



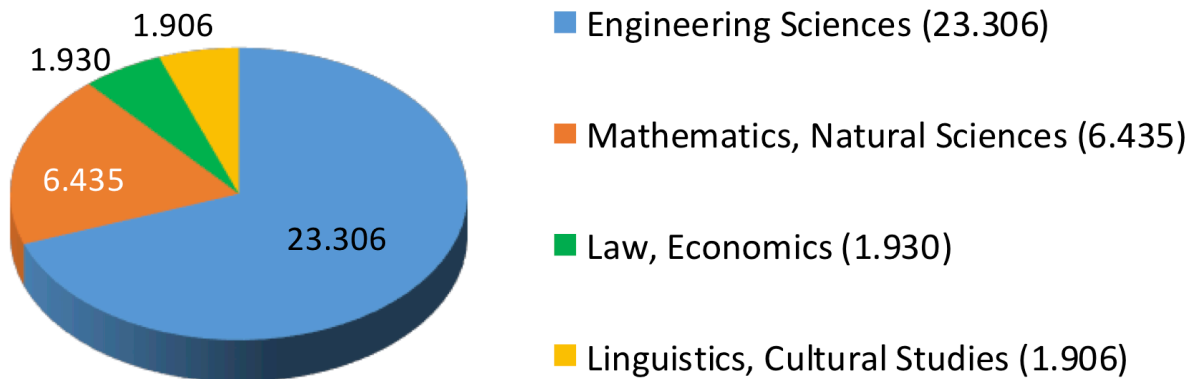
# A Response to the CITES Blockchain Challenge

Blockchain Fundamentals and Opportunities for a Secure Exchange of CITES Permits

*Dr. Anselm Busse, Prof. Dr. Stefan Tai*

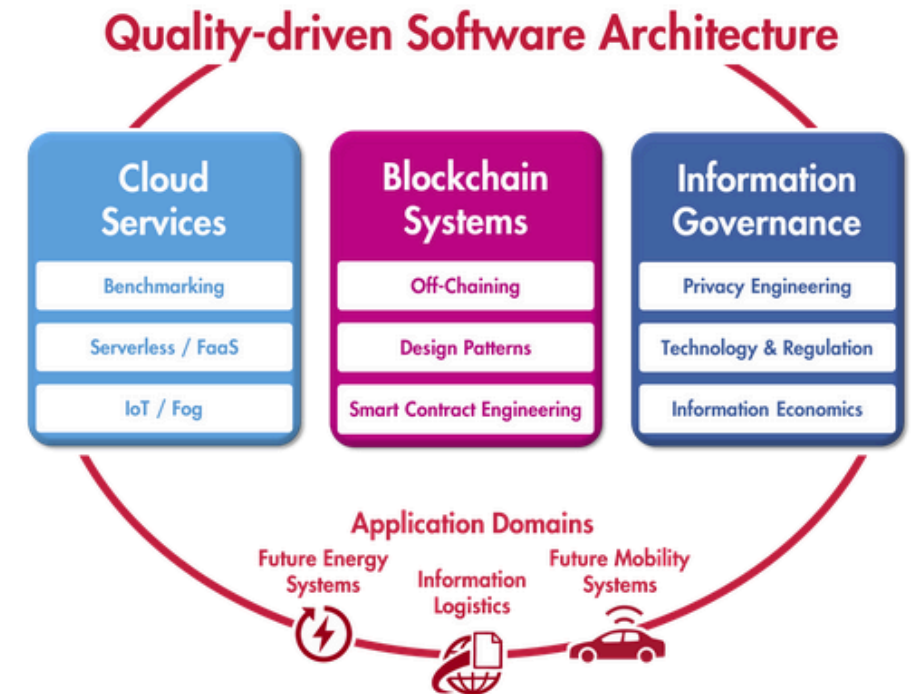
# Notes about Technische Universität Berlin

- One of Germany's largest and renowned universities, located in the heart of Berlin
- Broad international outreach
- Close cooperation between science and industry
- Over 8.300 employees
- Over 33.500 students:



# Notes about Information Systems Engineering Group

- Part of the faculty for Electrical Engineering and Computer Science
- Design and assessment of distributed, platform-based IT systems
- Shaping tomorrow's state of the art enterprise IT applications
- Close and continuous cooperation with various industry partners
- 2 PostDocs, 8 PhD candidates, student staff



## Part I: **What are Blockchains?**

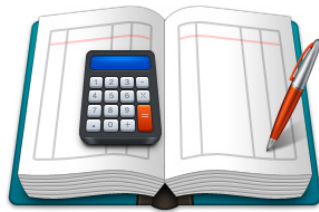
&

## Part II: **Our Response to the CITES Blockchain Challenge**

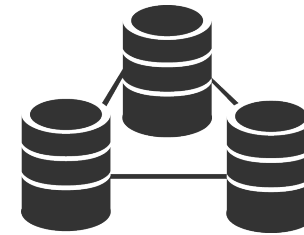
# Part I: What are Blockchains?

