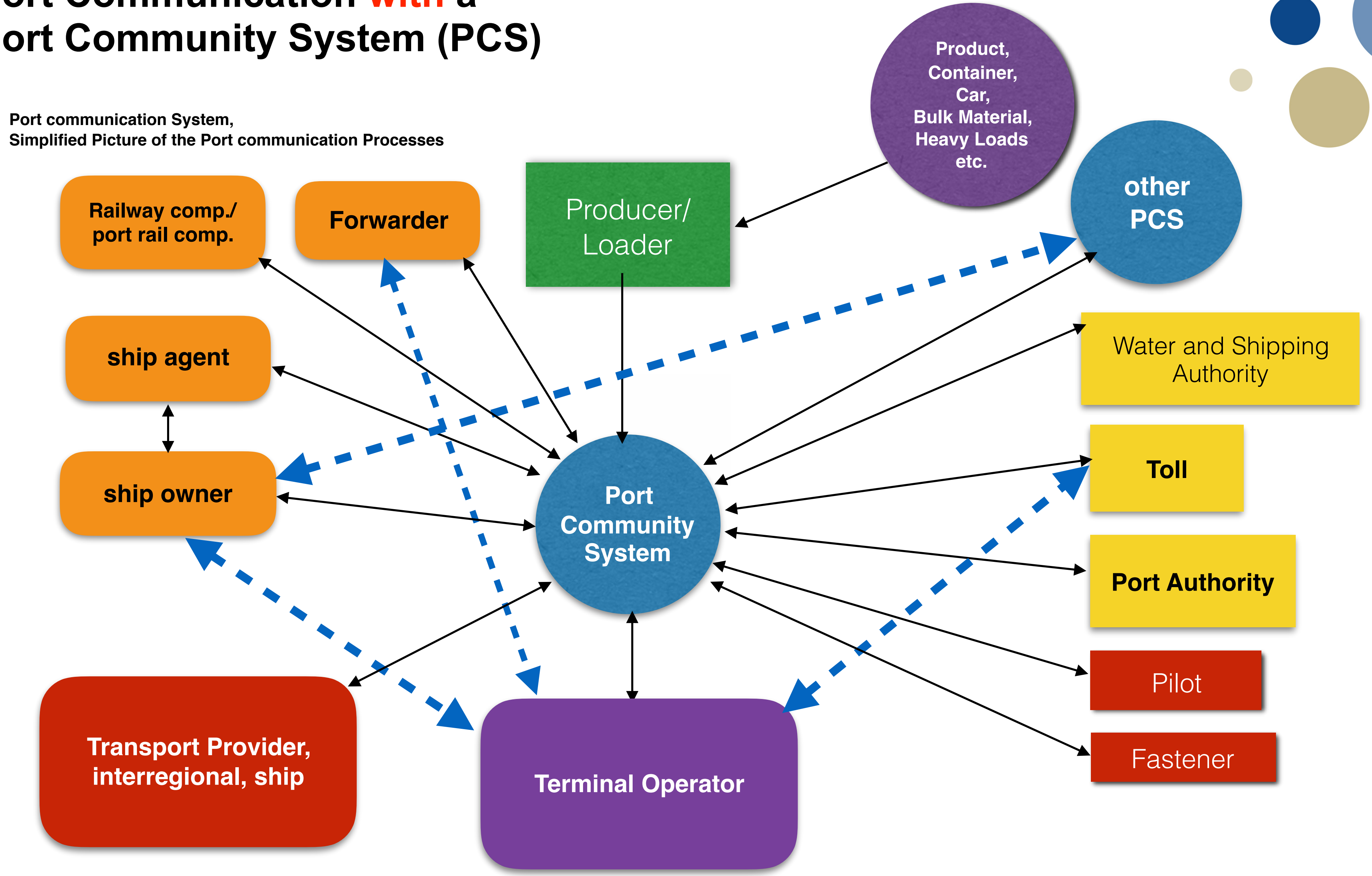
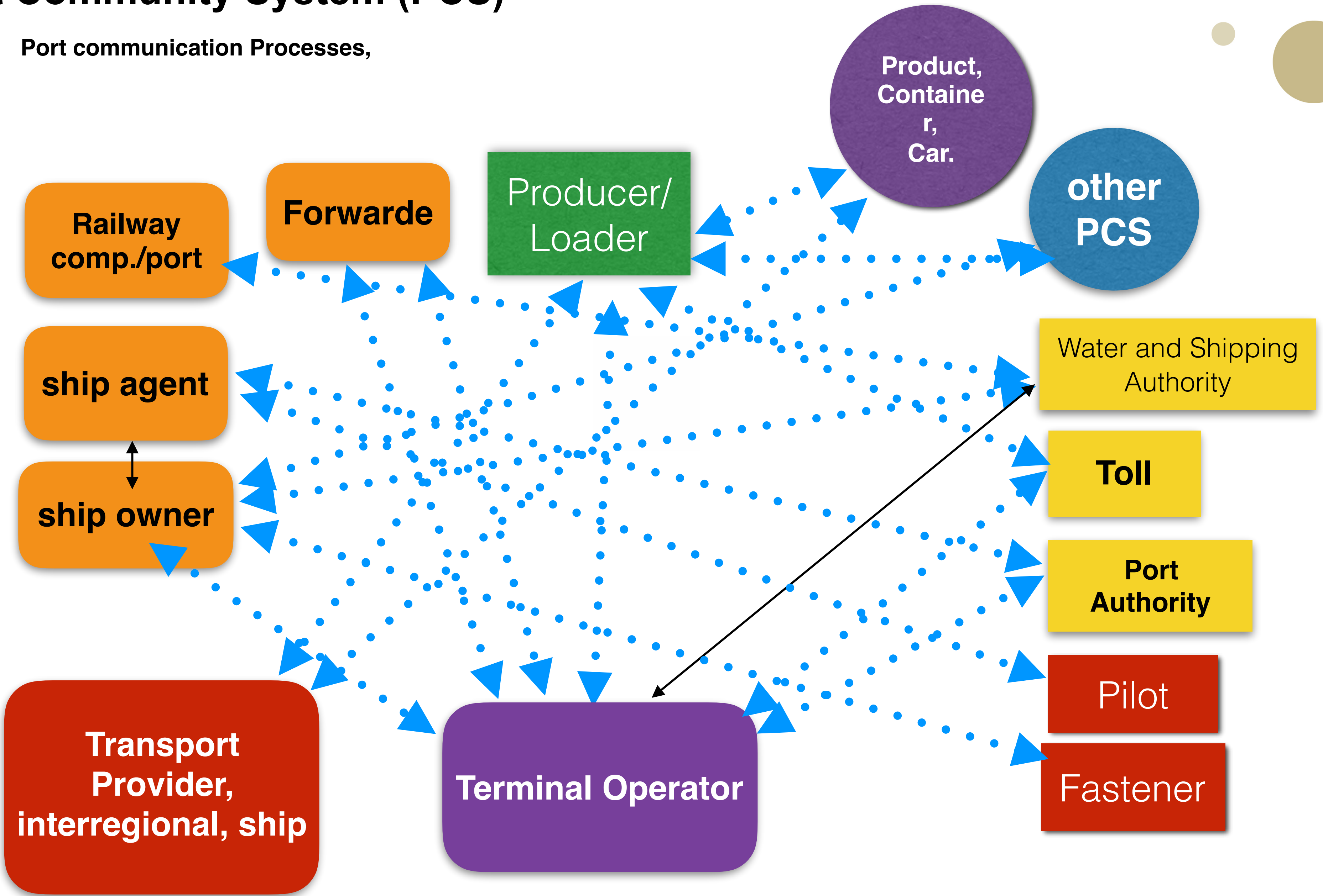
Port Communication with a Port Community System (PCS)

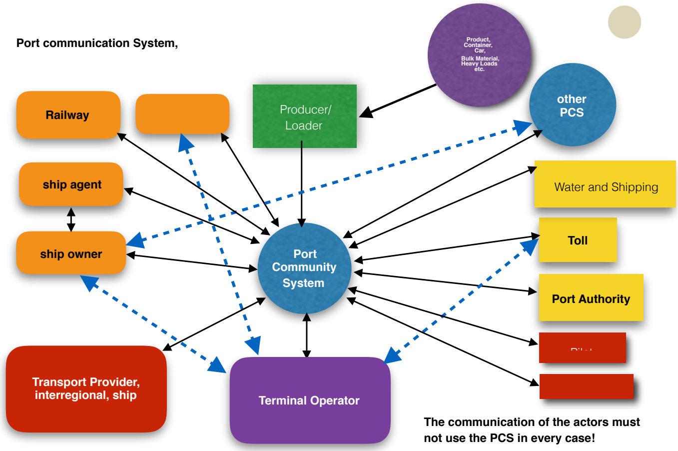


Port Communication without Port Community System (PCS)

Port communication Processes,



- The Port Communication Systems were developed during the last 20-30 years
- based on:
  - EDIFACT messages
  - database access
  - file exchange



- There is no **Security Architecture** existing for the Port Communication Systems
- There are no risk assessments existing for the Port Communication Systems

We need:

- Security Architecture
- Resiliency behaviour of the Port Communication System
- Migration models towards a secure Port Communication System

Research Project in Germany and in Norway (proposal)

Goals:

Develop a
Secure and Reliable Port Communication System
for the port, transport and logistics industry

Develop a **Security Model** for the
Port Community Communication System

Adopt a **Resiliency Model** to mitigate attacks against one or more partners - without a shutdown of the entire system

What do we need to implement Information Security?

