IC3 The Initiative For CryptoCurrencies & Contracts

Several participants of the 2017 IC3-Ethereum Crypto Boot Camp gathered for a photo after the Celebration Dinner in Ithaca on July 19. We are thankful for the generous sponsorship of this Boot Camp by **Chain, Cisco, Fidelity Labs, JP Morgan & Chase, Microsoft, Neural Capital, Tendermint, 21.co and Yellowstone Pathology.**

Thanks to the many talented blockchain engineers, architects, researchers, developers and students from around the world who made this week-long hackathon both fun and productive! We look forward to seeing you and many new faces next year!

Q3 2017 Greetings from IC3!

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 NEWS

Microsoft Joins IC3 in Advancing Blockchain Enterprise Readiness by Yorke Rhodes on September 5, 2017

Researchers Find Issues With 0x, An Ethereum-Based Project Aiming To Raise Millions In An ICO by Forbes on August 15, 2017

Emin Gun Sirer: SEC ICO Guidance is 'End of Beginning for Blockchains' by Coindesk on July 25, 2017

UPCOMING EVENTS

Blockchains Workshop
Friday October 6, 2017
Roosevelt Island, NYC
Cornell Tech is opening its new campus to the community in a series of public events. The Blockchains Workshop is co-orgainzed by IC3. Registration is open to
the public.

IC3 Members Fall Retreat
Thursday October 5, 2017
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. Registration is open for IC3 members.

IC3 Members Webinar
Tuesday September 26, 2017 Interactive Video Broadcast from Cornell, Ithaca, NY
Professor Emin Gün Sirer, IC3 co-Director will present " Making Crytpocurrencies Scale with Offline Payments".

PAST EVENTS

IC3 Members Webinar
Tuesday August 22, 2017 Interactive Video Broadcast from Cornell Tech, Roosevelt Island, NYC
Professor Ari Juels, IC3 co-Director presented "Solidus: Confidential Distributed Ledger Transactions via PVORM".

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 Members Webinar

Tuesday June 20, 2017 Interactive Video Broadcast from Gates Hall, Cornell
University, Ithaca, New York
Dr. Ittay Eyal, IC3 Associate Director presented "From Cryptocurrencies to
FinTech Blockchains".

Consensus 2017

May 22-24, 2017 New York, NY
Prof. Ari Juels spoke Monday afternoon at the Enterprise Ethereum Alliance
technical session. Prof. Emin Gun Sirer and Prof. Andrew Miller spoke
Wednesday morning at the Workshop on Academic Partnerships with
Industry.

NY Computer Science and Economics 2017

Friday May 19, 2017 NYC
Professor Emin Gün Sirer, IC3 co-Director, presented the keynote "The New
New Blockchains and How They Will Transform The World".

PROJECT RELEASES

TOWN CRIER A test version of TC was made available for IC3 members in May. Town Crier uses Intel SGX to provide strongly authenticated data to smart contracts, as well as enabling handling of private data.

SOLIDUS A test version of Solidus was made available for IC3 members in May. We'll be launching a fully functional and fully public alpha version of Solidus in late summer. Solidus is a cryptographic protocol for confidential distributed settlement of financial transactions on a public distributed ledger. It operates in a framework based on real-world financial institutions: a modest number of banks each maintain a large number of user accounts. Within this framework, Solidus hides both transaction values and the transaction graph (i.e., the identities of transacting entities) while ensuring that all actions are fully publicly verifiable. Also, see the Coindesk article cited immediately below.

IC3 IN THE PRESS

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

Burger King launches WhopperCoin crypto-cash in Russia by BBC News on August 29, 2017

Submarine Sends: IC3's Plan to Clamp Down on ICO Cheats by Coindesk on August 28, 2017

Researchers Find Issues With 0x, An Ethereum-Based Project Aiming To Raise Millions In An ICO by Forbes on August 15, 2017

Bitcoin Divides to Rule by The Economist on August 5, 2017

IC3 Boot Camp Winners by ETHNews on August 3, 2017

KEVM Wins IC3-Ethereum Crypto Boot Camp 2017 Competition by CoinJournal on August 2, 2017

Wait, Bitcoin Just Did What? by MIT Technology Review on August 1, 2017

Man Tells Federal Officials He Stole $40 Million in Bitcoin by US News & World Report on July 20, 2017

The Future of Money: Bitcoin and Other Cryptocurrency Technologies Are a Way of Life in This Small Swiss Town by Newsweek on July 11, 2017

Why You Won’t Be Buying A Coffee With Bitcoin Anytime Soon by Wall Street Journal on July 02, 2017

The Virtual-Currency War That Threatens to Tear Bitcoin Apart by Wall Street Journal on June 20, 2017

The Ether Thief by Bloomberg on June 13, 2017

RECENT IC3 BLOG POSTS

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.

An In-Depth Look at the Parity Multisig Bug
b y Lorenz Breidenbach , Phil Daian , Ari Juels , and Emin Gün Sirer on Saturday July 22, 2017
We do a deep-dive into Parity's multisig bug.

Parity's Wallet Bug is not Alone
by Emin Gün Sirer on Thursday July 20, 2017

The bug in the Parity multisig wallet that caused the loss of $30M has the same root cause as a bug in the BitGo multisig wallet that I found a year ago.

Atomically Trading with Roger: Gambling on the success of a hardfork
by Patrick McCorry , Ethan Heilman , and Andrew Miller on July 11, 2017
A new atomic trade protocol to allow two parties to publicly pledge support for
different forks in the event a blockchain splits into two.

Bancor Is Flawed
by Emin Gün Sirer and Phil Daian on June 19, 2017
Bancor just raised $144M through the biggest ICO in history. We describe why their approach is flawed.

Announcing The Town Crier Service
by Yan Ji, Ari Juels , and Fan Zhang on May 15, 2017
Town Crier is an oracle service for smart contracts.

Hijacking Bitcoin: Routing Attacks on Cryptocurrencies
by Maria Apostolaki , Aviv Zohar , and Laurent Vanbever on May 01, 2017
Cryptocurrencies are vulnerable to attacks targeting the network routing layer. In
this guest post, Apostolaki, Zohar and Vanbever show that BGP attacks are back,
and this time, they have a high value target.

RECENT PREPRINTS and PAPERS

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

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

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

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.

M. Milutinovic, W. He, H. Wu, and M. Kanwal. 2016. **Proof of Luck: an Efficient Blockchain Consensus Protocol.**. In Proceedings of the 1st Workshop on System Software for Trusted Execution (SysTEX '16).

SELECTED RECENT NEWS ITEMS FROM IC3 MEMBERS

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

London Stock Exchange Partners With IBM to Develop Securities Data Blockchain by Bitcoin Magazine on July 25, 2017

Intel to Improve the Privacy and Security of Blockchain Solutions by Finance Magnates on July 12, 2017

Chain CEO on Why B2B Payments Need Blockchain by PYMNTS.com on June 30, 2017

Fidelity Charitable Has Raised $9 Million in Bitcoin So Far in 2017 by Coindesk on June 29, 2017

Chain is Now Working on Six 'Citi-Sized' Blockchain Networks by Coindesk on June 7, 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

2 West Loop Road
Rooseveel Island
NYC
See what's happening on our social sites