Technische Universität Braunschweig

Institut für Betriebssysteme und Rechnerverbund

Seminar Distributed Systems

Byzantine Fault Tolerance-Based Consensus Protocols for Blockchains

Signe Rüsch

April 4, 2018

Table of Contents

Organisational

- Course
  - Course held in German/English
- Language
  - Essay and presentation in either German or **English**
- Certificate Requirements
  - Essay (6 pages, double column)
  - Presentation of own topic (25min + discussion)
  - Active participation in discussions

Procedure

- Not a single meeting with all presentations

→ Two presentations each meeting

- Time will be determined after this meeting

Procedure

Procedure (4 Weeks)

Today	Topic selection
W 1-3	Read the papers or find other work fitting the topic[1]
W 1-3	Write essay and create presentation
W 2	Presentation dry-run, first draft of essay
W 3	Presentation, receiving peer review of essay
W 3-4	Incorporate comments
W 4	Submission of essay & presentation slides

[1] How to read a paper, `http://dl.acm.org/citation.cfm?id=1273458`

Requirements Presentation

- 25mins talks = approx. 25 slides
- Pictures $\gg$ text
- Presentation best-practices
  - Title, author, page numbers on each slide
  - Corporate design TU Braunschweig
- Structure of presentation (recommendation)
  - Introduction, Motivation
  - Problem
  - Approach
  - Evaluation, Conclusion (one slide summary!)
- Templates: `https://www.ibr.cs.tu-bs.de/kb/templates.html`
- LaTeX is preferred

Requirements Essay

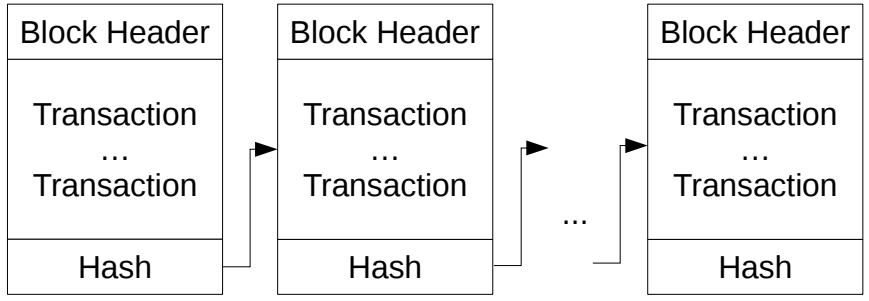
- 6 pages (ACM Proceedings template)
- Structural components
  - Introduction & Motivation
  - Problem outline
  - Solutions, approaches tackling the problem
  - Evaluation
  - Conclusion, Discussion of results, Outlook
- Look at multiple papers and your papers' related work!
- LaTeX is required!
- Templates:
  `https://www.acm.org/publications/proceedings-template`

Table of Contents

Topic Descriptions

What is a blockchain?

- Blocks containing transactions
- Each block contains hash of previous block
- Strict ordering of messages
- No message modification
- Rule-based read permissions, global write
- Often cryptocurrencies, e. g. Bitcoin

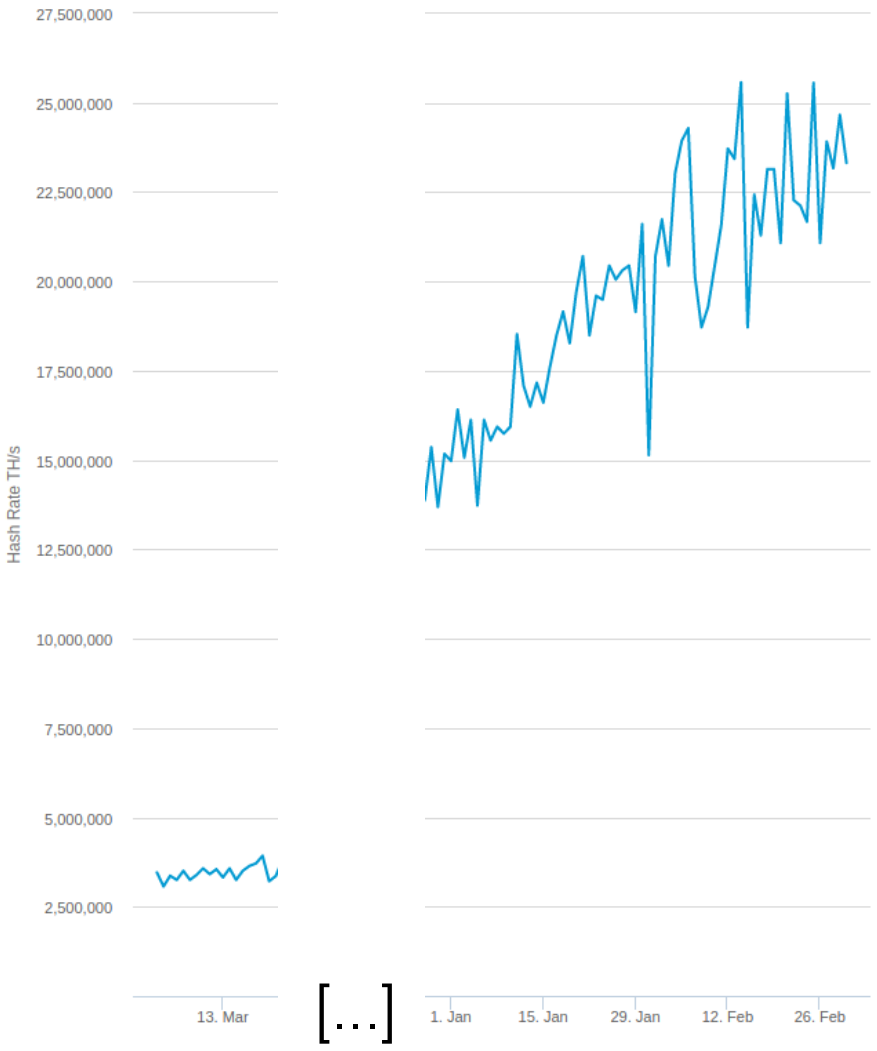


[Bessani et al., 2017]

