An Approach for Decentralized Authentication in Networks of UAVs

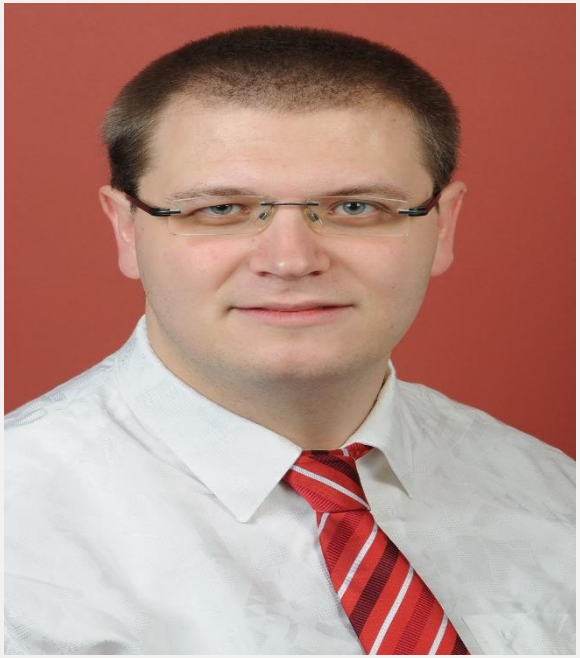
Nicholas Jäger
Andreas Aßmuth

Technical University of Applied Sciences OTH Amberg-Weiden
Department of Electrical Engineering, Media and Computer Science
Kaiser-Wilhelm-Ring 23, 92224 Amberg, Germany

