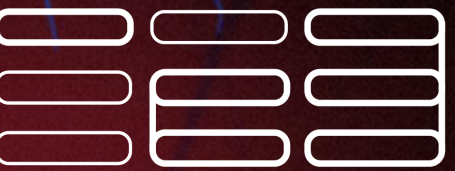
INFRACON

<Pocket Network Community Conference 2022>

Academic Cryptocurrency Research Space - An Overview, Spring 2022



The Initiative for CryptoCurrencies and Contracts

Tyler Kell
@relyt29

Goal of this talk

Give an overview of the last 5ish years of research in the academic space

“Papers you should probably know about”

Staying on top of the frontiers of research and human knowledge is a full time job

So this talk is biased by my limited perspective of the space, it won’t be exhaustive, but it’s probably a decent enough start

Tyler Kell
@relyt29

Research Engineer @ IC3 & Cornell Tech

Work with PhD students at Cornell Tech

Collaborate to publish papers

Assist in writing code to run experiments

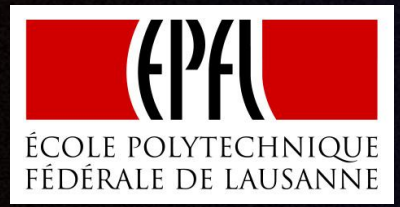
Do Industry outreach

You should follow me on twitter

You can scan this QR code

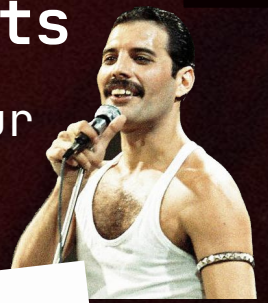
What is the Initiative for Cryptocurrencies and Contracts (IC3)?

- My employer (Cornell Tech)
- “An initiative of faculty members”
- University research groups from around the world that collaborate on cryptocurrency related research
- 9 campuses 4 countries



IC3's Greatest Hits

You may know us from our hit classics including:



Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges

Philip Daian, *Cornell Tech*, phil@cs.cornell.edu
Steven Goldfeder, *Cornell Tech*, goldfeder@cornell.edu
Tyler Kell, *Cornell Tech*, sk3259@cornell.edu
Yunqi Li, *UIUC*, yunqil3@illinois.edu
Xueyuan Zhao, *CMU*, xyzhao@cmu.edu
Iddo Bentov, *Cornell Tech*, ib327@cornell.edu
Lorenz Breidenbach, *ETH Zürich*, lorenz.breidenbach@inf.ethz.ch
Ari Juels, *Cornell Tech*, juels@cornell.edu

Majority is not Enough: Bitcoin Mining is Vulnerable*

Ittay Eyal and Emin Gün Sirer

Department of Computer Science, Cornell University
ittay.eyal@cornell.edu, egs@systems.cs.cornell.edu

A Fistful of Bitcoins: Characterizing Payments Among Men with No Names

Sarah Meiklejohn, Marjori Pomarole, Grant Jordan
Kirill Levchenko, Damon McCoy†, Geoffrey M. Voelker, Stefan Savage

University of California, San Diego, George Mason University†

NBER WORKING PAPER SERIES

DESIGN CHOICES FOR CENTRAL BANK DIGITAL CURRENCY: POLICY AND TECHNICAL CONSIDERATIONS

Prism: Deconstructing the Blockchain to Approach Physical Limits

Vivek Bagaria, vbagaria@stanford.edu, Stanford University
Sreeram Kannan, ksreeram@uw.edu, University of Washington at Seattle
David Tse, dntse@stanford.edu, Stanford University
Giulia Fanti, gfanti@andrew.cmu.edu, Carnegie Mellon University
Pramod Viswanath, pramodv@illinois.edu, University of Illinois at

OmniLedger: A Secure, Scale-Out, Decentralized Ledger via Sharding

Eleftherios Kokoris-Kogias†, Philipp Jovanovic†, Linus Gasser†, Nicolas Gailly†, Ewa Syta*, Bryan Ford†

†École Polytechnique Fédérale de Lausanne, Switzerland, *Trinity College, USA

Press Coverage / Coverage Metrics

- 1,722 articles in 4 years.
- 239,292 Google Scholar citations.
- Widely quoted in NYT, WSJ, BBC, Wired, Forbes, WaPo, MIT Technology Review, New Scientist, and almost every m
  record overseas.

