Selected Topics IT-Security 1

Blockchain, Distributed Ledger and its Use-Cases in eGovernment

Andreas Abraham
andreas.abraham@iaik.tugraz.at
Graz, 27.11.2019

EGIZ
E-Government Innovationszentrum

Das E-Government Innovationszentrum ist eine
gemeinsame Einrichtung des BMDW und der TU Graz

TU Graz

Overview

- Introduction
- Building Blocks
- Basic Principle
- Consensus Protocols
- Attacks
- Use Cases
- Conclusion

Overview

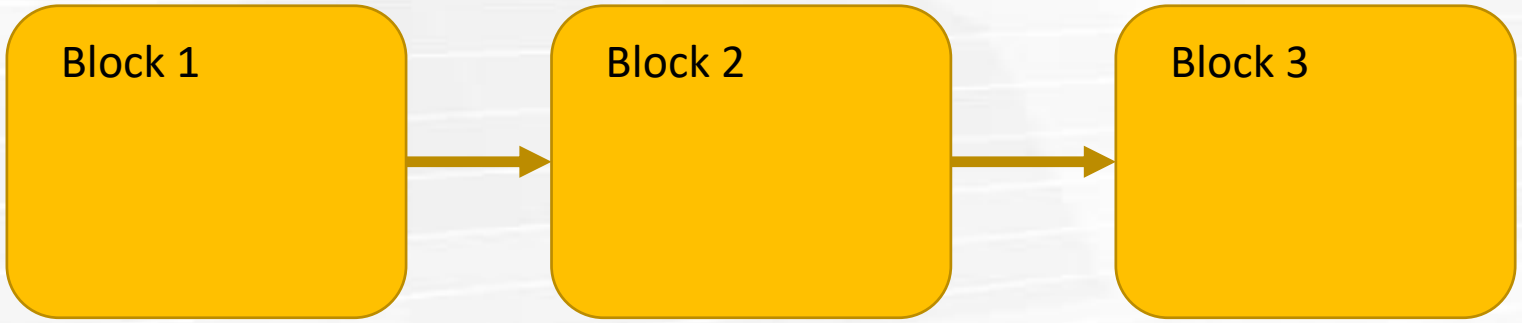
- « Introduction
- « Building Blocks
- « Basic Principles
- « Consensus Protocols
- « Attacks
- « Use Cases
- « Conclusion

Introduction

- Where does it come from?
  - Digital timestamps in 1991 introduced by Stuart Haber and W. Scott Stornetta
- What was the initial goal?
  - Creation of a timestamp service
  - Like a notary
- The idea was adopted by Satoshi Nakamoto in 2008
  - Bitcoin: A Peer-to-Peer Electronic Cash System

