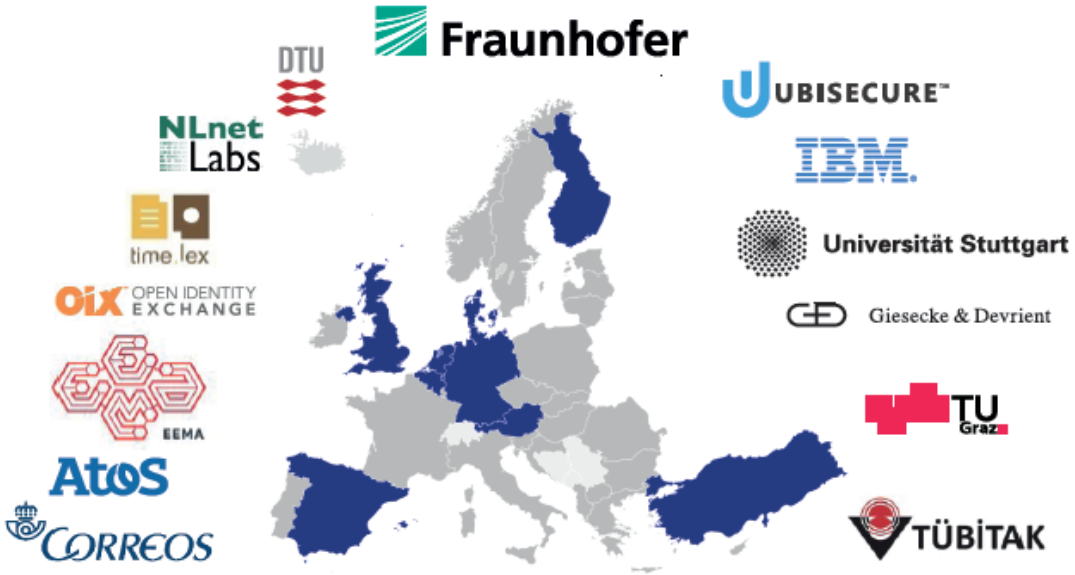
LIGHTest and Blockchain

A Lightweight Infrastructure for Global Heterogeneous Trust Management



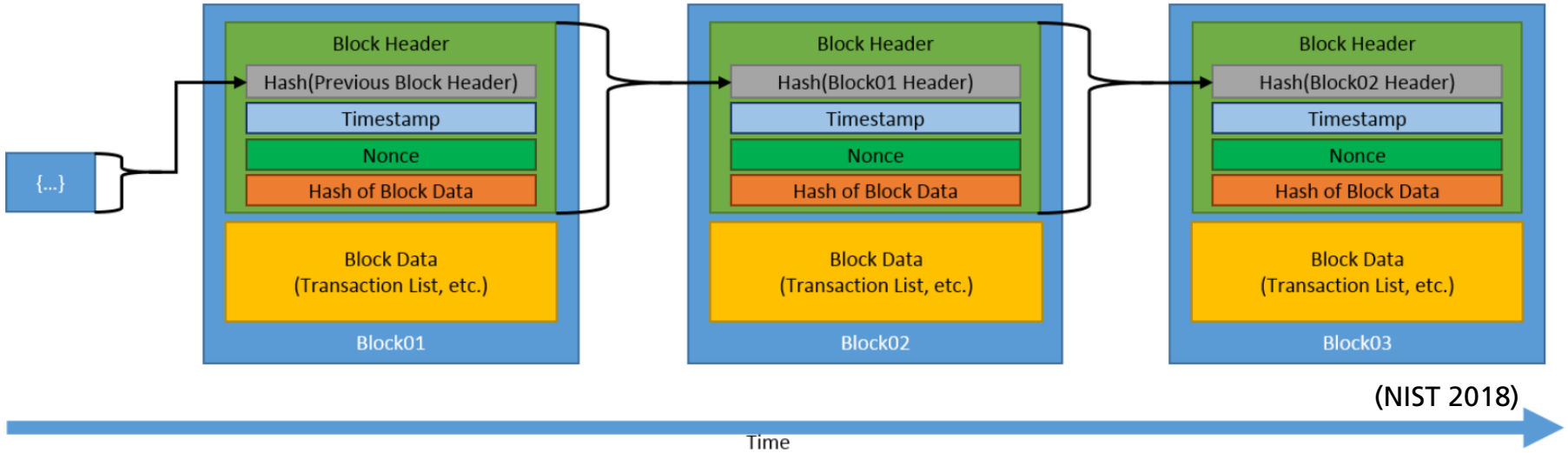
Lightweight **I**nfrastructure for **G**lobal **H**eterogeneous **T**rust management in support of an open **E**cosystem of **S**takeholders and **T**rust schemes