IC3 Partners

IC3 › Partners

IC3 Partners and Donors

IC3 acknowledges and appreciates a generous gift from the VMware Foundation to advance the science and technology of blockchains.

Chainlink ethereum FCAT FIDELITY CENTER for APPLIED TECHNOLOGY IBM intel J.P.Morgan

Meta Protocol Labs COIN OPERATED GROUP

Contact

For more information, please contact: sarahallen@cornell.edu.

IC3 Partnership Examples

CanDID: Can-Do Decentralized Identity with Legacy Compatibility, Sybil-Resistance, and Accountability

Deepak Maram*¶, Harjasleen Malvai†¶, Fan Zhang*¶, Nerla Jean-Louis‡¶, Alexander Frolov†¶, Tyler Kell*¶, Tyrone Lobban§, Christine Moy§, Ari Juels*¶, Andrew Miller‡¶
*Cornell Tech, †Cornell University, ‡UIUC, §J. P. Morgan, ¶IC3, The Initiative for CryptoCurrencies & Contracts

Aggregating and thresholdizing hash-based signatures using STARKs

Irakliy Khaburzaniya
Polygon/Meta
irakliy81@gmail.com

Kostantinos Chalkias
Meta
chalkiaskostas@gmail.com

Kevin Lewi
Meta
klewi@fb.com

Harjasleen Malvai
UIUC / IC3
hmalvai2@illinois.edu

Cohosting Hackathons, Networking Events

Several of the participants gathered for a Group Photo after lunch on Day 5, on the steps of Gates Hall, home of Cornell Computer and Information Science.

Building systems that industry doesn't have technical expertise for

Improving or working with industry systems

Groundbreaking research work to push the frontier of human knowledge

Or you may know us from the companies we've gone on to found and/or work intimately with:

Flashbots

$26.4B+

Value associated with IC3 linked companies (significant underestimate)… Nbd nbd

Chainlink

AVALANCHE

any.sender

Arbitrum

BLOXROUTE LABS

OASIS LABS

IC3 “Grand Challenges”

The Seven Grand Challenges

IC3 has many projects underway to address what we identify as seven “Grand Challenges” to widespread blockchain adoption. A number of examples are given below.

- **Secure Scaling and Performance**: Scaling up blockchains to handle intensive global workloads for both permissionless decentralized blockchains, and permissioned/consortium blockchains supporting >100,000 transactions/sec.
- **Correctness by Design and Construction**: Making it easy, and even automatic, for blockchain developers to produce secure protocols and code, by utilizing (1) programming language techniques to create correct code, and (2) cryptographic protocols with security proofs.
- **Confidentiality**: Combining transparency with confidentiality in blockchains, by utilizing (1) cryptographic techniques, as well as (2) trusted-hardware.
- **Authenticated Data Feeds**: Supporting a robust ecosystem of trustworthy data feeds for blockchains and contributing high-trust data feed solutions.
- **Safety and Compliance**: Enabling techniques and protocols for effective monitoring and targeted intervention in blockchains, informed by evaluations of traditional contract law and risks of crime in smart contracts.
- **Sound Migration**: Formulating practical migration paths to production blockchain deployments and enabling integration of new blockchain systems with legacy systems.
- **Social Good**: Applying cutting-edge blockchain technologies to pressing societal problems in order to illuminate overlooked technical needs and create impactful solutions.

