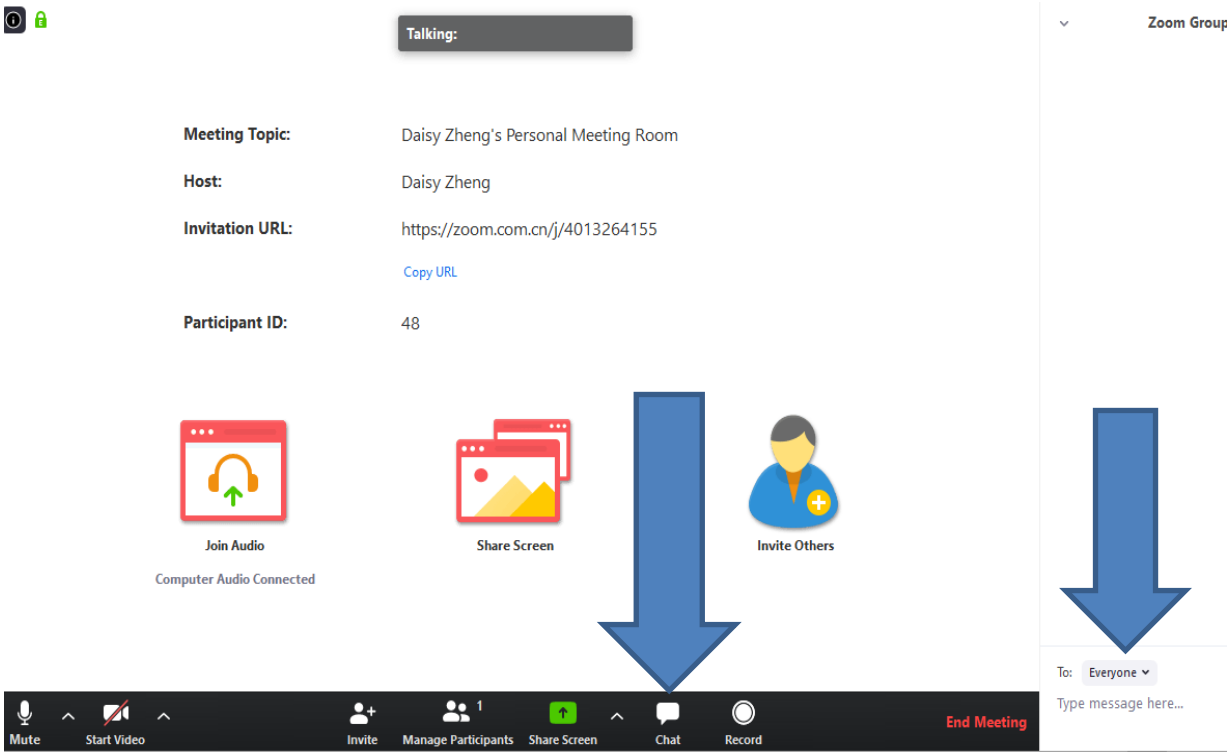
First, you can click **"More"**

Then, you can click **"rename".**

If you are **presenter**, your name need to be renamed as **ECXXXX (your paper id)+ your name.**

If you are **listener,** your name need to be renamed as **listener + your name.**

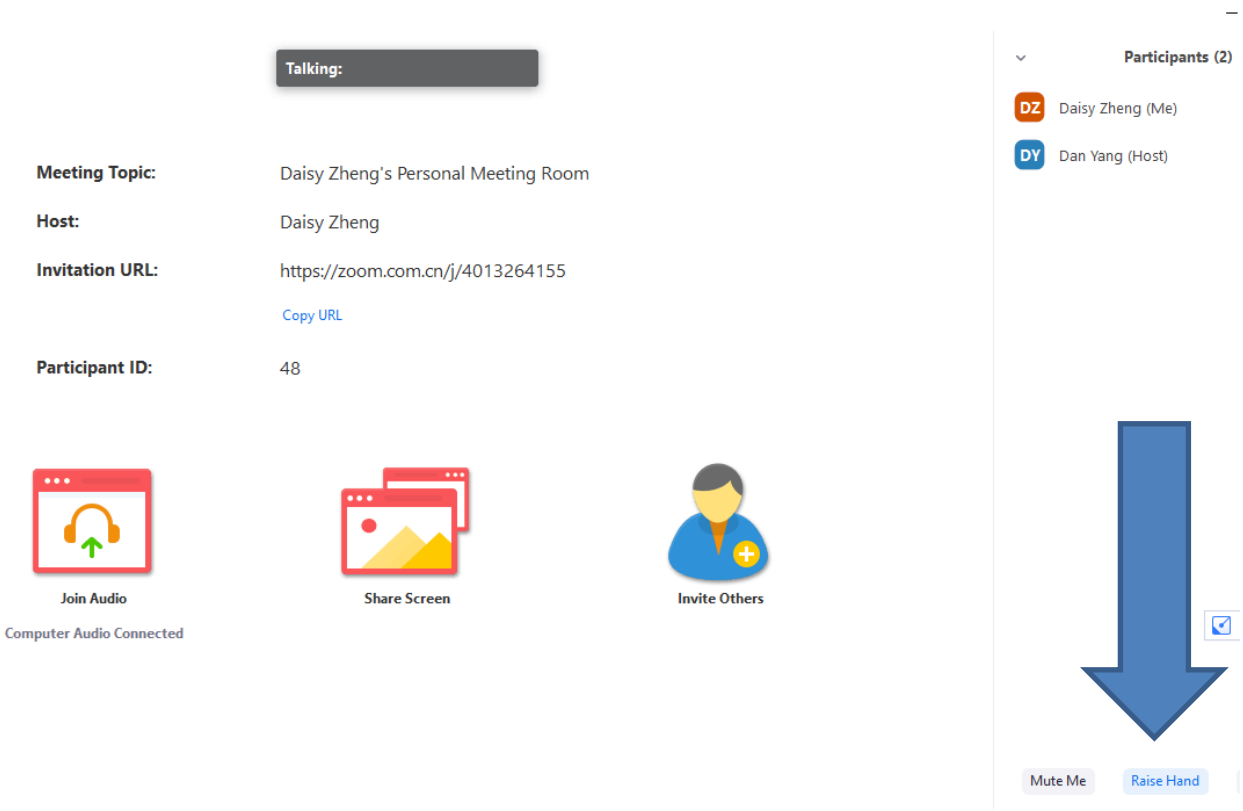
5. How to Chat with Others in Zoom:



You can click **"Chat"** first.

Then, you can click **"everyone"** to choose who you want to talk with.