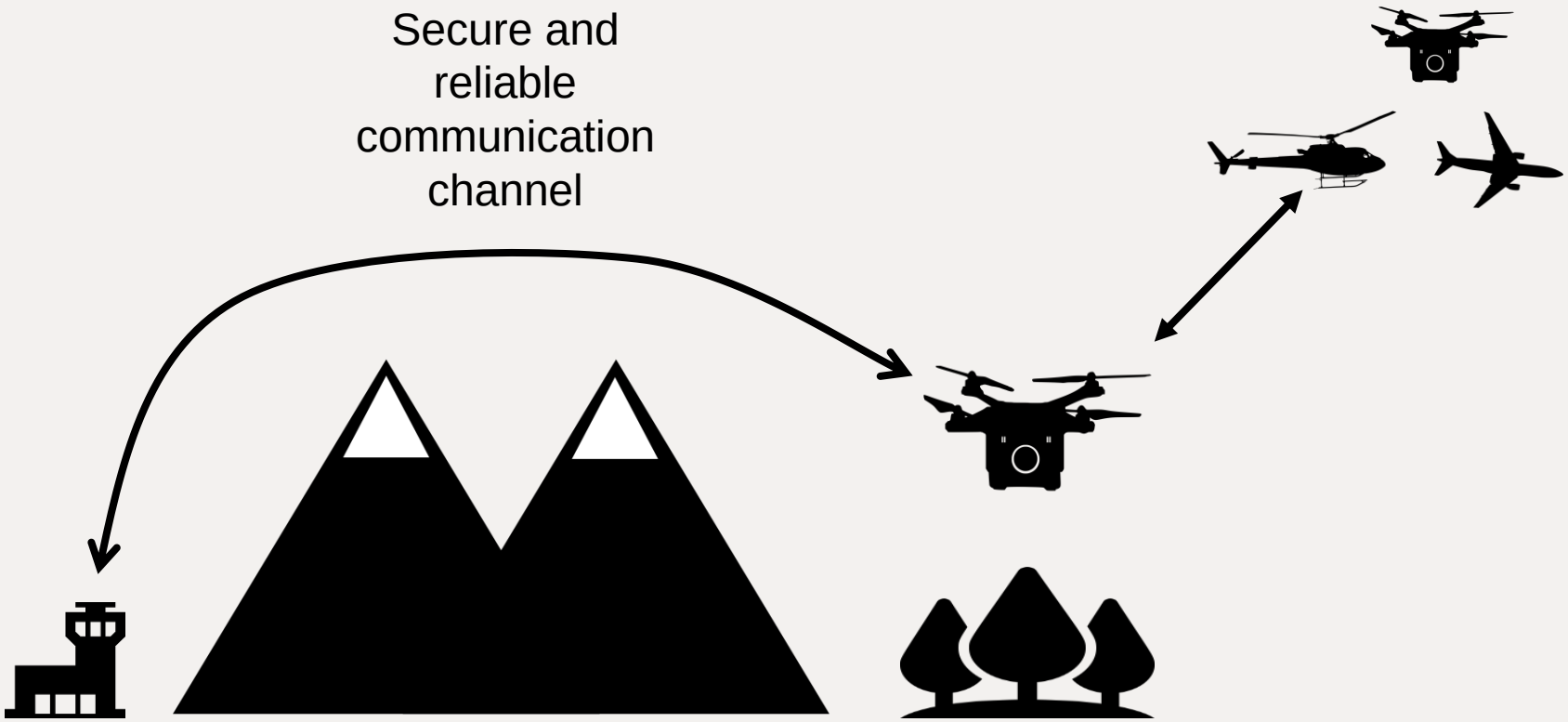
email: {n.jaeger|a.assmuth}@oth-aw.de

Short resume

- Nicholas Jäger
  - 2017-: Research Assistant at Technical University of Applied Sciences OTH Amberg-Weiden, Germany
  - 2008-2017: Study of physics and catholic theology at Johannes Gutenberg Univeristy Mainz, Germany
    - 2012 Bachelor of Science (physics)
    - 2017 Master of Science (physics), Diplom-Theologe



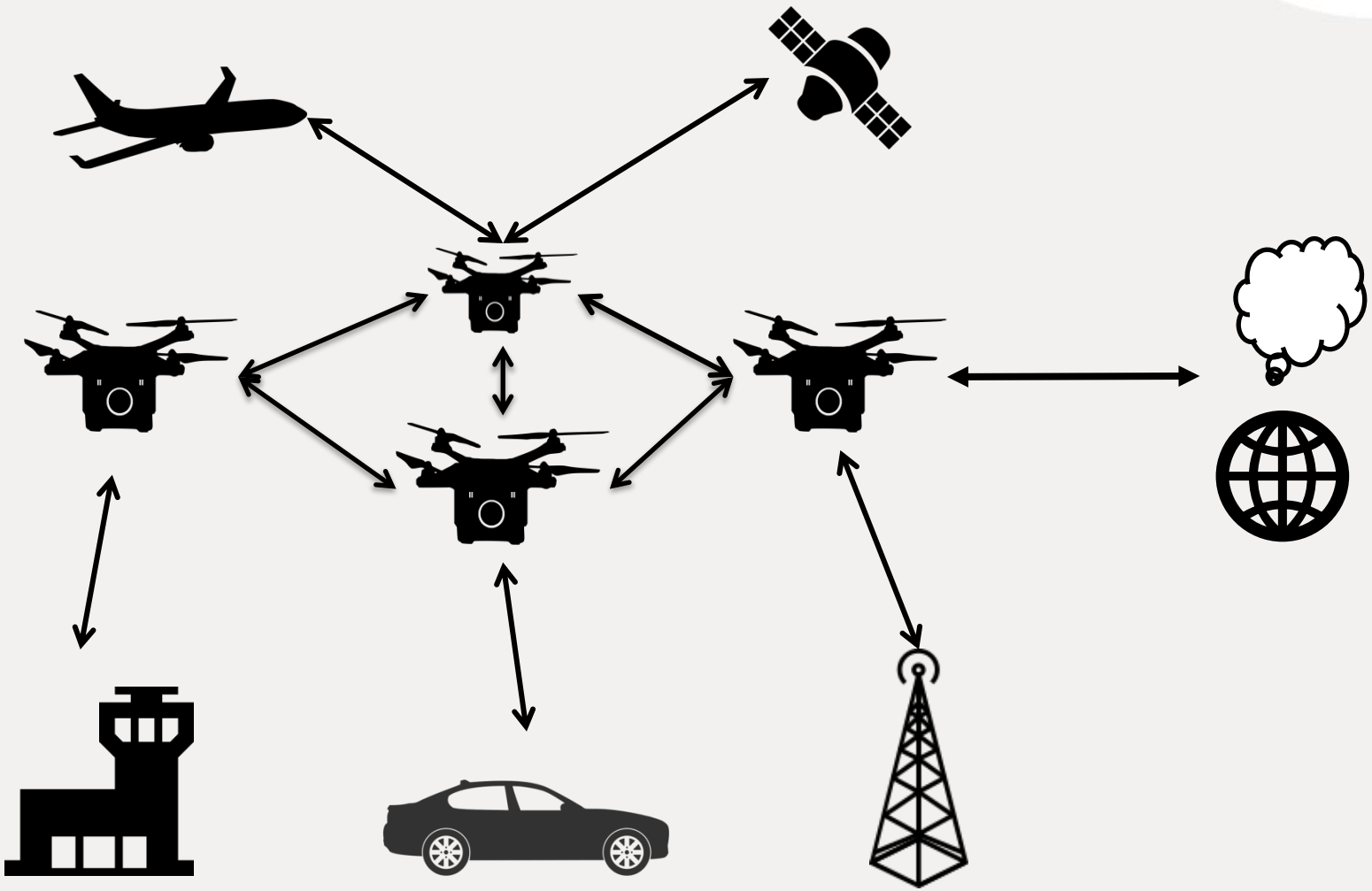
UAVs operating beyond visual line of sight