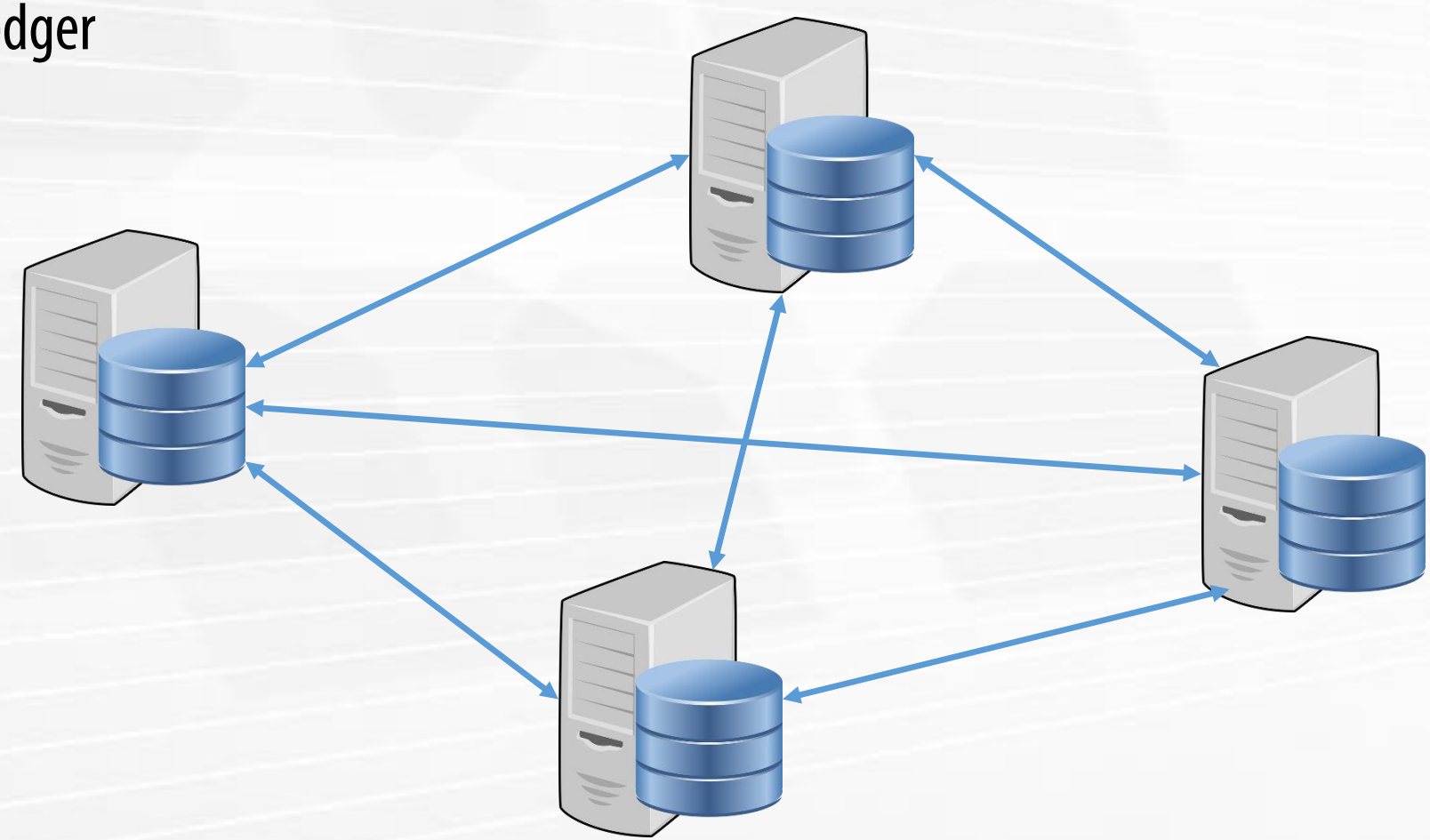
Introduction

- Chain of Blocks



Introduction

« Distributed Ledger



Introduction

- Confusion in the terminology
- The term can mean:
  - A actual chain of cryptographically connected blocks
  - A cryptocurrency
  - An umbrella term over a collection of tools and fancy cryptography
- Blockchain vs. Distributed Ledger Technology (DLT)

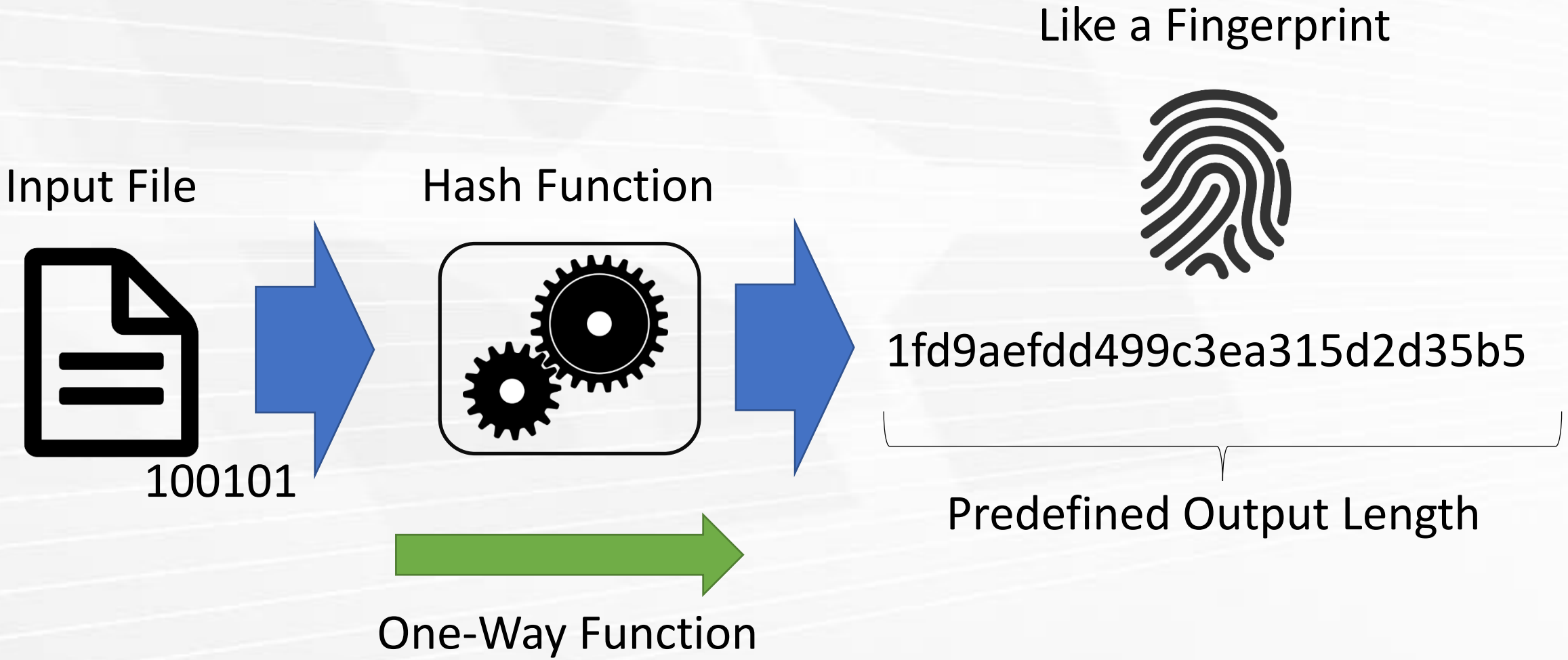
Introduction

- What does this technology solve?
  - Single point of failure
  - Central trusted party
    - Concentration of power
    - Trust issues

Overview

- Introduction
- Building Blocks
- Basic Principles
- Consensus Protocols
- Attacks
- Use Cases
- Conclusion

Building Blocks: Hash Functions (I)



Building Blocks: Hash Functions (II)

- Attacks
  - Brute Force
    - Trying all possibilities
  - Rainbow tables
    - Pre-calculated hash tables
  - Dictionary attacks
    - Using a dictionary for the attack

Building Blocks: Digital Signatures

- Based on public key cryptography
  - Public-private key pair
- Why signing?
  - Authenticity
  - Integrity

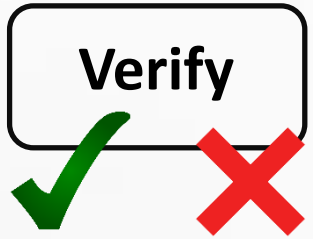
Building Blocks: Digital Signatures

Public-Private Key Pair

Document

Signed Document

1fd9aefdd499c3ea315d2



Control Questions

- 1. List and explain: what are the main Problems which could be addressed using the Blockchain and distributed ledger technology?

- 2. List three attacks on Hash functions and explain one in detail.