Firewall

AES 256

Blockchain

Research Project in Germany and in Norway (proposal)
Goals:

Develop a
Secure and Reliable Port Communication System
for the port, transport and logistics industry

Develop a **Security Model** for the
Port Community Communication System

Adopt a **Resiliency Model** to mitigate attacks against one or more partners
without shutdown of the entire system

Improve the security of distributed communication systems by using
Blockchain technologies (DLT)

Develop a **Migration Strategy**

13

SecProPort

Hapag-Lloyd

duisport
excellence in logistics

BLG LOGISTICS

Universität Bremen

ISL

dbh
dbh Logistics IT AG

DFKI

datenschutz cert

SecProPort: Scenario Driven Project

Demonstration and evaluation of the project:

The Security Model will be realised and evaluated by setting up Scenarios together at and with the industrial project partners.
Potential Scenarios could be:

- Container terminal: information and data exchange along the transport chain of container transport
- XXL-Logistics: Paper rolls, locomotives, wind mills, etc.
- Intermodal terminal: train-road, train-port, road-port
- Single National Window
- …

SecProPort: Process analysis:

Example: Container Export:

Phase 1: Order export

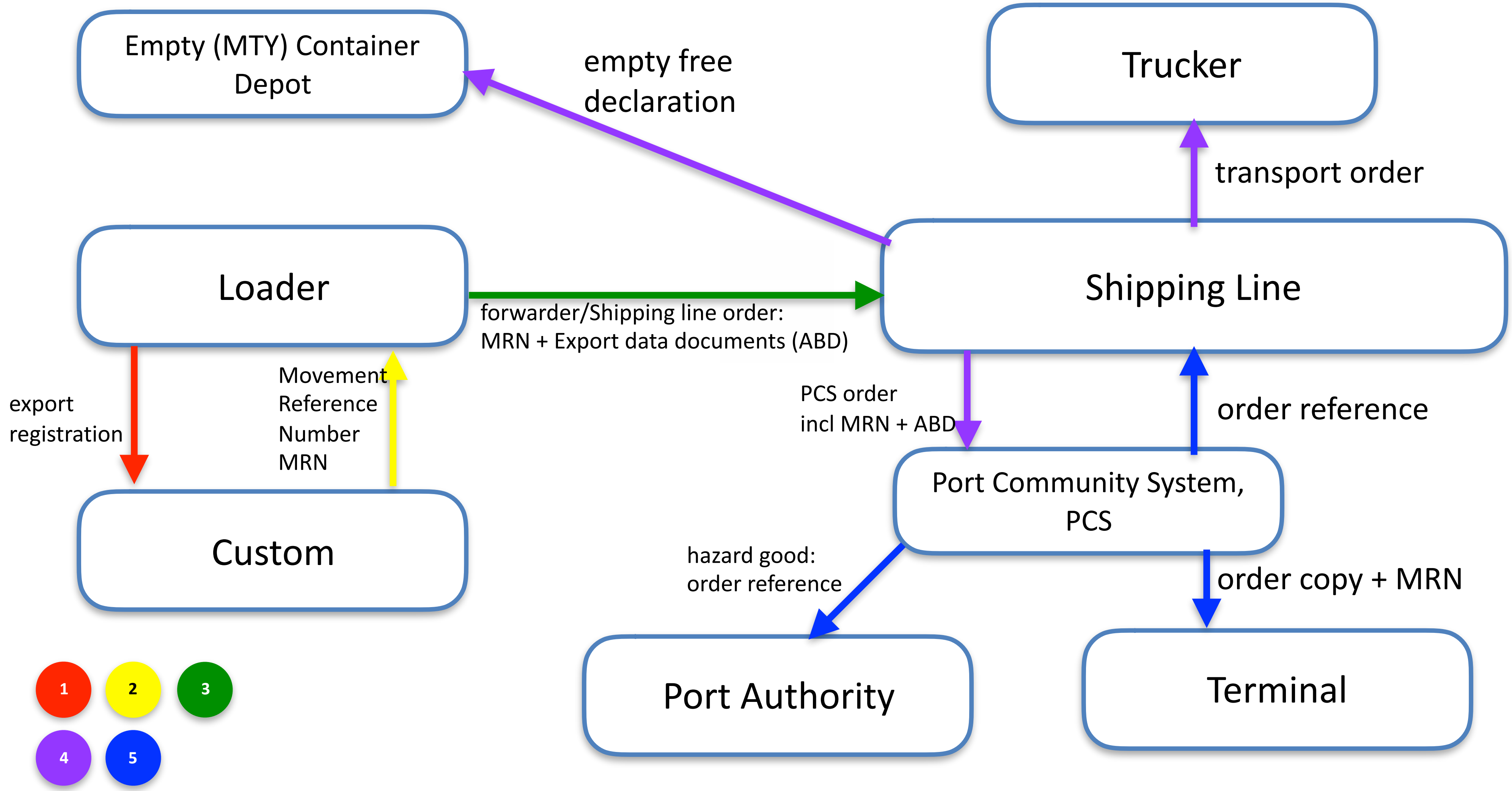
Phase 2: Start transport to the port,
planing ship handling

Phase 3: Delivery of the container by truck

Phase 4: Ship loading

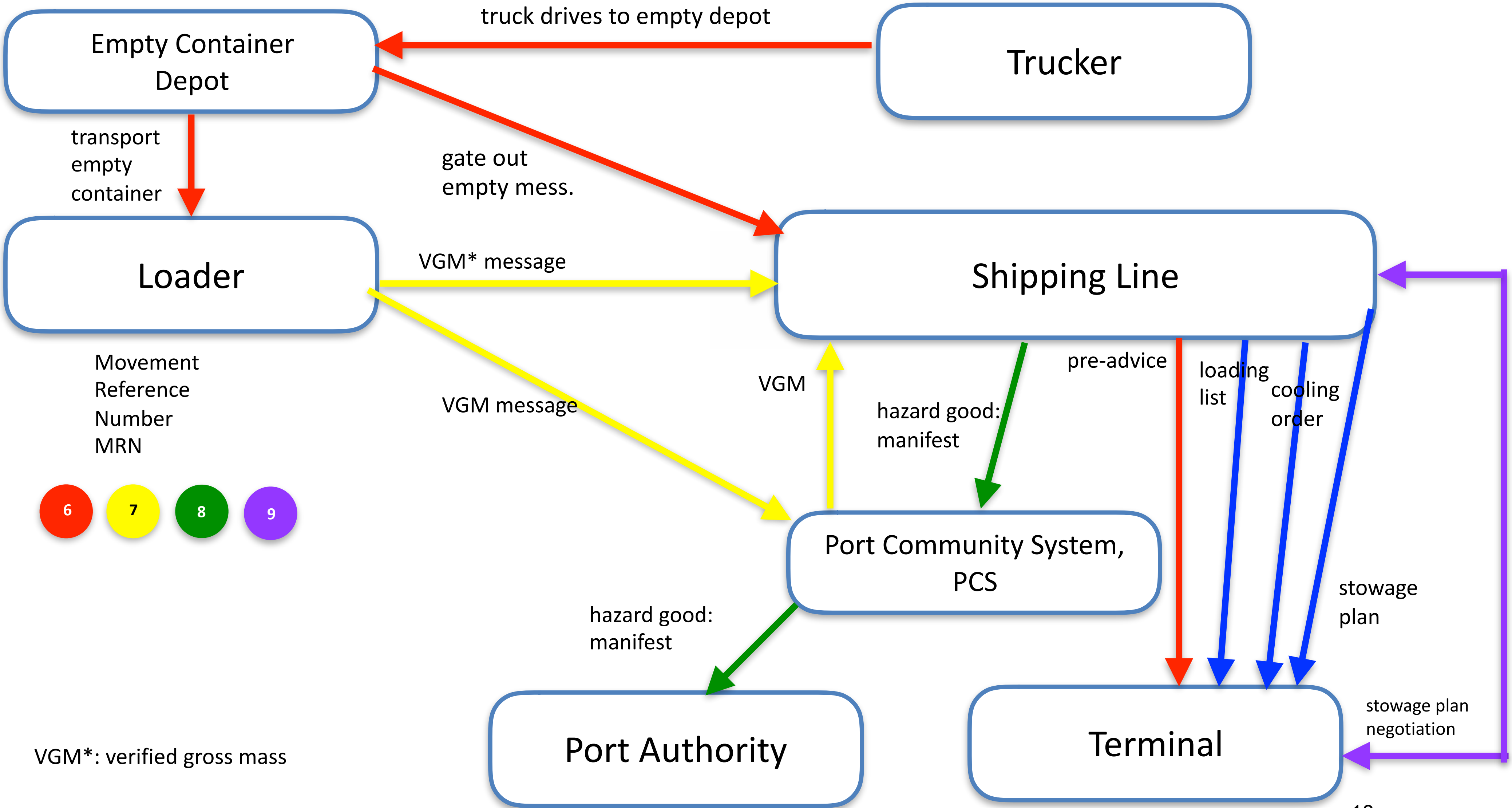
SecProPort: Process analysis:

Container: 1. Order export



SecProPort: Process analysis:

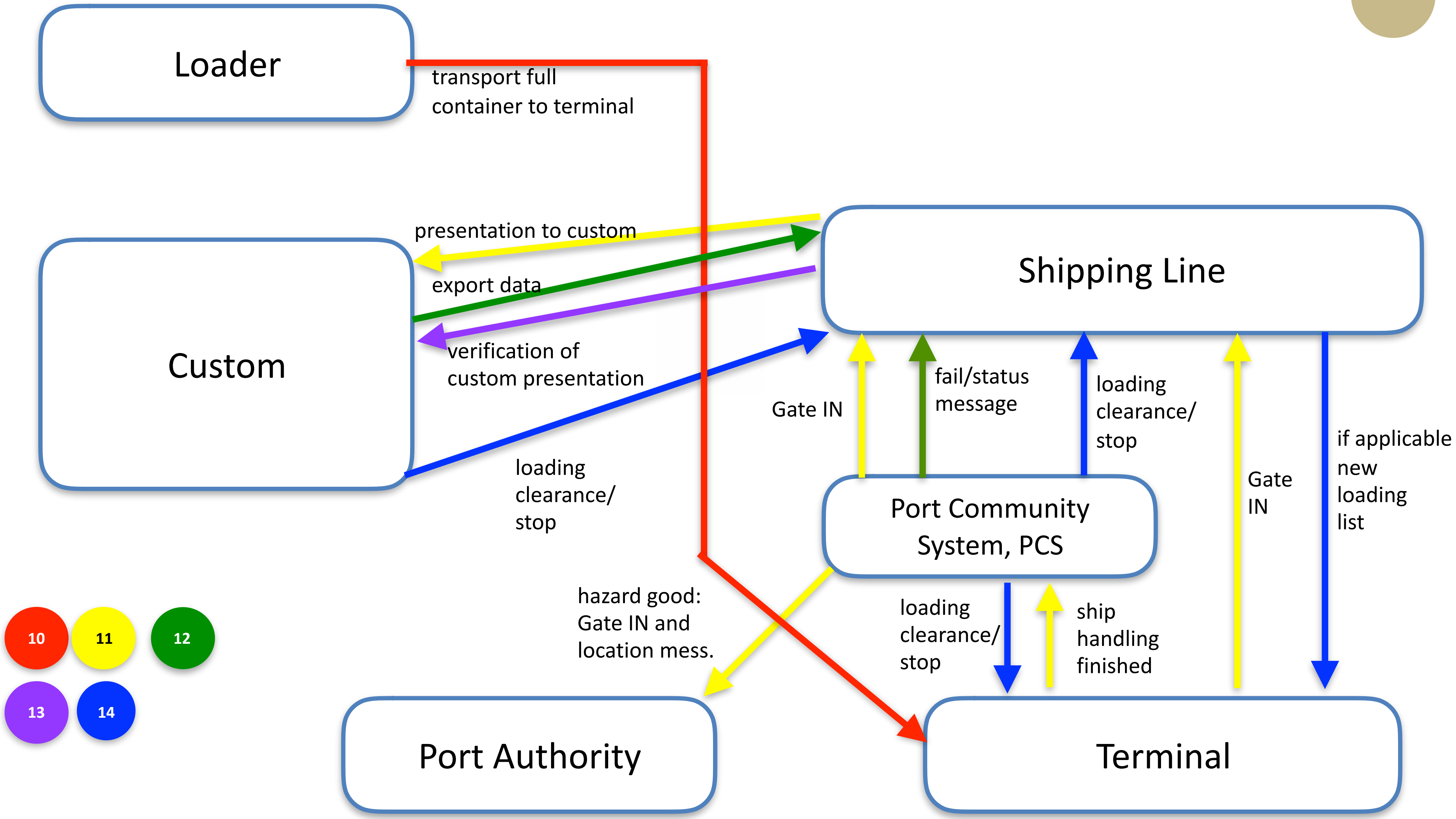
Container: 2. Transport to Port



VGM*: verified gross mass

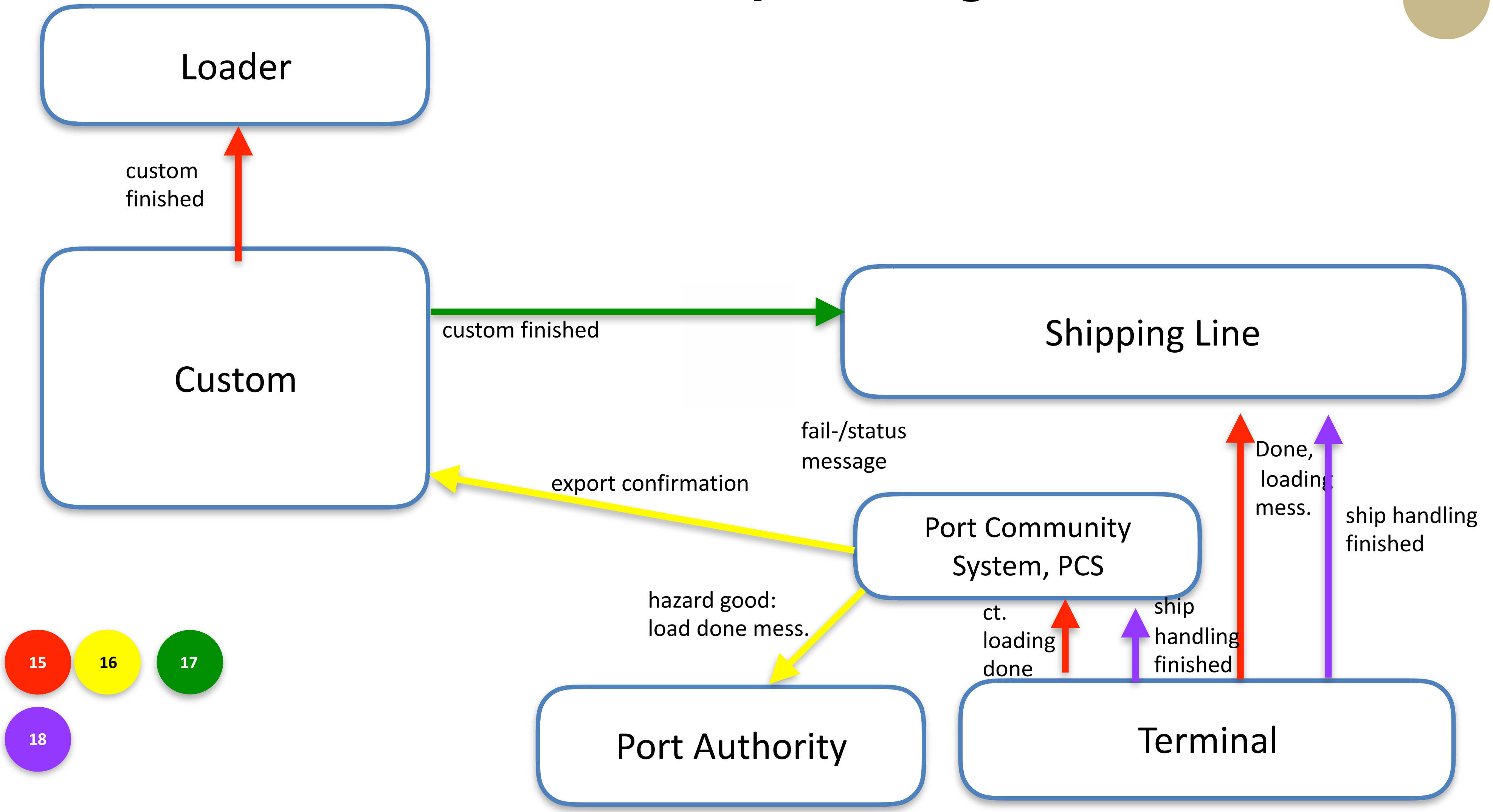
SecProPort: Process analysis:

Container: 3. Container delivery by truck



SecProPort: Process analysis:

Container:4. Ship loading



SecProPort: Process analysis:

There are many more processes available!