ground station, operator

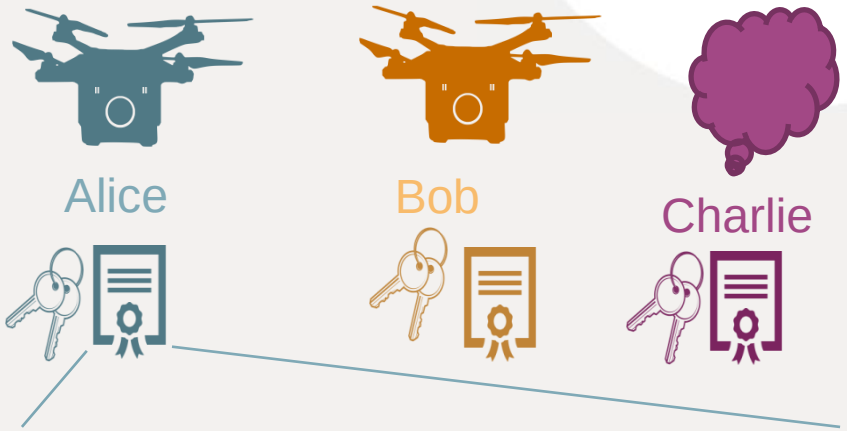
area of operation

Flying Ad-hoc Network (FANET)



Public Key Infrastructure (PKI)

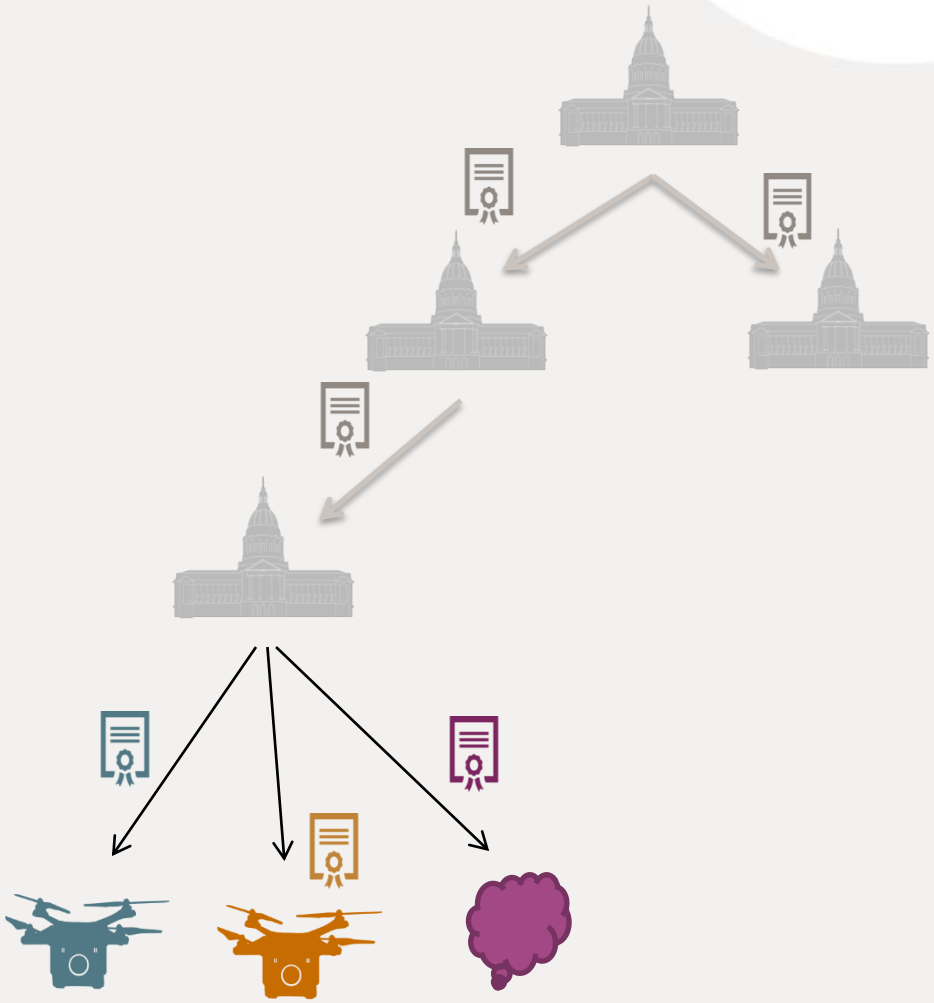
- Public Key Cryptography
  - Each entity has a pair of keys: a public and a private key
  - Certificates confirm the link between entities and public keys
- PKI types
  - Hierarchical
  - Peer-to-peer



