eGov-Campus Ringvorlesung, 31. März 2023

# Einsatz der Blockchain-Technologie im öffentlichen Sektor


## PROF. DR. NILS URBACH

FRANKFURT UNIVERSITY OF APPLIED SCIENCES,
RESEARCH LAB FOR DIGITAL INNOVATION & TRANSFORMATION

KERNKOMPETENZZENTRUM FINANZ- & INFORMATIONSMANAGEMENT

FRAUNHOFER-INSTITUT FÜR ANGEWANDTE INFORMATIONSTECHNIK FIT,
INSTITUTSTEIL WIRTSCHAFTSINFORMATIK

WWW.DITLAB.ORG | WWW.FIM-RC.DE | WWW.WIRTSCHAFTSINFORMATIK.FRAUNHOFER.DE

## Vortrag - Ringvorlesung

Prof. Dr. Nils Urbach

Frankfurt University of Applied Sciences
Leiter Fraunhofer Blockchain-Labor

©Nils Urbach

## Grußwort

Bettina Stark-Watzinger

Bundesministerin für Bildung und Forschung

©Bundesregierung – Guido Bergmann

# Die Digitalisierung in Deutschland geht eher schleppend voran

Onlineverwaltung

**Scholz verspricht schnellere Behörden-Digitalisierung – und rauscht ab**

Spiegel Online, am 9. Juni 2022

Digitalisierung der Verwaltung: Gegen jede Logik

heise, am 27. Januar 2023

**Berliner können nicht mal ein Viertel der Behördengänge online erledigen**

rbb24, am 7. Juni 2022

Digitalisierung der Verwaltung in Deutschland geht nur langsam voran

bidt, am 1. Mai 2021

DIGITALISIERUNG DER VERWALTUNG

**„Klar hinter den Erwartungen“ – Normenkontrollrat kritisiert die Innenministerin öffentlich**

Handelsblatt, am 9. Februar 2023

