IC3 The Initiative For CryptoCurrencies & Contracts

Prof. Andrew Miller, IC3 Associate Director and Amber Baldet, Head of the JP Morgan Blockchain Center of Excellence rock the new IC3 T-shirts at [Devcon3]() in Cancun on November 2-4, 2017.

IC3 faculty and student presenters at Devcon3 included Prof. Miller, Prof. Emin Gün Sirer, Prof. Elaine Shi, Dr. Patrick McCorry, and Phil Daian.

[Amber announced that JP Morgan joined IC3]() and IC3 has launched a [6th Grand Challenge.]()

[View a recent video interview]() of JP Morgan blockchain experts and IC3 co-Director Prof. Emin Gün Sirer, discussing the collaboration between JP Morgan and IC3, and the outlook for blockchain-based solutions.

Greetings! Happy New Year! Welcome to the IC3 Quarterly Newsletter!
This is an outreach to keep the blockchain community aware of IC3 innovations, events, news, publications, and other service to the community by IC3 faculty, students, and partners.

RECENT ANNOUNCEMENTS
[IC3 Expands Research Team in Europe and US]()
On October 31, we announced three eminent faculty members in Europe are joining IC3. These include:

- **Prof. Srdjan Capkun** , Full Professor in the Department of Computer Science, ETH Zurich and Director of the Zurich Information Security and Privacy Center

· **Prof. Bryan Ford** , Associate Professor, leads the Decentralized/Distributed Systems (DEDIS) lab at EPFL.
· **Prof. Sarah Meiklejohn** , Associate Professor, in the departments of Computer Science and Security and Crime Science at University College London.

Also, joining her IC3 colleagues from Cornell is one of the world's leading financial researchers: **Prof. Maureen O'Hara** , the Robert W. Purcell Professor of Finance at the Johnson Graduate School of Management, Cornell University.

New Members and Support for IC3
At the Fall Retreat on Oct 5, we announced that **JP Morgan** joined IC3, and that the**VMware** Foundation made a generous donation to IC3. We were delighted to have blockchain experts from both organizations at the Retreat. We are also very pleased to welcome **Cypherium** to IC3.

New IC3 Working Group Formed: Correct by Construction (CxC) Smart Contract Programming Languages
At our Fall Retreat, IC3 members unanimously highlighted the need for IC3's help to advance the capability and reliability of smart contract programming languages. Prof. Andrew Myers will chair a new Working Group. The charter is to aggregate and prioritize IC3 members' smart contract requirements, both technical and business, and pursue smart contract language R&D in collaboration with our members. Prof. Myers is Editor in Chief, **ACM Transactions on Programming Languages and Systems (TOPLAS)**, and he leads the Cornell Applied Programming Languages Group.

NEW PROJECT RELEASES
HYDRA A paper, example code, and a small bounty for our ERC20 implementation are posted. We are happy to work with our members on applying the Hydra Framework to their smart contracts.

FALCON We added the ultra-fast FALCON network support for Segwit and Bitcoin Cash in the last quarter.

UPCOMING EVENTS
Symposium on Principles of Programming Languages
January 8-13, 2018, Los Angeles, CA
IC3 faculty Prof. Andrew Myers is the Program Chair.

Blockchain Protocol Analysis and Security Engineering 2018
January 24-26, 2018, Arrillaga Alumni Center, Stanford University.
IC3 faculty including Bryan Ford, Ari Juels, Andrew Miller, and Elaine Shi are on the program committee.

IC3 Members Webinar
Tuesday February 20, 2018, Interactive Video Broadcast
Professor Andrew Myers, will kick off the new IC3 Working Group on Correct by Construction (CxC) Smart Contract Programming Languages.

Financial Cryptography and Data Security 2018 and the 5th Workshop on Bitcoin and Blockchain Research February 26–March 2, 2018, Curaçao

Prof. Sarah Meiklejohn is co-Program Chair for FC18 and Prof. Ittay Eyal is co-Program Chair for WBBR .

IC3 Spring Retreat in NYC
Thursday-Friday May 10-11, 2018, Cornell Tech, Roosevelt Island, NYC
IC3 faculty, students and industry members gather twice per year to discuss the major technical challenges and innovative solutions to widespread blockchain adoption.

PAST EVENTS
IC3 Members Webinar
Wednesday November 29, 2017, Interactive Video Broadcast
Professor Andrew Miller, IC3 Associate Director presented "I Accidentally Killed it:"yet another million-dollar Smart Contract mishap.

Devcon3
November 1-4, 2017, Cancun, Mexico
IC3 faculty and student presenters at Devcon3 included Prof. Andrew Miller, Prof. Emin Gün Sirer, Prof. Elaine Shi, Dr. Patrick McCorry, and Phil Daian.