Rachelle Sellung, University of Stuttgart IAT

LIGHTest has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

The Blockchain Concept in a Nutshell

- **Distributed database** (“distributed ledger”) consisting of a chain of datablocks
- Participants of the Blockchain exchange the data with each other (**Peer-2-Peer-Network**) and each full participant owns copy of all data
- A certain number of transactions gets aggregated to a block and connected to the previous one: the **Blockchain grows**
- The blocks are validated through a **consensus procedure** (Proof-of-Work, Proof-of-Stake…)
- Block integrity and chronology is ensured by **cryptographic linking of the blocks** (hash-valueof the previous block serves as „checksum“)
- **Asymmetric** (Public Key) **Cryptography** is usedto create wallets and sign transactions



(NIST 2018)

LIGHTest has received funding from the European Union’s Horizon 2020 research and innovation programme under G.A. No. 700321

Basic Properties of Blockchains

„ Blockchain systems combine data storage, data exchange and data security with new access and proofing methods, which make it possible to develop new solutions for the increasing requirements in the age of data economy. “

(Bitkom 2017)

- **Distribute Ledger Technology (DLT):** data is recorded, shared and synchronized across a distributed network of computers or participants
- **database is highly resistant against deletion and manipulation:** hashes and structure of the Blockchain make data manipulations evident and easy to reject, data is available multiple times in a decentralized way
- **transparency and traceability:** every transaction ever made is visible to everyone and all transactions are signed with unique cryptographic keys
- **no central governance:** participants mutually validate the correctness of the transaction – there is no single-point-of-failure, no need to trust in individual auditors / intermediaries

LIGHT*est* has received funding from the European Union’s Horizon 2020 research and innovation programme under G.A. No. 700321

There is no Such Thing as „the Blockchain“

Basic Concept can be Implemented in a Great Variety of Ways

Public, private or consortial Blockchain systems		
Differentiation by access	Public (at least read access for everyone)	Private (limited access)
Differentiation by administration	Permissionless (anyone can participate and write new blocks)	Permissioned (only authorized participants can check transactions and write blocks)
Purpose of use		
Means of payment („cryptocurrency“)	Other specific purpose (e.g. provision of decentralized storage space)	Generic Blockchains (enable a wide range of applications)
Features and degree of development (also blockchains 1., 2., X. generation):		
Support of Smart Contracts	Existence of a virtual machine	Scalability	…

LIGHT*est* has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

Application Potentials of Blockchains are Derived from Features like:

Features:

- No central governance, elimination of intermediaries
- Data transparency, timestamping and traceability
- Simplification of consent, protection and control of consumer/customer data
- Immutability, high trust in the repository of transaction data
- Identities based on asymmetric cryptography/digital signatures
- Automation and Smart Contracts
- …

Application potentials:

- Trust, transparency and efficiency for interorganizational information exchange
- Reduced transaction costs by eliminating intermediaries, e.g. in micro-payment
- Tracking and tracing: continuous transparency and real-time tracking of the supply chain processes
- Compliance and auditing – Tracking processes against regulations with predefined rules
- Automated business contracts between two or multiple organizations
- Decentralized Autonomous Organizations
- …

LIGHT*est* has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

Current Challenges

- **Technical**: Performance, scalability, energy consumption…
- **Centralization**: Mining pools, Cryptocurrency exchanges as intermediaries, wallet services
- **Key management**: handling of public and private keys
- **Transparency**: privacy challenges
- **Immutability**: privacy challenge (right to forget), handling of necessary corrections

LIGHT^est has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

- is **not** Blockchain
- is **not** based on Blockchain Technology
- is **not** the same as Blockchain

LIGHTest has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

- ❖ Has Similar High Level Goals
(automatic verification of transactions, transparency, secure transactions)

- ❖ Fundamentally Different Approach

- ❖ May be an Alternative to Blockchain in SOME use cases

- ❖ Could be used together to combine the strengths of both approaches

LIGHTest has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

What is LIGHTest?

Lightest enables the use of a **global and trusted infrastructure** to determine and verify digital trust assurances to facilitate decision making and assessing risk.

