Subscribe   Past Issues   Translate ▾   RSS

Hello,

*I've been thinking a lot lately about folklore -- something everyone assumes is true, but hasn't necessarily been properly analyzed and proven correct. For example, the security of proof-of-work: the key innovation in cryptocurrencies is the idea of a permissionless consensus protocol to secure a ledger of transactions, preventing reordering and double spending. Today, proof-of-work and Nakamoto Consensus secure more than $200B dollars of cryptocurrency. But how much do we really understand it? How do we know these protocols are economically secure, and that it won't ever be in the interest of a greedy miner to mine a fork and wreak havoc on the network? People make arguments about sunk cost in hardware and access to energy and ASICs, but ultimately there is some value at which it would be in a miner's economic interest to double spend; we want this to be very high but not *too* high -- as users we pay for that security with inflation and fees. Bitcoin has been secure against double spends for the last ten years, but many other cryptocurrencies have suffered attacks. We can't just look to the past as a blueprint for the future; as this asset class grows, attacks will only become more lucrative, and thus more sophisticated.*

In this newsletter, I'm excited to share DCI work that moves the ball forward on monitoring and analyzing the underlying security of proof-of-work. In research led by Dan Moroz, a PhD student at Harvard, we put forth a new proof-of-work game mechanic, counterattacking, which makes securing proof-of-work networks cheaper. Then, we actually observed double spends and a counterattack in the wild on Bitcoin Gold using a system developed by James Lovejoy, an MIT masters student with the DCI. So far there has been very little real-world monitoring and measurement of mining pools, which surprises me because pools are critical to security: If there is an attack in Bitcoin, it will probably come from mining pools. Individual miners don't necessarily know how their hashrate is being used, so we developed a system to check, and we are monitoring 75% of the Bitcoin hashrate. Please let us know if you're interested or would like to collaborate in any of this work.

This is all more important than ever as we approach the halving -- I'll be on a panel on this topic at Consensus:Distributed Monday May 11th at 10 AM ET with Hasu and Raphael Auer.

Finally, I want to acknowledge that the world has changed dramatically in the last few months, and many of us are still reeling. I hope you and your loved ones are doing OK. At the DCI, we are very fortunate to be able to do our research from home, and like everyone else, we've been living on Jitsi and Zoom. We hope to have the opportunity to do more live streamed conversations and events with our community.

Thanks as always for your curiosity and a special thank you to our member companies and donors for their support. Please let us know if you have any feedback, questions, or if we can help you in any way. We'd love to hear from you!

Thanks,
Neha

Projects and Research

Research Updates

- Pool Monitoring led by Gert-Jaap

  This project monitors the behavior of mining pools that operate on Proof-of-Work cryptocurrencies. Mining pools have ultimate control over the work that constituent miners process and therefore their (mis)behavior can have large consequences for the security of Proof-of-Work networks.

- 51% Attacks led by James

  The reorg tracker analyzes consensus security of proof-of-work cryptocurrencies and actively observes over twenty cryptocurrency networks. The reorg tracker can identify, analyze and estimate 51% reorg attacks, including double spends. To date the reorg tracker has detected over forty reorgs over six blocks deep across different cryptocurrencies, and several likely successful double-spend attacks.

- Dan M., Dan A., Neha, and David Parkes posted Double-Spend Counterattacks: Threat of Retaliation in Proof-of-Work Systems on arXiv.

  We formalize a defense to double-spend attacks in proof-of-work cryptocurrencies, showing that when the victim can counterattack in the same way as the attacker, this leads to a variation on the classic game-theoretic War of Attrition model. The threat of this kind of counterattack induces a subgame perfect equilibrium in which no attack occurs in the first place.

- Quanquan, Tadge, and Neha posted A Lower Bound for Byzantine Agreement and Consensus for Adaptive Adversaries using VDFs on arXiv.

  We propose a new communication-efficient consensus protocol using Verifiable Delay Functions (VDFs) that is secure against adaptive adversaries and does not require the same strong assumptions present in other protocols.