Threats against Transport, Logistics and Port IT

heise online > News > 2017 > KW 33 > NotPetya: Maersk erwartet bis zu 300 Millionen Dollar Verlust

NotPetya: Maersk erwartet bis zu 300 Millionen Dollar Verlust

16.08.2017 18:08 Uhr – Fabian A. Scherschel

vorlesen

Die Gunvor Mærsk der Maersk Line mit Kurs auf den Hamburger Hafen. (Bild: Bernhard Fuchs, CC BY 2.0)

Containerterminals standen still, Schiffe konnten weder gelöscht noch beladen werden: Mehrere Wochen hielt der Trojaner den dänischen Mega-Konzern Maersk in Atem. Die Reederei Maersk Line und der Hafenbetreiber APM Terminals wurden schwer getroffen.

What do we need to implement Information Security?

Firewall

AES 256

Blockchain

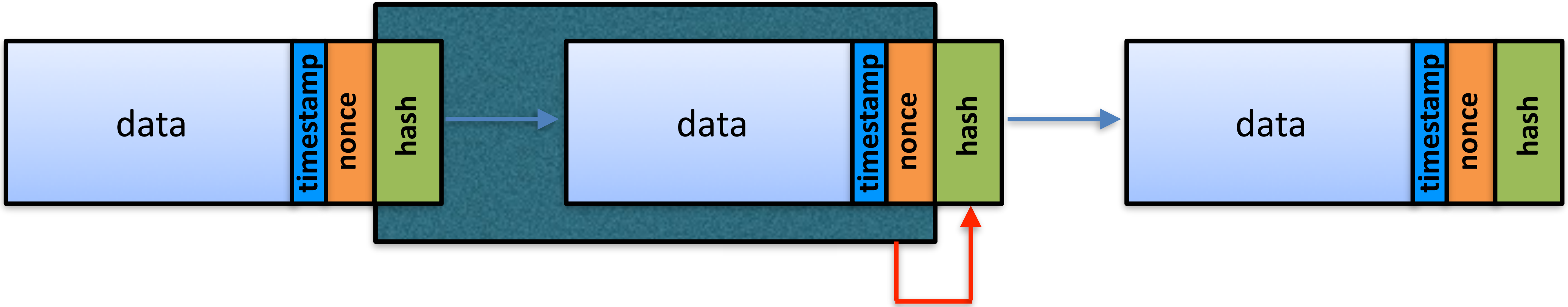
Distributed Ledger Technology (DLT)

=

Blockchain

DLT/Blockchain - Basics

Simplified schema of a DLT/Blockchain



e.q. Bitcoin:

- a new block will be added every 10 minutes
- block size 1 MB
- a timestamp is added to the block
- a nonce will be used for the Proof of Work (PoW)
- each transaction (part of the data) will be broadcasted to all other nodes

DLT/Blockchain - Basics

TK 07/19

Characteristics of a DLT/Blockchain

1. Consensus
2. Distributed
3. Trustless

Proof of Work

Proof of Stake

DLT/Blockchain - Basics

Consensus:

Give me the pen, please.

- You hear the words and you understand what to do

I say: X $\xrightarrow{\text{means}}$ Y

You understand: X $\xrightarrow{\text{means}}$ Y

⇒ common Knowledge

→ **Consensus**

DLT/Blockchain - Basics

TK
07/19

Distribution:

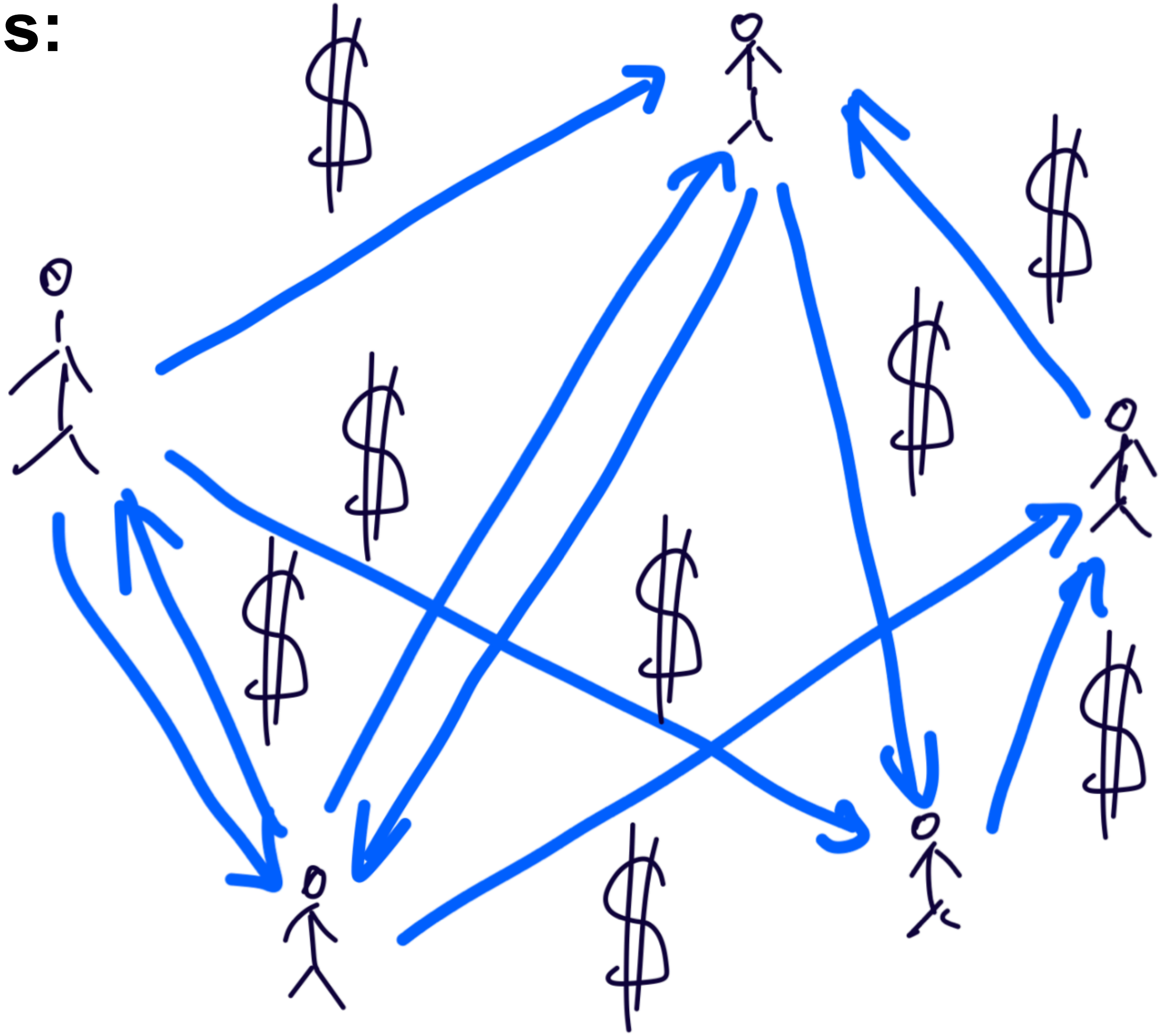
Centralized Database

Distributed Ledger (Blockchain)

- every participant has a copy of the ledger
- every participant can read and/or write to the ledger
- there is no centralised instance controlling the content and/or there status of the ledger

