BLOCKCHAIN TECHNOLOGIES

Introduction | Summer 2019

Prof. Dr. Florian Tschorsch
Distributed Security Infrastructures

Logistics

Module: Blockchain Technologies	
Type	Lecture + Project
Contact hours	2 h + 2 h
Credits	6 ECTS
Programs	Master (CS, CE, ISE, EE)
Electives	Distributed Systems and Networks; Communication Systems
Exam	Oral exam (graded)
Number of Participants	Limited to max. 50 Students
Prerequisite	No formal prerequisites

Organization

- infos, announcements, slides, literature, ... can be found on TUB's Information System for Instructors and Students (ISIS)
- course handle *BLKCHN '19*
- entry procedure will be explained later!

- questions, suggestions, feedback, ideas, ... are welcome!
- consultation by appointment
- please send an email to `florian.tschorsch@tu-berlin.de`

Acknowledgements

- even if you see most of the time only a few people,
  this course is influenced by many people

- we therefore thank (in alphabetical order):
  Joseph Bonneau, Edward Felten, Steven Goldfeder, Andrew Miller,
  Arvind Narayanan, Björn Scheuermann, and Roger Wattenhofer

  And the innumerable researchers whose work influenced this lecture

WHAT DO YOU EXPECT FROM THIS COURSE?

> The first five times you think you understand it, you don't.
>
> Dan Kaminsky, Black Hat 2011

Blockchains

- data structures and protocols make a blockchain
- blockchains consisting of three main elements
  1. distributed (as in multiple copies) but centralized (as in there is only one true) ledger (which is a way of recording what happened and in what order)
  2. consensus, which is a way to ensure all the copies of the ledger are the same (also distributed, i.e., you do not have to trust any particular node)
  3. incentive, which is some sort of digital token that has value and is publicly traded
- all three elements fit together and build a single network that offers new security properties
- the question is: is it actually good for anything?

It is a Matter of Trust

> We have proposed a system for electronic transactions without relying on trust.
>
> Satoshi Nakamoto, 2008

- the word “trust” is loaded with many meanings
- four different “trust architectures” (after Kevin Werbach)
  - peer-to-peer trust, e.g., personal trust in a friend
  - leviathan (or institutional) trust, e.g., contracts backed by the government
  - intermediary trust, e.g., credit card provider
  - distributed trust, e.g., blockchain
- a blockchain probably does not solve the security problems you think it solves
- in particular, a false trust in blockchain can itself be a security risk

Objectives

Hypothesis: blockchains are neither black magic nor the solution to everything, but still disrupted the way we perceive distributed systems.

1. teach conceptual knowledge on blockchains, including
   - fault tolerance and consensus
   - weak vs. strong identities
   - resilience and security
   - peer-to-peer networks

2. let students acquire practical skills
   - software development that interacts with blockchains
   - integrate ideas from blockchains into own software projects

Disclaimer: This Course is ...

#1 ... not about cryptocurrencies

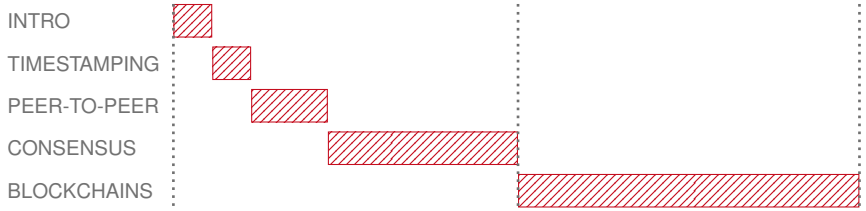
#2 ... not only about security

#3 ... work in progress

Lecture: Science of the Blockchain

Teach conceptual knowledge

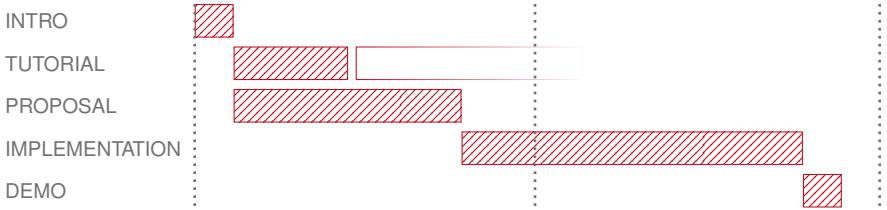
- weekly (last lecture is July 11, 2019)
- Thursday, 8–10am in MAR 0.011 (there will be some exceptions)
- participation is voluntarily, but suggested
- no homework assignments
- slides will be available
- interactive, please ask questions



Project: Blockchain Lab

Acquire practical skills

- assignment: implement a distributed application that somehow makes use of blockchain technology
- you determine the application's actual direction/idea/topic/use case/goal/...
- for example, take a (simple) application and get rid of any central authorities by implementing a smart contract which realizes the program logic
- contact: `muth@tu-berlin.de`



Project Organization

- we offer a tutorial to help you get started; dates are
  - April 17, 12:00–14:00 in Room FH 311
  - April 24, 12:00–14:00 in Room FH 311
  - May 8, 12:00–14:00 in Room FH 311
- yet, the project requires your own private study;
  in fact, the project is your responsibility!