Certificate	
Subject	Alice
Public Key of Subject	
Issuer	X
Public Key of Issuer	
…	…
Signature	

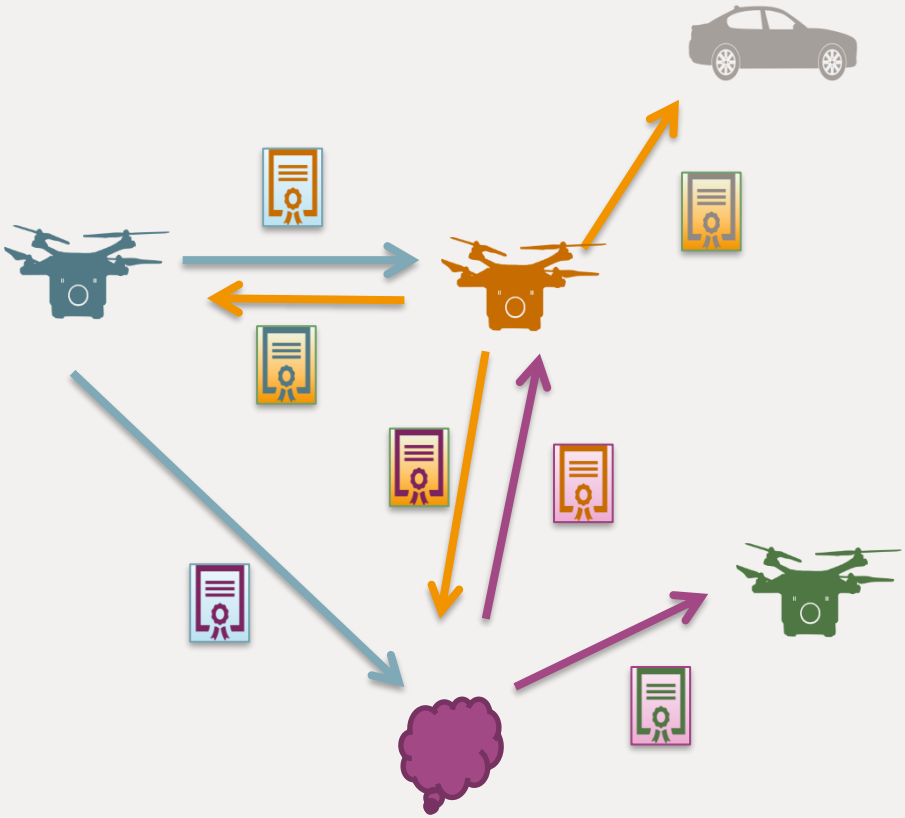
Hierarchical PKI

- Certificates are issued and managed by a central authority, trusted third party (TTP)
- Hierarchical Trust model
- Independent hierarchical PKIs build a network
- Weaknesses:
  - Single point of failure
  - Large infrastructure required