DLT/Blockchain - Basics

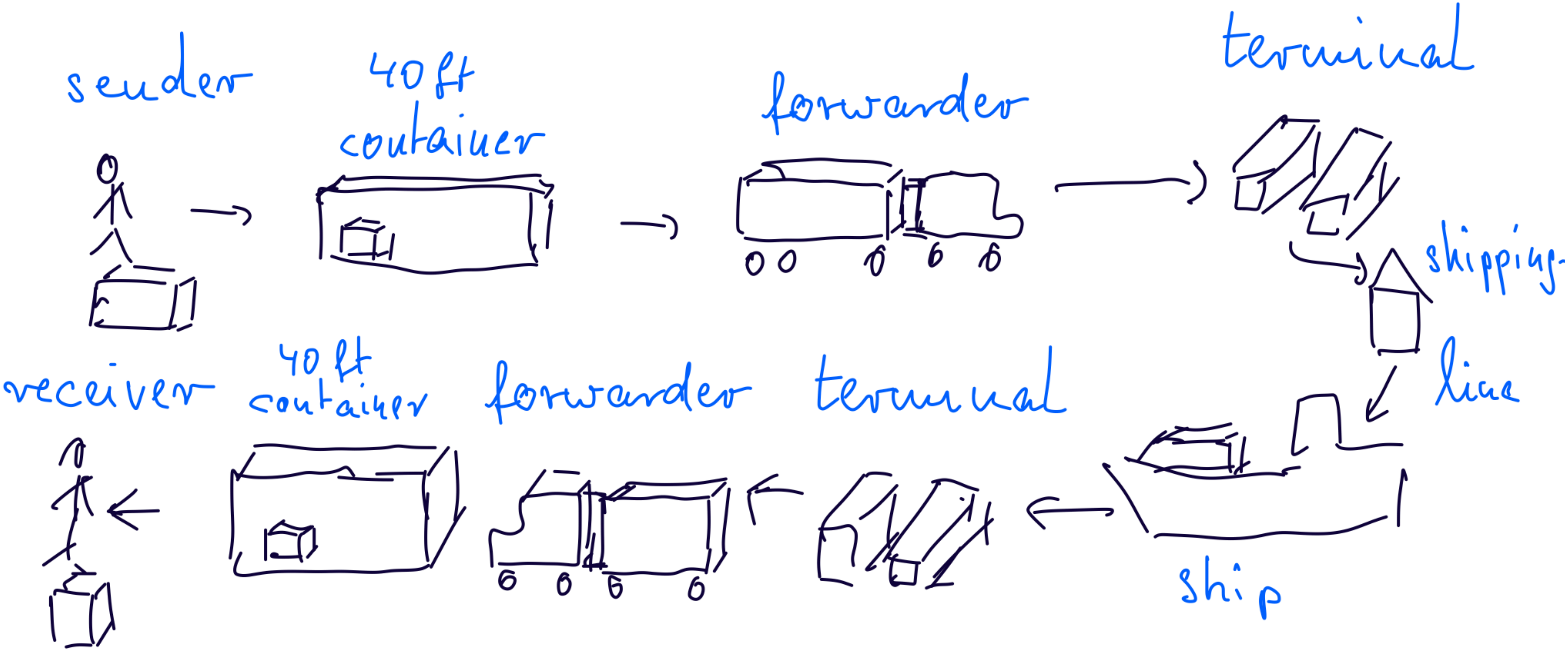
Trustless:



DLT/Blockchain - Basics

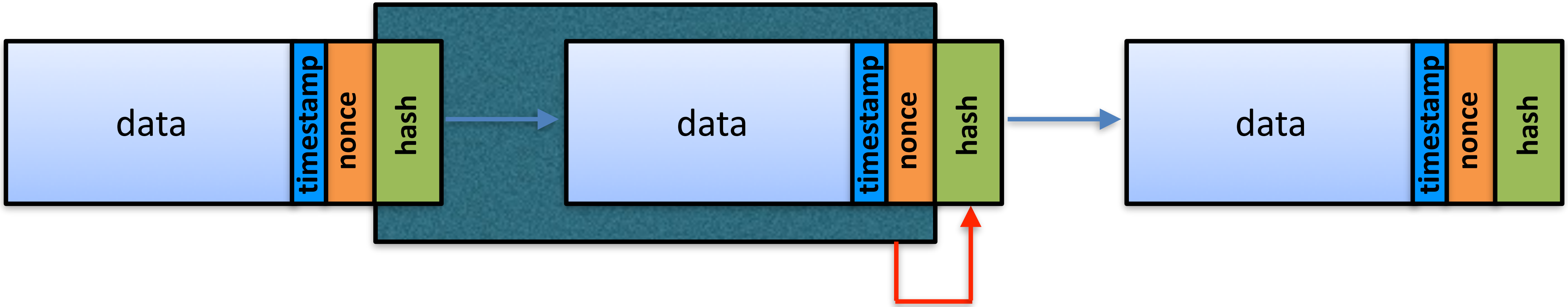
Trustless:

Example Transport Chain:



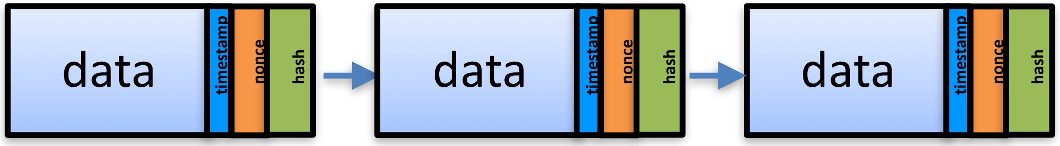
DLT/Blockchain - Basics

Consensus → **Proof of work:**



DLT/Blockchain - Basics

Consensus → **Proof of work:**

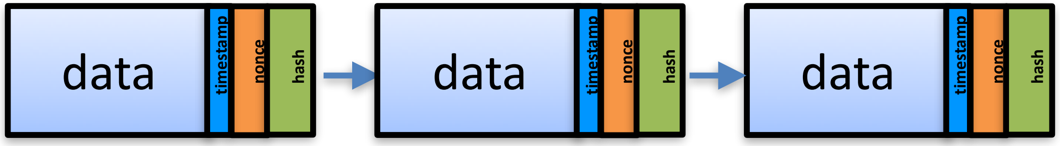


- **you see a state of a ledger that is good**
  - it will not be possible to show later a new ledger that state is better
  —> **that means: it is not possible to create a new ledger later, that is better than the old one!**

Adding a transaction to a verified block at a certain timestamp requires the computing power of the whole DLT network!

DLT/Blockchain - Basics

Consensus → **Proof of work:**



Proof of work:

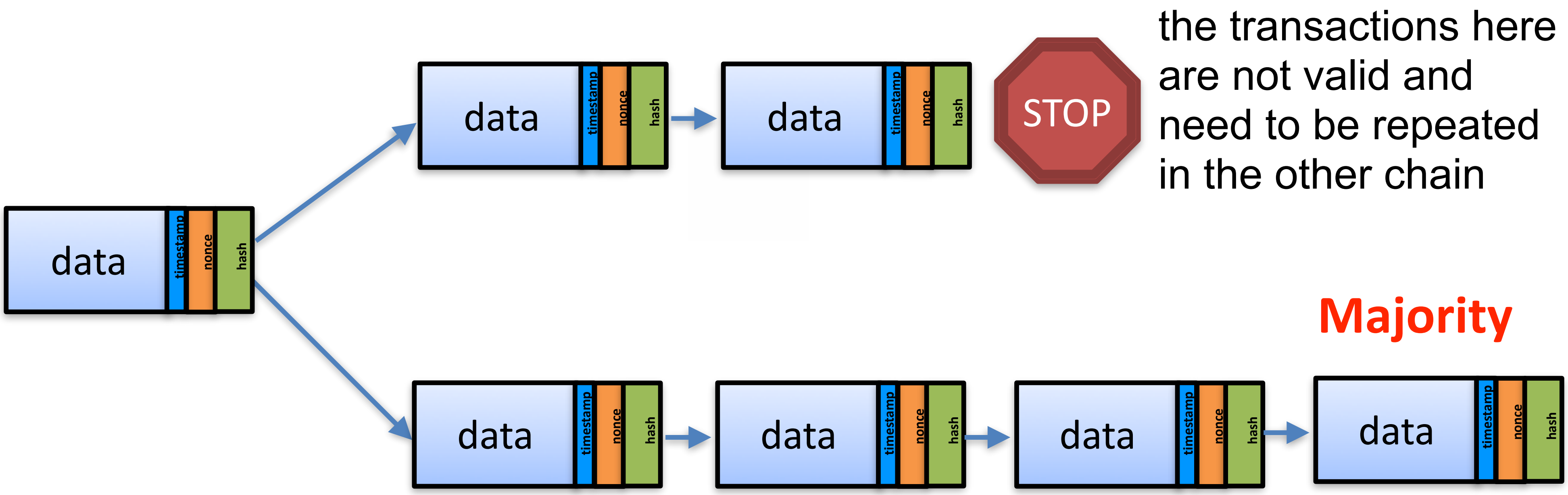
- Solve a cryptographic puzzle e.q. SHA 256 fulfilling certain conditions.
  E.q. find a hash value with a dedicated number of leading nils (Bitcoin)
- This verifies a block
- Incentives: who solves the puzzle receives coins in the next block of the DLT —> **MINING**

This requires a lot of computational power

Proof of work is only useful when trustless consensus is required!