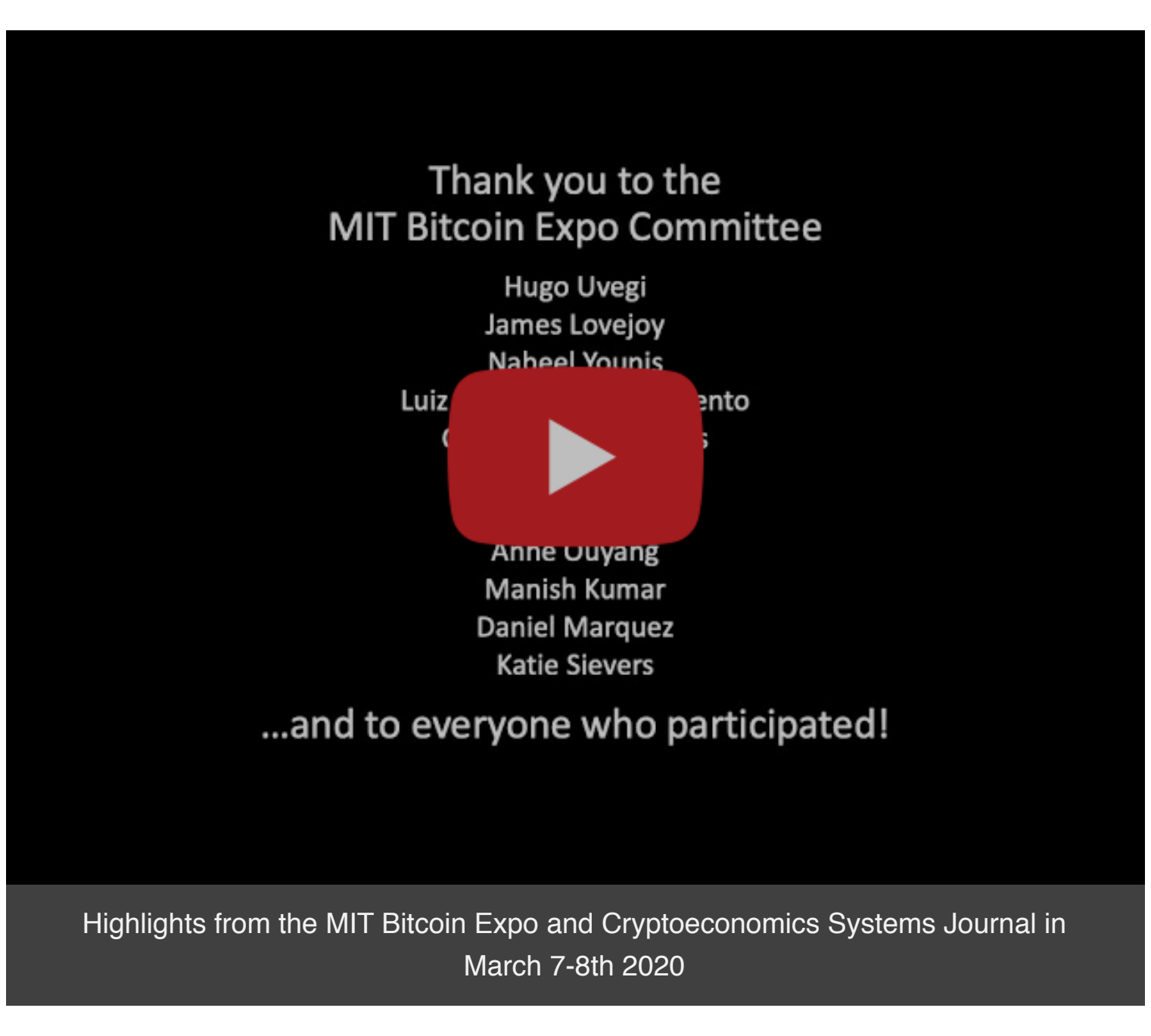
- DCI Co-op Dan Cline presented ClockWork: An Exchange Protocol for Proofs of Non Front-Running at the Stanford Blockchain Conference (joint work with Tadge and Neha).

  Using computationally expensive timelock puzzles, we built a verifiable exchange, ClockWork, which can prove to a user that it did not front-run their order.

- "Responsible Vulnerability Disclosures in Cryptocurrencies" authored by Rainer Boehme, Lisa Eckey, Tyler Moore, Neha Narula, Tim Ruffing, and Aviv Zohar to appear in Communications of the ACM

- Cryptanalysis of Curl-P and Other Attacks on the IOTA Cryptocurrency to appear in IACR Transactions on Symmetric Cryptology

Cryptoeconomic Systems and MIT Bitcoin Expo 2020



Highlights from the MIT Bitcoin Expo and Cryptoeconomics Systems Journal in March 7-8th 2020

