Blockchain Lab

Tut 01: Introduction & Blockchain Basics

Robert Muth
muth@tu-berlin.de

originally by Elias Rohrer

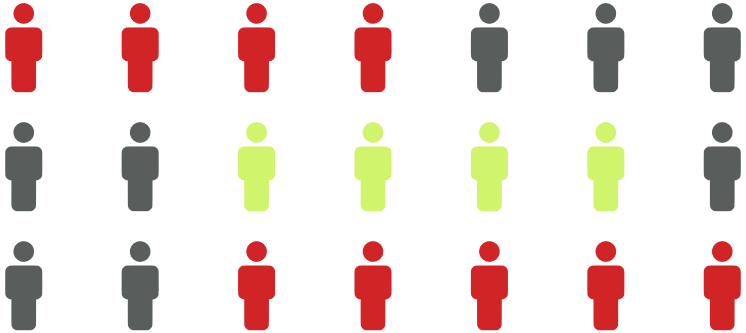
April 17, 2019

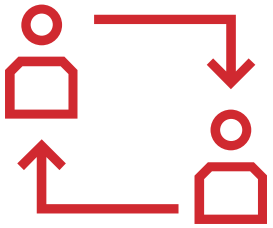
What to Expect (for today)

- Talk about what to expect from the whole lab
- Blockchain introduction
- Project work
- Team building

What to Expect from the Lab

- Blockchain-based systems are really hyped right now. You probably already have heard and know a lot about them.
- **Now:** build groups of $\sim$ 4 students! (only for today)



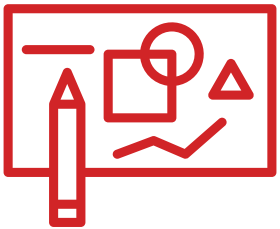


https://pad.systemli.org/p/lab

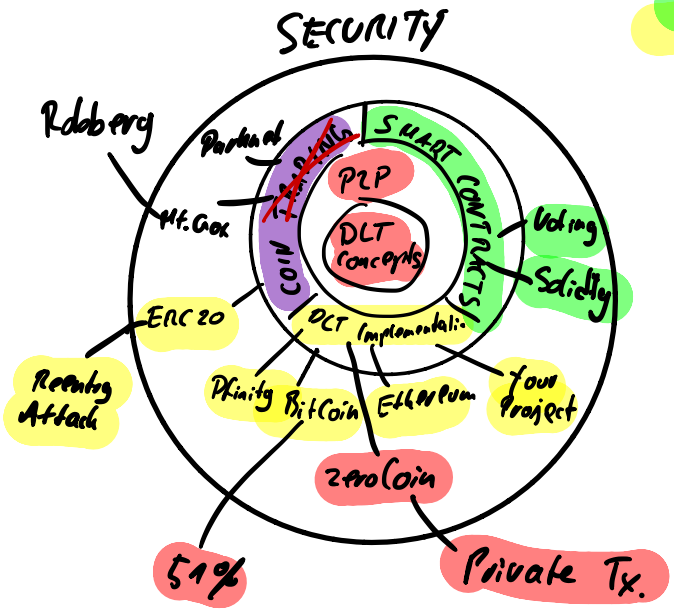
- Source code solutions
- The place to share snippets and links with your fellow students during this session
- Please don't be destructive!

- For 5 minutes: Discuss what you expect to hear in the lab about blockchains
- Settle on two personally most important aspects or implementations

What to Expect from the Lab



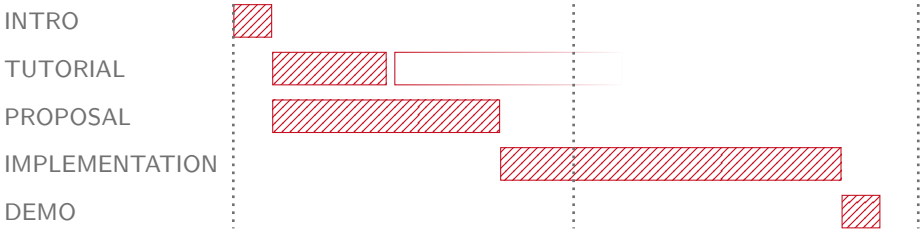
What to Expect from the Lab



What to Expect from the Lab

- The lecture covers the theoretic concepts of blockchain technologies
- In the lab, we focus on the practical side of blockchain technologies
- For example, you'll get your hands dirty and build something

Schedule



Tutorials

- During the first three tutorial dates I'll present some basic concepts to get you started
- The technologies we are going to use are very new and constantly changing
- This is the venue to help each other out, pose questions and discuss, **also with your fellow students**
- There will be live fiddling/coding, so **bring your laptops** to follow along!

