IC3 The Initiative For CryptoCurrencies & Contracts

Adam Ludwin, CEO Chain addresses IC3 members and guests at the IC3 Winter Retreat hosted by Chain in SF on February 23-24. Please see additional photos of speakers from the Retreat at the bottom of this newletter.

Q2 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 HIGHLIGHTS AND MENTIONS OF IC3 IN THE PRESS

- **Fidelity is First in Finance to Support IC3: Global Financial Leader Joins IC3 to Explore Blockchains** by Fidelity on April 10, 2017

- **IC3 Co-founds Enterprise Ethereum Alliance with Finance and Technology Leaders** by Fortune on February 27, 2017

- **IC3 Researchers Propose 'Solidus' Protocol for Private Transactions** by Coindesk on April 20, 2017

- **Inside IC3: How Cornell is Advancing the Science of Bitcoin** by Coindesk on March 29, 2017

UPCOMING EVENTS

- **IC3-Ethereum Crypto BootCamp: Registration is Open for Experienced Developers**
  July 13-19,2017 Gates Hall, Cornell University, Ithaca, NY
  IC3 and the EthereumFoundation will conduct our second annual Boot Camp, an immersive coding andlearning experience in blockchains and smart contracts with world-leadingresearchers, open source developers, and students. **NOTABLE ATTENDEES: Vitalik Buterin, Ethereum Foundation Chief Scientist and IC3 faculty Ittay Eyal, Ari Juels, Andrew Miller and Elaine Shi** are all scheduled for the full event. Join us to collaborate to advance blockchain applications.

- **Consensus 2017**
  May 24-26,2017 NYC
  IC3faculty, students and colleagues are participating in Consensus 2017 with more than2000 attendees from across the blockchain ecosystem.

- **NYComputer Science and Economics 2017**
  May 19, 2017 NYC
  ProfessorEmin Gün Sirer, IC3co-Director, will present the keynote "The NewNew Blockchains and How They Will Transform The World".

PAST EVENTS

- **NSF Watch Series**
  April 20, 2017 Washington, DC
  Professor Ari Juels, IC3 co-Director, presented "The Jekyll and Hyde of Smart Contracts".

- **Business of Blockchain**
  April 18,2017 Cambridge, MA
  Professor Emin Gün Sirer, IC3 co-Director, presented "What Could Go Wrong? When Blockchains Fail". Watch the short video of Prof. Sirer where he explains that "Code is Not Law."

- **IC3 Winter Retreat in SF**
  February 23-24, 2017 San Francisco, CA
  IC3 faculty, students and members gather twice per year todiscuss the major technical challenges and innovative solutions to widespreadblockchain adoption. Our Sponsor Member Chain hosted this 2-day Retreat attheir offices in SF.

- **2017 Blockchain Technology and Digital Currency NationalInstitute**
  April 10, 2017 NYC
  Professor Ari Juels, IC3 co-Director, explainedhow digital currency and blockchain technology function and described the recenttechnological developments at this event organized by the American BarAssociation.

- **Financial Cryptography and Data Security 2017**
  April 3-7,2017 Malta
  SeveralIC3'ers chaired technical sessions and presented their work at this major internationalforum for research, advanced development, education, exploration, and debateregarding information assurance, with a specific focus on commercialcontexts.

- **Enterprise EthereumAlliance Launch**
  February 28,2017 NYC
  IC3 is a foundingmember of EEA. Prof Andrew Miller, IC3 Associate Director is on the EEA board.IC3'er Phil Daian participated on the panel "How StartupsCan Help Ent.Eth 1.0".

- **Blockchain Protocol Analysis and SecurityEngineering 2017**
  January 26-27, 2017 Stanford, CA
  IC3'ers Efe Gencer, Andrew Miller, ElaineShi, and Emin Gün Sirer had papers at this Stanfordevent along with Dan Robinson of Chain (IC3 Sponsor Member).