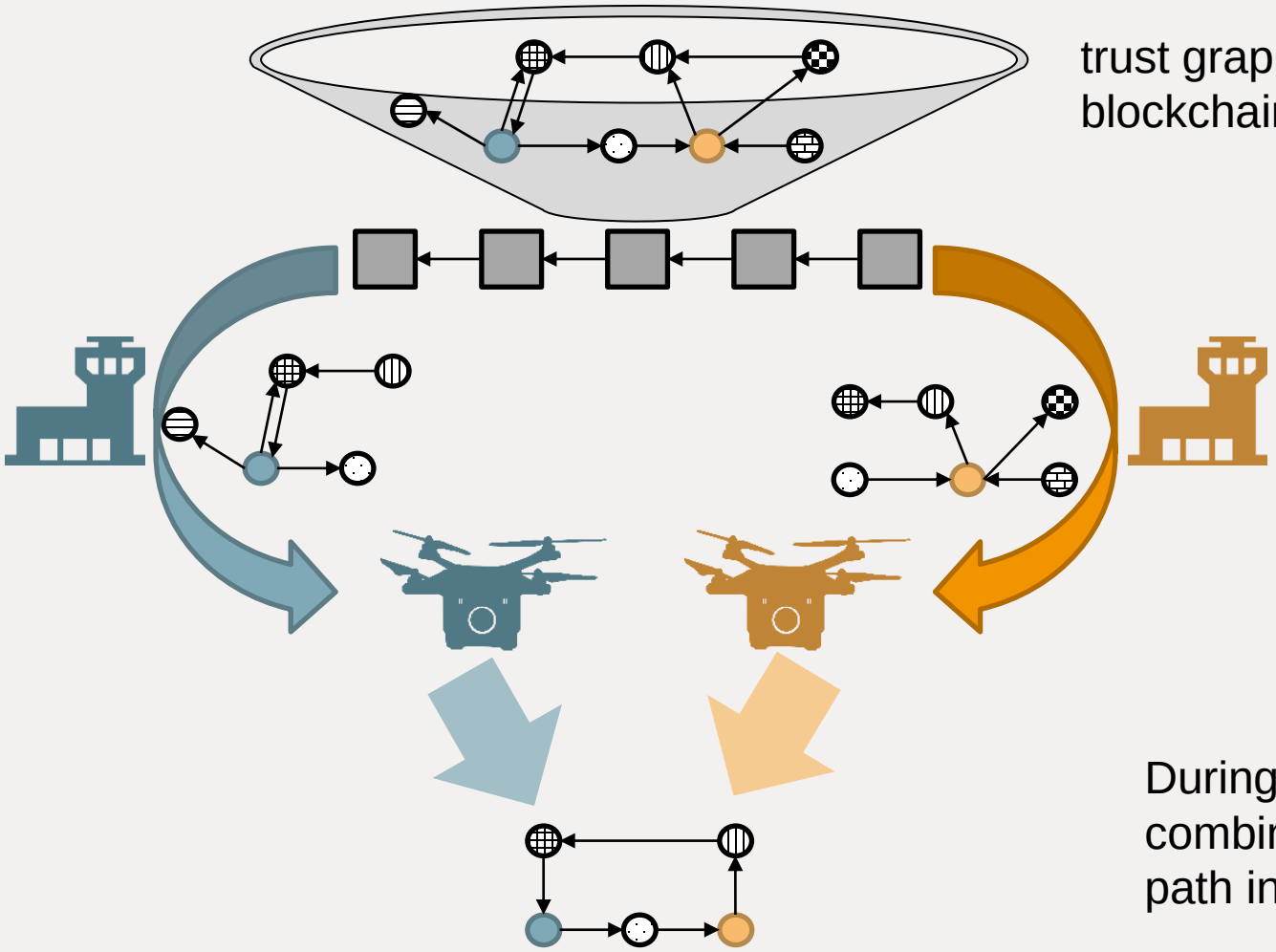


Peer-to-Peer PKI

- Users certify each other
- Peer-to-peer trust model
- Users share certificate information about each other
- Weaknesses:
  - High entry barrier
  - Easy introduction of malicious information
  - High requirements on each user



