f

JOHN JAY COLLEGE OF CRIMINAL JUSTICE

Center for Cybercrime Studies

presents

A Smart Contract for Boardroom Voting with Maximum Voter Privacy

Patrick McCorry

University of Newcastle, UK

Date: Wednesday, April 26, 2017
Time: 1:40 – 2:40 pm
Math & CS Conference Room (6.63.37), 6th Floor, New Building

Abstract:

We present the first implementation of a decentralised and self-tallying internet voting protocol with maximum voter privacy using the Blockchain. The Open Vote Network is suitable for boardroom elections and is written as a smart contract for Ethereum. Unlike previously proposed Blockchain e-voting protocols, this is the first implementation that does not rely on any trusted authority to compute the tally or to protect the voter's privacy. Instead, the Open Vote Network is a self-tallying protocol, and each voter is in control of the privacy of their own vote such that it can only be breached by a full collusion involving all other voters. The execution of the protocol is enforced using the consensus mechanism that also secures the Ethereum blockchain. (Note: This is a variation the speaker's talk given at FC'17 in Malta earlier this month.)

Bio:

Patrick McCorry is currently visiting Andrew Miller at the University of Illinois at Urbana-Champaign (UIUC) and will soon join Sarah Meiklejohn and George Danezis at University College London (UCL) as a post-doc. He recently finished his PhD at Newcastle University under the supervision of Feng Hao. His research interests include cryptocurrencies and cryptography. In the past, he worked at IBM Hursley UK for the CICS (Customer Information Control Systems) portfolio.