DLT/Blockchain - Basics

Consensus → Proof of work:



In crypto currency: the merchant waits around 6 blocks to be sure that the coins are valid

DLT/Blockchain - Basics

Consensus → Proof of Stake:

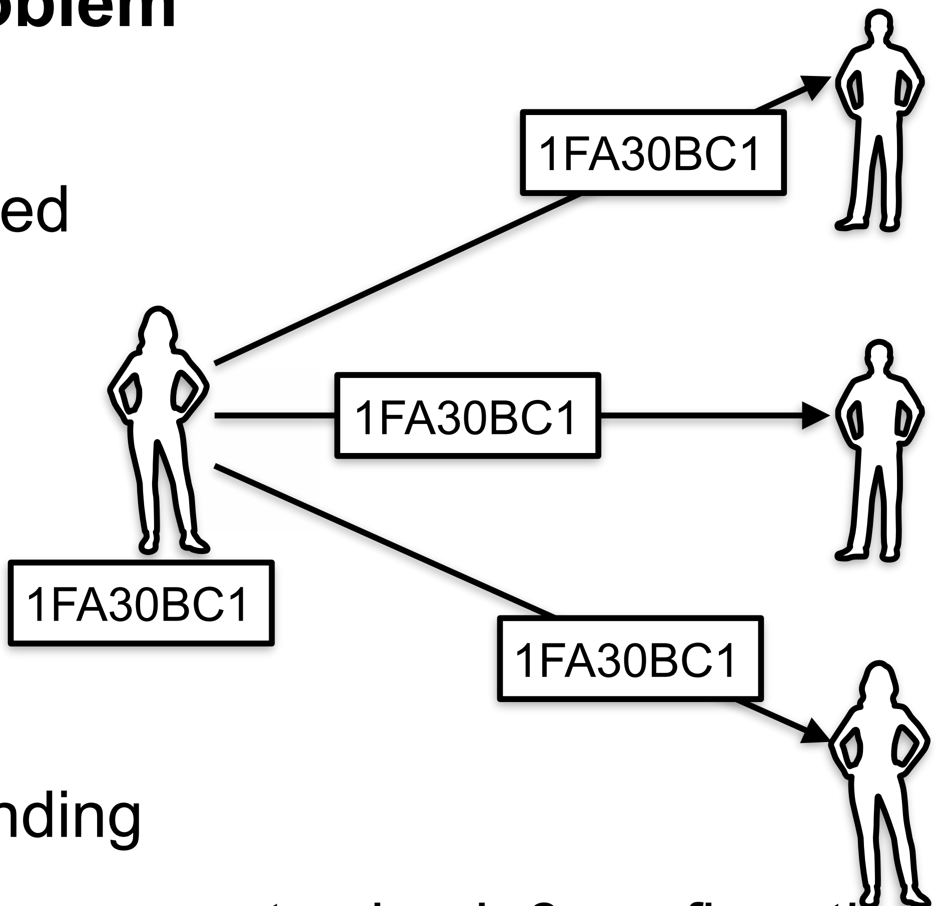
- A set of validators are taken on turns to vote on the next valid block
- The weight of each validator depends on his deposit (stake)
- The algorithm here pseudo randomly selects a validator during a distinct time slot (may be every 10 s)
  —> chain based
- Every validator votes for blocks, randomly selected. Many validators agree on a block
  —> Byzantine fault Tolerance Problem

Ethereum Casper relays on PoS, to reduce computational power

DLT/Blockchain - Basics

Double Spending Problem

- The transaction is added to the Blockchain
- Each block will be validated by a miner —> confirmation
- the merchant waits 6 confirmations to be sure of no double spending



It is unlikely that someone computes back 6 confirmations

36

DLT/Blockchain - Basics

Double Spending Problem

51% Attack:

An attacker owns 51% of the computing notes (hash power)

—> the attacker can withdraw any transaction and setup a ‘Private Blockchain/DLT’

- this is very cost intensive
- did not happen until now

What would happen if a state takes over 51% of the nodes?

DLT/Blockchain - Basics

Double Spending Problem

Race Attack:

An attacker sends at the same time the coins to the merchant and to himself (his address)

—> if the confirmation of the transaction of the attacker arrives first, the merchant will not get the coins

also here waiting 6 confirmations
the merchant can be sure to get the coins

DLT/Blockchain - Basics

Public vs. Private DLT/Blockchain

What have both in common:

- Peer-to-peer network
- Based on decentralization
- Each node has a copy of the DLT/Blockchain
- Verification by a consensus protocol
- immutable

DLT/Blockchain - Basics

Public DLT/Blockchain

Advantages:

- Open for everyone in an open eco-system
  everybody can verify the DLT/Blockchain
- Use of common networking protocols
- Consensus building by algorithms or similar
- Networking effects by use of many participants
- no fails and manipulations as it could appear in centralised systems
- high security, relatively low costs (PoW?)
- Mostly known: Bitcoin, Ethereum

DLT/Blockchain - Basics

Public DLT/Blockchain

Disadvantages:

- Memory space per block ≈ 1 MB
  —> to less for transaction and memory requirements of companies
- Transaction delay (PoW)
- Computational power, PoW —> costs
- open network —> no confidentiality and privacy

DLT/Blockchain - Basics

Private DLT/Blockchain

Advantages:

- Limited choice of participants (e.q. a company or community)
- One unit can be can be responsible for consensus building
- Blocksize can be increased
- Transactions can be withdrawn
- Known validators —> 51%-Attack is not possible
- transactions are cheaper:
  - less nodes necessary
  - no PoW —> less computational effort
- no delay because of no PoW
- only read access for dedicated nodes —> privacy (GDPO)

DLT/Blockchain - Basics

Smart Contracts

- Small program code as part of the DLT/Blockchain
- Smart Contracts are part of the transaction
- Smart Contracts are self-contained computer programs
- Smart Contracts can be verified by everyone
  (it is open in the DLT/Blockchain)

→ **Smart Contracts have changed DLT/Blockchain from a pure 'storage' to a system of 'Distributed Virtual Machines'**

DLT/Blockchain - Basics

Smart Contracts

Smart Contract is a different and new approach:

- Combination of data storage and connected active processes as a result of the transaction
- Provisioning of Services:

  - Transfer of goods (trade transaction)
  - Provisioning of Security Services
    * Virus detection
    * Encryption
    * Signature check
    * …

DLT/Blockchain - Basics

Publik Key Infrastructure, PKI

only a short description:

Database

Name	ID	Proof	Pub. -Key

Trusted Party:

- Public Administration
- Community
- Service Provider
- Dedicated Player
- …

What do we need to implement Information Security?

Firewall

AES 256

Blockchain

Virtual Network (Security) Functions

Software Defined Networks, SDN

Software Defined Network Design:

we divide the device into two parts:

Spanning Tree
Routing Protocols
ACL
IEEE 802.1q
HSRP
...