Secure Scaling and Performance

On Scaling Decentralized Blockchains

(A Position Paper)

Kyle Croman[0,1], Christian Decker[4], Ittay Eyal[0,1], Adem Efe Gencer[0,1], Ari Juels[0,2], Ahmed Kosba[0,3], Andrew Miller[0,3], Prateek Saxena[6], Elaine Shi[0,1], Emin Gün Sirer[0,1], Dawn Song[0,5], and Roger Wattenhofer[4]

[0] Initiative for CryptoCurrencies and Contracts (IC3)
[1] Cornell [2] Jacobs, Cornell Tech [3] UMD [4] ETH [5] Berkeley [6] NUS

HotStuff: BFT Consensus with Linearity and Responsiveness

Maofan Yin
Cornell University
VMware Research

Dahlia Malkhi
VMware Research

Michael K. Reiter
UNC-Chapel Hill

Guy Golan Gueta
VMware Research

Ittai Abraham
VMware Research

Thunderella: Blockchains with Optimistic Instant Confirmation

Rafael Pass Elaine Shi

Aggregating and thresholdizing hash-based signatures using STARKs

Irakliy Khaburzaniya
Polygon/Meta
irakliy81@gmail.com

Kostantinos Chalkias
Meta
chalkiaskostas@gmail.com

Kevin Lewi
Meta
klewi@fb.com

Harjasleen Malvai
UIUC / IC3
hmalvai2@illinois.edu

Bitcoin-NG: A Scalable Blockchain Protocol

Ittay Eyal Adem Efe Gencer Emin Gün Sirer Robbert van Renesse
Cornell University

OmniLedger: A Secure, Scale-Out, Decentralized Ledger via Sharding

Eleftherios Kokoris-Kogias†, Philipp Jovanovic†, Linus Gasser†, Nicolas Gailly†, Ewa Syta*, Bryan Ford†

†École Polytechnique Fédérale de Lausanne, Switzerland, *Trinity College, USA

Snow White: Robustly Reconfigurable Consensus and Applications to Provably Secure Proof of Stake

Phil Daian Rafael Pass Elaine Shi

Cornell/CornellTech

Correctness by Design and Construction

Efficient MDP Analysis for Selfish-Mining in Blockchains

Roi Bar-Zur
Technion

Ittay Eyal
Technion

Aviv Tamar
Technion

Enter the Hydra: Towards Principled Bug Bounties and Exploit-Resistant Smart Contracts*

Lorenz Breidenbach
lorenzb@inf.ethz.ch
Cornell Tech, IC3,† ETH Zürich

Philip Daian
phil@cs.cornell.edu
Cornell Tech, IC3†

Florian Tramèr
tramer@cs.stanford.edu
Stanford

Ari Juels
juels@cornell.edu
Cornell Tech, IC3,† Jacobs Institute

Themis: Fast, Strong Order-Fairness in Byzantine Consensus

Mahimna Kelkar[1,2] Soubhik Deb[†3] Sishan Long[†1,2] Ari Juels[1,2] Sreeram Kannan[3]

[1]Cornell Tech
[2]Cornell University
[3]University of Washington, Seattle

FruitChains: A Fair Blockchain

Rafael Pass
Cornell Tech
rafael@cs.cornell.edu

Elaine Shi
Cornell University
elaine@cs.cornell.edu

Securing Smart Contracts with Information Flow

Ethan Cecchetti Siqiu Yao Haobin Ni Andrew C. Myers

Cornell University
{ethan,yaosiqiu,haobin,andru}@cs.cornell.edu

Colordag: An Incentive-Compatible Blockchain

ITTAI ABRAHAM, VMware Research, Israel
DANNY DOLEV, The Hebrew University of Jerusalem, Israel
ITTAY EYAL, Technion and IC3, Israel
JOSEPH Y. HALPERN, Cornell University, NY, USA

Confidentiality

INFRACON

HoneyBadgerMPC

build passing coverage 77%

HoneyBadgerMPC is a robust MPC-based confidentiality layer for blockchains.

