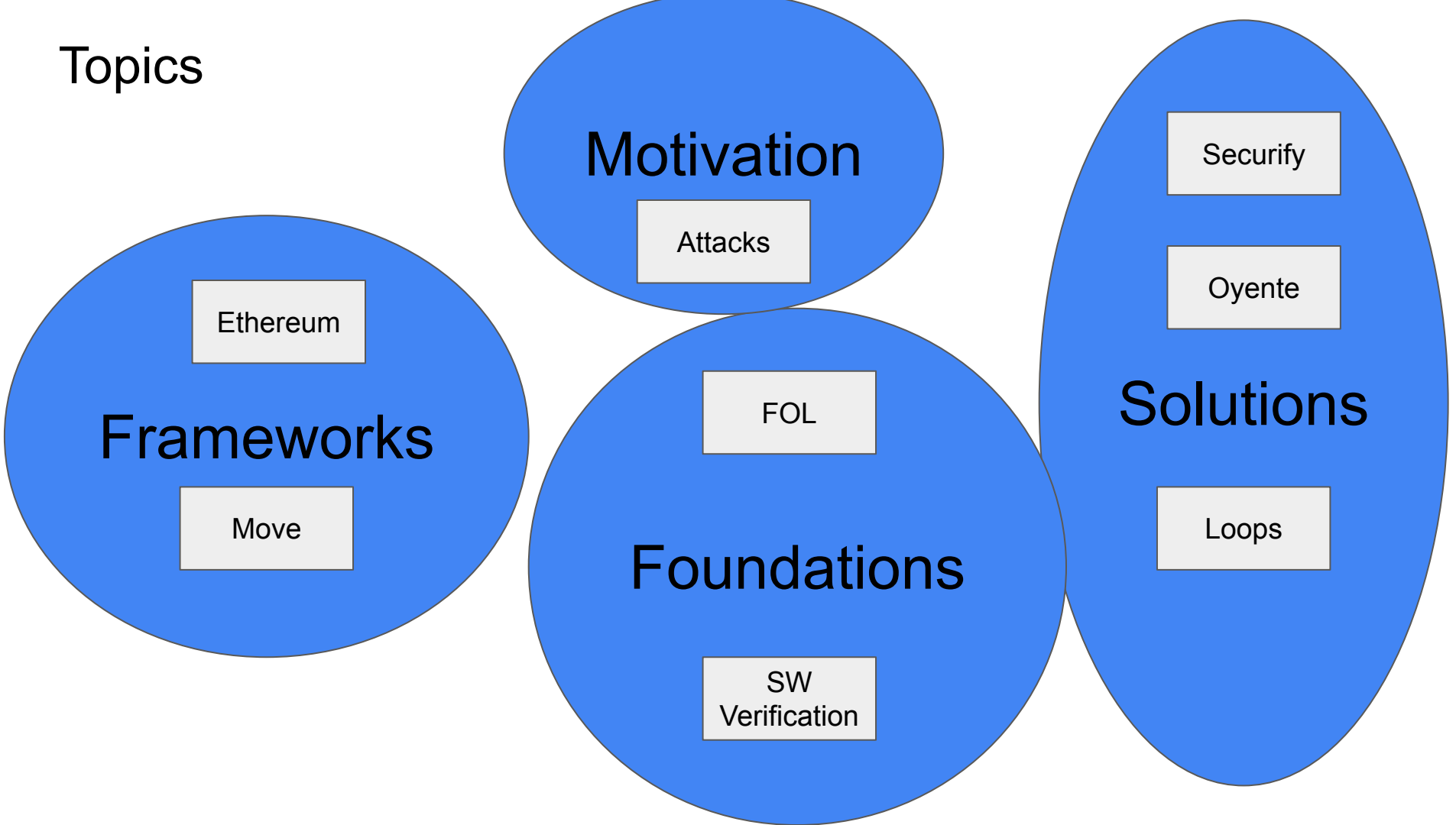
Smart Contracts Verification

Yoni Zohar

Outline

- Summary of presentations
- Summary of topics
- Summary of research area

Topics


Motivation
Attacks
Ethereum
Frameworks
Move
FOL
Foundations
SW
Verification
Securify
Oyente
Solutions
Loops

Recommendations

- Short bullets
- Demos
- Names on first slide (maybe more)
- Overview + Summary Slides
- Plots / Drawings / Graphics over text

Commercial Break

Open Positions:

1. Masters
2. Undergrad projects (paid / unpaid)

Topics:

1. Solving techniques
2. Frameworks aimed for smart contract verifications
3. Proving things about logic
4. Designing, Implementing and evaluating logical engines

Theory **Practice**

Examples

Papers:

1. The Move Prover
2. Sequences
3. Abstraction
4. Theory Combination

Collaborations:

1. Stanford University, The University of Iowa, …
2. Amazon Web Services, Meta (spin-offs), certora, …
3. Darpa
4. …

Key Takeaways

- Formal verification is possible
- SC verification is harder than SW verification
- SC verification is more critical than SW verification
- Hot topic in academia and industry:
  - Various classes, seminars, research centers
  - Various research projects
  - Certora
  - Veridise
  - Meta (and now Misten Labs, Aptos Labs, and many more)
  - Microsoft
  - More…

Links

- Centers:
  - https://cbr.stanford.edu/
  - https://blockchain.univ.ox.ac.uk/
  - http://blockchain.cs.ucl.ac.uk/
  - https://web3.princeton.edu/
- Classes
  - https://online.stanford.edu/courses/xcs251-cryptocurrencies-and-blockchain-technologies
  - https://web3.princeton.edu/principles-of-blockchains/
- Companies
  - https://www.certora.com/
  - https://veridise.com/
  - https://mystenlabs.com/
  - https://aptoslabs.com/

Feedback

- Interesting talks
- Interesting discussions
- Talks typically went beyond the papers
- Good understanding
- Good questions
- English

- Would love to hear suggestions from you: now and on email
  - Topic
  - Papers
  - Weakly paragraph
  - …?

Here I am supposed to have a summary slide…