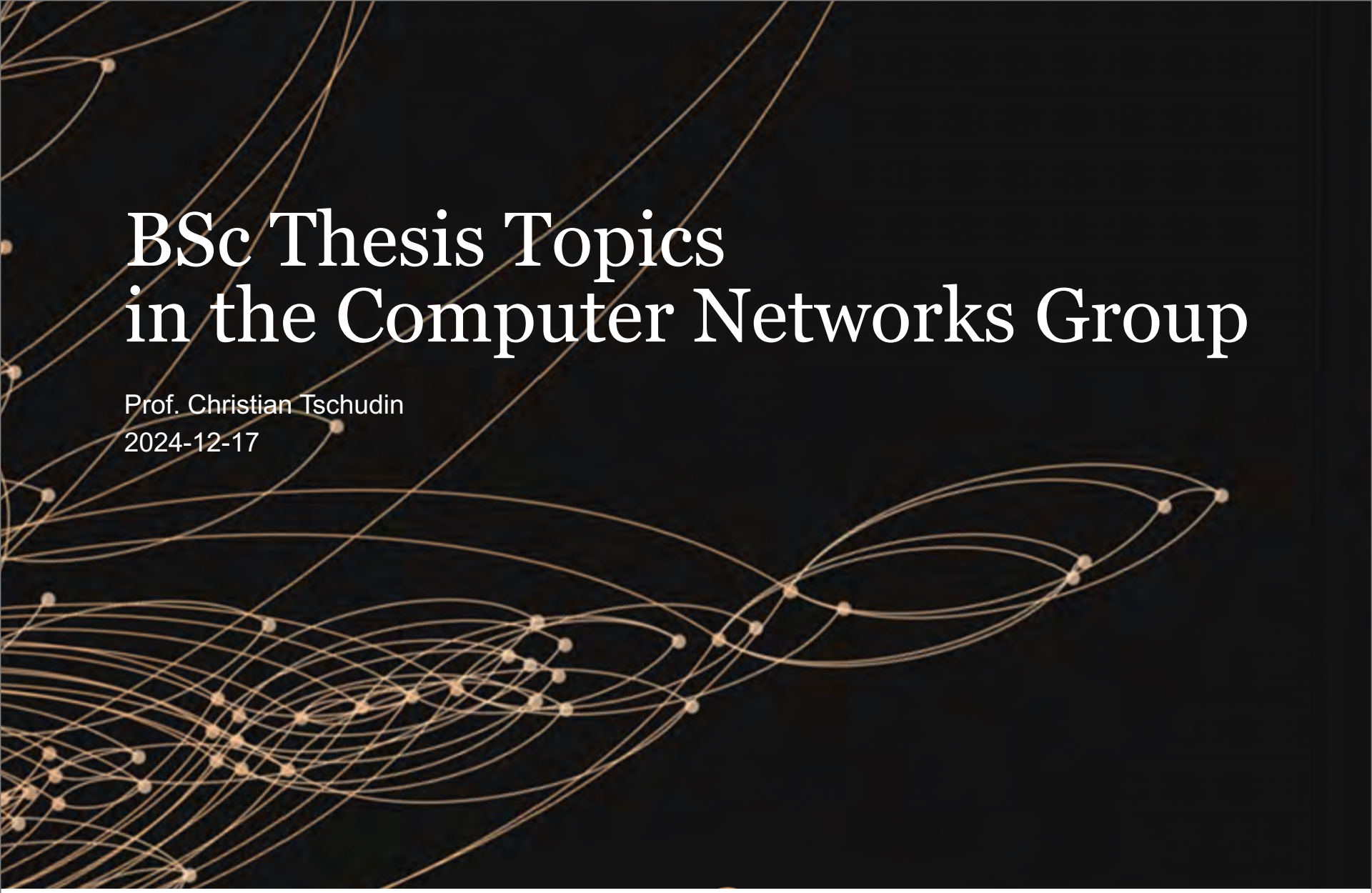


BSc Thesis Topics in the Computer Networks Group

Prof. Christian Tschudin

2024-12-17

University of Basel

Members of the Computer Networks Group

Christian Tschudin
computer networks

Erick Lavoie
peer-to-peer

Osman Biçer
cryptography

Ali Ajorian
compilers

Teaching

Fall Semester 2024

- Computer Architecture
- Foundations of Distributed Systems (with FC, HS, IW)
- Seminar “Radio Packet Networks”
- Seminar “101 Things I Learned in Computer Science”