Topic Descriptions

Proof-of-Work Mining

- Bitcoin mining has higher energy consumption than Ireland
- Long confirmation time of up to one hour

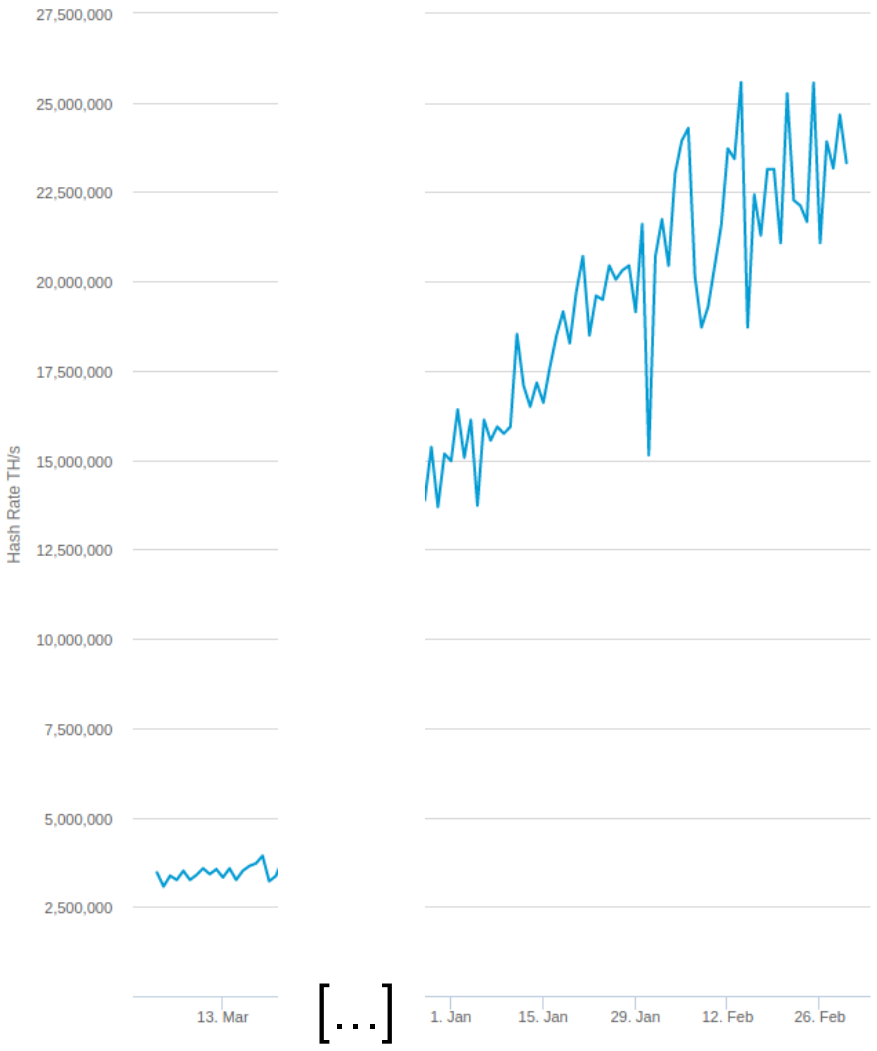


Topic Descriptions

Proof-of-Work Mining

- Bitcoin mining has higher energy consumption than Ireland
- Long confirmation time of up to one hour

→ Alternatives?



Topic Descriptions

Byzantine Fault Tolerance

- Permissioned / permissionless blockchains
  - Authentication vs open access
  - Known vs unknown users
  - Read / write rights
- Set of nodes responsible for block creation
- Nodes can behave arbitrarily faulty!

Topics Overview

- Traditional BFT Protocols
  1. Practical Byzantine Fault Tolerance
  2. CheapBFT: Resource-efficient Byzantine Fault Tolerance
  3. Efficient Byzantine Fault-Tolerance
- Further BFT Protocols
  4. Hybrids on Steroids: SGX-Based High Performance BFT
  5. Troxy: Transparent Access to Byzantine Fault-Tolerant Systems
  6. Non-determinism in Byzantine Fault-Tolerant Replication
  7. SmartCast

Topics Overview (2)

- Scalable BFT Protocols for Blockchains
  8. A BFT Ordering Service for Hyperledger Fabric
  9. The Honey Badger of BFT Protocols
  10. Algorand: Scaling Byzantine Agreements for Cryptocurrencies
  11. Stellar Consensus Protocol
  12. ByzCoin

Topics Overview (2)

- Scalable BFT Protocols for Blockchains
  8. A BFT Ordering Service for Hyperledger Fabric
  9. The Honey Badger of BFT Protocols
  10. Algorand: Scaling Byzantine Agreements for Cryptocurrencies
  11. Stellar Consensus Protocol
  12. ByzCoin

Topic Assignment