Overview

- Introduction
- Building Blocks
- Basic Principles
- Consensus Protocols
- Attacks
- Use Cases
- Conclusion

Basic Principle

- Blocks
  - Data
  - Hash
  - Previous Blocks Hash
- Data (Transactions in Bitcoin case)
  - From: Sender Account ID
  - To: Receiver Account ID
  - Amount
- Hash of previous block
- Nonce
- Hash of block

Basic Principle

- Properties
  - Distributed
  - Immutable
  - Append-Only
- Benefits
  - Transparency
  - Authentication
  - Audibility

Basic Principle

Types of Blockchains

- Public Blockchains
  - Anyone can join the network and take part
  - Cryptocurrencies and computing platforms
- Private Blockchains
  - Limited to authorized parties/users
  - Within organizations or governments
- Hybrid Blockchains (Consortium Blockchain)
  - Only authorized parties can run a node
  - More open for users
  - Many use cases e.g. cross-border money transfer, trust networks, legal systems, . . .

Overview

- Introduction
- Building Blocks
- Basic Principles
- Consensus Protocols
- Attacks
- Use Cases
- Conclusion

Consensus

- Different Protocols
- Achieve consensus

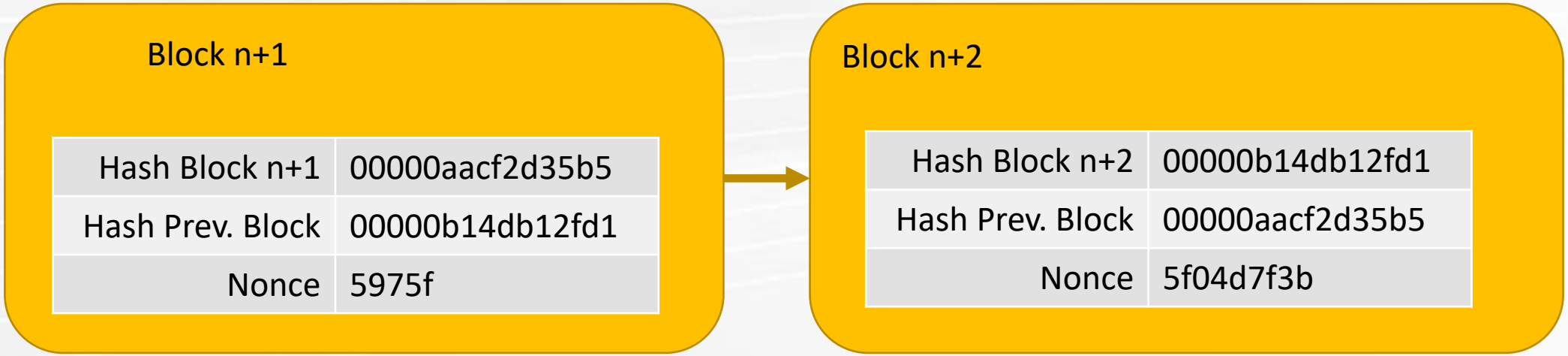
- Public Blockchains
  - Proof-of-work (Mining)
  - Proof-of-stake

- Private Blockchains
  - Byzantine Fault Tolerance Protocol
  - Proof-of-Authority

Consensus: Proof-of-Work

- Competing parties try to get the award
- Finding collusions
- Difficulty can be changed
- Mining pools

- Energy Consumption
- 75TWh/year for Bitcoin mining
- 58TWh/year Swiss energy consumption
- https://digiconomist.net/bitcoin-energy-consumption

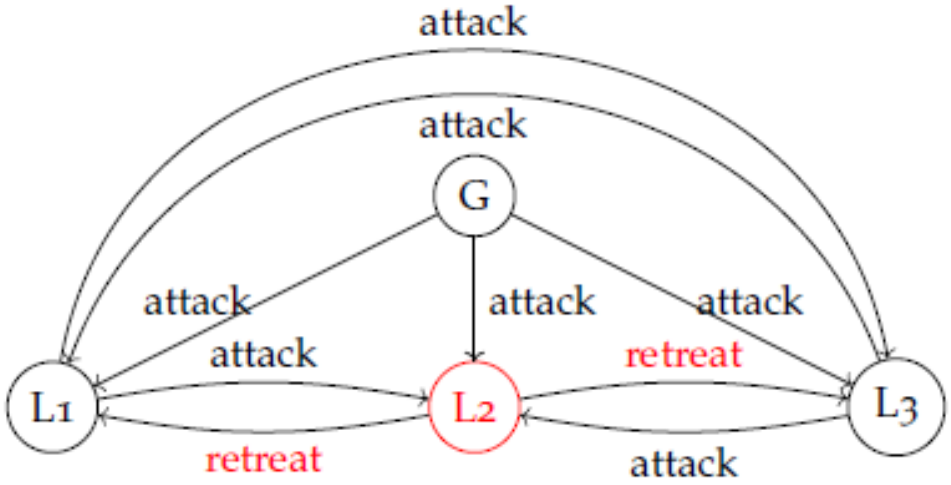


Consensus: Proof-of-Stake

- No miners but validators
- Randomly selected
- Validators place deposit
- Deposit is called stake
- Higher stake increases chances
- Behaving honest will be rewarded
- Malicious nodes will lose the stake
- Seem not fair

Consensus: BFT Protocol

- Byzantine Fault Tolerance Protocol
- For private/hybrid blockchains
- No mining
- Exchange and check requests of each other
- Based on the Byzantine Generals Problem



Consensus: Other Protocols

- Delegated Proof-of-Stake (DPoS)
  - Not random selected nodes but delegated
- Proof-of-Authority (PoA)
  - Authorized nodes are the authorities
  - Authorities have to achieve consensus
- Proof-of-Identity (PoI)
  - Authorized identities have additional permission
  - Problem selecting theses identities