6. How to Use Raise Your Hands and Ask Questions in Zoom:

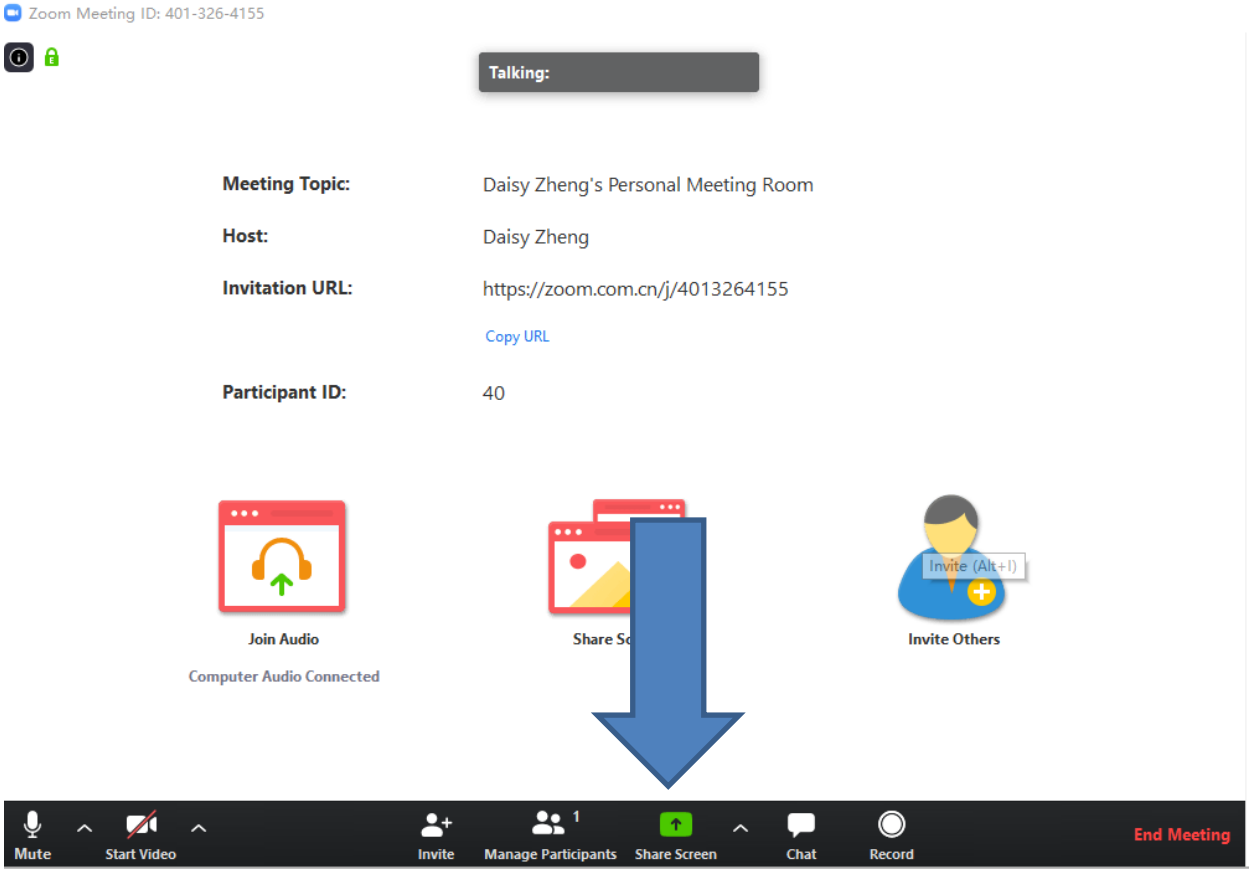


If you have any problems during the conference, you can click "**raise your hands**" or use "**chat**" to communicate with the conference secretary and the conference secretary will help you.

When you have questions about keynote speeches, you can also use "**raise your hands**" function.

After the keynote speech, keynote speakers will answer your questions.

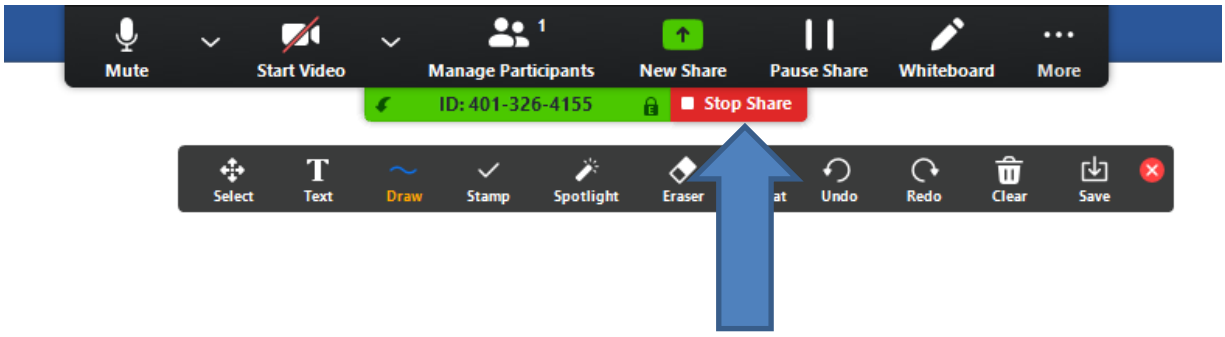
7. How to Share Your Screen



When you do your presentation, you need to share your screen.

You can click "**share screen**".

8. How to stop sharing your screen



After your oral presentation, you can click "**stop share**".

Presentation Instructions

Instructions for Oral Presentations

Materials Provided by the Presenters:

PowerPoint or PDF Files

Duration of each Presentation (Tentatively):

Regular Oral Presentation: about **10 Minutes** of Presentation and **5 Minutes** of Question and Answer.

Best Presentation Award

One Best Presentation will be selected from each presentation session, and the Certificate for Best Presentation will be sent after the conference.

Schedule for Conference

Tips: The time in the schedule is according to Singapore Standard Time.

***Online test is for testing the Internet connection and helping participants get familiar with software Zoom.**

Please make sure that you will attend online test.