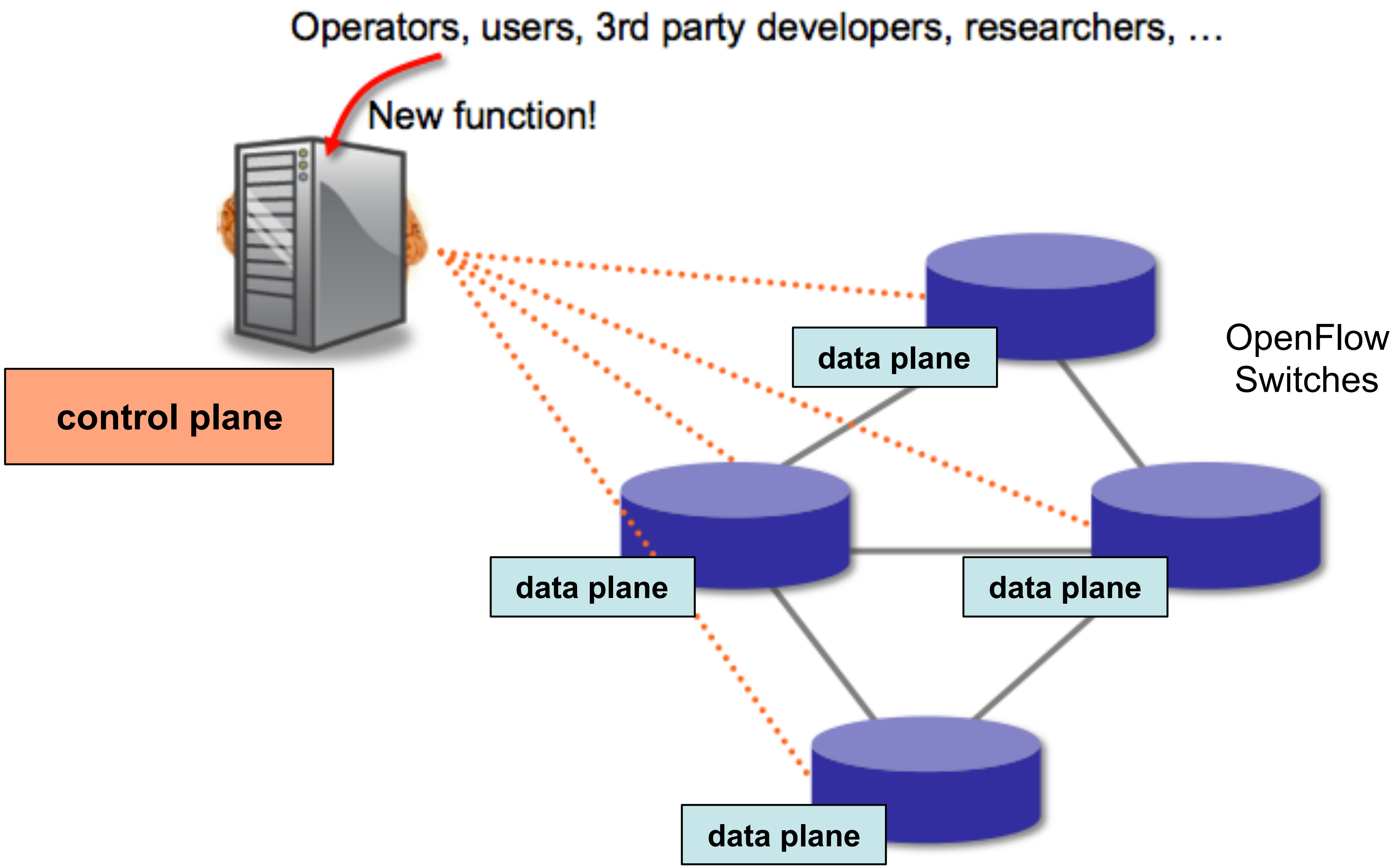
control plane

forwarding (data) plane

Switch

Software Defined Networks, SDN

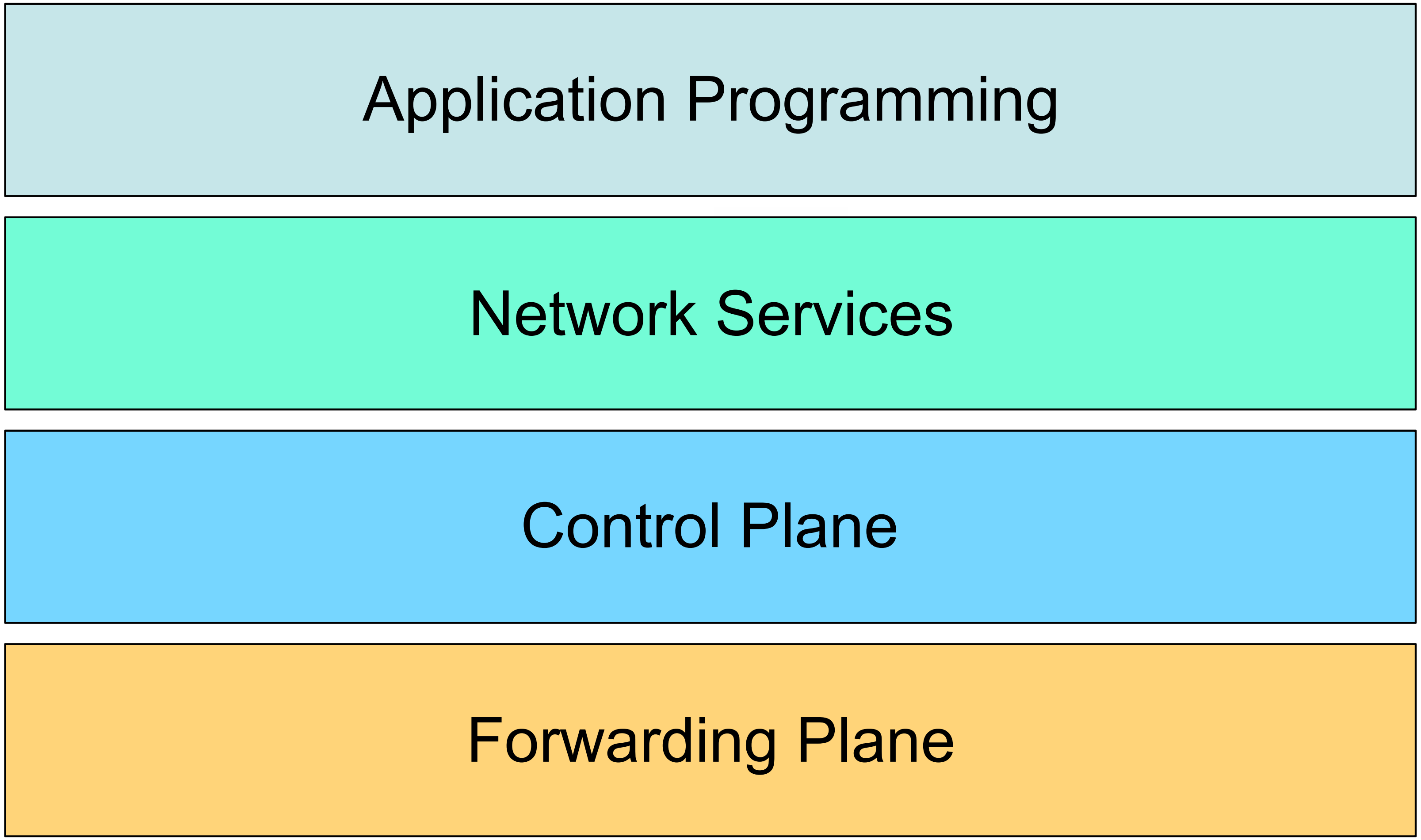
Software Defined Network Design:



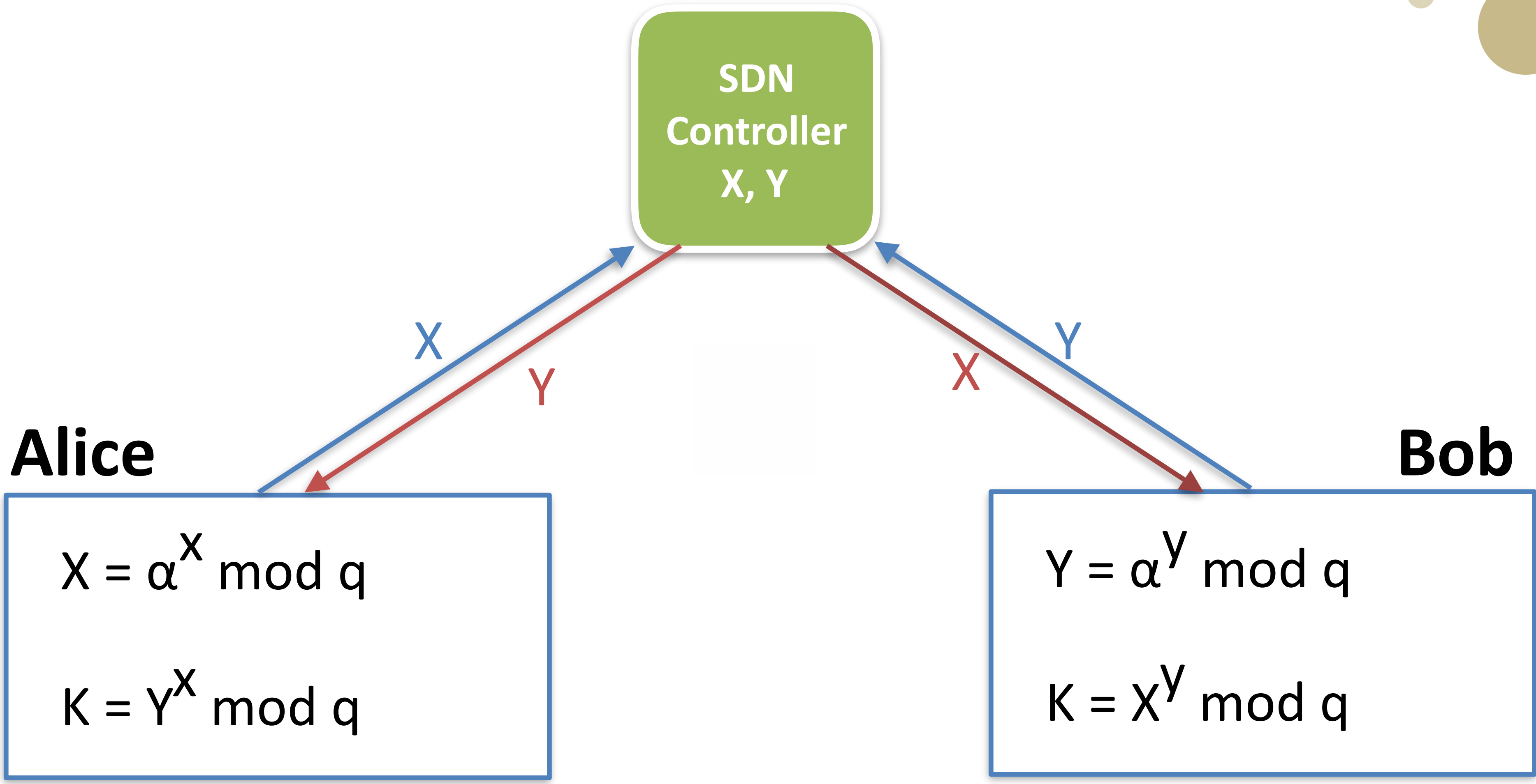
from Nick McKeown, Stanford University, VISA Workshop 2009