Consensus: Other Protocols

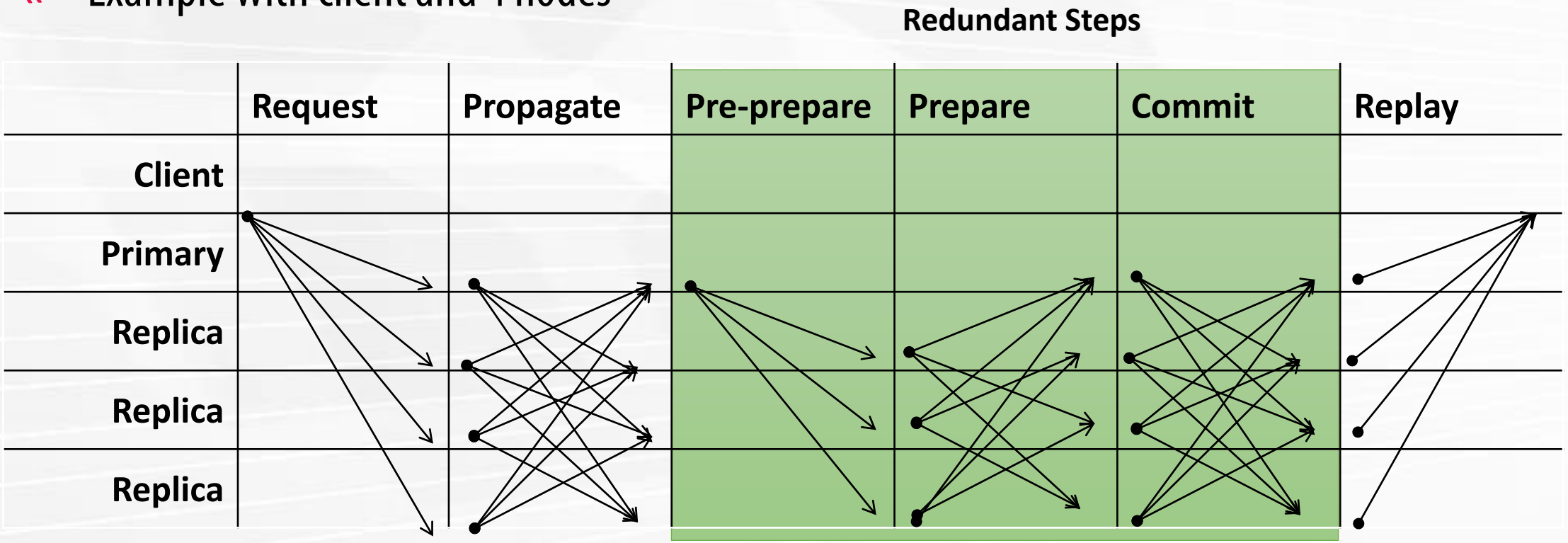
- Proof-of-Elapsed-Time (PoET)
  - Each node has to wait a randomly chosen period of time
  - After waiting the first one wins the new award
- Redundant Byzantine Fault Tolerance (RBFT) Protocol
  - Performing steps redundant
  - Increase security
  - Decrease efficiency
- Practical Byzantine Fault Tolerance (PBFT) Protocol
  - Better efficiency

Control Questions

- 1. What are the different Blockchain types and where can they be used?
- 2. List the properties of Blockchain technology and the resulting benefits and describe them briefly.
- 3. List two consensus protocols for private as well as for public blockchains and explain one protocol in detail.
- 4. Explain the Proof-of-Work (PoW) in detail including its advantages and problems.

Example: Redundant Byzantine Fault Tolerance Protocol

« Example with client and 4 nodes



[5] P. L. Aublin, S. Ben Mokhtar, and V. Quema, "RBFT: Redundant byzantine fault tolerance," *Proc. - Int. Conf. Distrib. Comput. Syst.*, pp. 297–306, 2013.

Overview

- Introduction
- Building Blocks
- Basic Principles
- Consensus Protocols
- Attacks
- Use Cases
- Conclusion

Attacks

- What can be the target of an attack?
  - The Blockchain Structure
  - Peer-to-Peer System
  - Blockchain Applications

Attacks: P2P System

- Selfish Mining Attack
  - Mining pool with strong computational power
  - First seen who strategy
  - Pool finds a block and withholds it
  - Secretly continue mining and appending blocks
  - Release later sequence of blocks
  - Other miners loose award

Attacks: P2P System

- Majority Attack (51% Attack)
  - Proof of work
  - Attacker with 51% of computational power
  - Can perform double spending
  - Longest chain will be followed
- Eclipse Attack
  - Many malicious nodes
  - Block connections of honest node
- Distributed Denial of Service (DDoS) Attack
  - Huge amount of requests until network collapses

Attacks: Blockchain Application

- Wallet Theft
  - Protection of wallet/key access
  - Private key theft
- Double-Spending
  - Same coins are spent twice
- Replay Attacks

- More information https://arxiv.org/pdf/1904.03487.pdf

Overview

- Introduction
- Building Blocks
- Basic Principles
- Consensus Protocols
- Attacks
- Use Cases
- Conclusion

Use Cases: Cryptocurrencies

- Bitcoin
  - Transactions are bundled in blocks
  - Blocks are mined
  - Mining competitors try to get the award
- Ethereum
  - Similar to bitcoin
  - Provides a distributed computing platform
  - Introduced smart contracts