A Fistful of Bitcoins: Characterizing Payments Among Men with No Names

Sarah Meiklejohn Marjori Pomarole Grant Jordan
Kirill Levchenko Damon McCoy† Geoffrey M. Voelker Stefan Savage

University of California, San Diego George Mason University†

An Empirical Analysis of Privacy in the Lightning Network

George Kappos[1*], Haaroon Yousaf[1*], Ania Piotrowska[1,2], Sanket Kanjalkar[3], Sergi Delgado-Segura[4], Andrew Miller[3,5], Sarah Meiklejohn[1]

Libra: Succinct Zero-Knowledge Proofs with Optimal Prover Computation

Tiancheng Xie* Jiaheng Zhang* Yupeng Zhang†
Charalampos Papamanthou‡ Dawn Song*

Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts

Ahmed Kosba*, Andrew Miller*, Elaine Shi†, Zikai Wen†, Charalampos Papamanthou*
*University of Maryland and †Cornell University
{akosba, amiller}@cs.umd.edu, {rs2358, zw385}@cornell.edu, cpap@umd.edu

Dandelion++: Lightweight Cryptocurrency Networking with Formal Anonymity Guarantees

GIULIA FANTI, Carnegie Mellon University
SHAILESHH BOJJA VENKATAKRISHNAN, Massachusetts Institute of Technlogy
SURYA BAKSHI, University of Illinois at Urbana-Champaign
BRADLEY DENBY, Carnegie Mellon University
SHRUTI BHARGAVA, University of Illinois at Urbana-Champaign
ANDREW MILLER, University of Illinois at Urbana-Champaign
PRAMOD VISWANATH, University of Illinois at Urbana-Champaign

Authenticated Data Feeds

INFRACON

DECO: Liberating Web Data Using Decentralized Oracles for TLS

The extended version

Fan Zhang*
Cornell Tech

Deepak Maram*
Cornell Tech

Harjasleen Malvai*
Cornell University

Steven Goldfeder*
Cornell Tech

Ari Juels*
Cornell Tech

Town Crier: An Authenticated Data Feed for Smart Contracts

Fan Zhang
Cornell University
IC3†
fanz@cs.cornell.edu

Ethan Cecchetti
Cornell University
IC3†
ethan@cs.cornell.edu

Kyle Croman
Cornell University
IC3†
kcroman@cs.cornell.e

Ari Juels
Cornell Tech, Jacobs Institute
IC3†
juels@cornell.edu

Elaine Shi
Cornell University
IC3†
rs2358@cornell.edu

†Initiative for CryptoCurrencies and Contracts

TLS-N: Non-repudiation over TLS Enabling Ubiquitous Content Signing for Disintermediation

Hubert Ritzdorf, Karl Wüst, Arthur Gervais, Guillaume Felley, Srdjan Čapkun
Department of Computer Science
ETH Zurich, Switzerland

Scalable Bias-Resistant Distributed Randomness

Ewa Syta*, Philipp Jovanovic†, Eleftherios Kokoris Kogias†, Nicolas Gailly†,
Linus Gasser†, Ismail Khoffi‡, Michael J. Fischer§, Bryan Ford†

Safety and Compliance

INFRACON

Centrally Banked Cryptocurrencies

George Danezis
University College London
g.danezis@ucl.ac.uk

Sarah Meiklejohn
University College London
s.meiklejohn@ucl.ac.uk

IC3
Mar 21 · 21 min read · Listen

Copyright Vulnerabilities in NFTs

by James Grimmelmann (Cornell and IC3), Yan Ji (Cornell and IC3), and Tyler Ke
(IC3)

Platypus: A Central Bank Digital Currency with Unlinkable Transactions and Privacy Preserving Regulation

Karl Wüst
*CISPA Helmholtz Center for Information Security**

Kari Kostiainen
Department of Computer Science ETH Zurich

Srdjan Capkun
Department of Computer Science ETH Zurich

Generalized Proof of Liabilities

Yan Ji
Cornell Tech & IC3
yj348@cornell.edu

Konstantinos Chalkias
Novi / Facebook
kostascrypto@fb.com

NBER WORKING PAPER SERIES

DESIGN CHOICES FOR CENTRAL BANK DIGITAL CURRENCY: POLICY AND TECHNICAL CONSIDERATIONS

Sound Migration

CanDID: Can-Do Decentralized Identity with Legacy Compatibility, Sybil-Resistance, and Accountability

