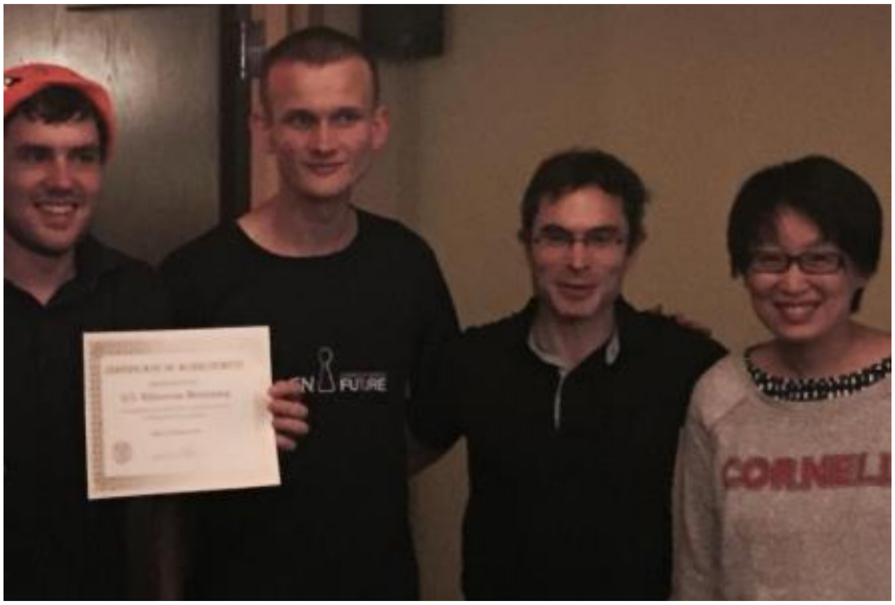
IC3 | INITIATIVE FOR CRYPTOCURRENCIES & CONTRACTS

IC3 NEWSLETTER – Q1 2017 – January 3, 2017



Happy New Year from IC3! IC3 Directors Andrew Miller, Ari Juels and Elaine Shi celebrate at the Awards Dinner for the IC3-Etheruem Crypto Boot Camp with Vitalik Buterin in Ithaca. Pictured (left to right) are Andrew, Vitalik, Ari, and Elaine (not pictured are IC3 Directors Emin Gün Sirer and Ittay Eyal).

Welcome to the IC3 Quarterly Newsletter!
This is a new outreach to keep the blockchain community aware of IC3 innovations, events, news, publications, and other service to the community by IC3 staff and partners.

UPCOMING EVENTS

- **IC3 Winter Retreat in SF February 23-24, 2017, San Francisco**
  IC3 staff and members gather twice per year to discuss the major technical challenges and innovative solutions to widespread blockchain adoption. Includes presentations, panels, and sessions for networking with the IC3 professors, students, and other IC3 members. Stay tuned for the agenda and further event info!

- **Blockchain Protocol Analysis and Security Engineering 2017 January 26-27, 2017, Stanford**
  Presentations by IC3 co-Directors Prof. Elaine Shi and Prof. Emin Gün Sirer

PAST EVENTS IN Q4 2016

- **Enterprise Ethereum Summit - December 15, 2016, NYC**
  Prof. Andrew Miller – “HoneyBadgerBFT”
- **Blockchain for Wall Street - November 29, 2016, NYC**

Prof. Ari Juels - Panel on "Financial Markets Smart Contracts - Implementing Legally Sound, Predictable and Secure Processes"

- **SEC Fintech Forum - November 14, 2016, DC**
  Prof. Emin Gün Sirer - Panel on "Impact of Recent Innovation on Trading, Settlement, and Clearance Activities"
- **Devcon2 - Smart Contract Security Panel - November 5, 2016, Shanghai**
  Phil Daian, IC3 grad student joins Vitalik Buterin, et al. on Devcon2 panel.
- **23rd ACM Conference on Computer and Comm Security - October 24-28, 2016, Vienna**
  Several papers by IC3 researchers.
- **Bitcoin Scalability Workshop - October 8-9, 2016, Milan**
  Prof. Emin Gün Sirer, "Bitcoin Covenants - Opportunities and Challenges"
- **IC3 NYC Blockchain Meetup - September 29, 2016, NYC**
  Prof. Ari Juels, "Town Crier: An Authenticated Data Feed for Smart Contracts"

INTERVIEWS AND MENTIONS OF IC3 IN THE PRESS

- The Teechan Solution: Scaling Bitcoin With Trusted Hardware by **Bitcoin Magazine** on Dec 28, 2016
- Bitcoin Block Size and Scaling Issues May Be Solved With This New Solution by **CoinTelegraph** on Dec 24, 2016

- Trusted Hardware Can Help Bitcoin Scale, But At What Cost? by **CoinDesk** on December 17, 2016 Donald Trump's Transition is a Trial Run for Smart Contracts by **CoinDesk** on December 06, 2016
- Blockchain Pros Debate 'Looming Challenges' for Smart Contracts by **CoinDesk** on November 30, 2016
- Bitcoin and blockchain seem more and more like solutions looking for a problem by **Quartz** on November 23, 2016
- SEC Panelists on "Astonishing" But "Not Very Sexy" Blockchain: Achieving Network Effect Will Produce Winners by **Bitcoin Magazine** on November 16, 2016
- Blockchain Won't Just Change Regulation, it Could Reshape the SEC by **CoinDesk** on November 15, 2016
- Meet The Immigrant Scientists Spooked By A Looming Trump Presidency by **Buzzfeed** on November 12, 2016
- Making 'cryptocurrency' safe and reliable by **Cornell Chronicle** on November 02, 2016
- How Vigilante Hackers Could Stop the Internet of Things Botnet by **Motherboard** on October 26, 2016
- Blockchain bandits hit crypto start-ups by **BBC** on October 25, 2016
- Chain Releases Open-Source Version of Chain Core Technology Powering Visa's New B2B Connect by **Bitcoin Magazine** on October 25, 2016
- Cornell Prof Uncovers Bugs in Smart Contract System, Urges More Safety in Program Design by **Cornell Sun** on October 25, 2016
- Cryptocurrency Exchange Poloniex is Insecure, Security Review Claims by **CryptoCoinsNews** on October 15, 2016
- Why Weight? Bitcoin Scaling is Moving Beyond Block Size by **CoinDesk** on October 09, 2016
- All in the Mind by **UCSB** on October 04, 2016