July 8, 2020 (Wednesday) Room ID: 690 6915 5259		
Online Test		
Morning Test (9:30-11:10)	9:30-9:50	Test for Prof. Qun Jin
	9:50-10:10	Test for Prof. Chin-Chen Chang
	10:10-10:30	Test for Prof. Liyanage C De Silva
	10:30-10:50	Test for Prof. Maode Ma
	10:50-11:10	Test for Prof. Zhi Zheng
Afternoon Test (13:30-17:30)	13:30- 14:30	Test for Presenters of EC0002, EC5020, EC5026, EC5034, EC5018, EC5035, EC0009
	14:30- 15:30	Test for Presenters of EC0004, EC0006, EC0005, EC0008, EC0001, EC5008
	15：30-16:30	Test for Presenters of EC5014，EC5016，EC5033, EC5022，EC5011，EC5015
	16:30-17:30	Test for Presenters of EC5028, EC5012, EC5005, EC5036，EC5013, EC5009-A
	flex time	Any questions about the test, please contact the staff at other time on July 8 Afternoon before 17:45（Singapore time）.
July 9, 2020 (Thursday) Room ID: 690 6915 5259		
Morning Session for Keynote Speeches		
9:00- 12:20 KN Speeches (Singapore Time)	9:00- 9:10	Opening Remarks
	9:10-9:55	Keynote Speech I Title: Enabling Privacy-Enhanced Sustainable Use of Health Data with Blockchain Prof. Qun Jin, Waseda University, Japan

	9:55-10:40	Keynote Speech II Title: Applying De-clustering Concept to Information Hiding Prof. Chin-Chen Chang, Feng Chia University, Taiwan
	10:40-10:50	Take a break
	10:50-11:35	Keynote Speech III Title: Monitoring the Jungle using Internet of Trees (IoT) Prof. Liyanage C De Silva, Universiti Brunei Darussalam (UBD), Brunei Darussalam
	11:35-12:20	Keynote Speech IV Title: Group-to-Route Handover Authentication in LTE-A Networks for High-Speed Railways Prof. Maode Ma, Nanyang Technological University, Singapore
Lunch time: 12:20- 14:00		
Afternoon Session: Session 1 and Session 2		
14:00- 15:45	Session 1 (EC0002, EC5020, EC5026, EC5034, EC5018, EC5033, EC5022)	
Break Time: 15:45- 16:00		
16:00- 17:30	Session 2 (EC5035, EC5016, EC5011, EC5028, EC5012, EC5009-A)	

July 10, 2020（Friday）Room ID: 690 6915 5259		
Morning Session: Invited Speech and Session 3		
Morning Session	Invited Speech (9:40-10: 00)	Invited Speech I Title: Target Localization for Distributed MIMO Radar Systems via Improved Semidefinite Relaxation Prof. Zhi Zheng, University of Electronic Science and Technology of China
	Session 3 (10:00- 11:30)	Session 3 (EC0009, EC0004, EC0006, EC0005, EC0008, EC0001)
Lunch time: 11:30- 15:00		
Afternoon Session: Session 4		
Afternoon Session	15:00- 16:30	Session 4 (EC5008, EC5015, EC5014, EC5005, EC5036, EC5013)

Morning Session

Morning, July 9, 2020 (Thursday)

Time: 9:00-12:20

Online-Meeting Room ID: 690 6915 5259

Opening Remarks & Testing (9:00-9:10)

Addressed by Chair Prof. Ma Maode from Nanyang Technological University in Singapore

Keynote Speech I (9:10-9:55)

Title: Enabling Privacy-Enhanced Sustainable Use of Health Data with Blockchain

Prof. Qun Jin

Waseda University, Japan

Abstract—In recent years, it has become possible and easy to collect a variety of life log data in the course of daily activities with wearable devices, sensors and digital traces. These data are regarded to be of great value to healthcare and can shed light on aspects of lifestyle and health that were previously difficult to examine and measure. However, using of these data may potentially cause a critical privacy issue. On the other hand, recently blockchain gained the spotlight as a promising technology of benefit to mankind with advanced features such as decentralization and data security protection. In this talk, we present our vision on how to fully harness the advantage of blockchain technology to protect and enhance security and privacy while sharing and using health data for good, and our work on blockchain-empowered sustainable use of health data. Furthermore, we describe and discuss privacy-preserving personal analytics and individual modeling, health data analysis enhancement for comprehensive anomaly detection and risk prediction, and extensively comparative analysis on health data and individualized visualization toward human-centric smart health.

Keynote Speech II (9:55-10:40)

Title: Applying De-clustering Concept to Information Hiding

Prof. Chin-Chen Chang

Feng Chia University, Taiwan

Abstract—Reversible steganography allows an original image to be completely restored after the extraction of hidden data embedded in a cover image. In this talk, I will talk about a reversible scheme based on declustering strategy for VQ compressed images. The declustering can be regarded as a preprocessing step to make the proposed steganographic method more efficient. Our experimental results show that the time required for the embedding process in the proposed method is few. In addition, the reversible steganography allows an original image to be completely restored after the extraction of hidden data embedded in a cover image. In this paper, we propose a reversible scheme for VQ-compressed images that is based on a declustering strategy and takes advantage of the local spatial characteristics of the image. The main advantages of our method are ease of implementation, low computational demands, and no requirement for auxiliary data.

Take a Break: 10:40-10:50

Keynote Speech III (10:50-11:35)

Title: Monitoring the Jungle using Internet of Trees (IoT)

Prof. Liyanage C De Silva

Universiti Brunei Darussalam (UBD), Brunei Darussalam

Abstract— We are constantly monitoring many parameters of the environment using a multitude of sensors. The importance of environment monitoring technology has become a vital field of research and development for ecological progression worldwide. The environmental/earth monitoring systems can be connected to receive information such as temperature, humidity, air/water pollution data, lake/river pollution information, land monitoring statistics and plant/crop growth indicators. Also, applications such as pollution monitoring, chemical hazard detections, flooding detection, and weather forecasting are becoming hugely importance to the society. These applications can be realized using a low-cost, reliable and efficient systems through an IoT framework.

In this presentation a review of the state of the art of smart homes using sensor technologies and Internet of Things (IoT) will be presented. At first a look into the research work related to smart homes from various viewpoints will be discussed. This includes looking from the viewpoint of specific techniques such as smart homes that utilize computer vision-based techniques, smart homes that utilize audio-based techniques and then smart homes that utilize multimodal techniques. I will look at it from the viewpoint of specific applications of smart homes such as eldercare and childcare applications, energy efficiency applications and then in the research directions of multimedia retrieval for ubiquitous environments. Using a survey, we found out that some well-known smart home applications like video-based security applications has seen the maturity in terms of new research directions while some topics like smart homes for energy efficiency and video summarization are gaining momentum. Finally, I will present some of our recent attempts to apply IoT into connected forests or smart forests leading to coining the phrase “IoT - Internet of Trees”. In the same note of using IoT in homes, use of IoT in the forests in the form of Internet of Trees (IoT) will give an added benefit to the living beings and plants in the jungle. Internet of Trees can help us to produce an equivalent of the “Face-book” in the jungle; a “Jungle-book”.

Keynote Speech IV (11:35-12:20)

Title: Group-to-Route Handover Authentication in LTE-A Networks for High-Speed Railways

Prof. Maode Ma

Nanyang Technological University, Singapore

Abstract—The introduction of mobile relay node (MRN) in LTE-advanced networks for high-speed railways is an attractive approach to provide uninterrupted connectivity for a group of user equipment on board. However, MRNs still suffer from frequent handovers and several security threats due to several rounds of message exchange and the insecure air interface between MRNs and donor eNBs (DeNBs). In this talk, I will present a group-to-route handover authentication scheme based on trajectory prediction for mobile relays.