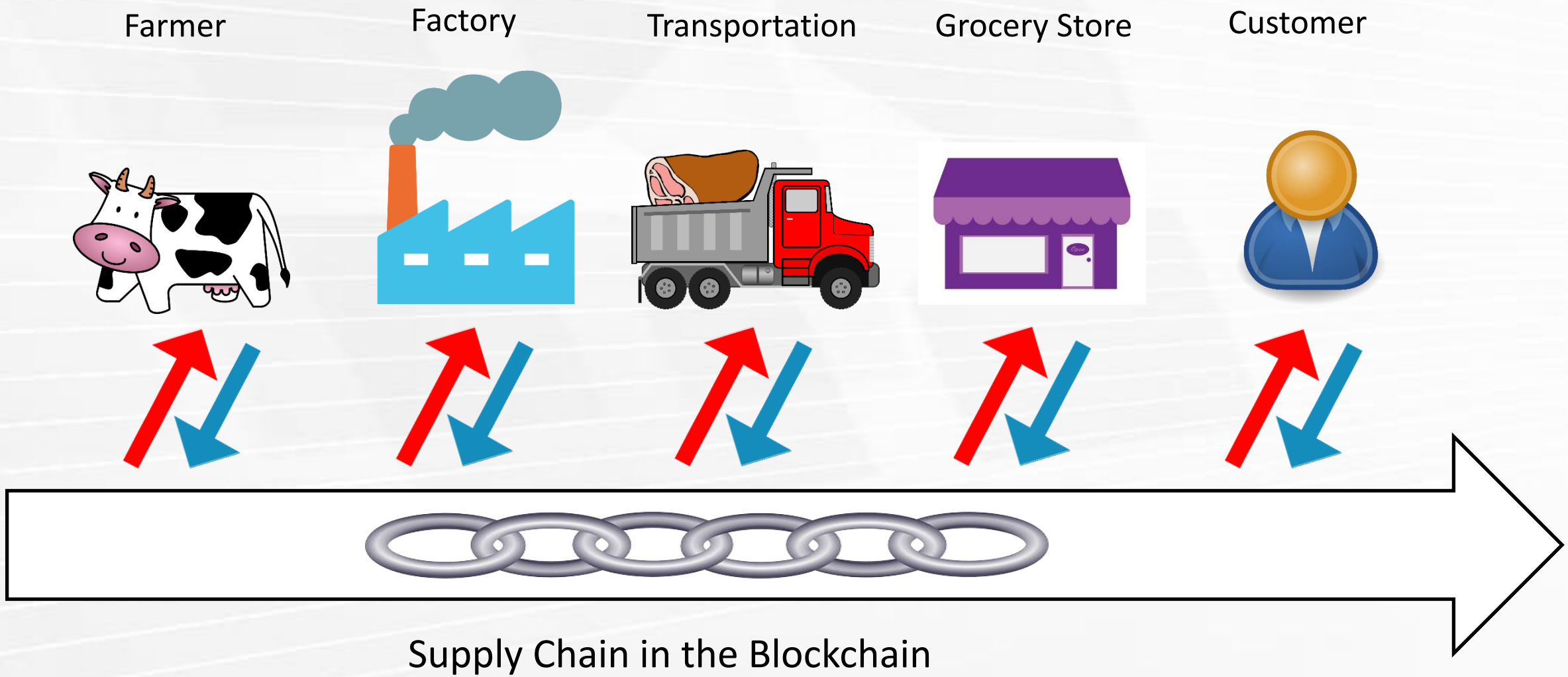
Use Cases: dApps

- Decentralized Applications
- Advantages
  - Tamperproof
  - Protecting application from hacking or intrusion
  - Records are stored unalterable
- dApps categories
  - Security
  - Finance
  - Games
  - Exchanges
  - …
- https://www.stateofthedapps.com

Use Cases: Land Register

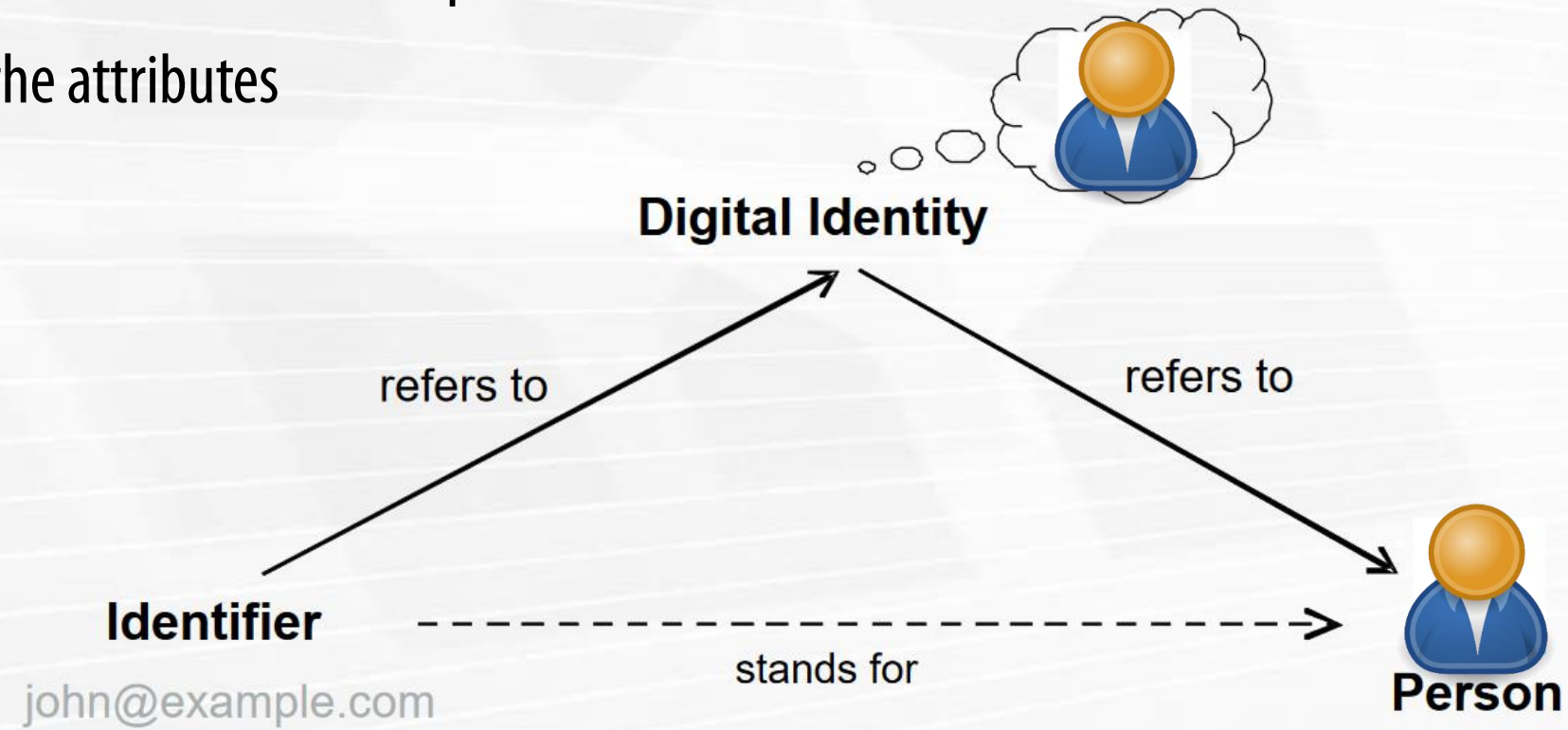
- Proof-of-Concepts in various countries like Canada, Estonia, etc.
- Nodes of the network run by the government
- Transaction describe the transition of ownership
- Transparency throughout all transactions