Network Virtualization Function, NFV

Network Virtualization:



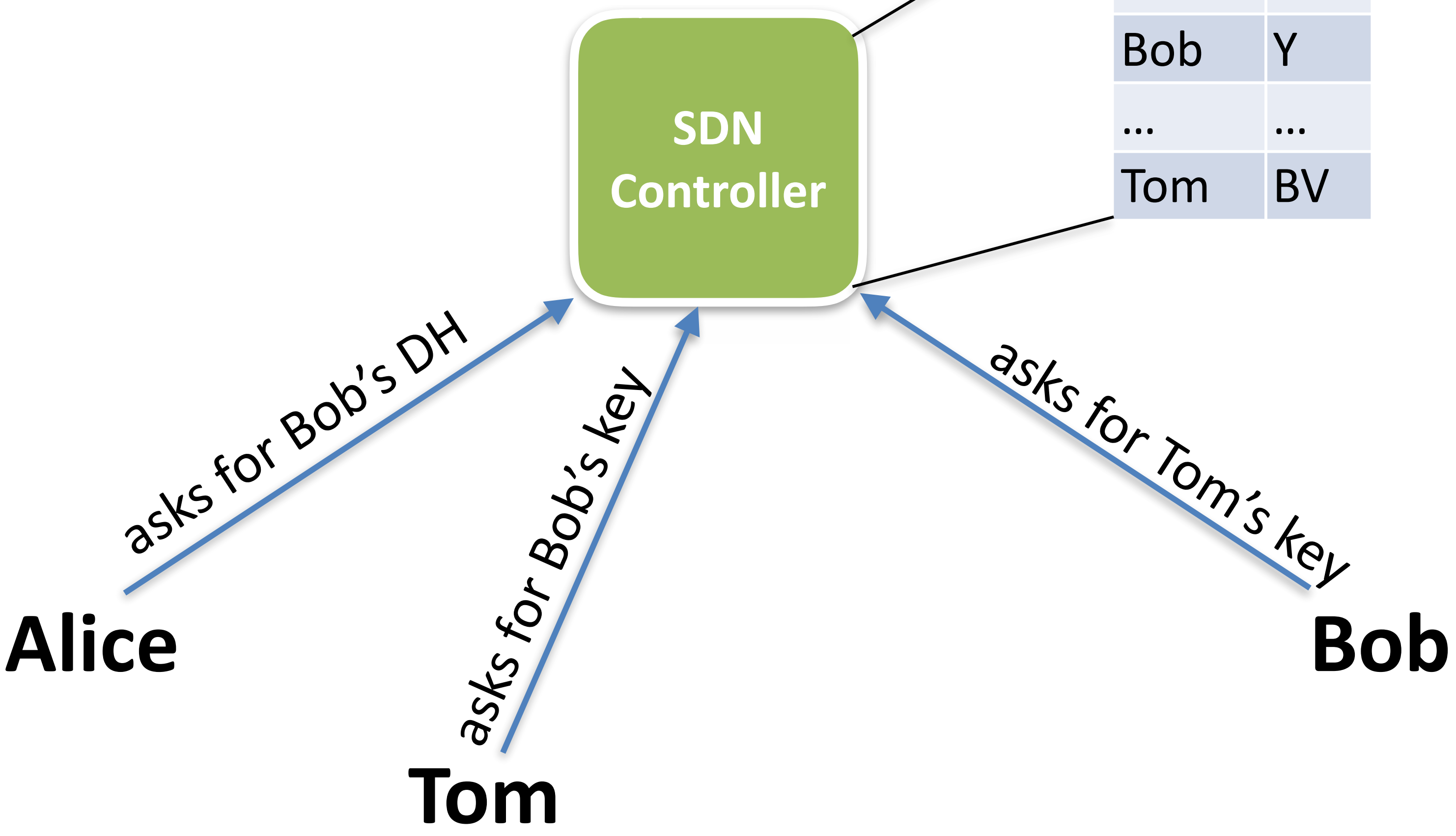
Secure Key Exchange, SDN and NFV



x: secret of Alice α, q: public y: secret of Bob

Diffie-Hellmann, DH

Secure Key Exchange, SDN and NFV

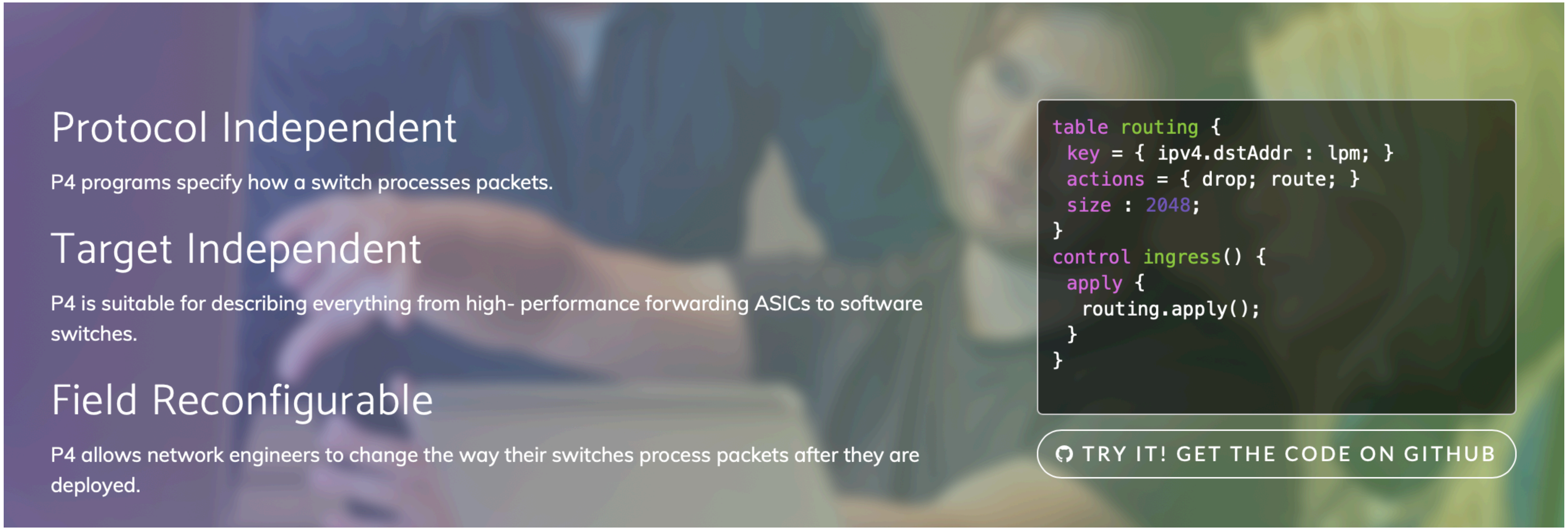


Name	DH
Alice	X
Bob	Y
…	…
Tom	BV

Diffie-Hellmann, centralized key distribution

P4: Programming Switches

Header Injection



www.p4.org

- **Segment Routing —> path direction of packets**
- **Direct packets to Network Service Functions (encryption, virus scan, …)**
- **…**

Information Security in Distributed Systems

We have different proposals:

- DLT/Blockchain
- Smart Contracts
- PKI (centralized/decentralized)
- NFV
- Network Header Injection (P4)
- …

Information Security in Distributed Systems

That is where we are now!

Thank you for your attention!

Information Security in Distributed Systems

How to improve Information Security in highly distributed systems?

→ Group work — 4-5 participants per group

- take one of the scenarios of the transport, logistics and port business
- use the proposed measures/techniques
- find new measures
- look for useful combinations
- find new, composed solutions and procedures

→ present your findings (10 minutes per group)

SecProPort: Scenario Driven Project

Demonstration and evaluation of the project:

The Security Model will be realised and evaluated by setting up Scenarios together at and with the industrial project partners.
Potential Scenarios could be:

- Container terminal: information and data exchange along the transport chain of container transport
- XXL-Logistics: Paper rolls, locomotives, wind mills, etc.
- Intermodal terminal: train-road, train-port, road-port
- Single National Window
- …