By better understanding operational risk, operational costs can be better controlled. LIGHTest is providing tools for the emerging cross-border trust services market.

EU Horizon2020 Project: LIGHTest

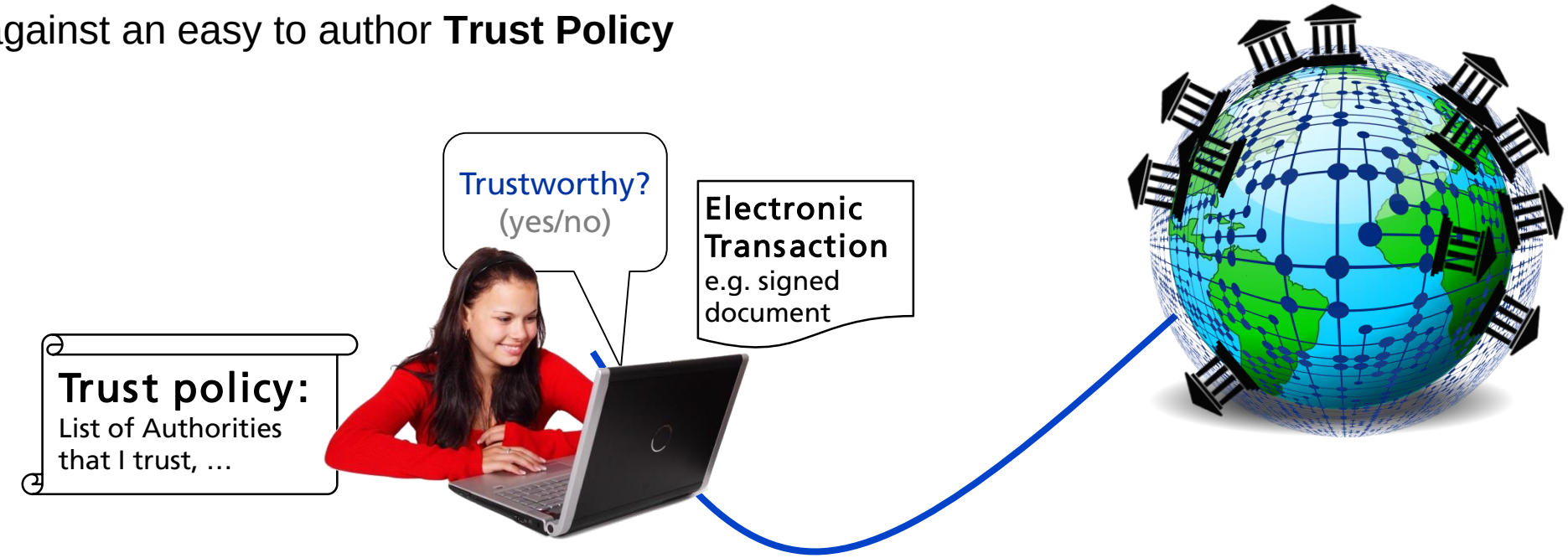
https://www.youtube.com/watch?v=lEaCMcVer28

LIGHTest has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

LIGHT^est has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

What does LIGHT^{est} do? Trust Policy and Automatic Trust Decisions

- Make it automatic for Verifiers to **query Trust Lists**
- Combine multiple queries to **validate**
  - an **Electronic Transaction**
  - against an easy to author **Trust Policy**