# Im Rahmen des OZGs sollten bis Ende 2022 insgesamt 575 Verwaltungsleistungen digitalisiert werden

# Was hat die Digitalisierung der öffentlichen Verwaltung bisher aufgehalten?

**Förderale Strukturen**

Förderale Verantwortlichkeiten verhindern die zentrale Speicherung von Daten

**Fälschungsgefahr**

Die Vervielfältigung von digitalen Dokumenten & Bescheinigungen ist leicht

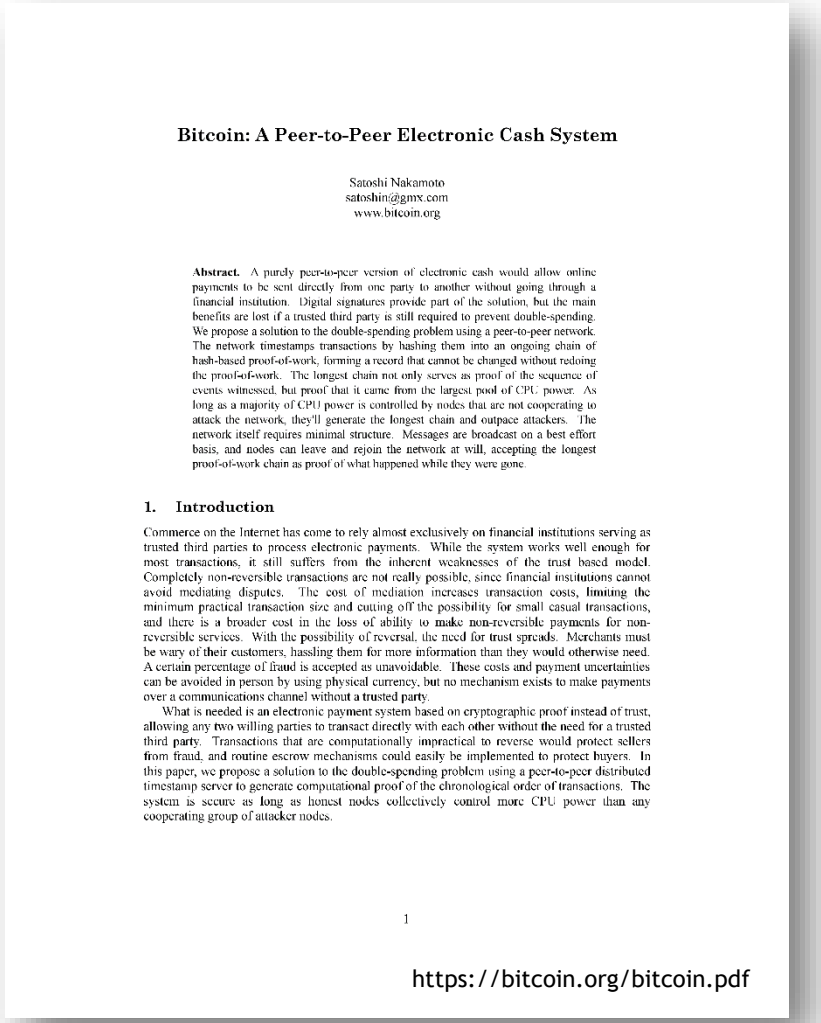
**Hoheitsverlust**

Kontrolle über die Hoheit von Dokumenten ist im digitalen Raum herausfordernd

# 01

# Grundlagen der Blockchain-Technologie

# Die Bitcoin-Blockchain wurde im November 2008 unter dem Pseudonym Satoshi Nakamoto vorgestellt



**Bitcoin: A Peer-to-Peer Electronic Cash System**

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

**Abstract.** A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

**1. Introduction**

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

1

https://bitcoin.org/bitcoin.pdf

bitcoin

**Aktuelle Marktkapitalisierung**
**[30. März 2023]**

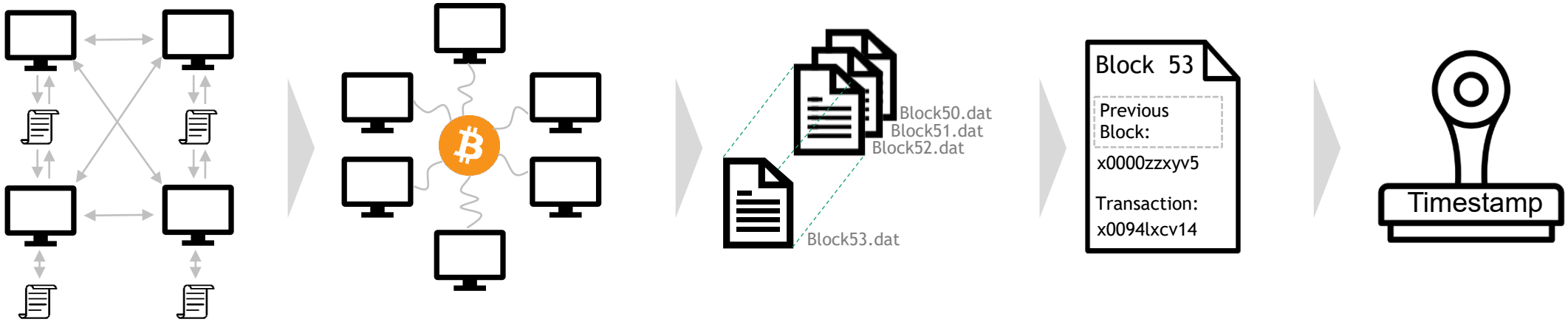
€510.736.560.274

# Blockchain speichert Transaktionen transparent, chronologisch und unveränderbar in einem Netzwerk

**Blockchain**

- *Laufend aktualisiertes*, *chronologisch* geordnetes und *öffentlich* einsehbares Register mit Informationen über *Besitzverhältnisse* und *Transaktionen*
- Kryptographische Prinzipien gewähren eine *rückwirkende Unveränderbarkeit* der Einträge