→ Room FH 311, Fraunhoferstr. 33-36 is available for the whole semester (Wednesday, 12-2pm)

Tut 02: Ethereum & Smart Contracts

- Introduction to the Ethereum Project
- Basic concept of smart contracts and distributed apps
- Sneak peak into Solidity and the development toolchain

Tut 03: DApp & Smart Contract Programming

- **May 8th** (May 1st is a holiday)
- DApp programming with Solidity
- Discussion of your experiences and challenges so far
- Your project ideas

Tut 04-xx: Live Coding and Technology Review

- May 8, 12-2pm in Room FH 311
- Live coding
  - Voting
  - ERC20 Token Transfer
  - Debbuging and EVM Assembly
  - Security
- Guest talk
- Technology Review
  - Dfinity
  - TBA (Ideas? $\Rightarrow$ mail me!)

Blockchain Project: Idea

- During this semester, you'll form working groups and build an application that makes use of blockchain technologies
- Be creative! For example:
  - Build a distributed application doing something funny/interesting
  - Convert a centralized system to decentralized one using smart contracts
  - Build a peer-to-peer application that uses blockchain technology as a backend
- Disclaimer: I'll present some basic concepts to get you started, but the project is your responsibility!

Blockchain Project: Working Groups

- **Assignment from today:**
  - Form working groups of 3-4 students on ISIS (Deadline: ~~May 26, 2019~~ April 24, 23:59, 2019)
  - Start brainstorming/collecting ideas
- The project yields $3CP \approx 90h$ **per student**

$\Rightarrow$ Your project idea should reflect an according workload, depending on your group size

Blockchain Project: Proposal

- Write-up your best idea in a one-page proposal:
  - 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
  - provide rough schedule (2-4 defined milestones with dates)
- **Proposal Deadline: May 20, 2019, 23:59** (Upload on ISIS course)

Blockchain Project: Implementation Phase

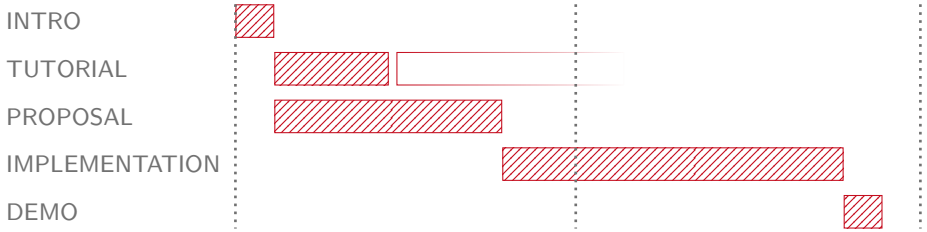
- Implementation phase starts after you get individual feedback from us **around May 22**
- Only live coding and discussions during this time
- We can schedule additional meetings, if you (we or) think they are needed

Blockchain Project: Demo

- You will present your projects by showing a *working demo* at **July 3, 2019**.
- Audience: your fellow students and others
- Best projects will be awarded

Important Dates

- Tutorial sessions
  - `Tut 01`: Today (April 17, 12-4pm in Room FH 311)
  - `Tut 02`: April 24
  - Holiday on May 1st
  - `Tut 03`: May 8
- Group forming deadline: April 24, 2019, 23:59
- Proposal deadline: May 20, 2019, 23:59
- Project demo: July 3, 2019 (we don't know where, yet)



- Always check dates on ISIS!

Short History of Blockchain-based Systems

- Foundations go way back:
  - 1990: Distributed Timestamping[1]
  - 2002: Hashcash[2]
- 2008: Bitcoin introduces decentralized verifiable money transfer[3]
- 2013: Ethereum introduces general purpose computation to the blockchain world[4]
- Since then: many interesting new approaches

[1] Haber, Stuart, and W. Scott Stornetta: How to Time-Stamp a Digital Document. Conference on the Theory and Application of Cryptography. 1990.

[2] Back, Adam: Hashcash - A Denial of Service Counter-Measure. 2002.

[3] Nakamoto, Satoshi: Bitcoin: A Peer-to-Peer Electronic Cash System. 2008.