Special Interest Group on Security, Audit and Control (SIGSAC)
October 30 - November 3, Dallas, Texas
Three papers were posted by IC3 researchers

IC3 Fall Retreat in NYC
Thursday October 5, 2017, Cornell Tech, Roosevelt Island, 2 West Loop Road, NYC
IC3 faculty, students and industry members gather twice per year to discuss the major technical challenges and innovative solutions to widespread blockchain adoption. Please see photos posted at the bottom of this Newsletter.

IC3 Members Webinar
Tuesday September 26, 2017, Interactive Video Broadcast
Professor Emin Gün Sirer, IC3 co-Director presented "Making Crytpocurrencies Scale with Offline Payments".

IC3 NYC Blockchain Meetup Comes to Si Valley - "Town Crier Authenticated Data for Smart Contracts"
Sunday August 13, 2017, Santa Clara, CA
Fan Zhang, a PhD student in CS at Cornell, spoke on Town Crier.

IC3-Ethereum Crypto Boot Camp at Cornell University
July 13-19, 2017, Gates Hall, Cornell University. Ithaca, New York
IC3 and the Ethereum Foundation conducted our second annual Boot Camp, an immersive coding and learning experience in blockchains and smart contracts with world-leading researchers, open source engineers & developers, and students.

IC3 IN THE PRESS
Bitcoin, Blockchain And Private Industry: You Ain't Seen Nothing Yet by Investor's Business Daily on January 5, 2018

A Guide to the World Bitcoin Created: The first big digital currency gave us a glimpse of a new economic order - one that raises more questions than answers by Scientific American on December 31, 2017 (January 2018, Vol 318, Issue 1)

Bitcoin May Not Be the Future, but the Technology Behind It Might Well Be
by Gadgets360 on December 19, 2017

Bitcoin futures soar amid frenzy over virtual currency
by Associated Press on December 12, 2017

Want to Issue a Red-Hot ICO? Rule No. 1 Is Do Very Little Work
by Bloomberg on December 12, 2017

Another Large Bitcoin Exchange Draws Warnings
by Toronto Star on November 25, 2017

Why America's Biggest Bank Digs Anonymous Cryptocurrency
by MIT Technology Review on November 24, 2017

How do you link the world's blockchains? With another blockchain
by New Scientist on November 22, 2017

Warning Signs About Another Giant Bitcoin Exchange
by New York Times on November 21, 2017

How To Keep Your Bitcoin Safe and Secure
by Wired on November 05, 2017

One of the Most High-Profile Initial Coin Offerings Has Crashed 50%
by Bloomberg on November 01, 2017

IC3 Blockchain Initiative Expands Research Team to Europe
by Coin Desk on October 31, 2017

The Flawed System Behind the KRACK Wi-Fi Meltdown
by Wired on October 17, 2017

Replacing Social Security Numbers Won't Be Easy, But It's Worth It
by Wired on October 13, 2017

'Mind-Boggling' Math Could Make Blockchain Work for Wall Street
by Bloomberg on October 05, 2017

The Ridiculous Amount of Energy It Takes to Run Bitcoin
by IEEE Spectrum on September 28, 2017

Blockchains: How They Work and Why They'll Change the World
by IEEE Spectrum on September 28, 2017

Microsoft Joins IC3: Membership Underscores Long-Term Commitment to Blockchain-based Solutions for Business
by Coin Desk on September 01,

Microsoft Membership in IC3 Underscores Long-Term Commitment to Blockchain-based Solutions for Business by Coindesk on September 1, 2017

RECENT IC3 BLOG POSTS
How Not To Run A Blockchain Lottery
by Emin Gün Sirer on Monday December 25, 2017
Devising a lottery based off of a blockchain is a lot harder than it seems. Also, this is a parable for the Bitcoin blockchain debate.

Parity Proposals' Potential Problems
by Phil Daian an d Lorenz Breidenbach on Wednesday December 13, 2017
This post argues that the recently proposed EIPs to rescue the frozen ethers are dangerous.

To Sink Frontrunners, Send in the Submarines
by Lorenz Breidenbach, Phil Daian, Ari Juels, and Florian Tramèr on Monday August 28, 2017
We discuss a novel scheme for preventing (miner) frontrunning in Ethereum.

Who Has Your Back in Crypto?
by Emin Gün Sirer on Saturday August 26, 2017
Between miners, businesses and developers, people think that the developers have their best interests at heart. I discuss why this is a fallacy.

The Cost of Decentralization in 0x and EtherDelta
by Iddo Bentov, Lorenz Breidenbach, Phil Daian, Ari Juels, Yunqi Li, and Xueyuan Zhao on August 13, 2017
This post examines decentralized exchanges

Bitcoin's Impending Accounting Disaster
by Emin Gün Sirer on Monday July 31, 2017
Shenanigans at Bitfinex are poised to mess up their accounting, confuse the price of BCC, and potentially bankrupt the already-bankrupt exchange.