By this scheme, all of the DeNBs deployed along the trajectory can be formed a route-DeNB group and all of the MRNs deployed in the same train can construct a MRN group. Compared with the current existing solutions, the proposed solution can accomplish a mutual authentication and key agreement between the MRN group and the target DeNB with an ideal efficiency in terms of authentication signaling overhead, bandwidth consumption, and computational cost. Security evaluation by using BAN logic and formal verification tool, Scyther, shows that the proposal can work correctly with the ability to withstand several protocol attacks.

Lunch 12:20-14:00

Oral Presentation Abstracts

Session 1

Tips: The schedule for each presentation is for reference only. In order not to miss your presentation, we strongly suggest that you attend the whole session.

Afternoon, July 9, 2020 (Thursday)

Time: 14:00- 15:45

Online-Meeting Room ID: 690 6915 5259

EC0002 (14:00-14:15 Singapore Standard time /15:00-15:15 Korea Standard time)

Secure Hierarchical Deterministic Key Generation Scheme in Blockchain-based Medical Environment

Tae-Hoon KIM and Im-Yeong LEE

Soonchunhyang University, South Korea

Abstract— Blockchain is essentially a form of distributed data storage technology. It is designed to prevent arbitrary manipulation by operators of distributed nodes and contains a list of changes that records the continuously changing data on the participating nodes. Currently, various blockchain-based services are appearing. In particular, blockchain-based medical convergence services are emerging worldwide. In a blockchain-based medical environment, hospitals, departments, doctors and patients must frequently update and use all public and private key pairs to minimize the leakage of personal information. As such, key pairs management is of great importance. To securely manage keys in such a medical environment, hierarchical deterministic wallet is used. Defined as Bitcoin's BIP32 standard, it is currently the most commonly used technology and allows hospitals to easily derive and manage the key of departments, doctors and patients. In addition, if the hospital, which is at the root level, backs up the first seed value, the doctor and patient can easily recover the key in the future, in case it is lost. However, problems have been found with hierarchical deterministic wallets. The attacker can infer the doctor's private key by obtaining doctor's public key, chain code, or the patient's index and private key. In addition, there is a privilege escalation attack that can be acquired up to the department or hospital's private key. Subsequently, an attacker can leak personal information, such as the personal information of doctors or medical records of managed patients. That is why the current BIP32 standard does not include the function to derive lower public keys from the higher public keys. In this scheme, we maintain the functionality removed from BIP32. In addition, we propose a secure scheme of hierarchical deterministic key generation scheme in blockchain-based medical environment by preventing privilege escalation attack.

EC5020 (14:15-14:30 Singapore Standard time /15:15-15:30 Japan Standard time)

Proof of Data Distribution Based on Trusted Hardware

Batnyam Enkhtaivan and Pooja Dhomse
NEC Corporation, Japan

Abstract— We consider a scenario in which two parties prove to a third party that communication between them occurred. This can be seen in advertisement in which the data are distributed to the user by a distributor on behalf of owner. Specifically, we propose a protocol and a modification of it to address the possibility of collusion between the distributor and user in which the owner is deceived to pay for false claim of distribution, and the possibility of the user not providing any data transfer confirmation as an acknowledgement after receiving data. In the original protocol, the distributor and user are both equipped with trusted hardware. The data are encrypted and decrypted by this trusted hardware, with a shared secret key. When decrypting the data, the user's hardware generates a proof and sends it to the distributor. This proof is used as the proof of distribution to show to the owner for payment. This prevents the collusion with the help of the trusted hardware. This protocol assumes that the user will not misbehave and always send the proof back to the distributor. To address this issue, the modified protocol uses blockchain as a public ledger for the user to publish acknowledgement of receiving encrypted data chunk, and for the distributor to publish the corresponding secret for decryption. In both the protocols, we use the blockchain technology as a method for the ID management and payment.

EC5026 (14:30-14:45)

Enhanced Security Approach Powered by Blockchain Technology with NFC to Prevent Fraudulence in Bank Letter of Credits

Rajendren Subramaniam, Saaidal Razalli Azzuhri and Teh Ying Wah
University Malaya, Malaysia

Abstract—Letters of Credit (Letter-of-Credit) frauds are deceptive attempts against financial institutions, primarily by providing availing false/falsify documentation as a proof of shipment of goods when, either, inferior goods were shipped, or no delivery was made at all. Letter-of-Credit also maybe forged to be provided to the supplier to supply goods. Whereas parties can forfeit the Letter-of-Credit by someone with vast experience and expertise in finance commerce laws, and international laws and business processes. In this research, we aspire to come up with an option of incorporating NFC-enabled mobile application into Letter-of-credit. The application is powered by blockchain technology and would be crucial in helping the recipient of the Letter-of-credit to achieve easy verification of the legitimacy of the document. The idea of using blockchain to prevent Letter-of-Credit fraud may not be novel where some have already been put into reality. However, not much work done in combining an NFC enabled mobile application leveraging on blockchain technology to prevent Letter-of-Credits frauds. The study is intended for banks who are still in migration to paperless business and still depending on a physical Letter-of-Credit for their business transactions.

EC5034 (14:45-15:00)

A Secure File Sharing System Based on IPFS and Blockchain

Hsiao-Shan Huang[1], Tian-Sheuan Chang[1] and Jhih-Yi Wu

1: National Chiao Tung University, Taiwan

2: Telecommunication Laboratories, Chunghwa Telecom Co., Ltd., Taiwan

Abstract— There is a great interest in many approaches towards blockchain in providing a solution to record transactions in a decentralized way. However, there are some limitations when storing large files or documents on the blockchain. In order to meet the requirements of storing relatively large data, a decentralized storage medium is produced. IPFS is a distributed file system which is content-addressable. It works very similar to the blockchain network. There are some attempts which take advantage of the blockchain concept and IPFS to design new approaches. Unfortunately, there are some inefficiencies in sharing data using the combination of IPFS and blockchain. In this paper, we proposed a secure file sharing system that brings a distributed access control and group key management by the adoption of the IPFS proxy. The IPFS proxy which plays an important role in the design is adopted to take responsibility for the control policies. The combination of the IPFS server and the blockchain network with the adoption of the IPFS proxy make a secure file sharing system which the members on the system can create new groups or join different groups by their own choice. Although there is no access control mechanism in IPFS server and blockchain network, the secure file sharing system manages the access control policies. The members access files only belong to the group they authorized.