## Funktionsweise




Verteiltes Hauptbuch | Konsens-mechanismus | Hinzunahme neuer Blöcke | Referenzierung vorheriger Blöcke | Permanenter Zeitstempel

# Chain Code bzw. Smart Contracts erweitern die Anwendungsmöglichkeiten von Blockchain

**Chain Code bzw. Smart Contracts**

- *Programmcode* in einer Blockchain („Chain Code“), der ausgeführt wird, wenn bestimmte Ereignisse eintreten oder Konditionen erfüllt sind
- Nach diesem Prinzip können Geschäftslogiken (z.B. Verträge) abgebildet werden

## Funktionsweise

- Skripte mit der vereinbarten Logik („Vertragsdetails“) werden in einer bestimmten Adresse der Blockchain gespeichert
- Externe Ereignisse lösen eine Transaktion an die spezifizierte Adresse aus
- Der gespeicherte Programmcode mit der vereinbarten Logik wird ausgeführt

# Mittlerweile gibt nicht nur mehrere Kryptowährungen, sondern auch eine Vielzahl unterschiedlicher Blockchains

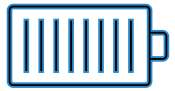
| | | | | |
|---|---|---|---|---|
| Anwendung | Kryptowährung als alternatives Zahlungsmittel | Blockchain als Weltcomputer | Blockchain für Unternehmen | „Blockchain“ für das Internet der Dinge |
| Technologie | Bitcoin-Blockchain | Ethereum-Blockchain | Hyperledger-Blockchain | IOTA-Tangle |

Die Blockchain kann als Technologieklasse betrachtet werden, je nach Umsetzung unterscheiden sich ihre Eigenschaften

# Charaktereigenschaften der Blockchain-Technologie

**Unveränderbarkeit**
Eine *rückwirkende Veränderung* der Transaktionen ist aufgrund des notwendigen Rechenaufwands unwahrscheinlich.

***und***



**Verfügbarkeit**
Durch den Einsatz eines *verteilten Netzwerks* werden Transaktionen redundant ausgeführt, was zu einer Verfügbarkeit auch bei Ausfall einzelner Knoten führt.

***und***

**Neutralität**
Stakeholder müssen sich nicht auf zentrale Infrastruktur einigen, sondern können sich am Netzwerk *selbst beteiligen*.