PROJECT RELEASES

- **TOWN CRIER** A test version of TC is available for IC3 members. We'll be launching a fully functional and fully public alpha version of TC 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 will be 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.

RECENT INTERVIEWS AND MENTIONS OF IC3 IN THE PRESS

- **IC3 Researchers Propose 'Solidus' Protocol for Private Transactions** by Coindesk on April 20, 2017

- **Monero Transactions History Can Be Revealed and Exposed: Research** by CoinTelegraph on April 15, 2017

- **Fidelity Becomes First Asset Manager to Join Blockchain Group IC3** by Reuters on April 10, 2017

- **Blockchain: A Better Way to Track Pork Chops, Bonds, Bad Peanut Butter?** by New York Times on March 04, 2017

- **Hardware Over Hard Forks: How Accenture Plans to End Blockchain's Security Debate** by CoinDesk on February 14, 2017

- **What Makes Bitcoin Great? One Scientist is On a Quest to Find Out** by CoinDesk on February 08, 2017

RECENT IC3 BLOG POSTS

- **Revealing the hidden links in the Monero blockchain** by Andrew Miller on Wednesday April 19, 2017 at 10:11 AM

- **A Thinking Person's Guide to the Latest Bitcoin Drama** by Emin Gün Sirer on Wednesday April 05, 2017 at 08:48 PM - Prof. Sirer's quick reaction to the latest salvo of shots fired in the war between Core developers and miners.

- **BitFury's Smallest-First Mining Is Bad For Bitcoin** by Emin Gün Sirer on February 27, 2017 at 10:33 AM BitFury has been mining smallest-transactions-first. We argue why this is bad for Bitcoin.

- **The Greening of Blockchains** by Phil Daian and Ari Juels on February 23, 2017 at 12:23 PM Blockchains are beginning to turn green. This post describes some of the IC3 research in this direction.

- **State of the Bitcoin Network** by Adem Efe Gencer and Emin Gün Sirer on February 15, 2017 at 10:18 AM We characterize the state of the Bitcoin network as of this year, and discover that it has improved by 70% in terms of bandwidth compared to last year alone.

- **Miniature World: Measuring and Evaluating Blockchains** by Adem Efe Gencer and Emin Gün Sirer on February 10, 2017 at 10:10 AM

Miniature world is an evaluation platform which provides a principled way of evaluating different blockchain proposals.

- **Will Cryptocurrencies Be Centrally Controlled? What Would Hamilton Do?**
  by Jim Ballingall on January 09, 2017 at 08:42 AM
  As regulators take a closer interest in cryptocurrencies, IC3 faculty weigh in on if and how they should be regulated.

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 startup Chain teams with Thales to bolster security** by Reuters on March 30, 2017

- **IBM is going all in on blockchain for trade finance** by Business Insider on April 12, 2017

- **Intel Reveals Its Plan For Blockchain Technology With 'Sawtooth Lake' Distributed Ledger** by IB Times on April 8, 2017

- **Digital Asset and Blockchain Foundation of India seeks to showcase bitcoin benefits to government** by Econo Times on April 18, 2017

- **Chain Inc. Hires Goldman's Jessop to Boost Blockchain Effort** by Wall Street Journal on April 17, 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

111 8th Avenue
NYC

See what's happening on our social sites

Photos below from the IC3 Winter Retreat hosted by Chain in SF on Feb 23-24

IC3 Winter Retreat: Vinay Phegade, Chief Security Solution Architect, Intel, provides a detailed update on Intel Software Guard Extentions (SGX).

IC3 Winter Retreat: James Litsios, Head of Development at Digital Asset, describes "Semantically Rich Segmented Blockchains"

IC3 Winter Retreat: Professors Andrew Miller and Emin Gün Sirer assist Vinay Phegade to set up for his talk.

IC3 Winter Retreat: Binh Nguyen, Blockchain Chief Architect IBM provides details on the Hyperledger Fabric Architecture.