Use Cases: Supply Chain



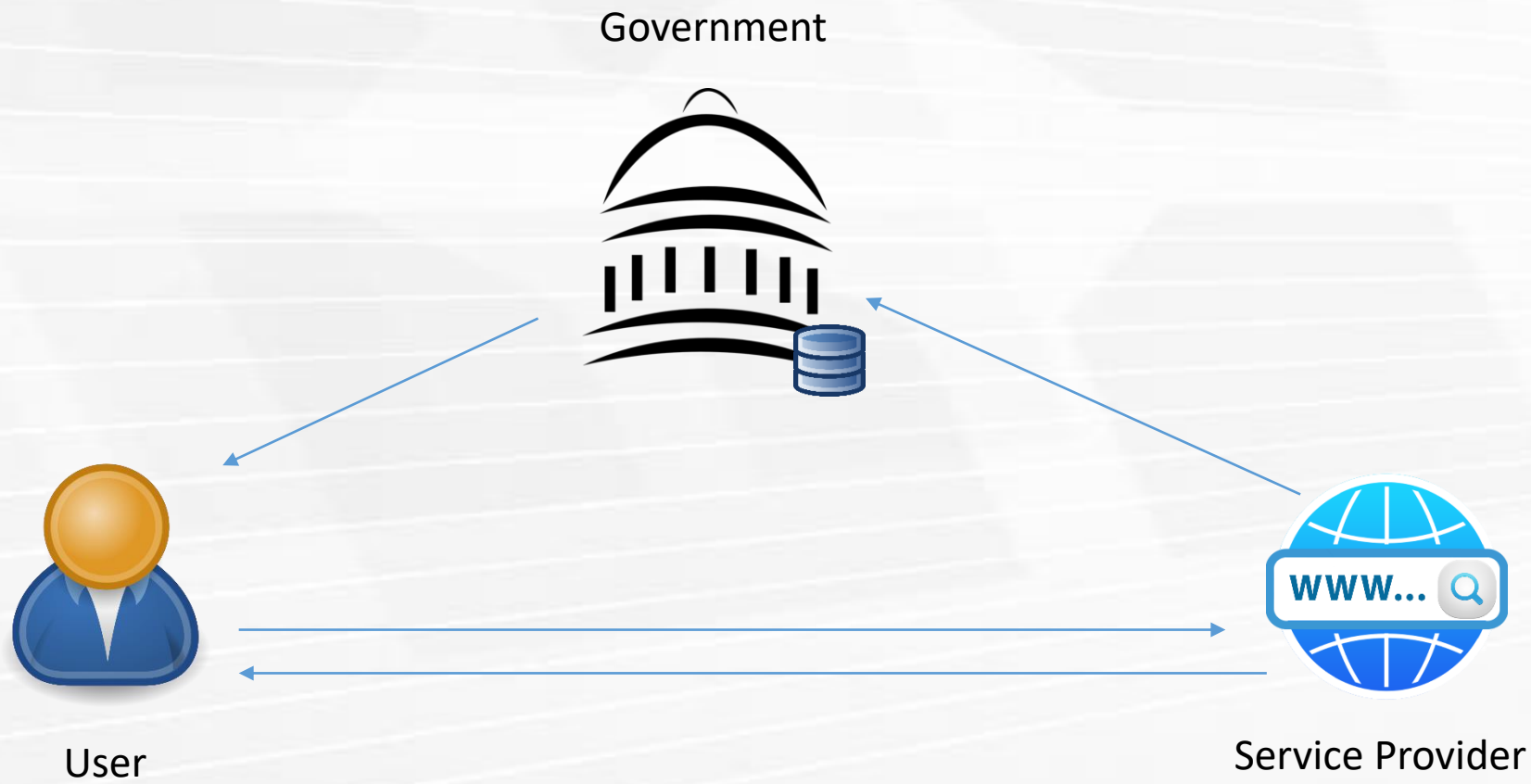
Use Cases: Digital Identity

- What is a digital identity
- Set of attributes linked to a person
- Prove the attributes