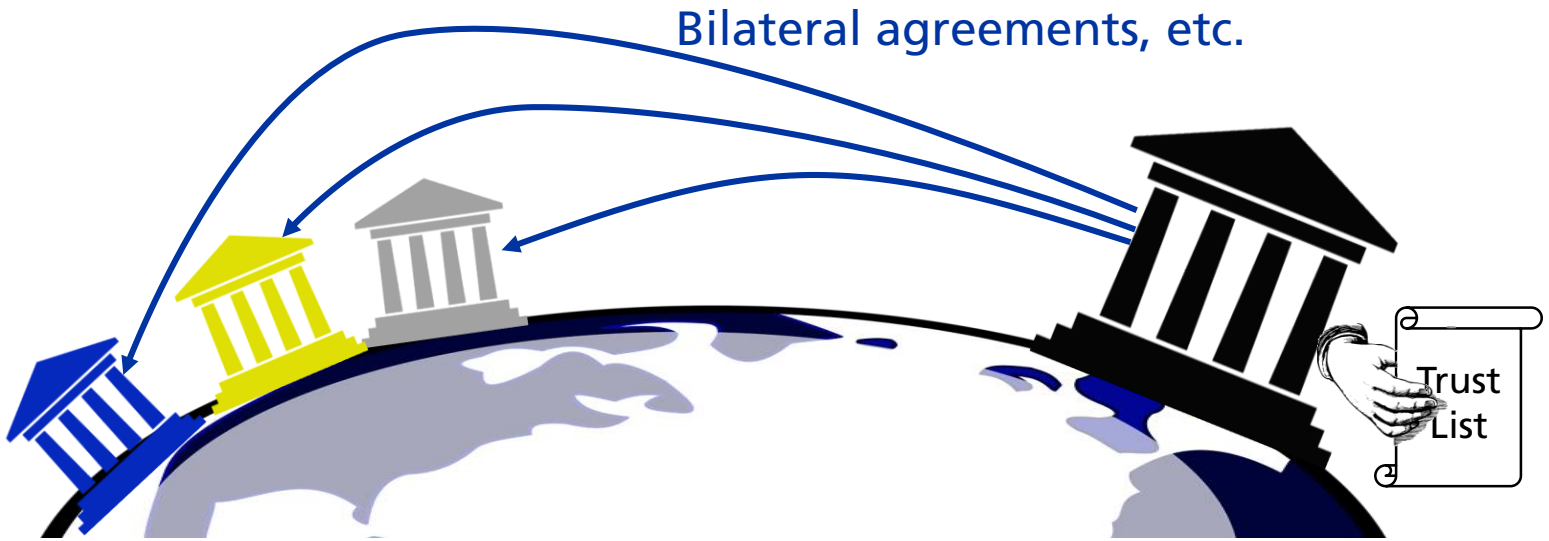
LIGHT^{est} has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

What does LIGHT*est* do?

Infrastructure for the Translation across Trust Domains

Authority publishes Trust List on..

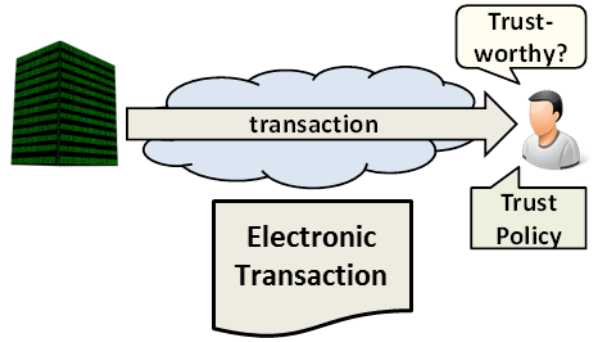
- ..which authorities from other trust domains are trustworthy
- ..how to translate foreign into native trust schemes
  - NIST: Level “3” == EC eIDAS: Level “substantial”



LIGHT*est* has received funding from the European Union’s Horizon 2020 research and innovation programme under G.A. No. 700321

LIGHT*est* *in a nutshell: Goal*

provide parties of electronic transactions with **automatic validation of trust** based on their **individual trust policies**