# What is a Blockchain: Four Perspectives

## Shared Ledger



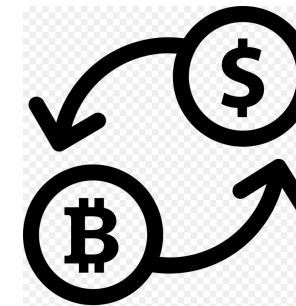
## Decentralized Database



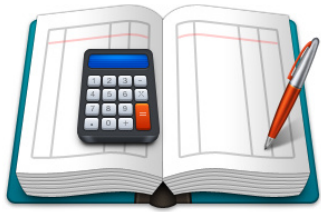
## Programming Platform



## Crypto Economy



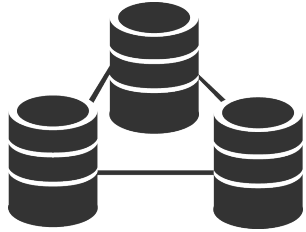
# The Business Perspective: Shared Ledger



Blockchain technology enables business disintermediation while promising lower cost of transactions.

- Cut out the middleman
- Single source of truth → Golden Record
- Open data platform for value-add services

# The Data Management Perspective: Decentralized Database



A blockchain is a special type of a peer-to-peer database with key properties:

- Stores an append-only ordered linked list of transaction records  
→ complete transaction history
- The transaction history is fully replicated among all peers using a decentralized consensus protocol
- The transaction history is practically immutable and tamper-proof (under some assumptions)

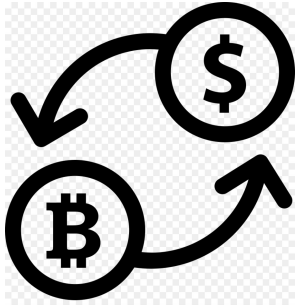
# The Developer Perspective: Programming Platform



Blockchains enable building decentralized applications (DApps)

- Smart contracts = decentralized business logic, to be executed at every node
- Emerging decentralized software stack for storage, messaging, naming, routing, etc.
- “Web 3.0”; decentralized internet

# The (Crypto-) Economic Perspective: Economic System



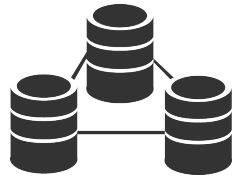
Blockchains enable the implementation of a decentralized digital currency (aka cryptocurrency).

- Payment method
- Decentralized incentive and governance mechanism
- Financing model (ICOs); Token economy

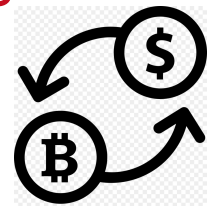
# Blockchains in a Nutshell



In summary,



blockchains are a **commonly agreed-upon, manipulation-resistant reliable source of data,**  
along with **programmable business logic** and  
**decentralized incentive and governance mechanisms**