Overview of the Approach



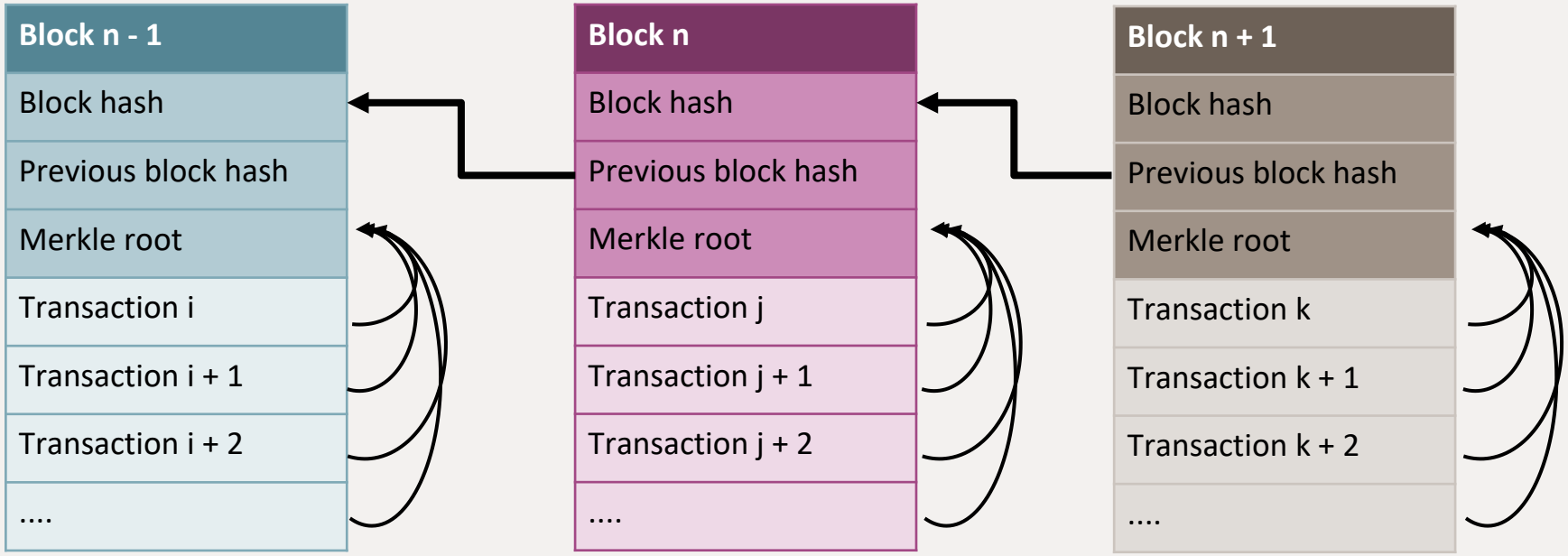
trust graph is stored on the blockchain

Before mission: selected parts of the graph are transferred to the UAV

During mission: UAVs combine their parts to find a path in the graph

Blockchain

Data structure with cryptographic connections distributed in a peer-to-peer network



Types of Transactions of the blockchain system

Ostbayerische Technische Hochschule
Amberg-Weiden

Token Creation:	• Alice is rewarded with 10 tokens
Token Transfer:	• Alice sends Bob 5 tokens
Public Key Binding:	• Alice publishes her public key and her identity information
Confirmation:	• Alice confirms that Bob actually controlls his public key
Revocation:	• Alice revokes her previously given confirmation of Bobs public key binding
Other types:	• For example: Deletion of own public key

Trust Model

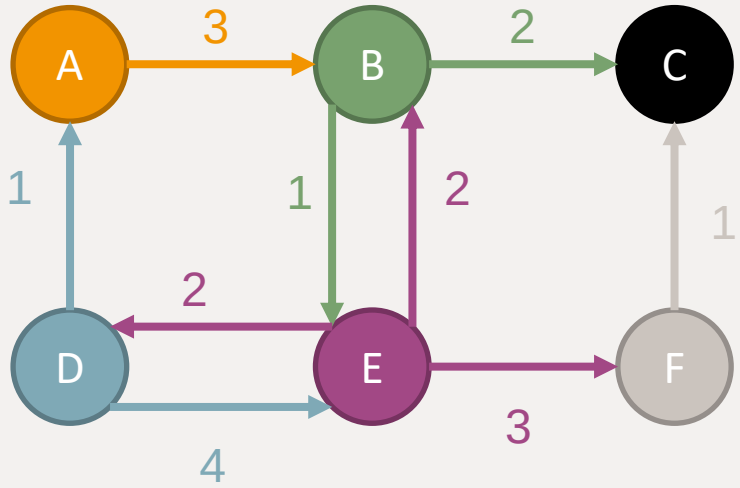
Goal: Finding a valid path to the destiny in the trust graph