- We had a wonderful turnout and a surprisingly smooth conference considering nearly half of our speakers chose to present remotely. The event was live streamed and there were numerous lively discussions on Telegram led by one of the journal editors, Andrew Miller, who attended remotely.
- The conference was divided into three events:
  - Cryptoeconomic Systems 2020 - Videos here
  - MIT Bitcoin Expo 2020 - Videos from Day One and Day Two
  - The Hackathon - Results
- The Call for Papers for the Cryptoeconomic Systems Journal deadline is May 31st 2020. More information
- During the 2020 MIT Bitcoin Expo/Cryptoeconomic Systems, a few members of the DCI community participated on panels and presented:
  - Wassim Alsindi moderated both days of the Cryptoeconomic Systems conference
  - Rob Ali on the Central Bank panel
  - Cory Fields on the Bitcoin Core Devs panel
  - Tadge Dryja on Discreet Log Contracts and Node Modes: Taxonomy of Bitcoin Network Nodes + An Addition
  - Quanquan Liu (DCI Student Researcher) on Consensus Under Adaptive Adversaries
  - Neha Narula on the Regulation and Compliance Panel
  - Neha Narula, Dan Moroz (DCI Collaborator), and Dan Aronoff (DCI Collaborator) on Double-Spend Counter-Attacks: Threat of Retaliation in PoW Systems
  - Jeremy Ney (DCI Student Researcher) and Nicolas Xuan-Yi Zhang (DCI working group) on Central Bank Digital Currencies and the Long-Term Advancement of Financial Stability

World Economics Forum at Davos

Neha attended the World Economic Forum and spoke on two panels:

From Token Assets to a Token Economy: Blockchain tokens are being created that allow real property, corporate securities and other financial assets to be traded on secondary markets. How can tokenization make illiquid assets more accessible without creating new systemic financial risks?

Speakers: Jeremy Allaire, Neha Narula, Sheila Warren

Creating a Credible and Trusted Digital Currency : The possibility of a trusted global digital currency has sparked political, economic and regulatory discussions worldwide. What trends are shaping the future of digital currencies? On the Forum Agenda:

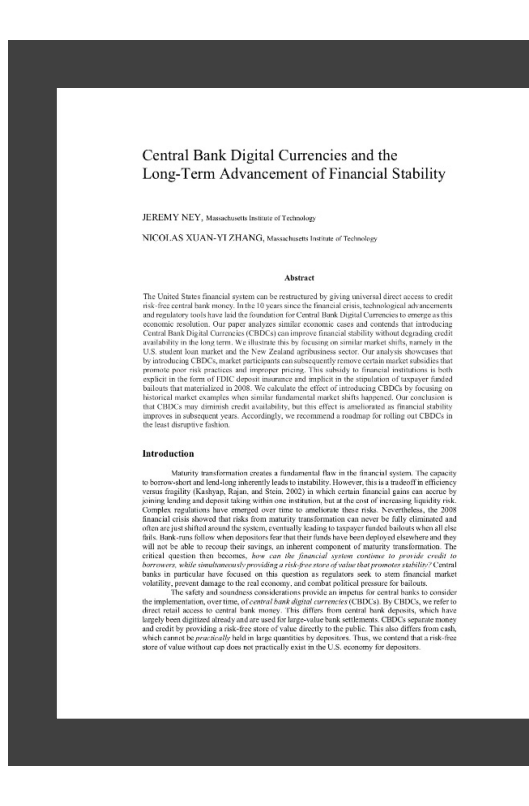
- Addressing financial inclusion
- Implications for security and digital trust
- Role of central banking and supervision

Speakers: Sheila Warren, Tharman Shanmugaratnam, David Marcus, Valdis Dombrovskis, Benoît Coeuré, Neha Narula

---

Education

- We are in full (now virtual!) swing for our 2019-2020 Cycle of Working Groups in Blockchain Lab, 15.217, and all groups are working hard with their companies. The projects this cycle are as follows:
  - Boston Consulting Group (BCG)
    - Blockchain Consortium - What are the factors behind a successful blockchain consortium?
    - CBDC Privacy - What types of privacy concerns should central banks consider when launching digital currencies?
  - Monetary Authority of Singapore (MAS)
    - KYC - How can a P2P-based solution for KYC be designed?
    - CBDC Flowback - What are the effects/consequences if Singapore decides against adoption of a digital currency but other countries/institutions launch one?
  - Fidelity
    - Spot vs. Unregulated - Are there correlations in pricing between bitcoin spot and the unregulated derivatives market?
    - BTC Market Crash - What caused the March 2020 Bitcoin Market Crash?



