

- **Introduction – 2. minutes**
  - Show news articles on promises
  - Why not here? 'Through of disillusion or technical problems'
- **Background & Problem Description – 10 minutes**
  - Blockchain 101
    - **Why** the blockchain promise appealed to the masses.
      - Trustless (petrol station example)
    - **How** would it do this?
      - Blocks chained together
      - Hashes are essentially fingerprints of data.
      - Consensus problem
        - Nakamoto -> Proof of Work
  - State of the art.
    - Hyperledger, Ripple, Algorand, honeybadgerBFT, tendermint.
      - *'Not gonna go in detail, but what do they all have in common'* (single ledger)
    - Trustchain
      - Detection vs prevention
  - state problem description
    - Global consensus' problems (overkill, unnatural, maybe unnecessary?)
    - Research question
      - *"How to achieve a truly scalable secure distributed ledger without global consensus?"*
    - Breakdown in: 3 types of scalability, security aspect, no global consensus.
- **Design & Poc -15 minutes**
  - Research question -> design goals
    - Scalability: minimal communication and time complexity
    - Security.
      - summarize threat model (failing nodes vs malicious)
    - No global knowledge
      - Explain causal relationship of Trustchain
        - Similarity with Schiper-Eggl-Sandoz algorithm
  - FWSP (my solution):
    - Witnesses
      - Random: No node should pick its witness
      - Must be verifiable: easy to check fair play
      - Use hash function
    - Explain the algorithm
      - Witness selection algorithm
      - 2/3 signatures + witness set extension
      - Show: constant witness set size vs network size.
    - Correctness, Liveness, security.
  - Proof of Concept
    - Traditional banking vs. new way of banking.
    - Software architecture?
    - Screenshots
- **Evaluation - 7,5 minutes**

- *Set up of the experiments*
  - *DAS-5, Orchestrator, 20 servers -> 16 cores 64GB ram*
  - Show figure 5.1 (setup overview)?
  - Show figure 5.2 (experiment flow)?
- *Scalability:*
  - Throughput vs latency
  - Throughput:
    - Experiment setup + results.
    - Peak performance throughput.
      - *“While the main goal was to create the most scalable, not the best performing, still a simple experiment was run, where no waiting in between transactions were implemented.”*
  - Latency:
    - Experiments setup + results
- Performance under adversarial influence
  - Experiments + results.
  - Explain why latency only.
- Compare to state of the art
  - Blockbench: explain the tests
    - Performance as function of validators
    - Absolute performance
      - Algorand: 750 MiB/h (500.000 users run on 1.000 machines,), this work: 15.8 GiB/h (280 nodes on 20 machines).
  - Summary Table
- **Conclusion** – 5 minutes
  - Link back to research question
    - Liveness, Correctness, and security theoretically shown.
    - Scalability proven experiment
  - EV charging -> Extend to businesses
  - Demonstration