Spring Semester

- Distributed Programming and Internet (formerly “Internet and Security”)
- (Advanced) Computer Networks

Topics of some ongoing/past seminars

. Interpretation and Compilation of Programming Languages (Lavoie, Ajorian)
. Conflict-free Replicated Data Types (CRDT, w/ Lavoie)
. Programming with Monads, Haskell (w/ Lüthi)
. Programming with LISP (w/ Lüthi)

General Areas for BSc Projects

A. Distributed Applications / Peer-to-Peer

B. Hostile Environments (like the Internet, or your SmartPhone)

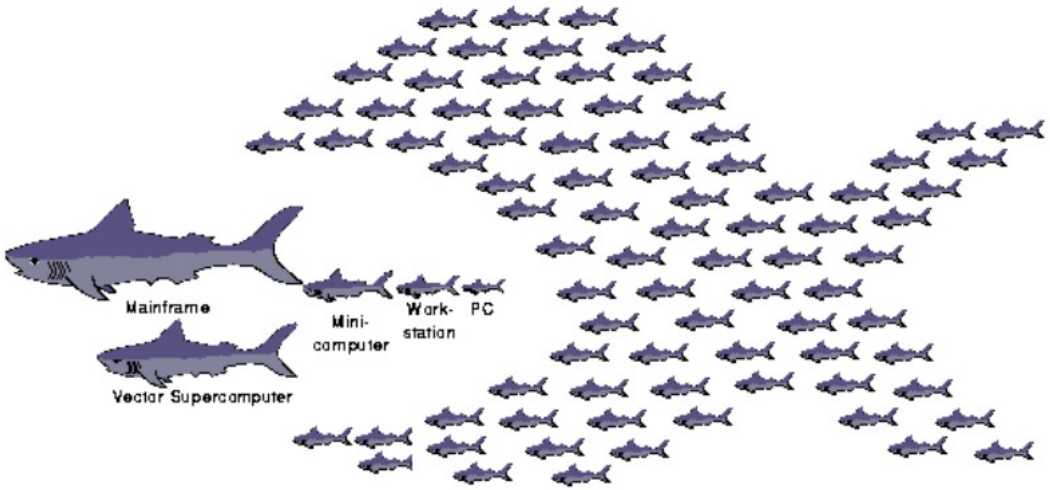
C. BYOT

– Ali Ajorian's list

– Erick Lavoie's list

A) Distributed Applications

Aristotle: *«The whole is more than the sum of its parts»*



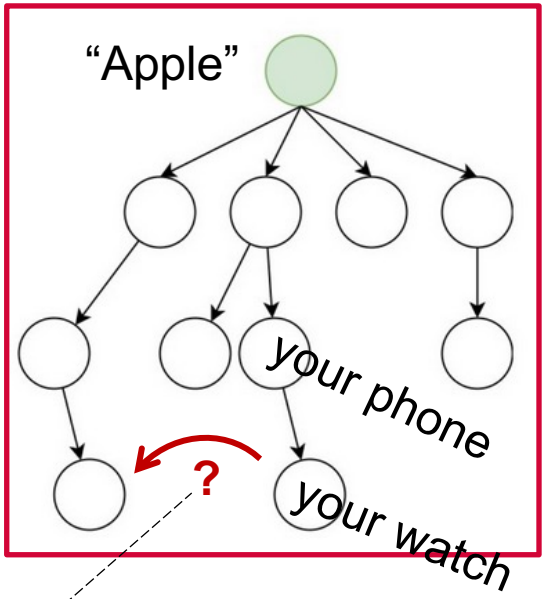
"scale out" instead of "scale up"

Despite the cloud: statement is not obvious in Computer Science, as server-based solutions dominate, central mgmt

Science question: What «DNA» for successful peer-to-peer applications?

A) Distributed Applications:

a decentralized scenario



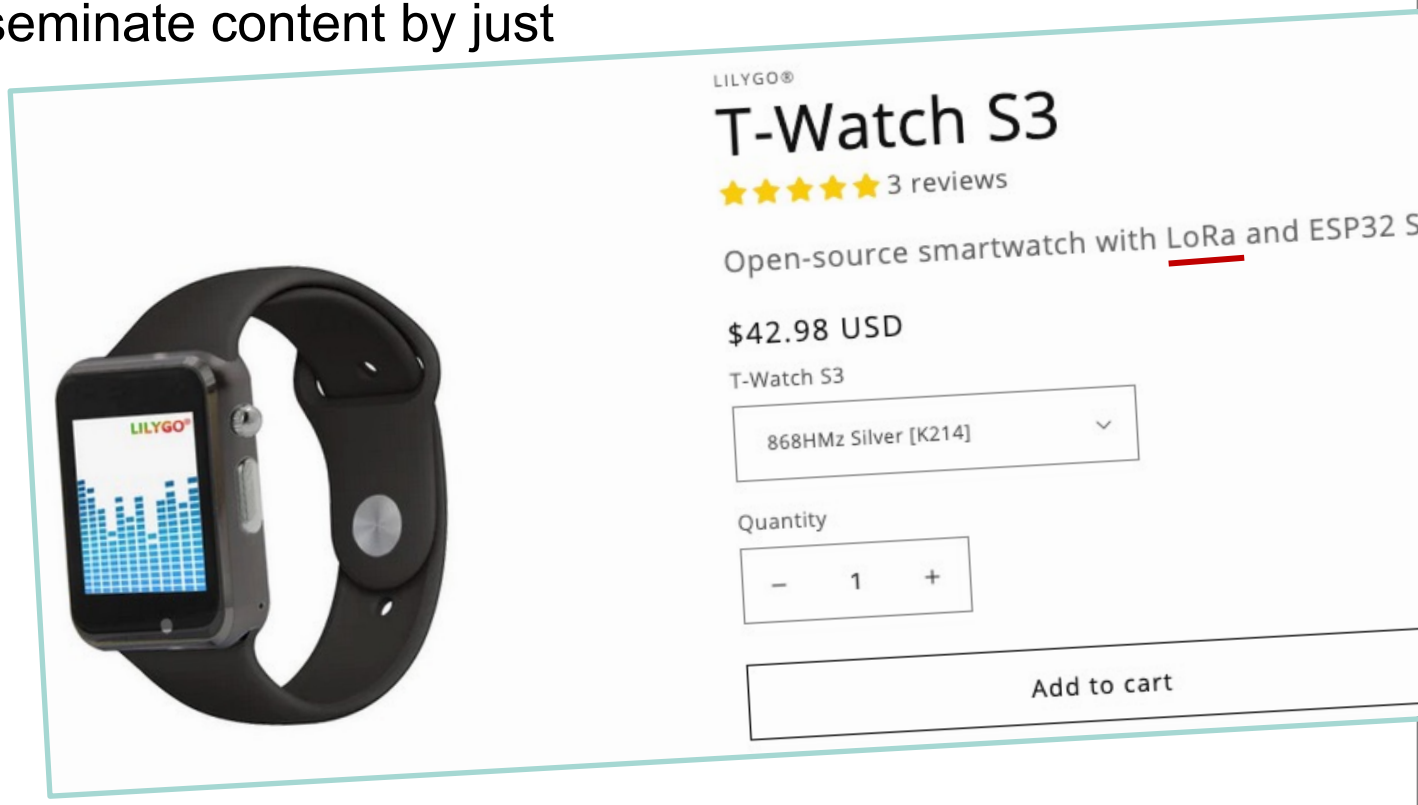
Today's distribution economics:
- buy a smart watch
- buy a smartphone
  (to connect your smart watch)
- buy a mobile plan
  (to connect your smartphone to the cloud)
- buy a cloud subscription
  (to access Apple's services)

An alternate economic model:
- buy some device
- let the device talk to its peers, directly

There is a market for P2P knowhow, startups

A) Distributed Applications:
abundance of devices and connectivity

Long-range connectivity is available today
(and you can disseminate content by just
walking around)



LoRa (Long-Range radio): 100m to multiple kilometers

A) Distributed Applications (contd):

re-structuring «the stack»

A post-Internet architecture for distributed applications:

distributed applications based on CRDTs *)

data replication via trustable append-only logs

peer-to-peer connectivity

CRDT=«Conflict-free Replicated Data Types», discovered 2011

And: Cut out the middle men, build your own network → go radio

B) Hostile Computing Environments

How to safely use a computer, post-compromise?

yes, this is about your SmartPhone and your Laptop
(forced updates of OS and apps, not blockable
scanning of your content)

Cryptographic solutions exist in the client/server model.
But what about peer-to-peer?

First theory result in our group, «oblivious homomorphic encryption»
awaits exploration with implementations, and obfuscation approaches

C) BYOT (bring your own topic)

Many ways «to do distribution», and a BSc thesis on this question.

If you have an idea or use case:

come and talk to us!