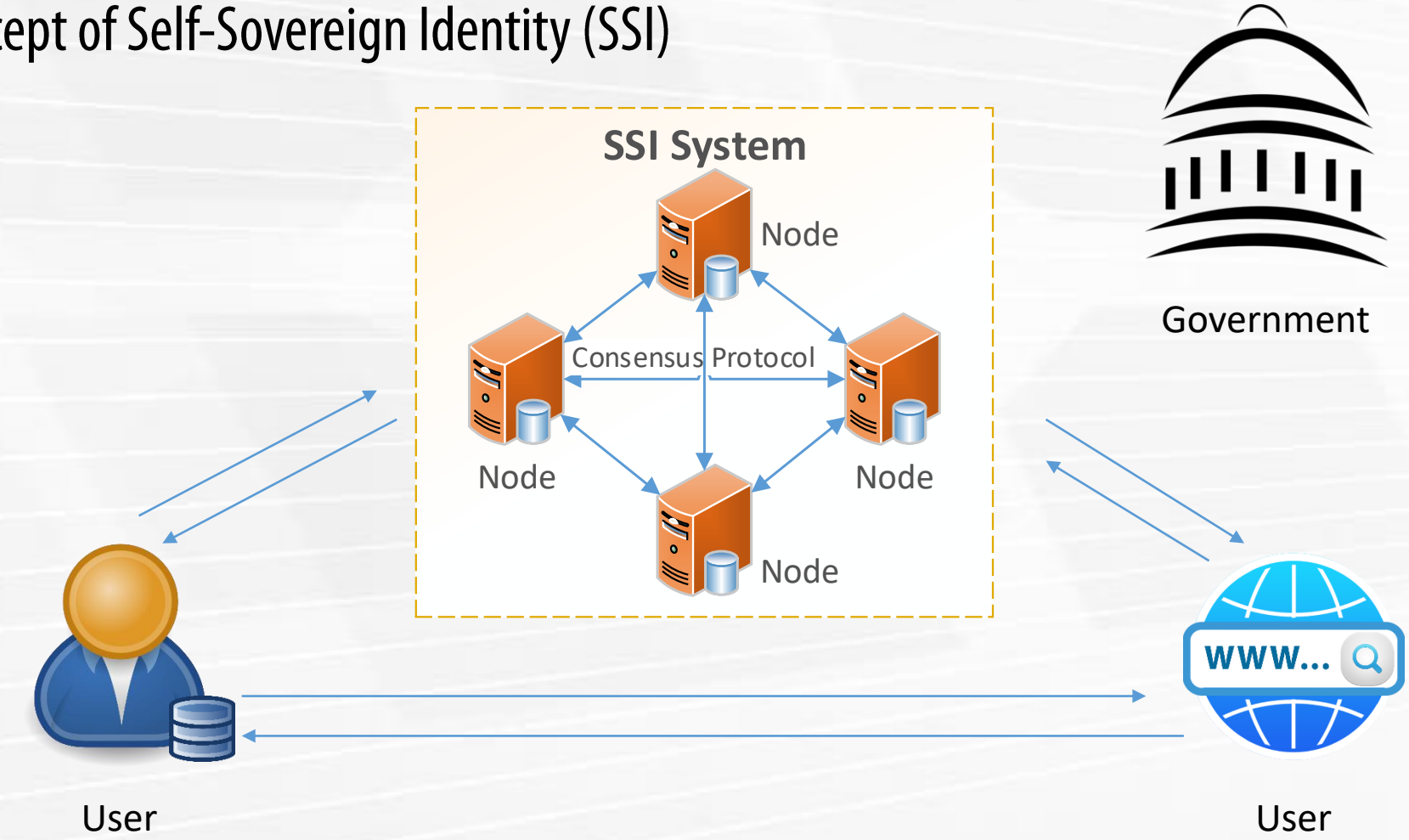
Use Cases: Digital Identity

« Current State



Use Cases: Digital Identity

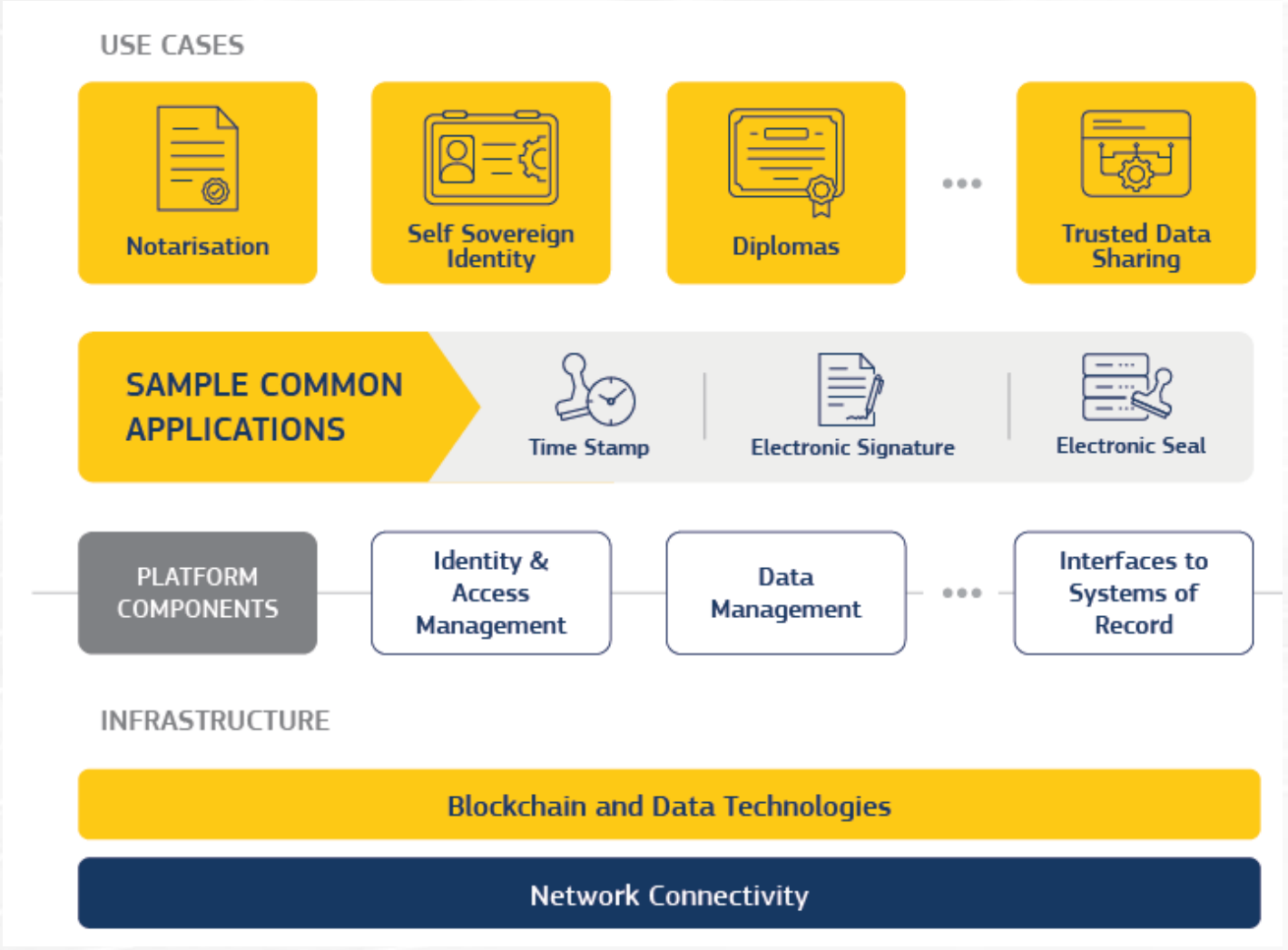
« Concept of Self-Sovereign Identity (SSI)