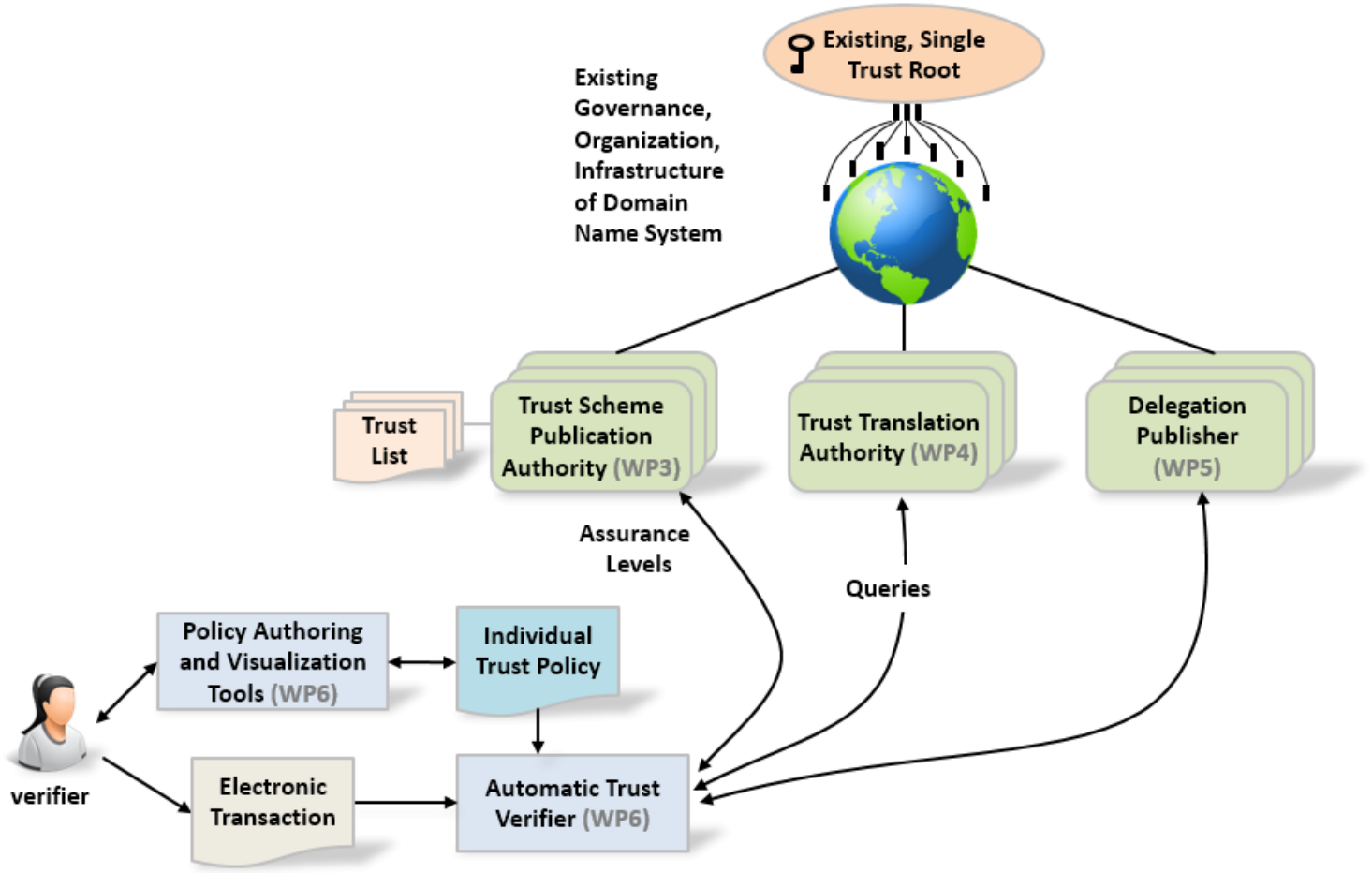
- Development of a lightweight, global trust infrastructure for
  - publication,
  - querying, and
  - cross-jurisdiction translation

  } of relevant information (e.g. trust scheme, level of assurance)
- using the existing global Domain Name System (DNS)

- ➢ Enables retrieval & discovery of ID information
- ➢ Facilitates your own decision making

LIGHT*est* has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

The LIGHT*est* Architecture



LIGHT*est* has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

What LIGHT*est* is and what LIGHT*est* is NOT

- LIGHTest does not provide an alternative to eIDs or business registers
- LIGHTest does not allow you to outsource trust decisions
- LIGHTest does allow you to use a global, known and trusted infrastructure to:
  - Retrieve declared policy details from partners
  - Verify those declared policies partners from Trust Lists
  - Determine trust assurances behind partners
  - Facilitate your own decision making
- While also providing a path for trustworthy future business

LIGHT*est* has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

The European LIGHT*est* Project

- Horizon 2020
- Innovation Action
- Call: H2020-DS-2015-1 *Trust eServices*
- Started September 1, 2016
- 36 months
- Estimated cost of 8.7 Mio Euros
- 14 partners from 9 countries
- Coordinated by Fraunhofer

LIGHT*est* has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

Conclusions: LIGHTest and Blockchain

- Blockchain needs assistance to be applied in Use Cases
- Combining Blockchain and LIGHTest could address some of the limitations or challenges in blockchain solutions (ability to verify and make transactions)
- Provides benefits for LIGHTest as it would ensure that transactions are documented in an unchangeable register/ledger with identities that could be verified which could

LIGHTest and Blockchain could complement eachother and compensate for one anothers weaknesses

LIGHTest has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321