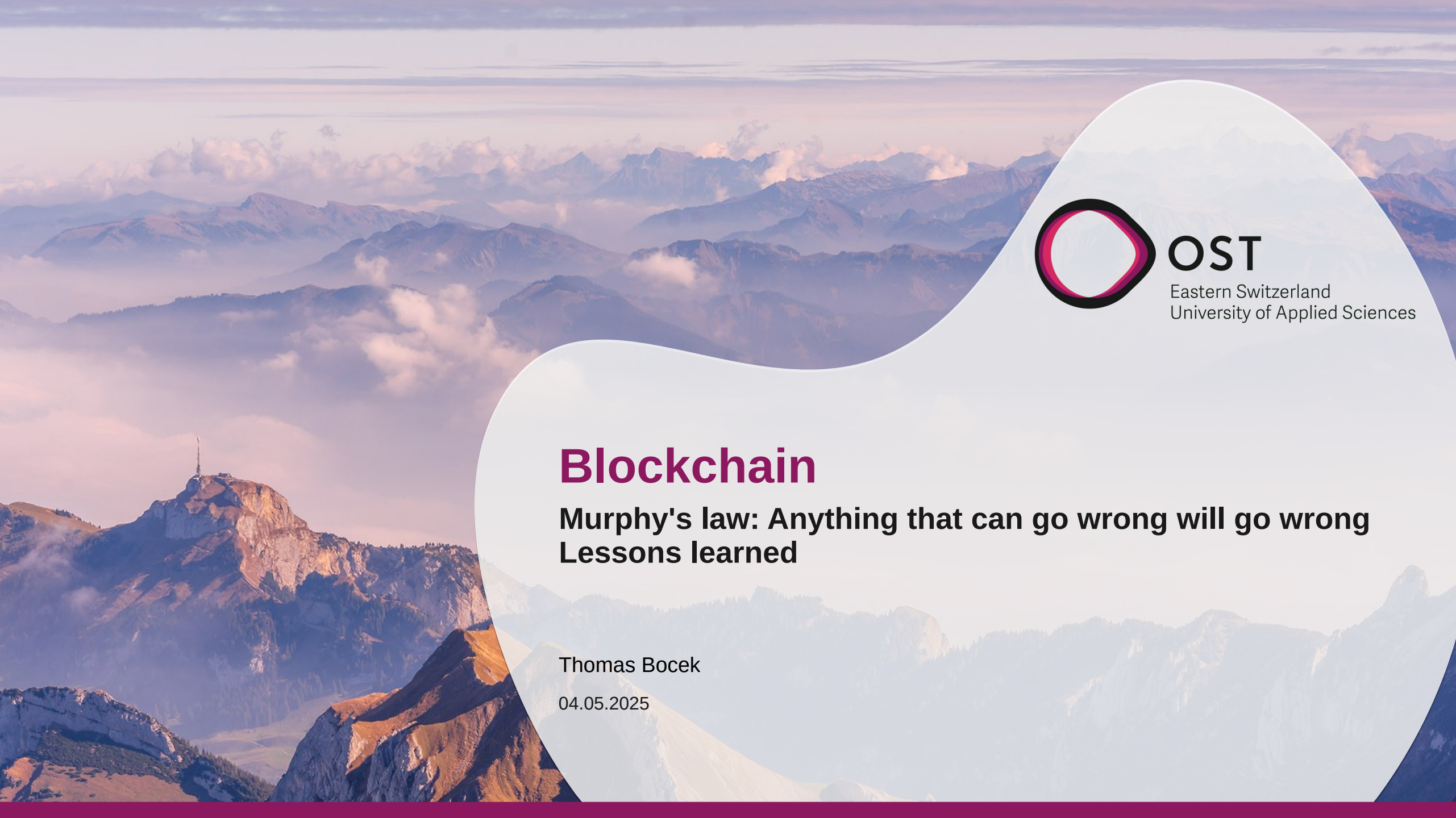


OST
Eastern Switzerland
University of Applied Sciences

Blockchain

Murphy's law: Anything that can go wrong will go wrong
Lessons learned

Thomas Bocek

04.05.2025

About Me

- Past: PhD at UZH at CSG [link]

- Now: OST, Lecturer
  - Distributed systems [link] and blockchains [link]
  - Since Corona prerecording, also on youtube [link]
  - Focus: practical implementation

- Past: Co-founder & CTO Axelra AG
  - Tech Delivery, MVP in 100 days - Digitalization / Blockchain

Universität Zürich

Lecture 11

P2P Applications and Mechanisms II

Universität Zürich[UZH]