# 02

# Anwendungsbeispiel: Organisationübergreifende Prozesse

# Was hat die Digitalisierung der öffentlichen Verwaltung bisher aufgehalten?

**Förderale Strukturen**

Förderale Verantwortlichkeiten verhindern die zentrale Speicherung von Daten



**Fälschungsgefahr**

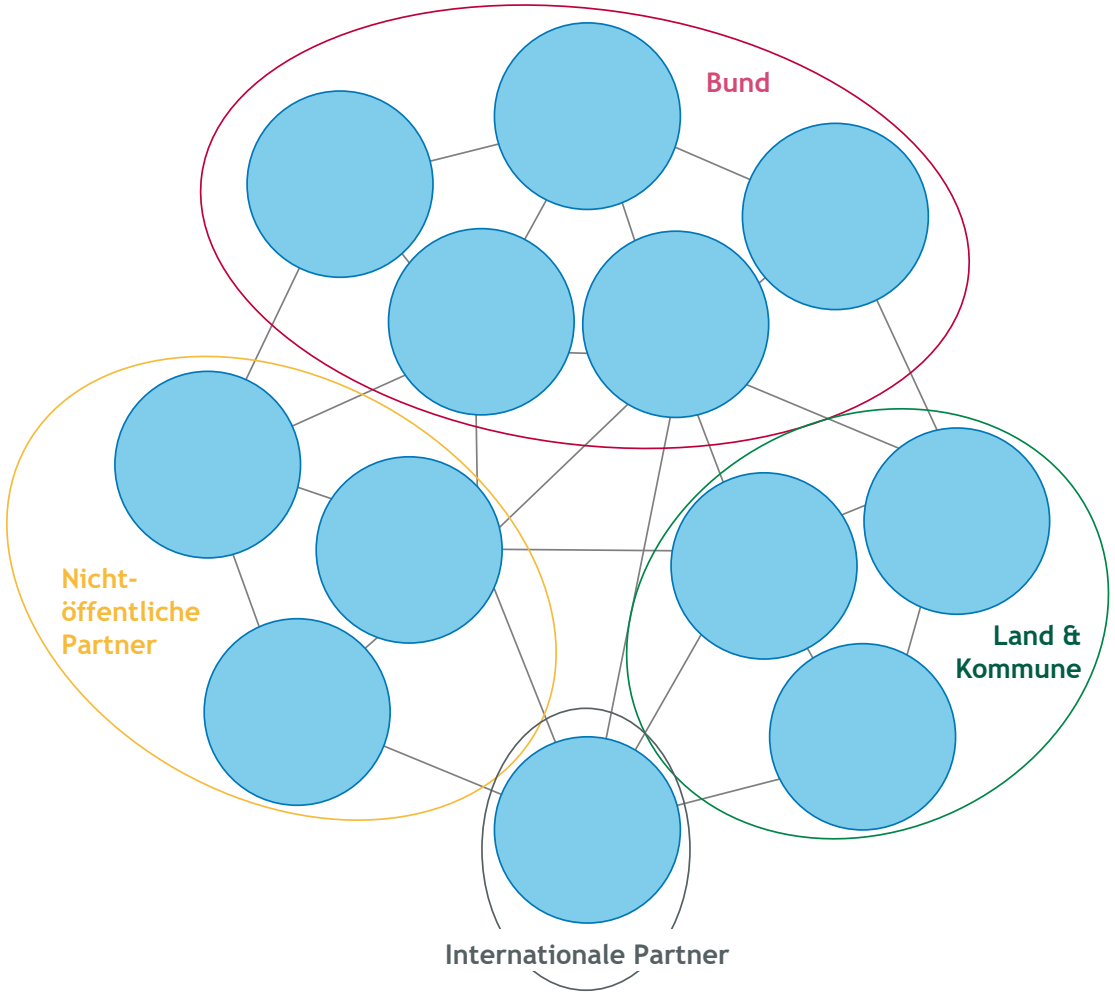
Die Vervielfältigung von digitalen Dokumenten & Bescheinigungen ist leicht



