Blockchain and Cryptocurrencies Seminar$^+$

סמינר בבלוקצ'יין ומטבעות קריפטוגרפיים

Technion EE, Ittay Eyal

Admin, Plan, Requirements

Winter 2017-18, **Sundays 10:30-12:10**, **Meyer 354**

Goals

Yes:

1. Blockchains, cryptocurrencies, smart contracts
2. Paper reading
3. Presentation

Phase I: Introduction (lectures)

Phase II: Seminar format

No:

- Financial advice

Blockchains, cryptocurrencies, and smart contracts

Basics:

- Security and Privacy
- Distributed systems
- Cryptography
- Game theory

Recent papers

Oakland (S&P), CCS, NDSS, USENIX Security, SOSP, NSDI, FC, BITCOIN, PODC, DISC… also preprints (w/ permission)

not: White papers (exceptional cases w/ permission)

not: Weakly related contributions containing the word Blockchain

Paper choice mechanism will be announced when relevant

Paper Reading

Read next week's paper and write a concise (up to page) review.

Older papers for phase I

- Summarize paper's contribution (1 par)
- List pros and cons (2-3 points)
  - Correctness, Novelty and topic significance, clarity, elegance, completeness
- Propose future directions
  - What would you do next?
  - How would you go about it?

Presentation (1/2)

- Background (signatures, hashing functions, consensus, etc.)
- Context – prior art, maybe followups, non-academic
- Contribution
  - Present as authors would, be ready to answer questions
- Concerns

Presentation (2/2)

- Use good slides
    - Yours Ok
    - Original / other also Ok
    - Ok not to use slides
- Concise slides
    - 3-4 bullets per slide
    - 3-4 words per bullet
- Use graphics

Grade, Registration

- Grad course; Excellent undergrads w/ permission
- Ok to sit, better register
- Mandatory attendance
- Grade structure:

Presentation:	60%
Paper reports:	30%
Participation:	10%

Register for mailing list.
http://tinyurl.com/049018

Disclaimer

- Booming market
    - Cryptocurrencies
    - ICOs
    - Companies

- No financial advice here
    - Neither positive nor negative
    - Not by me, not by you

Textbooks

- **Bitcoin and Cryptocurrency Technologies**
  Narayanan, Bonneau, Felten, Miller, Goldfeder; Princeton, 2015
  https://piazza.com/princeton/spring2015/btctech/resources

- **Mastering Bitcoin**
  Antonopoulos; O'reilly, 2014
  http://chimera.labs.oreilly.com/books/1234000001802