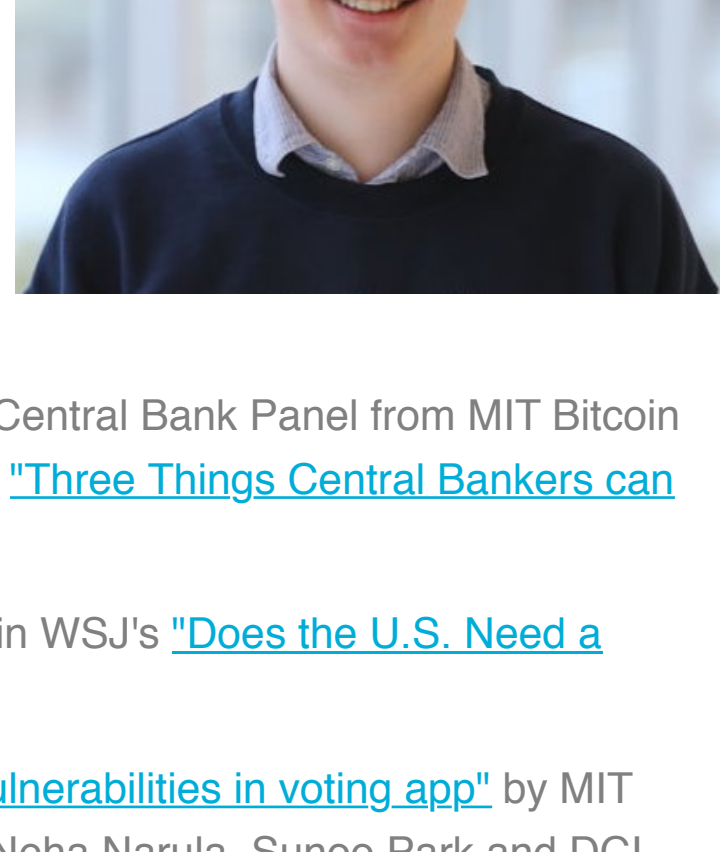
2018-2019 Class highlight! - Nicolas Xuan-Yi Zhang and Jeremy Ney's paper from the DCI's working group, Digital Fiat Currencies with Boston Consulting Group (BCG) was presented at the Cryptoeconomic Systems Conference (CES) in March, here at MIT; after being accepted to the journals first edition.

- All 2017-2018 Working Group Cycle's reports can be found on the DCI 2017-2018 Pilot Program webpage
- This term we have two UROPs!
  - Anne Ouyang is working on analyzing algorithms that attempt to protect against reorgs, specifically the delayed block penalty algorithm in Horizen. She is being mentored by James and Neha
  - Ananya Gurumurthy is working on a CBDC prototype implementation in Python to demonstrate an interface for atomic swaps between different CBDCs. She is being mentored by James and Rob

---

Media

Forbes Magazine's article on "Bitcoin Rival Suffers Devastating Attack" covers DCI's James Lovejoy's discovery of a 51% Attack on Bitcoin Gold



- MIT Technology Review Discusses Central Bank Panel from MIT Bitcoin Expo, which included DCI's Rob Ali: "Three Things Central Bankers can Learn from Bitcoin"
- DCI's Neha Narula supports CBDC in WSJ's "Does the U.S. Need a National Digital Currency?"
- "MIT researchers identify security vulnerabilities in voting app" by MIT News discusses research by DCI's Neha Narula, Sunoo Park and DCI Advisor Ron Rivest
- "Crypto Thoughts From Davos: Encouraging, But Beware Unintended Consequences" Covers the panel Creating a Credible and Trusted Digital Currency at WEF 2020
- CNBC Interviews DCI's Neha Narula and reports on WEF Davos 2020 "Calls for a US 'digital dollar' rise as China powers ahead with a digital yuan"
- DCI's Robleh Ali was quoted in MIT Technology Review's "An elegy for cash: the technology we might never replace"
- The New York Times quotes Neha Narula in "Twitter and Facebook Want to Shift Power to Users. Or Do They?"

Items of Interest

- ELI5: Utreexo — A scaling solution by Calvin Kim - This is a really nice explainer of UTreeXO.
- DCI Working Group 'Blockchain Consortium' is asking that organizations that are members of blockchain consortia fill out this survey to gather more data for their paper. Please fill out or share with appropriate individuals. The deadline is May 12th.

digital currency initiative

Empower individuals by making it as fast and easy to move value across the world as it is to move information
dci.mit.edu