EC5018 (15:00-15:15)

A Novel Supply Chain Model based on Smart Contract

Haitao LIU

Jiangxi Provincial State-Owned Enterprise Assets Operation (Holdings) Co., Ltd., China

Abstract— Facing on bursting of the huge quantity of trade, the problem of finance by micro and small firms, the expansion of business development of core enterprise in supply chain, the development of comprehension finance services, it is not well worked by traditional ways. And it is more and more restricting the development of supply chain. Considering the advantages of automatic executing and high efficiency of smart contract, the feature of decentralization, security, trustworthiness and anti-tampering of blockchain, there was advanced a novel supply chain model based on smart contract and blockchain for solving the problem totally. The model relied on the core enterprise of supply chain, integrated the upstream and downstream industries, constructed a consortium chain, that consisted of core enterprise, financial institutions, suppliers and dealers, formed an encrypted credit named ET (Electronic Trust) based on the trustworthiness of the trust industries chain. ET is equal to the actual credit, it could be paid for the suppliers according to the cargo value before the last settlement. So the ET could combine the virtual and actual capital. Thus it also could further solve the common pain points of supply chain.

EC5033 (15:15-15:30 Singapore Standard time/ 9:15-9:30 Luxembourg Standard time)

Decentralised Compliant Data Trading for Banks

Robert Norvill[1], Jean Hilger[1], Irfan Awan[2] and Radu State[1]
1: University of Luxembourg, Luxembourg
2: University of Bradford, United Kingdom

Abstract— Banks must comply with a complex set of regulatory and legislative requirements in order to be sure they know who they are doing business with. Current Know Your Customer processes are inefficient and costly, often being repeated by multiple banks. As such, financial institutions have a need to reduce the cost of compliance. Banks can reduce their costs through inter-bank Know Your Customer data trading. In this paper, we build upon an industry-strength, blockchain-based, Know Your Customer data sharing platform to facilitate a novel data marketplace by detailing a method of pricing data such that banks save money and are suitably incentivised to trade their data. The pricing model we detail enables banks to reduce the cost of document acquisition and verification by at least 45%, and even profit by providing documents. In addition, we discuss how decentralised pricing is realised through the use of smart contracts.

EC5022 (15:30-15:45 Singapore Standard time/ 8:30-8:45 UK Standard time)

TheChain: A Fast, Secure and Parallel Treatment of Transactions

Mohamed Ikbal Nacer, Simant Prakoonwit and Ismail Alarab
Bournemouth University, UK

Abstract— The Smart Distributed Ledger (aka blockchain) has attracted much attention in recent years. According to the European Parliament, this technology has the potential to change the lives of many people. The blockchain is a data structure built upon a hashed function in a distributed network, enabled by an incentive mechanism to discourage malicious nodes from participation. The consensus is at the core of the blockchain technology, and is driven by information embedded into a data structure that takes many forms such as linear, tree, and graph chains. The found related information will be subject to various validation incentives among the miners, such as proof of stake and proof of work. However, all the existing solutions suffer from a heavy state transition before dealing with the problem of a validation mechanism which suffers from resource consumption, monopoly or attacks. This work raises the following question: “Why is there a need for consensus where all participants can make a quick and correct decision?”, and underlines the fact that sometimes ledger is subject to maintenance from regional parties in the data that leads to partial territories and eliminates monopoly, which is the hurdle to eliminating the trusted party. The validity of the blockchain transaction comes from the related information scattered above the data structure, and the authenticity lies in the digital signature. The aim is to switch from a validator based on incentives to a broadcaster governed by an unsupervised clustering algorithm, and the integrity does lie in the intersection among regions. However, the data structure takes advantage of the Petri network regarding its suitability. Building the entire ledger in the Petri network model will allow parallel processing of the transactions and securing of the total order between the participants on the memory reference layer. Moreover, it takes account of validation criteria quickly and safely before adding the new transaction list using the graph reachability.

Take a Break: 15:45-16:00

Oral Presentation Abstracts

Session 2

Tips: The schedule for each presentation is for reference only. In order not to miss your presentation, we strongly suggest that you attend the whole session.

Afternoon, July 9, 2020 (Thursday)

Time: 16:00- 17:30

Online-Meeting Room ID: 690 6915 5259

EC5035 (16:00-16:15 Singapore Standard time/ 18:00-18:15 Australia Standard time)

A Conceptual Model for Blockchain-based Auditing Information System

Ke Wang, Yu Zhang and Elizabeth Chang
UNSW Canberra, Australia

Abstract—Blockchain is viewed as one of the most promising and disruptive inventions and is considered to have the potential to significantly change current auditing profession and reshape the business ecosystem. With the advancement of blockchain, it has been concerned in some studies that auditing could be significantly impacted and eventually replaced. Meanwhile, another viewpoint argues that blockchain technology would push the existing auditing industry to a new direction rather than eliminating the need for auditing in the immediate future. This discussion can hardly be settled without evaluation, however, studies exploring how blockchain technology can be employed in auditing practice or how continuous auditing can be conducted using blockchain technology are limited. This paper analyses the impact of blockchain features on existing audit processes and discusses the possibility of applying blockchain characteristics including immutability, distributed ledger, real-time settlement to the auditing domain. Based on the systematic analysis, this study proposes a conceptual model for blockchain-based auditing information system, which provides solutions to employ blockchain technology in auditing profession, significantly improving the efficiency and effectiveness of auditing and promoting the transformation of the auditing paradigm to real-time, continuous and intelligent auditing.

EC5011 (16:15-16:30 Singapore Standard time/ 10:15-10:30 Netherlands Standard time)

Traceability Blockchain Prototype for Regulated Manufacturing Industries

Utkan Eryilmaz[1], Remco Dijkman[1], Willem van Jaarsveld[1], Wouter van Dis[2] and Kaveh Alizadeh[2]
1: Eindhoven University of Technology, Netherlands
2: Fokker Services B.V.,Netherlands

Abstract— Blockchain emerged as a peer-to-peer trust platform for trading virtual currencies and evolved to be used for different problems including supply chain provenance. Due to stringent requirements of safety, regulated manufacturing and service industries such as aerospace, healthcare, and transportation require regulated traceability for parts, from source to the last customer, with detailed information requirements for each handover and operation. In this research, we analyzed the current traceability problem and list use cases of a traceability blockchain platform. A prototype platform is developed for the aerospace industry where every single part is equired to have source and path traces recorded by certified supply chain actors. We evaluate the efficiency benefits of the platform in terms of duration and address future research topics.