*Original slides for this lecture provided by David Hausheer (TU Darmstadt, Germany), Thomas Bocek, Burkhard Stiller (University of Zürich, Department of Informatics, Communication Systems Group CSG, Switzerland), Larry Peterson, Vivek S. Pai et al. (Princeton University, USA), and Timothy Roscoe (Intel Research Berkeley, USA)

0. Lecture Overview

1. Introduction
2. Incentives
   1. Categorization
   2. TFT, transitive TFT
3. MapReduce
   1. Introduction
   2. Examples, Demo
4. Rsync
   1. Introduction
   2. Mechanism, Example
5. Bitcoin
   1. Introduction
   2. Mechanisms, Demo
6. Summary
7. References

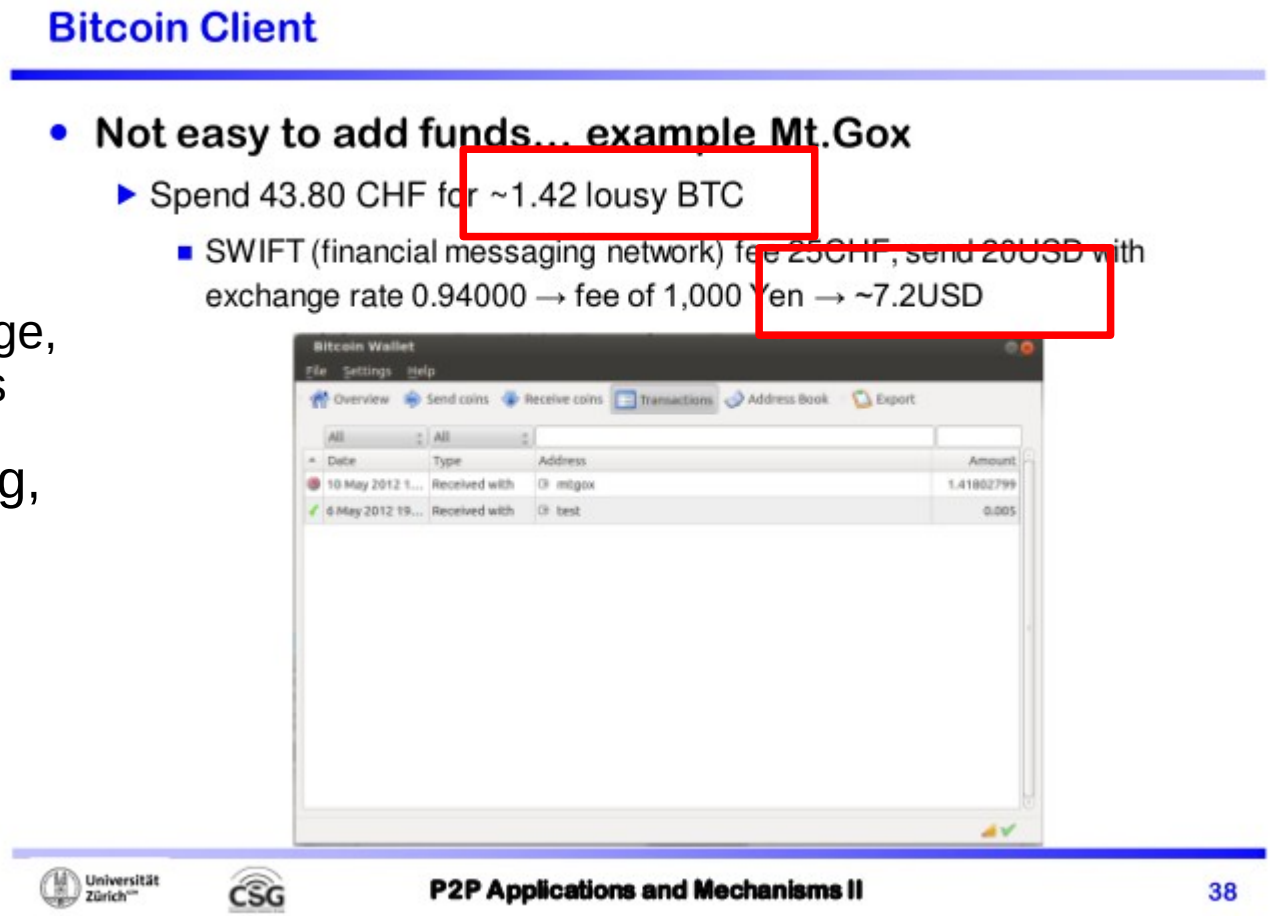
- Guilherme sent email – in 2011
- FS12, Lecture 11 → My first Bitcoin lecture
  - I was hooked :)