“Project Aporia” (Ali Ajorian)

Objective: Achieve software obfuscation with provable cryptographic security.

Approach: Formalizes obfuscation as instruction decorrelation, providing a framework for mathematical proofs.

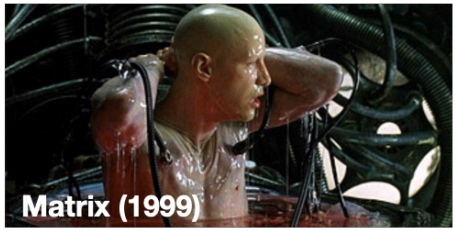
Current Status: Implementation of a compiler and interpreter

Available BSc Topics

a) Compiler Front End for Aporia: Converts high-level languages (Python, JavaScript, C, etc.) to Aporia internal language $\mathcal{L}_{\text{cfi}}$

b) Trusted-Execution Environment Support: Implementation of interpreter components on a Trusted Execution Environment (TEE).

Did you *enjoy* implementing your own chat application with Git for *Distributed Programming and Internet Architecture (HS 2024)*?

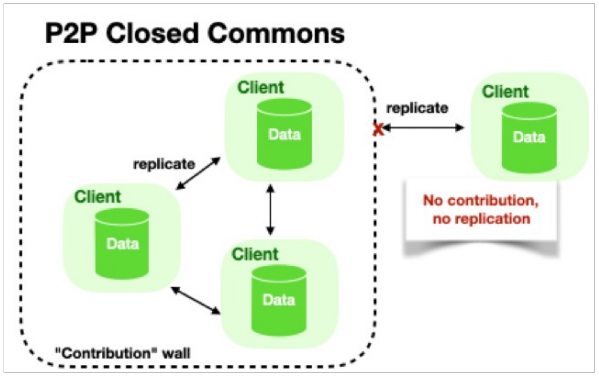


Would you like to *build* alternative networked applications where the data you produce will be shared *only with the people you actually interact with*?

Not sold to advertisers nor used to train next gen AIs...

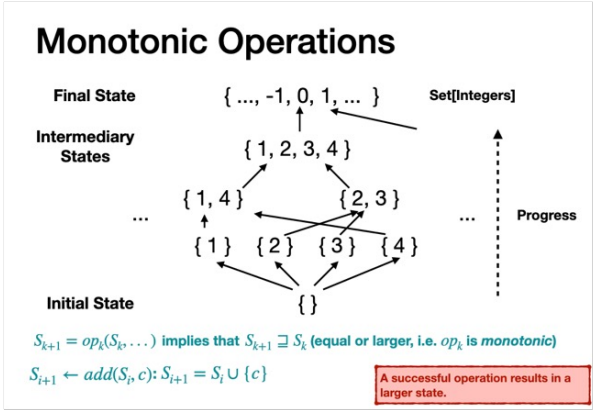
erick.lavoie@unibas.ch

New Economic Model and Crypto-Token Design



https://dl.acm.org/doi/10.1145/3631310.3633491

Eventually-Consistent Data Structures



GOC-Ledger: https://arxiv.org/abs/2305.16976

Applications

Catan

Image: Matěj Baťha, CC BY-SA 3.0 via Wikimedia Commons

Blog

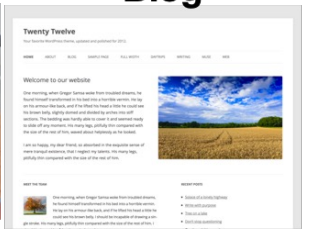


Image: WordPress foundation, GPL

Podcasting

Image: JKizzieHumanities, CC BY-SA 4.0 via Wikimedia Commons

Could lead to your own startup / indie dev career!

Last supervised theses and projects:

Jannick Heisch, "Delta-GOC-Ledger: Incremental Checkpointing and Lower Message Sizes for Grow-Only Counters Ledgers with Delta-CRDTs", Master Thesis