Use Cases: EBSI

- In 2018, 27 EU Member States, Norway and Lichtenstein signed a declaration creating the European Blockchain Partnership (EBP)
- European Blockchain Services Infrastructure (EBSI)
- Four defined Use Case Groups
  - European Self-Sovereign Identity Framework (ESSIF)
  - Notarization of Documents for Auditing Purposes
  - Certification of Diplomas
  - Trusted Data Sharing

Use Cases: EBSI



https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI

Use Cases: EBSI

Benefits

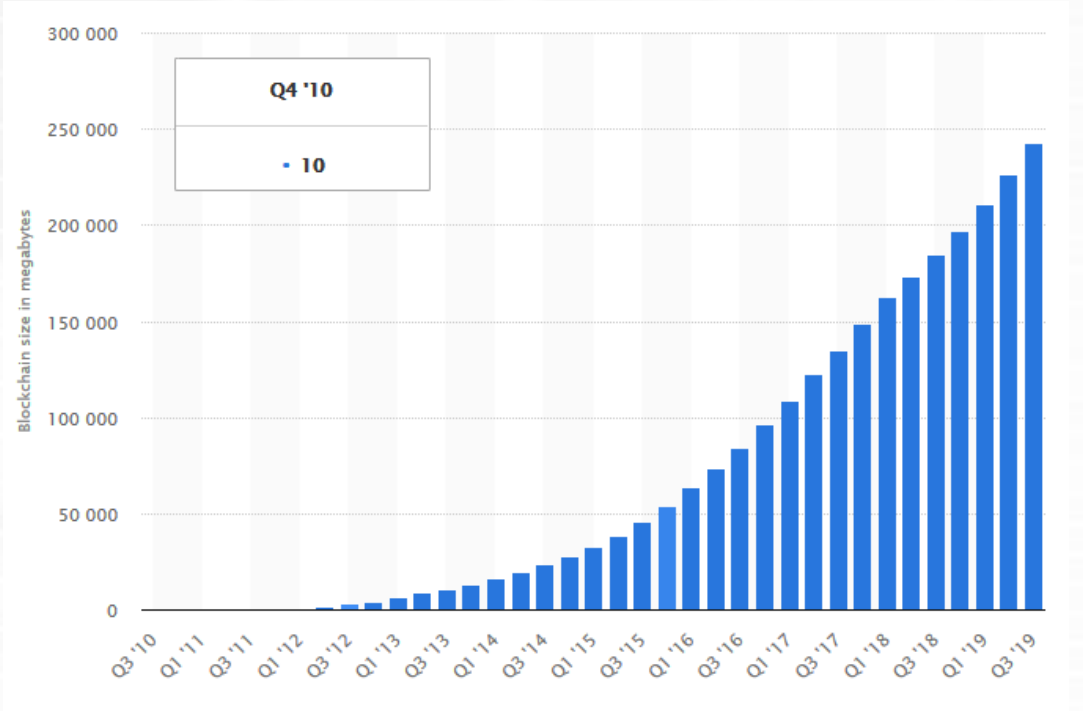
- EU citizens
  - Transact cross-border more securely
- EU institutions
  - Easy onboarding
  - Enable regulatory compliance
  - Increase efficiency in cross-boarder administrative processes
- National Administrations
  - Simplify administrative processes
  - Increase efficiency
  - Elevate trust

Use Cases: Research

- Redactable/Modifiable Blockchain
  - Immutability as Problem
  - E.g. when illegal content on the blockchain
- Redaction Capabilities Based on
  - Chameleon Hash and Secret-Sharing
  - or additional chains
- A predefined number of nodes have to agree
- Threshold determines number of consensual nodes

Use Cases: Research

- Compressible Blockchain
  - Blockchain is permanently growing
  - Size is becoming a problem
  - 242 GB Sep. 2019
- Research projects focusing on size efficiency
- Compressing or pruning



Control Questions

- 1. Describe the Majority Attack (51%) and where it applies.
- 2. List use cases for public blockchains and describe one in more detail.
- 3. Describe the Land Register use case using Blockchain technology.
- 4. Describe the idea and goal of Self-Sovereign Identity and how the Blockchain Technology / Distributed Ledger helps to achieve these.

Overview

- Introduction
- Building Blocks
- Basic Principles
- Consensus Protocols
- Attacks
- Use Cases
- Conclusion

Conclusion

- Building Blocks
  - Hash Functions
  - Digital Signature
- Basic Principles
  - Chain of Blocks, containing transactions, stored on a distributed ledger
- Consensus Protocols
  - Vary for the use case
- Attacks
- Use Cases
  - Cryptocurrency, land register, identity management, etc.