EC5028(16:30-16:45 Singapore Standard time /10:30-10:45 Norway Standard time)

VerifyMed - A blockchain platform for transparent trust in virtualized healthcare: Proof-of-concept

Jens-Andreas Hanssen Rensaa, **Danilo Gligoroski**, Katina Kralevska, Anton Hasselgren and Arild Faxvaag
Norwegian University of Science and Technology, Norway

Abstract— Patients living in a digitized world can now interact with medical professionals through online services such as chat applications, video conferencing or indirectly through consulting services.
These applications need to tackle several fundamental trust issues: 1. Checking and confirming that the person they are interacting with is a real person; 2. Validating that the healthcare professional has competence within the field in question; and 3. Confirming that the healthcare professional has a valid license to practice. In this paper, we present VerifyMed - the first proof-of-concept platform, built on Ethereum, for transparently validating the authorization and competence of medical professionals using blockchain technology. Our platform models trust relationships within the healthcare industry to validate professional clinical authorization. Furthermore, it enables a healthcare professional to build a portfolio of real-life work experience and further validates the competence by storing outcome metrics reported by the patients. The extensive realistic simulations show that with our platform, an average cost for creating a smart contract for a treatment and getting it approved is around 1 USD, and the cost for evaluating a treatment is around 50 cents.

EC5012 (16:45-17:00 Singapore/ Malaysia Standard time/ 11:45-12:00 Saudi Arabia Standard time)

A Blockchain-Based Smart Network for IoT-Driven Smart Cities

Nada Alasbali[1], Saaidal Razalli Azzuhri[2] and Rosli Salleh[2]

1: King Khalid University, Saudi Arabia

2: University of Malaya, Malaysia

Abstract— Internet-of-Things (IoT) networks interoperability is of a crucial role in driving innovation to achieve smart city agenda. However, the potential for a unified and connective digital linkage is undermined by competitive private sector standards and protocols that are dissociated and disunited. In this paper, we propose a blockchain-based standard for IoT integration which is democratized, scalable, and decentralized. As a transactional ledger, the blockchain serves as a central data warehouse capable of monitoring the entrance and exit of user-triggered information. Network interchange and authentication can be facilitated through blockchain-relegation of network communication and security protocol. The outcome is linked with integrated communications, efficiency and a highly functional user experience as the constructs of interoperability develops. Therefore, this paper vouches for a non-proprietary, unified, and standardised protocol for linking IoT based smart city solutions with a blockchain middle layer to protect both commercial (proprietary APIs) and user (privacy, security, autonomy) interests in a distributed, smart city ecosystem.

EC5009-A (17:00-17:15 Singapore Standard time / 18:00-18:15 Korea Standard time)

Hyperledger Fabric-based Electronic Voting System Using Reliable Permissioned Blockchains

Kyoung-Jin Kim

Sungshin Women's University, Korea

Abstract— Electronic voting (e-voting) offers various benefits, such as voting rate increase and spatial and temporal cost reduction, so many countries have attempted to adopt it. However, as conventional e-voting is conducted by people or organizations providing the service, there are concerns regarding the assurance of a secret ballot and security in terms of hacking and manipulation. Blockchain technology prevents hacking and manipulation and ensures reliability by allowing many people share information. Hence, studies have been actively conducted for its adoption, providing a solution for the problems of conventional e-voting.

Blockchains can be classified into public, private, and permissioned according to the type of participation and data disclosure level. Anyone can participate in permissioned blockchains after undergoing an appropriate authentication process, and as only authenticated voters can comprise a network, permissioned blockchains are most suited for voting systems. In a voting system, encryption and anonymization technologies are mainly used to ensure privacy. However, encryption leads to low efficiency because of the decryption issue, where in the anonymization, collision can occur when classifying the votes of voters because random strings are used. In this study, we propose a homomorphic encryption algorithm that performs computation without decryption to guarantee privacy. Although blockchains are generally known to ensure anonymity by using addresses produced with random numbers, there is a risk that a user may be identified using a combination of data produced from an address and remittance information. Zero-knowledge proof refers to a proving method that does not expose any information other than true or false of corresponding propositions when a prover attempts to prove an arbitrary proposition to a verifier. In this study, zk-SNARK was applied.

The system suggested in this study a permissioned blockchain-based e-voting system that is most suitable for e-voting. The proposed system maximizes the privacy of voters by using a homomorphic encryption algorithm and prevents manipulability of votes through calculation of result values based on multi-party. In addition, problems that may arise when adopting blockchains in e-voting were determined and solutions were provided. For intuitive understanding, a fabric network was constructed using a virtual machine of VirtualBox in the implementation environment of the proposed system, in which multiple nodes are installed on a single host PC. After implementation and operation of the proposed system, its encryption time was not significantly different from the conventional encryption time. This paper proposed used blockchain-based e-voting to improve its reliability compared to conventional e-voting.

EC5016 (17:15-17:30 Singapore Standard time / 13:15-13:30 UAE Standard time)

Performance Evaluation of a Patient-Centric Blockchain-based Healthcare Records Management Framework

Leila Ismail, Huned Materwala and Moien AB Khan
United Arab Emirates University, United Arab Emirates

Abstract— Healthcare records management system has been revolutionized over the last decade aiming to provide accurate, efficient and enhanced patient care. The existing management system is either based on a client/server approach where each hospital maintains its own database or on a cloud approach where the health records are stored in a cloud server and managed by a third-party cloud service provider. However, these approaches suffer from the issues of security, privacy, data vulnerability and fragmentation. Furthermore, healthcare providers and patients are unable to have a unified view of a patient's medical history from all visited medical care centers. This results in additional treatment costs, repeated medical tests and increased time to diagnosis. The data traceability, immutability, transparency, replication, security and privacy traits of the emerging blockchain technology have a promising potential in the healthcare domain addressing these issues. In this paper, we propose BlockHR, a patient-centric healthcare records management system for efficient medical care at an optimal cost. The system enables healthcare providers to enter the patients' medical record data to the blockchain network and allows patients to enter their social data such as sleeping habits, physical activities, and current location. Consequently, BlockHR provides support to doctors for better diagnosis and prognosis. We evaluate the performance of BlockHR in terms of execution time and the total amount of data transferred for ledger update with an increasing number of hospitals and blocks in the network.

Morning Session

Morning, July 10, 2020 (Friday)

Time: 9:40-11:30

Online-Meeting Room ID: 690 6915 5259

Invited Speech I (9:40-10:00)

Title: Target Localization for Distributed MIMO Radar Systems via Improved Semidefinite Relaxation

Prof. Zhi Zheng

University of Electronic Science and Technology of China, China

Abstract—Target localization in distributed multiple-input multiple-output (MIMO) radar systems has attracted considerable interest due to its wide applicability in tracking and surveillance. These existing localization methods, including two-step weighted least square methods and semidefinite relaxation methods, can achieve high accuracy at low noise levels, but they will suffer from the threshold effect when the noise level is high. Moreover, an initial guess of the target position and velocity is often required in these methods. In this report, we will present two improved semidefinite relaxation methods for target localization in distributed MIMO radar systems. The first method is aimed at static targets, which solves directly the maximum-likelihood localization problem through semidefinite relaxation. To improve the solution accuracy, an additional procedure is also devised in this method. The second method is developed for moving targets, this method achieves better performance by tightening the feasible region of the SDP problem. The presented methods exhibit evidently better threshold behavior than various existing approaches. Furthermore, they do not require any initial estimate of the target position.