- you work in groups of 3–4 students
  make groups and indicate your preference on our course website
- the volume of each project is 3 CP ($\approx$ 90 h per person)
  your application should reflect this volume

- we have no mercy for plagiarism!
- it directly leads to the exclusion from the course;
  we keep the right to initiate further steps

Project Proposal

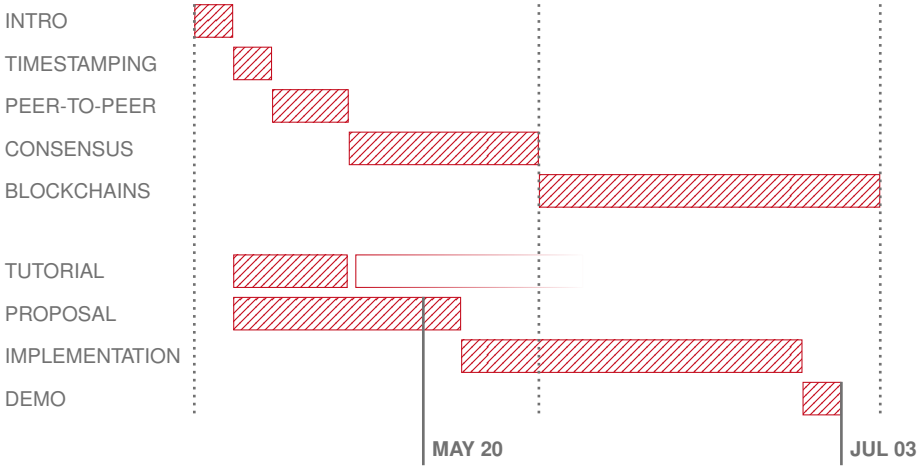
- during the first weeks, come up with your project idea
- write a project proposal as an “one pager”, that is,
  a document that gives an overview of your idea, not exceeding one page
- in your proposal, address the following points ...
  - motivate and describe the application’s general idea
  - indicate how to achieve this goal by describing the technical approach
  - state the technical challenges you aim to solve
- project proposals are due **May 20, 2019**
  (mind the submission instructions on our course website)
- after, you will get individual feedback on your proposal (probably May 22)

Project Demo

- implement your project idea *before* your exam
- you will present your application by giving a *working* demo

- project presentation/demos take place **July 3, 2019**
- your fellow students will be the audience
- the best projects will be awarded based on
  - creativity
  - technical level
  - quality of the implementation
  - quality of the demo

Outlook and Agenda



Course Prerequisites

- no formal prerequisites
- however, the lecture is very technical in nature
- basic knowledge in ...
  - data structures and algorithms
  - computer networking
  - distributed systems
  - network security

  ... will be extremely helpful

- Recommended reading:

  Computer Networking - A Top-Down Approach
  by James Kurose and Keith Ross

  Distributed Systems: Principles and Paradigms
  by Andrew Tanenbaum and Maarten van Steen

Literature

- by now, there are a number of books on Bitcoin, cryptocurrencies, and blockchains with different focuses and of different quality
- some positive examples include:

  Distributed Ledger Technology: The Science of the Blockchain (2nd Edition)
  by Roger Wattenhofer

  Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction
  by Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder

  Mastering Ethereum: Building Smart Contracts and Dapps
  by Andreas Antonopoulos and Gavin Wood

- in this lecture, I will reference the sources, mostly scientific papers, on the slides
- I do not expect you to read all these books or papers,
  but they are there for your private study

Exam and Grading

- oral exam (typically 30 minutes)
- project must be completed before taking the exam
- lecture and projects are an integral part of the exam

- **Important:** register on QISPOS for the exam (deadlines t.b.a.)
- exam dates will be at the beginning and at the end of the semester break, i. e., July 2019 and October 2019

Class Entry Policy

- the number of participants is limited to 50 students
- reasons for the limitation are manifold
  - interaction and discussions in the lecture
  - project requires resources for supervision/guidance/...
  - ...

- register/enroll to the ISIS course
- passing an online quiz, which asks some CS basics
- both closes **Friday, April 12 at 23:55**

- “lucky 50” will be selected randomly
- student notification: Monday, April 15 (by email)

Summary and Next Steps