RECENT PREPRINTS and PAPERS
Iddo Bentov Yan Ji, Fan Zhang, Philip Daian, Yunqi Li Xueyuan Zhao, and Ari Juels
Tesseract: Real-Time Cryptocurrency Exchange using Trusted Hardware

L. Breidenbach, P. Daian, F. Tramer, and A. Juels. **Enter the Hydra: Towards Principled Bug Bounties and Exploit-Resistant Smart Contracts .** 2017. In submission. Visit the **Hydra Project website** for code. Video presentation **here.**

S. Matetic, M. Ahmed, K. Kostiainen, A. Dhar, D. Sommer, A. Gervais, A. Juels, and S. Capkun. **ROTE: Rollback Protection for Trusted Execution**, USENIX Security, 2017.

E. Cecchetti, F. Zhang, Y. Ji, A. Kosba, A. Juels and E. Shi. **Solidus: Confidential Distributed Ledger Transactions via PVORM ,** ACM CCS, 2017

F. Zhang, I. Eyal, R. Escriva, A. Juels and R. V. Renesse. **REM: Resource-Efficient Mining for Blockchains**, USENIX Security, 2017

Andrew Miller, Iddo Bentov, Ranjit Kumaresan, and Patrick McCorry. **Sprites: Payment Channels that Go Faster than Lightning**

Patrick McCorry , Ethan Heilman and Andrew Miller. **Atomically Trading with Roger: Gambling on the success of a hard fork** , accepted at the 1st International Workshop on Cryptocurrencies and Blockchain Technology.

Aggelos Kiayias, Andrew Miller, Dionysis Zindros. **Non-interactive proofs of proof-of-work** .

Changyu Dong, Yilei Wang, Amjad Aldweesh, Patrick McCorry and Aad van Moorsel. **Betrayal, Distrust, and Rationality: Smart Counter-Collusion Contracts for Verifiable Cloud Computing** , accepted at ACM Conference on Computer and Communications Security 2017.

Sarah Azouvi, Mustafa Al-Bassam, and Sarah Meiklejohn. **Who Am I? Secure Identity Registration on Distributed Ledgers**, International Workshop on Cryptocurrencies and Blockchain Technology

Andrew Miller, Malte Moeser, Kevin Lee, Arvind Narayanan. **An Empirical Analysis of Linkability in the Monero Blockchain** .

P. Daian, I. Eyal, A. Juels, and E. G. Sirer. **PieceWork: Generalized Outsourcing Control for Proofs of Work** . BITCOIN, 2017.

Matthew Green , Ian Miers, **Bolt: Anonymous Payment Channels for Decentralized Currencies** . CCS 2017 : 473-489

F. Tramer, F. Zhang, H. Lin, J.P. Hubaux, A. Juels and E. Shi. **Sealed-Glass Proofs: Using Transparent Enclaves to Prove and Sell Knowledge.** . IEEE Euro S&P, 2017.

SELECTED RECENT NEWS ITEMS FROM IC3 MEMBERS

Japanese shipping giant and IBM to trial blockchain in cross-border trade by Coindesk on Dec 14, 2017

Chain Launches Sequence, a Cloud-based Ledger Service for Managing Balances by Coinspeaker on Oct 24, 2017

Top Secret? Microsoft Opens Door to Government Blockchain Use by Coindesk on Oct 17, 2017

VMware Considers Blockchain Use in Data Transfers by Coindesk on Nov 16, 2017

Intel Patent Describes PoW Mechanism that Researches DNA by ETHNews on Dec 15, 2017

JPMorgan, Goldman Sachs Trial DLT for Equity Swaps by Coindesk on Nov 20, 2017

Blythe Masters: ASX Blockchain Embrace 'Precedent Setting' bu Coindesk on Dec 7, 2017

Blockchain technology will change the world: Fidelity Labs SVP by CNBC on August 11, 2017

BECOME AN IC3 MEMBER: JOIN US IN ADVANCING THE SCIENCE AND APPLICATIONS OF BLOCKCHAINS

Please feel free to contact us for more info on these items.

Best,

Jim Ballingall
Executive Director
The Initiative for Cryptocurrencies and Contracts (IC3)
jim.ballingall@gmail.com
cel: 408-212-1035

IC3 | 2 West Loop Road, Roosevelt Island, NYC, NY 10044

See what's happening on our social sites

Several of the attendees of the **IC3 Fall Retreat** and **Blockchains Workshop** gather for a group photo long after the events ended on Oct 6. Photo includes Oct 6 speakers Jonathan Levin, Chainanalysis (center of back row), Prof. Emin Gün Sirer, and Prof. Andrew Miller (both to Jonathan's left). Other speakers are Prof. Joe Bonneau (second from the right in back row), and Brian Schroeder, JP Morgan (front row, between Professors Sirer and Miller).

Left: Dan Middleton, Intel, shares his perspectives on blockchain research areas requiring more attention during the industry session at the Fall Retreat.

Right: Dr. Patrick McCorry, University College London presents "Bribery Attacks on Miners (Smart Contract Edition)" at the Fall Retreat