Oral Presentation Abstracts

Session 3

Tips: The schedule for each presentation is for reference only. In order not to miss your presentation, we strongly suggest that you attend the whole session.

Morning, July 10, 2020 (Friday)

Time: 10:00- 11:30

Online-Meeting Room ID: 690 6915 5259

EC0009 (10:00-10:15 Singapore Standard time/22:00-22:15 USA Standard time on July 9th)

Performance Evaluation of TCP and UDP over IPv4 and IPv6 for the ESP8266 Module

Eric Gamess and Brody Smith

Jacksonville State University MCIS Department, Jacksonville, AL, USA

Abstract— Due to the increasing popularity of the Internet of Things (IoT), several modules, development boards, and single-board computers have been proposed by the community and manufacturers. In this paper, we selected the ESP8266, an inexpensive module, to make a performance evaluation of its networking subsystem. Since the popular benchmarking tools of the area have not been ported for the ESP8266, we wrote several benchmarks to evaluate its TCP and UDP performance over IPv4 and IPv6, as an end-point device or as an access point. In our tests, we report parameters such as one-way delay and throughput. To cover a wider range of developers, we give performance measurements for two development tools: Arduino IDE and Espressif SDK.

EC0004 (10:15-10:30)

A Lightweight D2D Authentication Scheme against Free-riding Attacks in 5G Cellular Network

Man Chun Chow and Maode Ma
Nanyang Technological University, Singapore

Abstract— As a promising feature in 5G, device-to-device (D2D) communication is the technology allowing adjacent mobile devices to communicate directly without relaying the data over base stations. D2D technology can potentially increase the network capacity by offloading network traffic in a distributed manner. However, there are also new security challenges such as free-riding attack prevention, device anonymity protection and end-to-end data secrecy. Also, since there are many mobile devices which have limited computational resources in 5G cellular network, there is a need to develop a lightweight authentication protocol which addresses all these security requirements with low computational overhead. In this paper, we propose a lightweight D2D authentication and key agreement protocol based on elliptic curve cryptography (ECC). Specifically, our proposed scheme makes use of the elliptic curve digital signature algorithm (ECDSA), elliptic curve Diffie-Hellman (ECDH) and authenticated encryption with associate data (AEAD) to provide secure device discovery, mutual authentication, key agreement and data transmission for all 5G D2D devices. Our scheme is computationally lightweight to be supported in any resource-constrained 5G devices, and it can resist several active and passive protocol attacks including eavesdropping, replay attack, man-in-the-middle attack and free-riding attack. We analyze the security of our protocol with Scyther to show our scheme is resistant to these attacks. Finally, performance evaluation shows our scheme is efficient for both UEs and CN with rationally low computational costs.

EC0006 (10:30-10:45)

The Impact of Interaction on The Travel Arrangement: Cultivating Serendipity and Reducing Psychological Distance in Tourism Platforms

Anzhuo Xie[1] and Dong Tan[2]
1: Jilin university, China; 2: Nankai University, China

Abstract— More and more people, in this age and day, choose to travel when they are in their convenience. At the same time, many tourism platforms appear to assist tourists to make their travel choices. For these platforms, the most efficient way to help tourists is to offer tourists relevant information concerning the destinations, so that tourists can acquire a better understanding of the resorts before making their decision. This article mainly studies what kind of information enables tourists to familiarize themselves with the destinations to more extent from the perspective of psychological distance and serendipity. Based on the method of group experiment, this paper studies five kinds of information, including VR, and the interaction before tourists, and finally finds that the high level of serendipity and the low level of psychological distance can higher tourists' decision-making satisfaction and decision outcome satisfaction, which is conductive to making a better final decision.

EC0005 (10:45-11:00)

Design of Feature Selection Algorithm Based on MOEA for IDSs in VANETs

Liang Junwei and **Ma Maode**
Nanyang Technological University, Singapore

Abstract— Intrusion detection systems (IDSs) is crucial for the security of Vehicle Ad Hoc Networks (VANETs), as it can accurately detect both the inner and outer attacks. However, the redundant features and the sparse samples of fatal attacks in VANETs datasets cause the heavy time-consumption and imbalanced problems respectively. In this paper, a feature selection algorithm based on a many-objective optimization algorithm (FS-MOEA) is proposed for IDSs in VANETs, in which Non-dominant Sorting Genetic Algorithm-III (NSGA-III) serves as the many-objective evolutionary algorithm. Two improvements, called Bias and Weighted (B&W) niche-preservation and Analytic Hierarchy Process (AHP) prioritizing, are further designed in FS-MOEA. B&W niche-preservation is used to counterbalance the imbalanced problem among the different classes of datasets by assigning rare classes higher priorities in the niching selection process. AHP prioritizing is employed to search the optimal feature subset from the non-dominant feature subsets in the Pareto Front of FS-MOEA. Experimental results show that the proposed FS-MOEA can not only improve the performance of IDSs in VANETs by decreasing the redundancy and irrelevances of features but also alleviate the negative impact of the imbalanced problem.

EC0008 (11:00-11:15)

A Group Authentication Scheme with Privacy-preserving for D2D Communications in 5G HetNets

Alican Ozhelvaci and Maode Ma
School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore

Abstract— The next-generation mobile communication, which is 5G wireless mobile networks, has become the paradigm to bring not only solutions for the rising demand for huge data traffic, and massively connected devices such as IoT but also new services. One of the promising solutions is that device-to-device communications are expected to play a key role to improve efficiency and have low latency. Most importantly, D2D communications will be the key enabler for group-based services. However, the new case scenarios and new system architecture of 5G Heterogeneous Networks are vulnerable against various attacks since the 5G is still in the early stage. It is utmost important to have a secure and privacy-preserving scheme for D2D communications in 5G HetNets. Even though various research studies have been done by the researchers for D2D communications but many of them fail to address the heterogenous access scenarios, identity protection, and group authentication. In this paper, we propose a certificateless privacy-preserving authentication and key agreement scheme for D2D communications in 5G HetNets using identity-based encryption and elliptic curve digital signature algorithm (ECDSA) to achieve secure and robust communication. The proposed scheme has been analyzed in terms of security and performance. The result of the formal verification using AVISPA and performance analysis shows that the scheme is secure, lightweight and efficient.

