Topic: Cross-disciplinary Workshop on Blockchain Research and Applications
(with a complementing special session of peer-reviewed papers link)

Description: Blockchain has emerged as a novel distributed consensus scheme that allows transactions, and any other data, to be securely stored and verified in a decentralized way. Blockchain-based services are implemented through smart contracts, which require the design and interactions of multiple intelligent agents within and among contracts. This field is highly interdisciplinary, and has the potential for research projects and results sitting at the intersection of computer science, cryptography, computational intelligence, engineering, finance, economics, etc. There is interest in applying blockchain to different application scenarios and in solving complex problems, and the technology offers opportunities to support the transformation of business models. However, many technical challenges arise with the rapid development of distributed ledgers. It is also needed to study and implement conditions that ensure blockhains cannot be broken and that privacy is protected.

Keytalk: "Blockchain: A Cautionary Viewpoint," Yvo Desmedt

Abstract: For 2000 years cryptographers have been predicting unbreakable cryptosystems. Unfortunately, no cryptosystem has lasted more than 300 years. The only systems we know that can not be broken (such as the one-time pad) are useless for blockchains. In this talk, we start by having a critical look at the field of cryptography. We analyze what assumptions are needed to make sure blockchains can not be broken. We also discuss some potential applications of blockchains and what their impact could mean for privacy.

Bio: Yvo Desmedt is the Jonsson Distinguished Professor at the University of Texas at Dallas, and an Honorary Professor at University College London (UCL). He is a pioneer of threshold cryptography, and is a Fellow of the International Association for Cryptologic Research, and a Member of the Belgium Academy of Science. He received his Ph.D. (1984, Summa cum Laude) from the University of Leuven, Belgium. Prof Desmedt held positions at Universite de Montreal, University of Wisconsin-Milwaukee and Florida State University, as well as numerous visiting appointments at other universities. At Florida State, he was Director of the Laboratory of Security and Assurance in Information Technology, one of the first 14 NSA Centers of Excellence. At Wisconsin-Milwaukee, he was Founding Director of the Center for Cryptography, Computer and Network Security, and at UCL, he was BT Chair and Chair of Information Communication Technology. Yvo is the Editor-in-Chief of IET Information Security and Chair of the Steering Committees of CANS and ICITS. He was Program Chair of e.g., Crypto 1994, the ACM Workshop on Scientific Aspects of Cyber Terrorism 2002, and ISC 2013. He has authored over 200 refereed papers, primarily on cryptography, computer security, and network security. He has made important predictions, such as his 1983 technical description of how cyber could be used to attack control systems (realized by Stuxnet), and his 1996 prediction that hackers will target Certifying Authorities (DigiNotar was targeted in 2011).

workshop presentations:

"Security of Cryptocurrency Wallets," Nicolas Courtois

Bio: Dr Nicolas Courtois is a cryptologist and has done his PhD thesis in cryptology at Paris 6 University. His current H-index is 37 according to Google Scholar. Nicolas is a Senior Lecturer at University College London, with responsibilities on the M.Sc. programme in Information Security. For seven years he worked as a cryptologist in the largest secure hardware manufacturer in the world Gemalto, and has filed eight patents on industrial applications of cryptology, embedded security, smart cards and side-

channel attacks. Dr Courtois is also an influential code-breaker and author of more than 100 publications with over 5800 citations. He is responsible for the cryptanalysis of many real-life ciphers used by many people every day, such as the Bluetooth cipher E0, the automobile cipher KeeLoq, and the MiFare Classic Crypto-1 system (oyster card). His research interest cover all topics in Bitcoin, Ethereum, Darkcoin, etc., as well as speeding up the hashing process with SHA256, hash rate vs. security, and computational cryptanalysis of symmetric and asymmetric ciphers. His research focuses on the security analysis of cryptographic schemes with focus on realistic attack scenarios where the amount of data available to the attacker is very low. Dr Courtois is recipient of the UK University Cipher Champion 2013 award, and the best paper award at Computation Tools 2012.

"Blockchain and Crypto-currencies: Challenges and Considerations for Law-Enforcement," Kacper Gradoń

Abstract: The paper delivers an overview of challenges that the crypto-currencies and associated blockchain technologies pose for the law-enforcement and Intelligence agencies and security services. Specific stress is placed on the potential criminal and terrorist misuse of technology, especially in the area of financing of terrorism and money laundering. The research is based on the interviews with law-enforcement practitioners representing several jurisdictions worldwide, as well as the literature review and open-source data. The aim of the paper is to provide the blockchain research and development community with the set of concerns arising in the criminal justice and policing circles, and to point where the emerging technologies should be addressed in order to facilitate public security and safety.