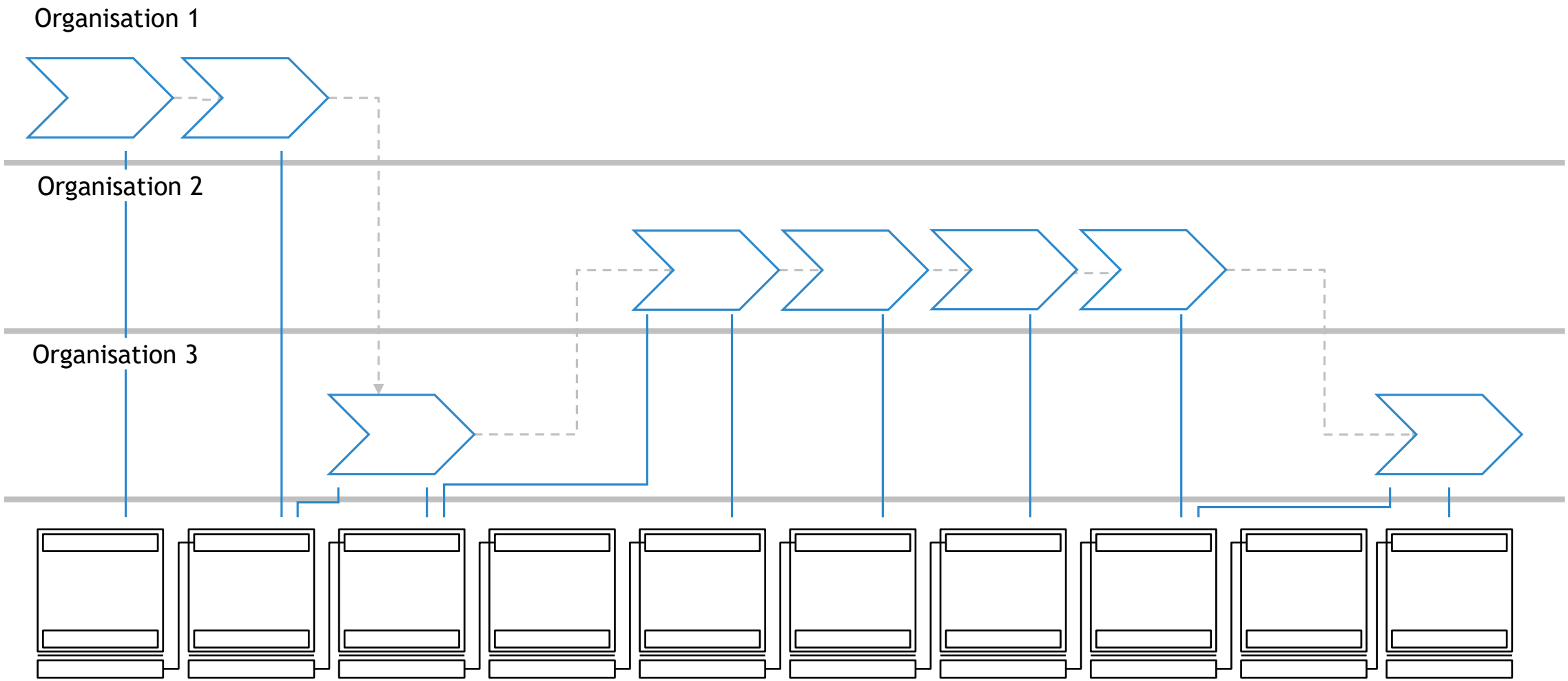
**Hoheitsverlust**

Kontrolle über die Hoheit von Dokumenten ist im Digitalen Raum herausfordernd

# Bei Prozessen der öffentlichen Verwaltung arbeiten oftmals viele unterschiedliche Behörden zusammen



# Die Blockchain-Technologie erlaubt das Management organisationsübergreifende Prozesse



# Unser Projekt beim Bundesamt für Migration und Flüchtlinge

Bundesamt
für Migration
und Flüchtlinge

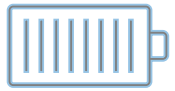
**Lösungsansatz:** Entwicklung einer Föderalen Blockchain-Infrastruktur Asyl (FLORA) für behördenübergreifende Zusammenarbeit im Asylprozess

**Anwendungsbereich „Registrierung, Aktenanlage und Anhörung“**

# Welche Charaktereigenschaften der Blockchain-Technologie spielen eine besondere Rolle?

**Unveränderbarkeit**
Eine *rückwirkende Veränderung* der Transaktionen ist aufgrund des notwendigen Rechenaufwands unwahrscheinlich.

*und*



**Verfügbarkeit**
Durch den Einsatz eines *verteilten Netzwerks* werden Transaktionen redundant ausgeführt, was zu einer Verfügbarkeit auch bei Ausfall einzelner Knoten führt.

***und***

**Neutralität**
Stakeholder müssen sich nicht auf zentrale Infrastruktur einigen, sondern können sich am Netzwerk *selbst beteiligen*.