EC0001(11:15-11:30 Singapore Standard time/10:15-10:30 Thailand Standard time)

High Performance Peer-to-peer Data Dissemination for Decentralized Wireless Sensor Networks Firmware Updating

Natchanon Nuntanirund and Natawut Nupairoj;
Chulalongkorn University Bangkok, Thailand

Abstract— Data dissemination is an important feature to enable reconfigurations and firmware updates in wireless sensor networks. Typically, data disseminations in modern wireless sensor networks are based on multicast-based algorithms which may not be the most efficient ways because they do not guarantee packet delivery. In this paper, we present a reliable data dissemination algorithm for distributed wireless sensor networks. It derives some features from BitTorrent such as segmented file transfer, choking, and optimistic unchoking to improve performance. The evaluation result shows that our algorithm performs better than multicast-based algorithms in term of download speed up to 58.97% and energy efficiency up to 79.39%

Session 4

Tips: The schedule for each presentation is for reference only. In order not to miss your presentation, we strongly suggest that you attend the whole session.

Afternoon, July 10, 2020 (Friday)

Time: 15:00- 16:30

Online-Meeting Room ID: 690 6915 5259

EC5008 (15:00-15:15 Singapore Standard time/16:00-16:15 Korea Standard time)

Sybil Tolerant Consensus Method Using Mutual Proof of Validation

Hoon Shin, Kyuho Son and Dongsoo Han

Korea Advanced Institute of Science and Technology, Korea

Abstract— This paper introduces a method to make a consensus by recording proof of block validation, which operates in a public blockchain environment, with a consensus algorithm named Sybil Tolerant Equality Protocol (STEP). To solve the problem of centralization,which is pointed out as a problem of existing consensus algorithms, all nodes are given the same power. Also, methods to prevent Sybil attack in which one principal creates multiple nodes are proposed. To this end, STEP randomly selects nodes to create blocks, divides the validation process into two stages, and provides a reward for rapid and correct validation. Through simulations and experiments on STEP, we confirmed whether the random number generation method, the incentive function for block validation, and the network following this consensus algorithm work correctly within the practicable scope of execution time.

EC5015 (15:15-15:30)

BC-Store: A Scalable Design for Blockchain Storage

I-Te Chou[1], Hung-Han Su[1], Yu-Ling Hsueh[1] and Chih-Wen Hsueh[2]
1: National Chung Cheng University, Taiwan
2: National Taiwan University, Taiwan

Abstract— The blockchain technology has obtained significant success in the past decades. However, a serious underlying problem still exists in the blockchain system – data bloating. In the blockchain system, each (full) node must store the full data set in blockchain history, incurring significant storage pressure in the initial synchronization process and the following maintenance of the blockchain system.
Data bloating is a challenging problem to be confronted in the immediate future of blockchain. To address this problem, in this paper, we introduce the BC-Store framework that deploys a data accessing model on an IPFS-cluster system to classify the hot and cold blockchain data. The hot data are stored in the local cache, whereas the cold data are stored in the IPFS cluster, thereby substantially shortening the blockchain initial synchronization time and saving a considerable amount of data storage. Empirical experimentation shows that our framework can reduce the local storage size from over 265GB to 4GB with a hit ratio of 77% for Bitcoin without significant performance degradation with the whole data shared in an IPFS cluster.

EC5014 (15:30-15:45 Singapore Standard time/10:30-10:45 Russia Standard time)

Responsible Self-Funding in Dash Governance System

Ivan Chistiakov[1] and **Yury Yanovich[2]**
1:National Research University Higher School of Economics, Russia
2: Skolkovo Institute of Science and Technology, Russia

Abstract— Decentralized voting and self-funding allow cryptocurrencies to make joint decisions and finance their development. Dash cryptocurrency has a working self-funding and decision making system for event and improvement proposals support–Dash Governance System. While it is fully operational, as currently designed, it does not incentivize voting efficiency.
Dash Governance System struggles to scale with the number of proposals rising as each participant needs to review each proposal. In this work, a new mechanism for proposal processing is introduced. It meets scalability and makes thoughtful voting the most profitable strategy.

EC5005 (15:45-16:00 Singapore Standard time/9:45-10:00 Germany Standard time)

Transaction Dependency Model for Block Minimization in Arbitrary Blockchains

Wolf Posdorfer, Heiko Bornholdt and Winfried Lamersdorf
University of Hamburg, Germany

Abstract—Blockchains are distributed replicated state machines with a continuously increasing data storage underneath. The size of the storage can cause problems especially in limited IoT devices. In order to address that, this paper is based on the following ideas: While two state transitions could be replaced by a single one to represent the same state, this is not commonly done to reduce the blockchains storage size. To facilitate squashing of transactions independent of the application semantics a blockchain frameworks needs to know the interdependencies of transactions.
In this paper we propose an explicit dependency model for any transaction in a blockchain. In this way a blockchain-framework can preselect connected transactions without business process semantics
for a squash operation. These connected transactions are passed to the application for the squash to be performed. This ideally produces less transactions while achieving the same application state to be used for a reintroduction as new blocks within a fork for a smaller overall storage footprint.

EC5036 (16:00-16:15 Singapore Standard time/11:00-11:15 Russia Standard time)

Optimal Portfolio Sold-Out via Blockchain Tokenization

Vyacheslav Davydov[1] and **Yury Yanovich[2]**
1: Moscow Financial University at the Government, Russia
2: Skolkovo Institute of Science and Technology, Russia

Abstract— Financial institutions own balanced portfolios with many assets and hence a small risk. But they are not able to split them into smaller parts with comparable risk for resale due to regulators' restrictions caused by a lack of auditability. Blockchain and smart contracts allow overcoming this problem via tokenizing assets into a commodity. The paper seeks to answer the question: how to assemble as many as possible standardized packages from a given portfolio. The optimal algorithms for two special cases–discrete and continuous homogeneous–are provided.

EC5013 (16:15-16:30 Singapore Standard time/ 10:15-10:30 Austria Standard time)

From Blockchain to Web: Paving the Last Mile for Releasing Chained Data from the Blocks

Belal Abu Naim, Martin Hronsky and Wolfgang Klas
University of Vienna, Austria

Abstract— Blockchain systems make use of the Internet infrastructure to connect thousands of nodes in peer-to-peer (P2P) networks. These connected nodes form complex ecosystems encompassing various technologies that collaborate to offer millions of users distributed, decentralized, secure, and read-only data stores. With the proliferation of various private and public platforms and applications that are built on top of blockchain technology, rich sources of several types of simple or complex datasets have been created. Consequently, new requirements for managing these rich data sources, integrating them with their hosting environment, and making them discoverable have emerged. Fulfilling these requirements calls for extending the architecture of current blockchain systems by adding different layers that offer dedicated services for handling the data and allowing for integrating the blockchain-based platforms and applications with other systems, including Web-based applications. In this paper, we present a novel approach aiming at extending the architecture of current blockchain systems by adding new service layers for processing the data and offering new services to provide a bridge between blockchain systems and Web-based external applications enabling them to query, retrieve, and access the datasets managed by robust permission-based access control.

Note

Note