Bio: Kacper Gradon is an Associate Professor at Faculty of Law, and Director of Centre for Forensic and Investigative Sciences, University of Warsaw. He was awarded three research scholarships by the Canadian International Development Agency, and three grants by the Polish Ministry of Science. Dr Gradon has held Visiting Professorships at University College London, University of Colorado at Boulder, University of Southern California, John Jay College of Criminal Justice – CUNY, and Memorial University of Newfoundland. He received the Polish Ministry of Science Scholarship for Outstanding Academics, in 2011, and more recently was awarded a National Centre for Research and Development grant for training at Fraunhofer-Gesellschaft Institute, Germany, and IBM T.J. Watson Research Center, USA. Dr. Gradon participated in the creation of the Polish Criminal Analysis and Intelligence Units, and also completed the London Metropolitan Police Specialist Operations Training for Hostage Negotiations; and courses led by the Federal Bureau of Investigation (FBI), Dutch Police, Guardia di Finanza, Bundeskriminalamt, Royal Ulster Constabulary and the Royal Canadian Mounted Police. He is currently Primary Investigator in the European Commission FP7 Project PRIME (Preventing, Interdicting and Mitigating Extremism).

"Evaluating Blockchain Adoption: Disruptive not Destructive," Antoaneta Serguieva

Bio: Antoaneta Serguieva has a background in systems engineering / cybernetics, finance, computer science / computational finance, and mathematics. She is a Senior Researcher with nChain, focused on blockchain research and applications, and has been a quant consultant for investment funds. She became aware of regulatory priorities in systemic risk during fellowships at the Bank of England, Bank of Mexico, Federal Reserve, and U.S. Treasury. She is a Research Associate with the Systemic Risk Center, London School of Economics, a Visiting Professor with the Center for Computational Finance and Economic Agents, University of Essex, and until recently a member of the Research Center for Blockchain Technologies, University College London. Her research interests include nature-inspired computational intelligence and heuristics for modeling complex sociotechnical systems, contagion mechanisms, and cognition. Dr. Serguieva is an Associate Editor for IEEE Transactions on Fuzzy Systems,

and Chaired the Computational Finance and Economics TC of IEEE Computational Intelligence Society in 2014–15.

Applications-focused Panel Discussion:

Gavin Allen, nChain, London, UK; Nicolas Courtois, NaviAddress, Cyprus;
Leonardo Passos, Quantstamp, Waterloo, Canada; David Yue, SkyLedger, Shanghai, China

Gavin Allen, nChain, London, UK

Bio: Gavin Allen is Chief Technology Officer at nChain, London. He is an experienced Enterprise Architect, with a proven track record of converting organizational visions into optimized architectures that achieve sustainable business value across a range of financial businesses. He has a strong background in design and delivery, and is engaging across all levels within an organisation. Gavin has acquired knowledge across a range of technology deliverables – from mission-critical, real-time, transaction processing systems that achieve true 100% availability, through to more traditional enterprise applications built upon client-server and service-oriented architectures. His technical skills are supplemented with knowledge of business process design and optimization to achieve a true end-to-end design.

Nicolas Courtois, NaviAddress, Cyprus

Bio: (see above)

Leonardo Passos, Quantstamp, Waterloo, Canada

Bio: Leonrado Passos is a Senior Research Engineer at Quantstamp Technologies, Canada. He has a Ph.D in Electrical and Computer Engineering from the University of Waterloo, for his work on mining patterns from the Linux kernel source code and other systems. Leonardo is a Microsoft research competition medalist, with industry experience in backend development, compilers, and scalable data pipelines.

David Yue, SkyLedger, Shanghai, China

Bio: David Yue is an early angel investor in blockchain. He was the judge of the 1st Global Blockchain Competition in Singapore, and of the 1st China Blockchain Technology Innovation and Application Contest. He is executive member of Asia-Israel Blockchain Association. David is a visiting professor at the Blockchain Institute of Jiangxi Pioneer Software College, and a guest lecturer in blockchain within the EMBA program at Beijing University of Posts and Telecommunications. He has almost 2 decades of diverse experience in MNC and high-tech companies including Alcatel-Lucent, Cisco and Marconi prior to joining the private-equity / venture-capital industry.

Workshop Website: The Workshop will be added to the special session website at www.ieee-cifer.org.

Technical Sponsors: Cindicator, EtherSat, NaviAddress, nChain, Nebula, Quantstamp, SkyLedger, Trustedhealth

Workshop Organizers:
Alexander Lipton, MIT Connection Science; Nicolas Courtois, University College London;
Jon Matonis, Bitcoin Foundation; Nikola Kasabov, International Neural Network Society;
Antoaneta Serguieva IEEE Computational Intelligence Society

Workshop Contact: cifer@ieee.org