# Part II:

# Our Response to the CITES Blockchain Challenge

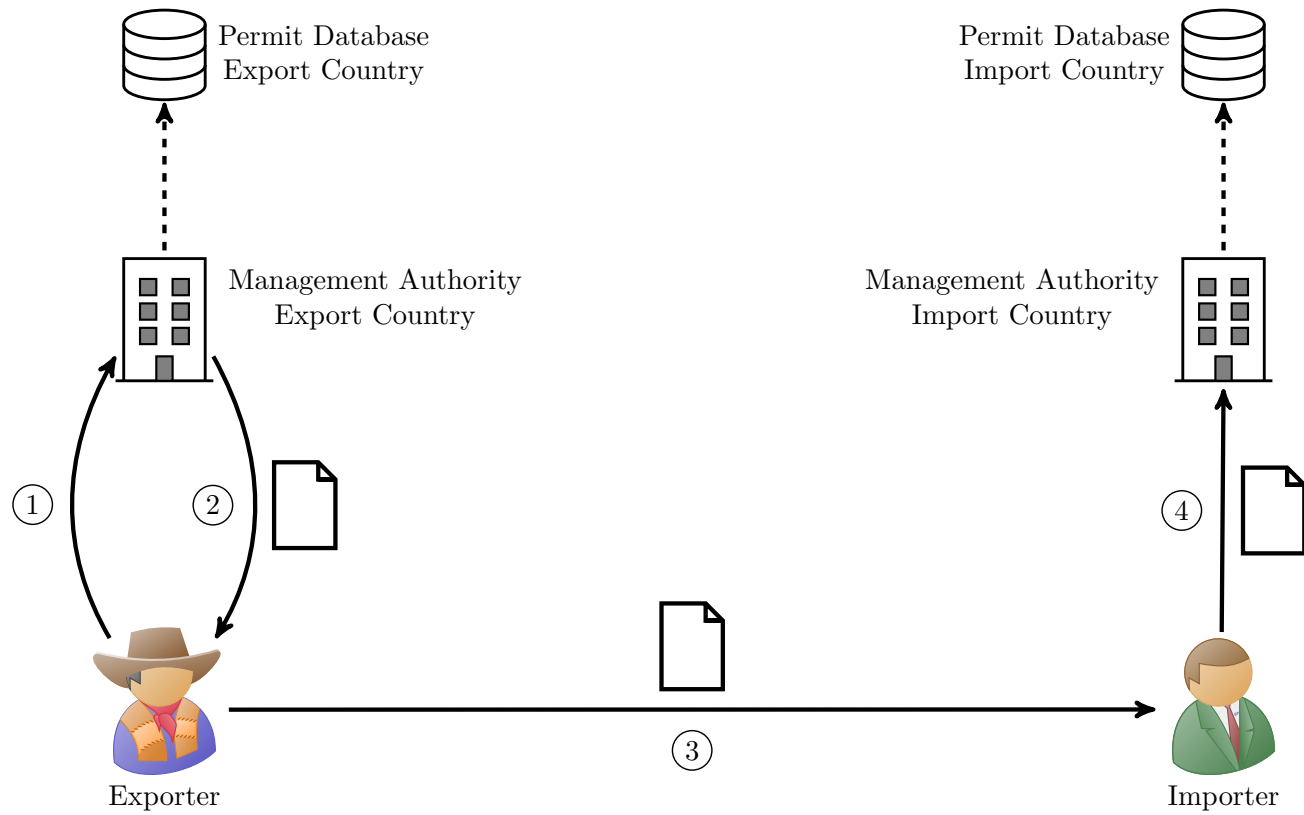
# Acknowledgement

The prototype was developed in a project at TU Berlin. The development was supported by adesso Schweiz AG. We like to thank the people who worked on and supported the project:

- Matthias Roth (adesso Schweiz AG, now Impart GmbH)
- Jacob Eberhardt (TU Berlin, PhD Candidate)
- Dong-Ha Kim (TU Berlin, Student)
- Patrick Reuter (TU Berlin, Student)
- Sebastian Frost (TU Berlin, Student)
- Thore Hans-Jörg Weilbier (TU Berlin, Student)
- Juri Alexander Zoubarev (TU Berlin, Student)
- Lukas Adam Renner (TU Berlin, Student)

# CITES Paper Permit Issues

## Paper Permit cross border workflow



Paper is relatively easy to...