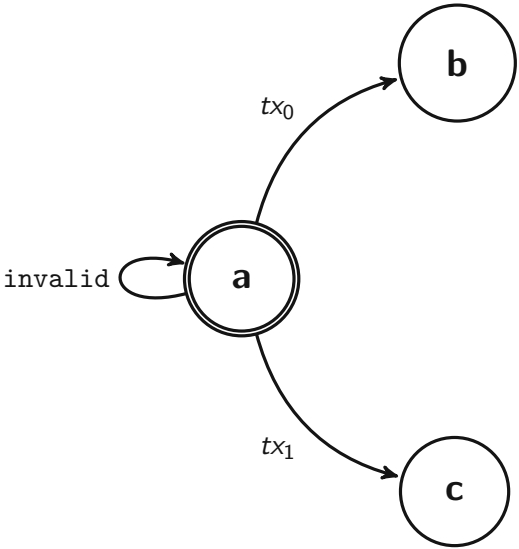
[4] Wood, Gavin: Ethereum: A Secure Decentralised Generalised Transaction Ledger. 2014.

Blockchain Problem Statement

- We want to issue transactions (as in financial transactions *or* data base transactions) from one party to another
- We want *someone* to apply the transactions, after verifying that they are indeed valid given a set rules
- However, we do not want to trust a centralized authority for this

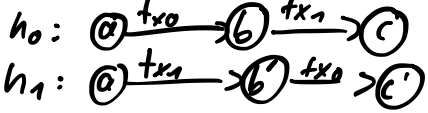
Distributed Ledger

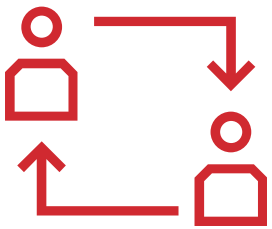
- Idea: Instead of having a single centralized authority controlling which transactions are valid, distribute it to a whole network of nodes
- All transactions are distributed (e.g., by broadcast) in the network and all nodes builds a local *ledger* of valid transactions
- This ledger is then again the basis upon which new transactions are deemed valid or invalid
- This can be thought of in terms of state machines: transactions are then transitions of the state machine from one valid ledger state to another


b
tx_0
invalid
a
tx_1
c

Consensus

- Conflicting ledger states may occur





- node n_0 first sees tx_0, then tx_1 and n_1 first sees tx_1, then tx_0. Which one should be recorded first?
- The consensus protocol is responsible for state conflict resolution
- It does so by applying a predefined set of consensus rules

$\Rightarrow$ Eventual consistency

Concept of a Blockchain

- Aggregate transactions into blocks
- Blocks are then cryptographically chained together, building a blockchain
- A blockchain introduces a total order over the blocks and transactions, simplifying conflict (fork) resolution

Group Work

- Why do we need blocks? (5 minutes)

- Throughput Problems
- Fork Problems
- Missing Information
- Reorg. Prob.

Group Work

- Why do we need blocks? (5 minutes)
- In theory, a purely transaction-based approach would work, but may be heavily dependant on network effects
- Speed of light is a lower bound
  $min(distance = 20.000\ [km]) = \frac{20000\ [km]}{c\ [\frac{km}{h}]} = 0.06671\ [s]$
- Aggregate transactions into blocks, which are created in higher intervals.

Mining and Proof-of-Work

- But whom do we allow to add blocks?
- Idea: Make adding blocks very hard, but lucrative. Then, multiple parties will compete to add a block.
- Proof-of-work is a computational heavy puzzle, depending on the input data: given the input data $\mathtt{d}$, find a variable $\mathtt{nonce}$, so that $H(\mathtt{d}||\mathtt{nonce})$ has a pre-defined number of leading zeros.[5]
- In Bitcoin, the number of zeros is defined by the "difficulty" parameter. It is adapted every 2016 blocks, so that a new solution is found roughly every ten minutes.

[5] First introduced in: Back, Adam: Hashcash - A Denial of Service Counter-Measure. 2002.

Blockchain Demo

Follow along, you find the link on the pad:

`https://pad.systemli.org/p/lab`

Assignments

Due April 24, 2019, 12:00:

- Read Sec. II of Prof. Tschorsch's survey paper.[6]
- Read blog post "How does Ethereum work, anyway?".[7]

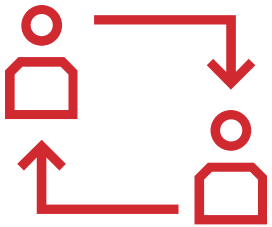
Due April 24, 2019, **23:59**:

- Form working groups of 3-4 students
- Register groups on ISIS

[6] Tschorsch, Florian, and Björn Scheuermann: Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies. IEEE Communications Surveys & Tutorials. 2016.

[7] `https://medium.com/@preethikasireddy/how-does-ethereum-work-anyway-22d1df506369`

Project discussions



Do Internet research

- Hands on! [redacted] for blockchain projects (10 mins)
- Think about aweseome projects without blockchain
- Brainstorm for new projects!