Deepak Maram*¶, Harjasleen Malvai†¶, Fan Zhang*¶, Nerla Jean-Louis‡¶, Alexander Frolov†¶, Tyler Kell*¶, Tyrone Lobban§, Christine Moy§, Ari Juels*¶, Andrew Miller‡¶
*Cornell Tech, †Cornell University, ‡UIUC, §J. P. Morgan, ¶IC3, The Initiative for CryptoCurrencies & Contracts

Solidus: Confidential Distributed Ledger Transactions via PVORM

Extended Version

Ethan Cecchetti
Cornell University; IC3†
ethan@cs.cornell.edu

Fan Zhang
Cornell University; IC3†
fanz@cs.cornell.edu

Yan Ji
Cornell University; IC3†
jyamy42@gmail.com

Ahmed Kosba
University of Maryland; IC3†
akosba@cs.umd.edu

Ari Juels
Cornell Tech, Jacobs Institute; IC3†
juels@cornell.edu

Elaine Shi
Cornell University; IC3†
runting@gmail.com

†Initiative for CryptoCurrencies & Contracts

Identity and Personhood in Digital Democracy: Evaluating Inclusion, Equality, Security, and Privacy in Pseudonym Parties and Other Proofs of Personhood

Bryan Ford
Swiss Federal Institute of Technology in Lausanne (EPFL)

NFTs for Art and Collectables: Primer and Outlook

Sarah Allen[1], Ari Juels[2], Mukti Khaire[3], Tyler Kell[4], and Siddhant Shrivastava[5]

Social Good

INFRACON

PAIDIT: PRIVATE ANONYMOUS IDENTITY FOR DIGITAL TRANSFERS

Jan, 2022 → Dec, 2023

Partner: ICRC, funded by HAC

Partner contact: TBD

ICRC

Early Evidence of Effectiveness of Digital Contact Tracing for SARS-CoV-2 in Switzerland

Marcel Salathé, Christian L. Althaus, Nanina Anderegg, Daniele Antonioli, Tala Ballouz, Edouard Bugnion, Srdjan Čapkun, Dennis Jackson, Sang-Il Kim, James R. Larus, Nicola Low, Wouter Lueks, Dominik Menges, Cédric Moullet, Mathias Payer, Julien Riou, Theresa Stadler, Carmela Troncoso, Effy Vayena, Viktor von Wyl

Statement of Prof. Ari Juels

Faculty Member at Cornell Tech
New York, NY

Submitted to the U.S. House Energy and Commerce Committee,
Subcommittee on Oversight and Investigations,
for the hearing

Cleaning Up Cryptocurrency: The Energy Impacts of Blockchains

January 20, 2022

Forsage: Anatomy of a Smart-Contract Pyramid Scheme

Tyler Kell
Cornell Tech
IC3
sk3259@cornell.edu

Haaroon Yousaf
University College London
IC3

Sarah Allen
Cornell Tech
IC3

Sarah Meiklejohn
University College London
IC3

Ari Juels
Cornell Tech
IC3

AIRS: Automated Incentives for Reforestation Stewardship

Support Grand Challenges: Social Good

The accelerating effect of global climate change is a major challenge for humanity. One critical is reforestation. As large and effective carbon sinks, forests are important to both conserve and equally effective at carbon sequestration. To create, monitor, and manage effective reforestatio measure forest carbon accurately and with high geospatial precision. Our project will build infra trustworthy source of data on forest carbon and (2) Implements a system of automated monet and/or increase forests that effectively reduce carbon emissions. By combining the two capabi rewards, we believe we can provide powerful support for climate change programs that aim to global economy. For instance, the REDD+ program, under development by parties to the United Change, aims to incentivize developing countries to reduce emissions resulting from deforesta and enhancing forest carbon sticks. We will build a public performance-based payment system is an *oracle*, a trustworthy source of data for blockchain applications, it obtains and analyzes

INFRACON

Thank You!

Follow IC3 on Twitter for research updates!

@initc3org

Go to our website at https://initc3.org!

Read our blog at https://medium.com/@initc3org!

Attend our Events and Conferences!

Scan this QR code to leave feedback about my presentation!

Partner with us to do research together!
Join IC3 as Industry Members!

IC3 Partners and Donors

Follow me on Twitter!

Tyler Kell

@relyt29