- manipulate
- copy
- forge

# Improving the Permit Process

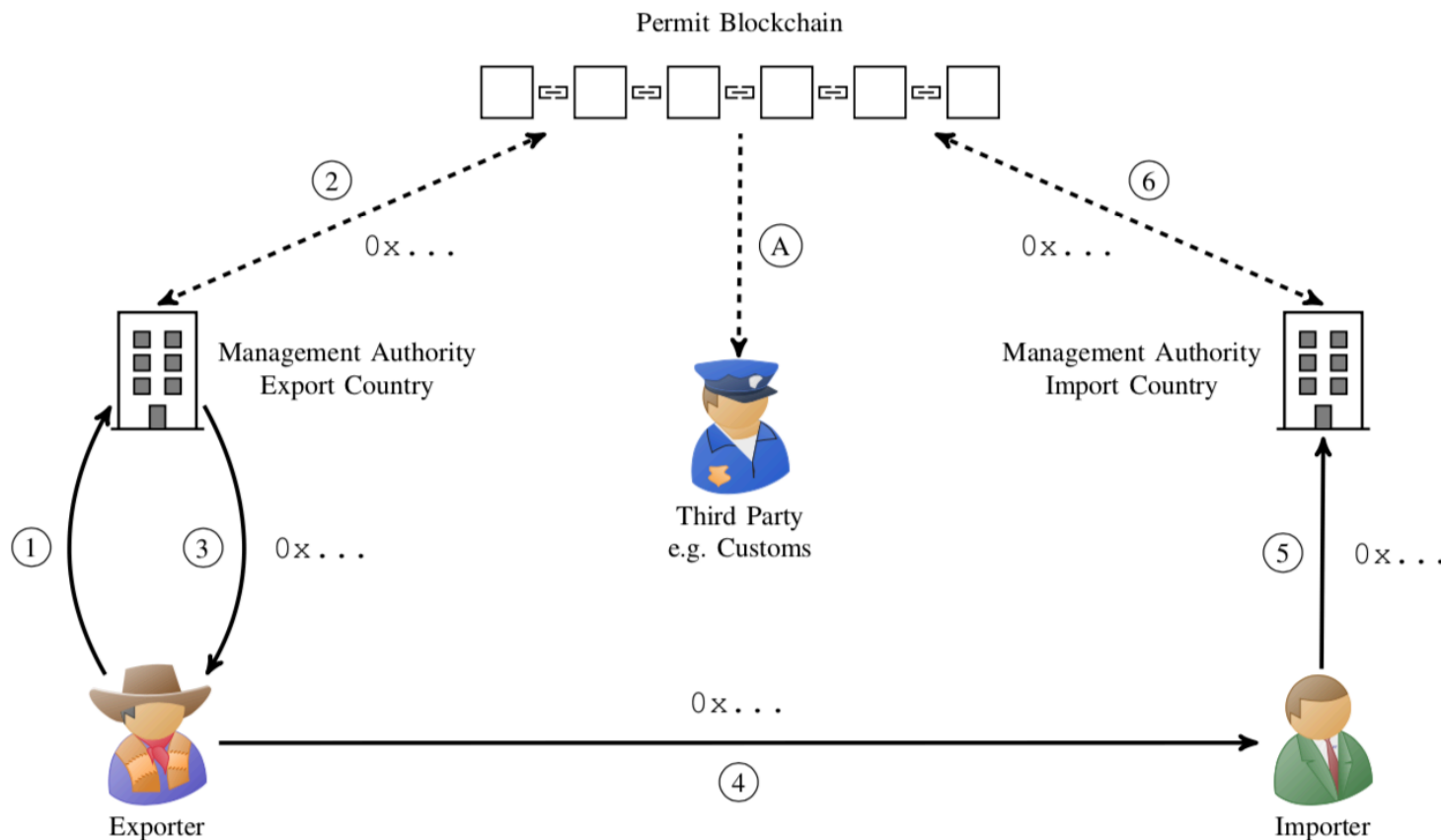
## The Goals

- Find a way to digitalize the CITES permit process (not to automate, 'only' to digitalize)
- To make the handling of CITES permit more secure
- To improve the trackability of a species

## The Restrictions

- The paper permits as they are used today should still be supported
- The permit issue process should be as it is today
- Export of a permit in UN/CEFACT ebXML format should be possible
- The clients should also run on low cost infrastructure

# Blockchain-Based Permit System



- Permit data are stored in the CITES blockchain network
- Every country has to establish a connection to the network
- No dedicated data exchange between two countries
- Shared Infrastructure reduces cost for one participant
- Lightweight clients for countries with a low IT budget

[1] [A. Busse et al., A Response to the United Nations CITES Blockchain Challenge: Incremental and Integrative PoA-based Permit Exchange, 2019 IEEE International Conference on Blockchain and Cryptocurrency \(ICBC\), 10.1109/BLOC.2019.8751373](#)

# Demo Video Lightweight Clients

## *Demo*

<https://depositonce.tu-berlin.de/bitstream/11303/9164/2/CITES%20Blockchain.mp4>

# Benefits of a Blockchain Solution in General

- **Tamper-proof**: Manipulation of information in a blockchain based system is very hard
- **Broad access**: Easy to connect from everywhere over the internet
- **Transparent**: Transaction and state information (e.g., of a permit) are visible for everyone in the network
- **Privacy-preserving**: Sensitive data can be hidden and kept confidential
- **Validated and trusted**: Third parties can easily check if information is valid or not, by direct accessing the blockchain
- **Consistent, reliable, and available**: Research and statistic can be made based on the information in the blockchain, available at each peer, without the need to collect data from distributed nodes

# Additional Benefits of the CITES Blockchain Solution

- **Parallel:** The blockchain solution runs in parallel with the existing paper, eCites and aCites solutions
- **Incremental:** Countries can join the CITES blockchain network one after each other
- **Data Analytics:** Trading and trading volumes can be analyzed continuously
- **Lightweight Clients** can be developed and distributed across the countries

A Blockchain-based CITES system is reliable, tamper-proof, and trust-building, naturally reflecting the needs of current and future decentralized CITES exchanges

## Next Steps

- From the challenge to the demo to a PoC to a viable live solution
- Looking for sponsors for a MVP (Minimal Valuable Product)
  - Revisit design decisions and assumptions
  - Refine use cases
  - Establish a CITES blockchain network as base infrastructure
  - Developing lightweight clients
- Run and improve a CITES blockchain network
- Ensure a secure, reliable and cost-efficient operation

# Let's Get in Touch

Thank you for your attention and let's get in touch!

Anselm Busse  
anselm.busse@tu-berlin.de  
**www.ise.tu-berlin.de**