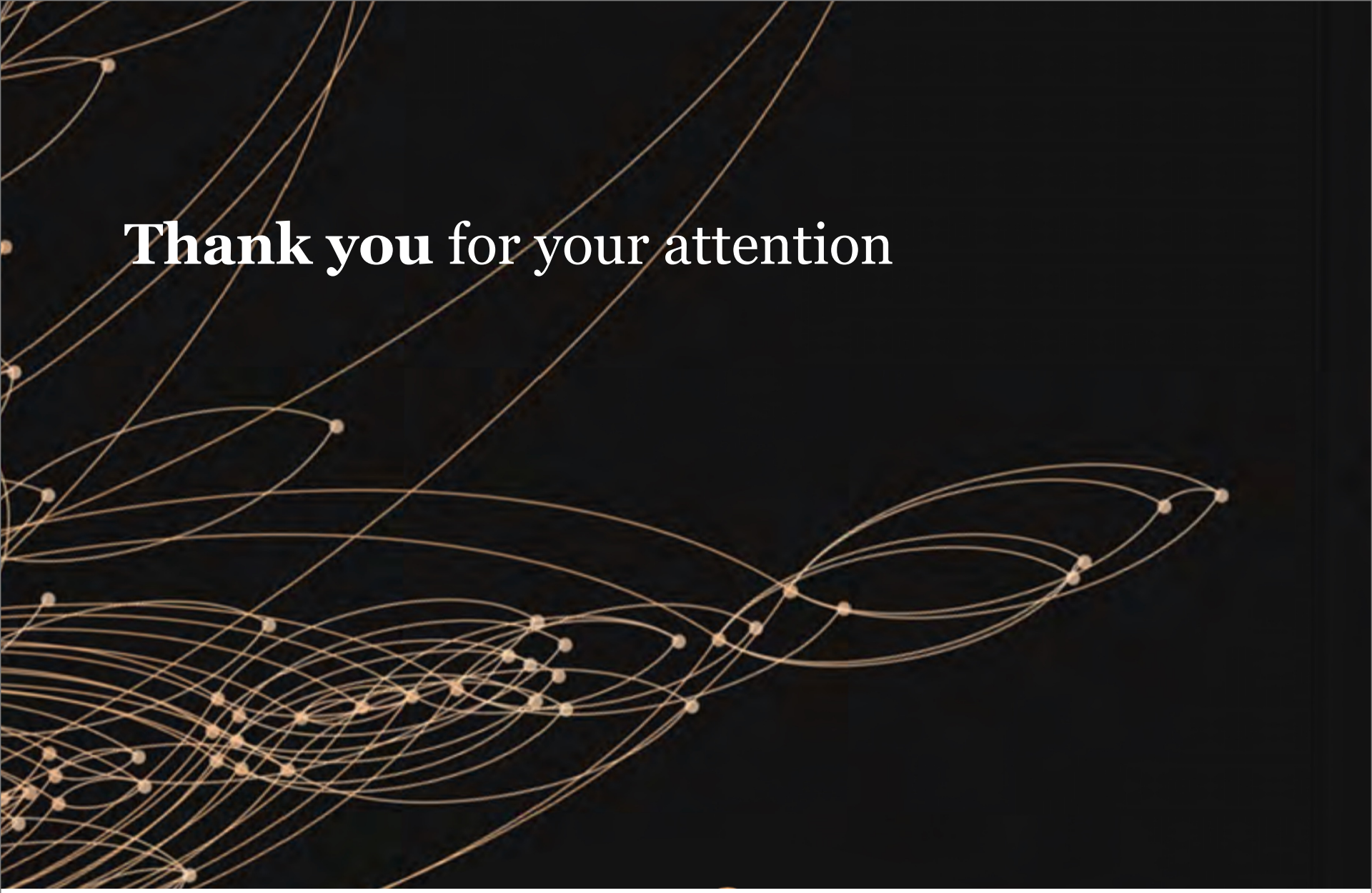
Abhilash Mendhe, "Peer-to-Peer Offline Chat Application based on CRDT", Master Thesis

Tim Matter, "Monotonic Editable Blog Data Structure with Support for Comments", Master Project

Tim Matter, "Modelling and Implementing the "Catan" Boardgame as a Replicated State Machine for Peer-to-Peer Systems", Master Thesis (ongoing)

See more BSc topics on the Web Site

- Compiler Front End for Aporia [Compilation]
- Run-Time Interleaving for Aporia [Compilation]
- Trusted-Execution Environment Support for Aporia [Interpretation][Security]
- Software Engineering of Commitment Scheme [Crypto]
- Software Engineering of Fully Homomorphic Encryption Scheme [Crypto]
- SSH-based Access Control of Server-Hosted Replicas for Git-based Applications [Distributed Systems][Git]
- Adding Pull-based Replication Hooks to Git Core [Git][C Programming][Open Source Contribution]
- Optimize the Processing Time and Memory Size of Delta-GOC-Ledger [Lower-level Programming][Optimization][Git]
- Decentralized Application Design with CRDTs [Distributed Systems][DWeb][Startup]



University of Basel