Nodes
- public keys and identities

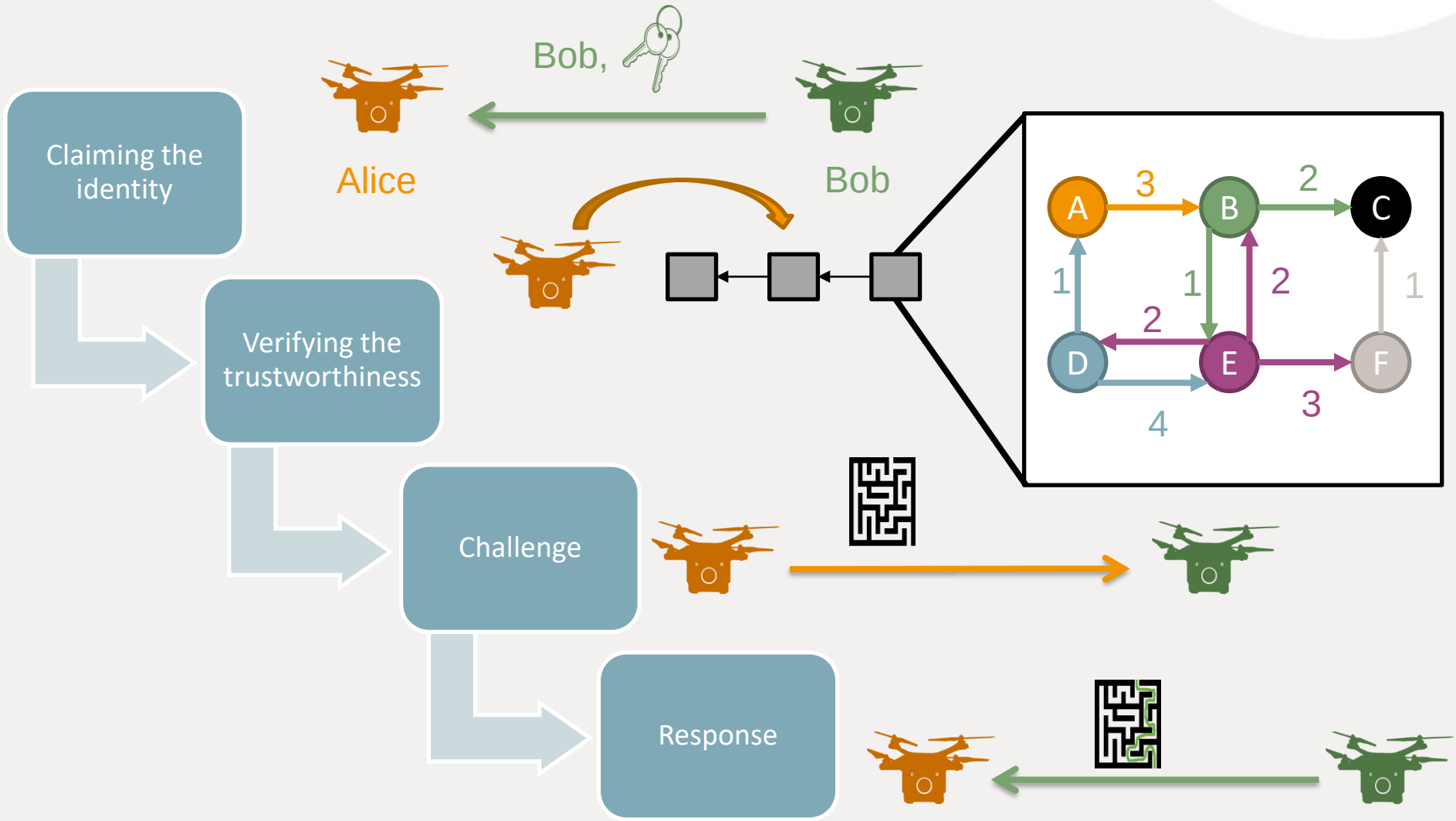
Directed Edges
- confirmations

Edge Weight
- Maximal allowed path length starting with this edge

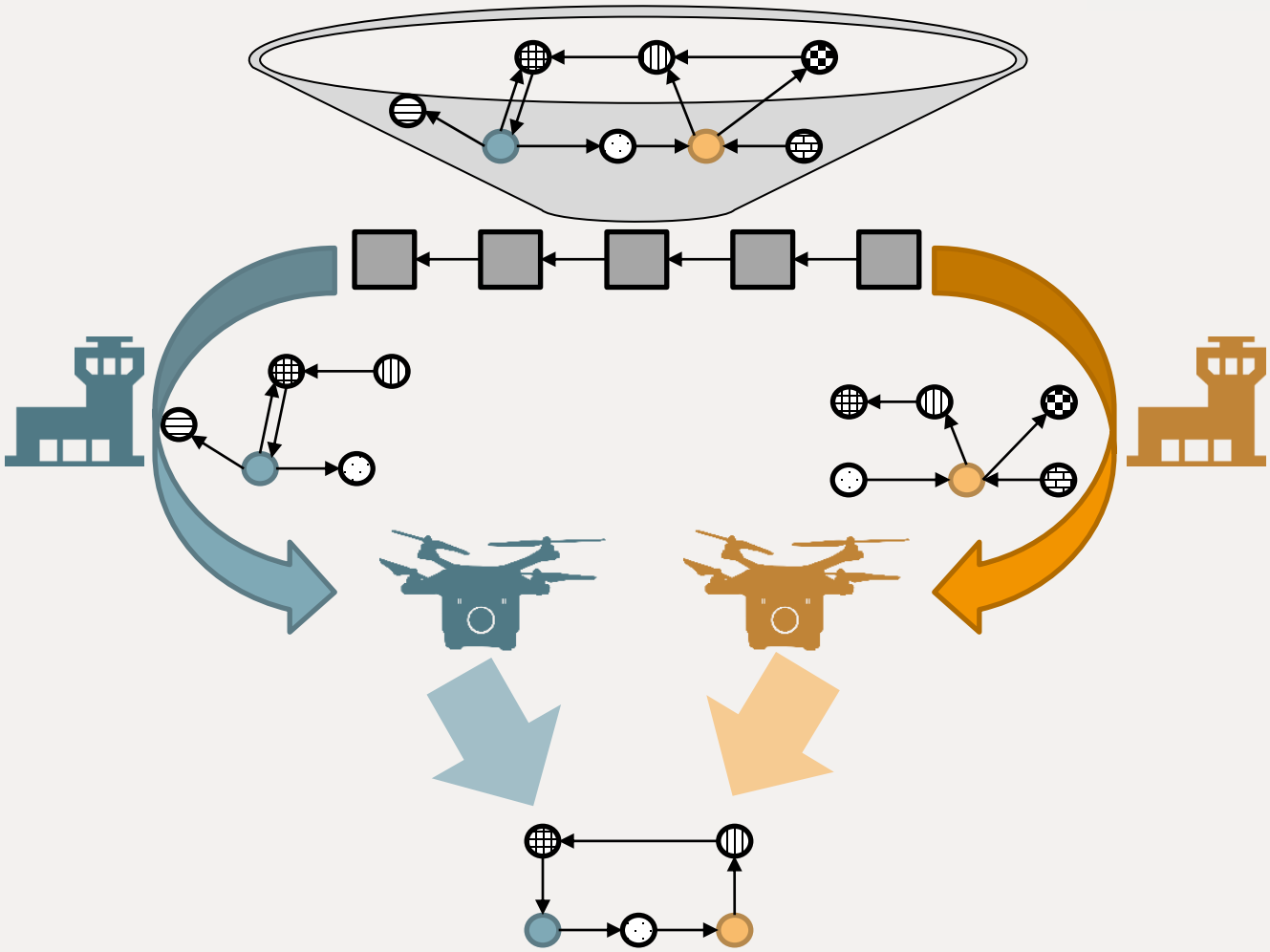
Trust graph



Authentication



Summary



Ostbayerische Technische Hochschule
Amberg-Weiden

Thank you very much for your attention!

ADACORSA

Adacorsa is supported by ECSEL Joint Undertaking (JU) under grant agreement No 876019. The JU receives support from the European Union's Horizon 2020 research and innovation programme and Germany, Netherlands, Austria, Romania, France, Sweden, Cyprus, Greece, Lithuania, Portugal, Italy, Finland, Turkey.

ECSEL Joint Undertaking
Electronic Components and Systems for European Leadership