- Started investigating…

OST

Mt. Gox

- Bought BTC with Mt. Gox
- Mt. Gox created in 2009 as a trading card exchange for "Magic: The Gathering"
  - Between 2010-2014, largest Bitcoin exchange, handling over 70% of all Bitcoin transactions
- February 2014, Mt. Gox suspended trading, shut down its website, filed for bankruptcy
  - 880’000 BTC stolen



Mt. Gox

- Dodged a bullet: transferred almost all funds for the lecture everything to my machine…
- After bankruptcy, 140’000 BTC recovered
  - July 2024, repayment process 36% complet
  - Lost: 880k BTC in 2014 ~800USD → 704m USD
  - Payed: 140k BTC in 2024 ~65kUSD → 9100m USD
  - Mt.Gox users only received 1/6 of BTC funds, but price increased 80x
- Lessons learned: only keep small amounts on centralized platforms

  Not your keys, not your coins

OST

Smart Contracts

- Smart Contract Reviews
  - Invest lot of time to review few lines of code
    - Need to understand every side effect
    - Time-consuming → Uninterrupted focus
    - Low-medium complexity contracts - doable
- Startup: add 3 lines of logic for token lockup
  - Dodged a bullet: caught it, 2nd reviewer did not
- Startup: lets go with the expensive review company (20k)
  - Worst review (most parts just generated)

Critical

- Approve can be called when the tokens are locked → Locked investor A approves to his other account B [approve(B, all), msg.sender is A]. Locked investor calls [transferFrom(A, B, all), msg.sender is B]. Thus, the locked investor could bypass the locking. The check on line 172 needs to be done with _from and not msg.sender.

- Startup: refactoring after review
  - Factored out permission checks - white hat hacker found issue
  - Immediate action: disable the vulnerable contract
  - White hacker got reward, contract fixed
- Lessons learned: **1) Always review your smart contract. 2) After review, do not change**

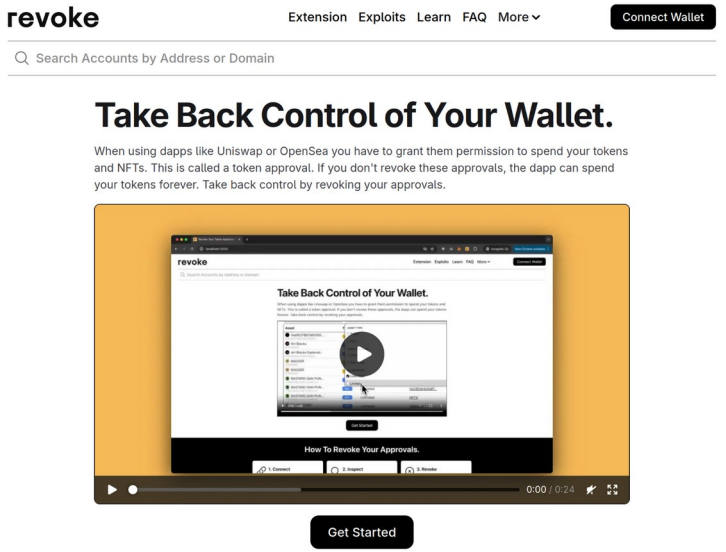
  3) Check reputation of reviewer

OST

Airdrop

- Colleague: Nice free tokens, lets try this
  - Wallet address only has few ETHs, nothing else
- It was a scam
  - Connect wallets to "verify their account" or "confirm holdings", “reserve airdrop”
  - Transaction contains approval to spend e.g., USDCs of user
  - After approval, scammers can drain USDC at any time
  - Colleague did not realize that scammer got approval, but no USDC on address, nothing happened
  - Two years later, colleague used this address to transfer funds ~4k USDC
  - Scammer watches those addresses, as soon as USDC are on this address, USDCs gone
- Lessons learned: **Always transfer in 2 tx, a small, then the rest. Check the small tx**

Verify allowances of your wallet [link]