- What Does Cornell's Emin Gun Sirer See As The Main Security Threats In Cryptocurrency? 'Everything' by **CoinDesk** on October 04, 2016
- In Formal Verification Push, Ethereum Seeks Smart Contract Certainty by **CoinDesk** on September 28, 2016
- Can This 22-year-old Coder Out-Bitcoin Bitcoin? by **Fortune** on September 27, 2016
- IPFS Protocol Selects Ethereum Over Bitcoin, Prefers Ethereum Dev Community by **The Cointelegraph** on September 24, 2016
- China's Mining Dominance: Good Or Bad For Bitcoin? by **CryptoCoinsNews** on September 14, 2016
- Blockchain Based Sports Game Wins Thomson Reuters HackETHon by **CryptoCoinsNews** on September 13, 2016
- The bizarre world of bitcoin 'mining' finds a new home in Tibet by **Washington Post** on September 12, 2016
- The Fight for On-Blockchain Bitcoin Scaling Soldiers On by **CoinDesk** on September 02, 2016
- The bizarre world of bitcoin 'mining' finds a new home in Tibet by **Washington Post** on September 12, 2016
- Chain Joins Industry-Academia Blockchain Initiative to Solve Interoperability and Scalability Issues by **Bitcoin Magazine** on August 22, 2016
- After $65 million hack, questions arise over whether Bitcoin can be safe by **Houston Chronicle** on August 19, 2016
- Chain Inc. Announces Partnership with the Initiative for Cryptocurrency and Contracts by **Bitcoinist** on August 11, 2016

PREPRINTS AND WHITE PAPERS

- R. Pass and E. Shi, FruitChains: A Fair Blockchain
- R. Pass and E. Shi, Hybrid Consensus: Efficient Consensus in the Permissionless Model
- I. Bentov, R. Pass and E. Shi, The Sleepy Model of Consensus
- I. Bentov, R. Pass and E. Shi, Snow White: Provably Secure Proofs of Stake
- 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. Under submission. May 2016.
- A. E. Gencer, R. V. Renesse, and E. G. Sirer, Service-Oriented Sharding with Aspen.

PUBLISHED PAPERS

- K. Nayak, S. Kumar, A. Miller, E. Shi. Stubborn Mining: Generalizing Selfish Mining and Combining with an Eclipse Attack., IEEE Euro S&P, 2016
- F. Zhang, E. Cecchetti, K. Croman, A. Juels and E. Shi. Town Crier: An Authenticated Data Feed for Smart Contracts. ACM CCS, 2016.
- Miller, Y. Xia, K. Croman, E. Shi, and D. Song. The Honey Badger of BFT Protocols. ACM CCS, 2016.
- Juels, A. Kosba, and E. Shi. The Ring of Gyges: Investigating the Future of Criminal Smart Contracts. ACM CCS, 2016.
- Eyal and E. G. Sirer. Bitcoin-NG: A Scalable Blockchain Protocol. NSDI, 2016.
- Marino and A. Juels. Setting Standards for Altering and Undoing Smart Contracts. Rule ML, 2016.

- K. Croman, C. Decker, I. Eyal, A.E. Gencer, A. Juels, A. Kosba, A. Miller, P. Saxena, E. Shi, E. G. Sirer, D. Song, and R. Wattenhofer. On Scaling Decentralized Blockchains (A Position Paper). BITCOIN'16. (Full version here)

THE GRAND CHALLENGES TO BLOCKCHAIN ADOPTION: IC3 SOLUTIONS FOR FAST, RELIABLE, AND SECURE BLOCKCHAINS

SOLUTION SPOTLIGHT

HoneyBadgerBFT: HoneyBadgerBFT is the first practical asynchronous BFT protocol, which guarantees liveness without making any timing assumptions; providing high throughput with low latency in adverse environments.

RECENT IC3 BLOG POSTS

- **Scaling Bitcoin with Secure Hardware**
  by Joshua Lind, Ittay Eyal, Peter Pietzuch, and Emin Gün Sirer on December 22, 2016
  We unveil a new technology for secure, high throughput, low latency Bitcoin transactions using secure hardware, on the current Bitcoin network.

- **Service-Oriented Sharding with Aspen**
  by Adem Efe Gencer and Emin Gün Sirer on Tuesday December 06, 2016
  We introduce the first workable sharding solution for blockchains.

SELECTED NEWS ITEMS FROM IC3 MEMBERS

- **Visa Taps Blockchain for Cross-Border Payment Plan:** In collaboration with Chain Inc., a startup in which it has invested, Visa B2B Connect is unveiled by **Fortune** on October 21, 2016
- **IBM building blockchain ecosystem:** To help build an ecosystem around IBM Blockchain and the Linux Foundation Hyperledger Fabric, Big Blue is offering a program that includes tools and expert support by **CIO** on Dec 6, 2016
- **Blythe Masters Talks 'Tipping Point' for Business Blockchain Adoption** by **Coindesk** on December 12, 2016

  Intel is Winning Over Blockchain Critics By Reimagining Bitcoin's DNA
  by **CoinDesk** on December 5, 2016

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