ThorFi

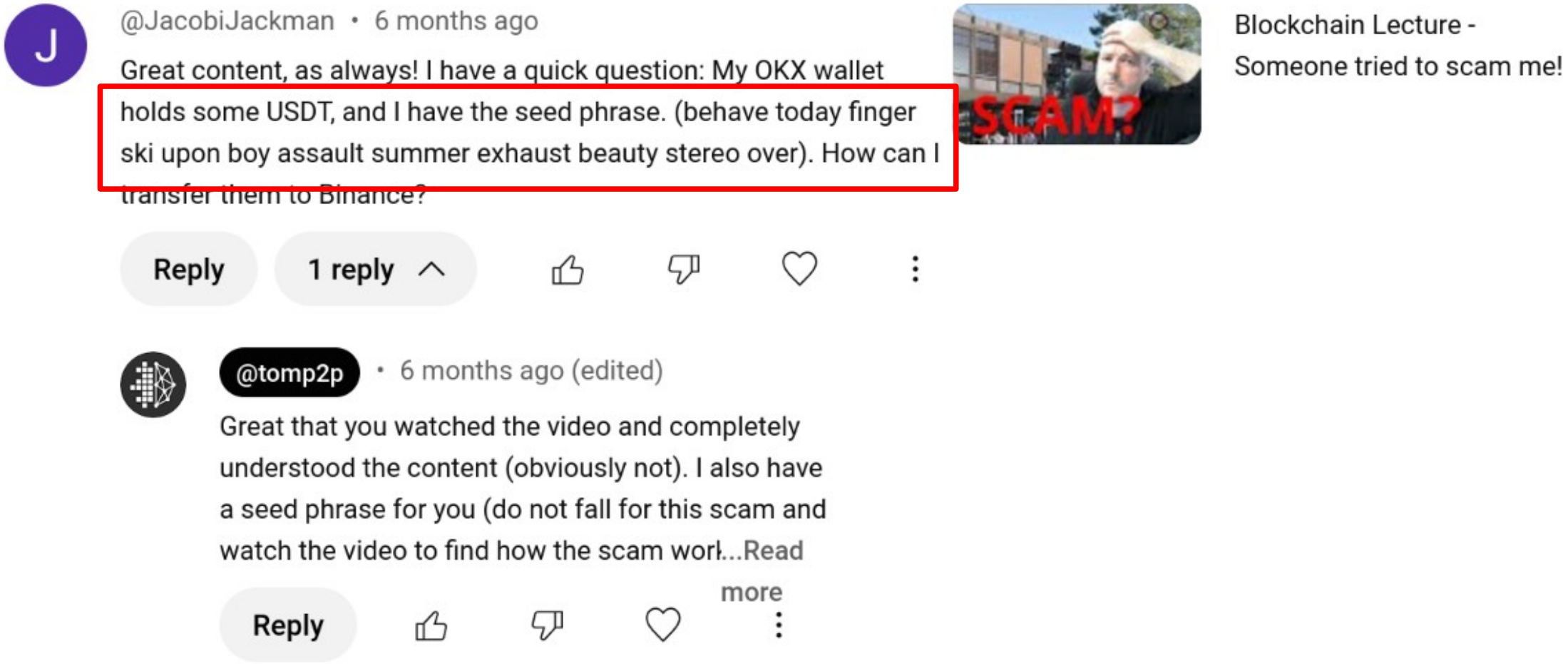
- ThorFi was a lending and savings service that operates as part of THORChain
  - Generated yield for BTC, ETH
- THORChain enables cross-chain asset swaps without wrapped tokens or centralized exchanges,
  - RUNE as internal currency
- Not centralized, so all good?
- ThorFi Savings: BTC, ETH swapped to synthetic BTC, ETH, backed by RUNE
  - Yield from swap fees – makes sense
  - But, due to RUNE exposure
    → works with strong RUNE, weak BTC
- January 2025, Strong BTC, weak RUNE: stopped - $200 million in toxic debt

- Current solution (proposal 6)
  - 200m TCY tokens, representing $1 of THORChain's debt
  - TCY holders receive 10% of protocol fees indefinitely
  - A RUNE/TCY pool starts at $0.10 with an initial $500k
  - $5m from treasury for buybacks over 10 weeks
- Lessons learned: **Try to understand the mechanisms before investing**

OST

YouTube - Scam

- Lectures online: https://www.youtube.com/@tomp2p



YouTube - Scam

- Scammers post comments appearing to be crypto beginners
  - Need help transferring funds, carelessly revealing their complete wallet seed phrase
- Wallet seems to have 20k of an obscure token
- But not enough SOL, BNB, etc. to do transaction

- Scammer monitors wallet → as soon as some BNB, SOL are transferred, scammer drains
  - Scammer scams small amount
- How to make your coin appear to valuable
  - Anyone can create and add liquidity to a token → see memecoins, SushiSwap
  - Scammer can withdraw liquidity at any time
- Ongoing since a long time, but seems to generate profit :(
  - Annoying to remove comments

- Lessons learned: **There is no free money**

OST

Questions?

Dr. Thomas Bocek
thomas.bocek@ost.ch