# Welche Herausforderungen der öffentlichen Verwaltung werden hier adressiert?

**Förderale Strukturen**

Förderale Verantwortlichkeiten verhindern die zentrale Speicherung von Daten



**Fälschungsgefahr**

Die Vervielfältigung von digitalen Dokumenten & Bescheinigungen ist leicht



**Hoheitsverlust**

Kontrolle über die Hoheit von Dokumenten ist im Digitalen Raum herausfordernd

Ein organisationsübergreifendes Register sollte **nicht** als zentraler Datenspeicherort verwendet werden, sondern auf Informationen verweisen

# 03

# Anwendungsbeispiel: Gültigkeitsregister

# Was hat die Digitalisierung der öffentlichen Verwaltung bisher aufgehalten?



**Förderale Strukturen**

Förderale Verantwortlichkeiten verhindern die zentrale Speicherung von Daten

**Fälschungsgefahr**

Die Vervielfältigung von digitalen Dokumenten & Bescheinigungen ist leicht

**Hoheitsverlust**

Die Hoheit über die Gültigkeit von Dokumenten ist im digitalen Raum herausfordernd

# Unser Projekt bei der Bundesnotarkammer

BUNDESNOTARKAMMER
KÖRPERSCHAFT DES ÖFFENTLICHEN RECHTS

Bayerisches Staatsministerium der Justiz

**Lösungsansatz:** Entwicklung eines digitalen Gültigkeitsregisters auf Blockchain-Basis



# Über Desktop-PC, Tablet oder Smartphone kann die Gültigkeit der Urkunden jederzeit online geprüft werden



- Über **Desktop-PC, Tablet oder Smartphone** kann die Gültigkeit der Urkunden **jederzeit online** geprüft werden
- Die Urkunden müssen **nicht mehr in Papierform** mitgeführt werden
- Das Frontend ist **einfach und intuitiv**
- Wenn eine Urkunde ungültig wird, kann sie **sofort im Register gesperrt** werden; eine Rückerlangung oder Kraftloserklärung von Papierurkunden entfällt
- Der Bayerische Justizminister Georg Eisenreich in einer Pressemitteilung am 26. Mai 2020:

  **„Was in der Papierwelt drei Monate dauert, könnte künftig mit drei Klicks erledigt sein“**

# Welche Charaktereigenschaften der Blockchain-Technologie spielen eine besondere Rolle?

**Unveränderbarkeit**
Eine *rückwirkende Veränderung* der Transaktionen ist aufgrund des notwendigen Rechenaufwands unwahrscheinlich.

***und***

**Verfügbarkeit**
Durch den Einsatz eines verteilten Netzwerks werden Transaktionen redundant ausgeführt, was zu einer Verfügbarkeit auch bei Ausfall einzelner Knoten führt.

***und***

**Neutralität**
Stakeholder müssen sich nicht auf zentrale Infrastruktur einigen, sondern können sich am Netzwerk *selbst beteiligen*.

# Welche Herausforderungen der öffentlichen Verwaltung werden hier adressiert?



**Förderale Strukturen**

Förderale Verantwortlichkeiten verhindern die zentrale Speicherung von Daten

**Fälschungsgefahr**

Die Vervielfältigung von digitalen Dokumenten & Bescheinigungen ist leicht

**Hoheitsverlust**

Kontrolle über die Hoheit von Dokumenten ist im Digitalen Raum herausfordernd

Ein Gültigkeitsregister sollte möglichst interoperabel sein, um viele Anwendungsfälle unterstützen zu können

# 04

# Anwendungsbeispiel: Self-Sovereign Identities

# Was hat die Digitalisierung der öffentlichen Verwaltung bisher aufgehalten?



**Förderale Strukturen**

Förderale Verantwortlichkeiten verhindern die zentrale Speicherung von Daten

**Fälschungsgefahr**

Die Vervielfältigung von digitalen Dokumenten & Bescheinigungen ist leicht

**Hoheitsverlust**

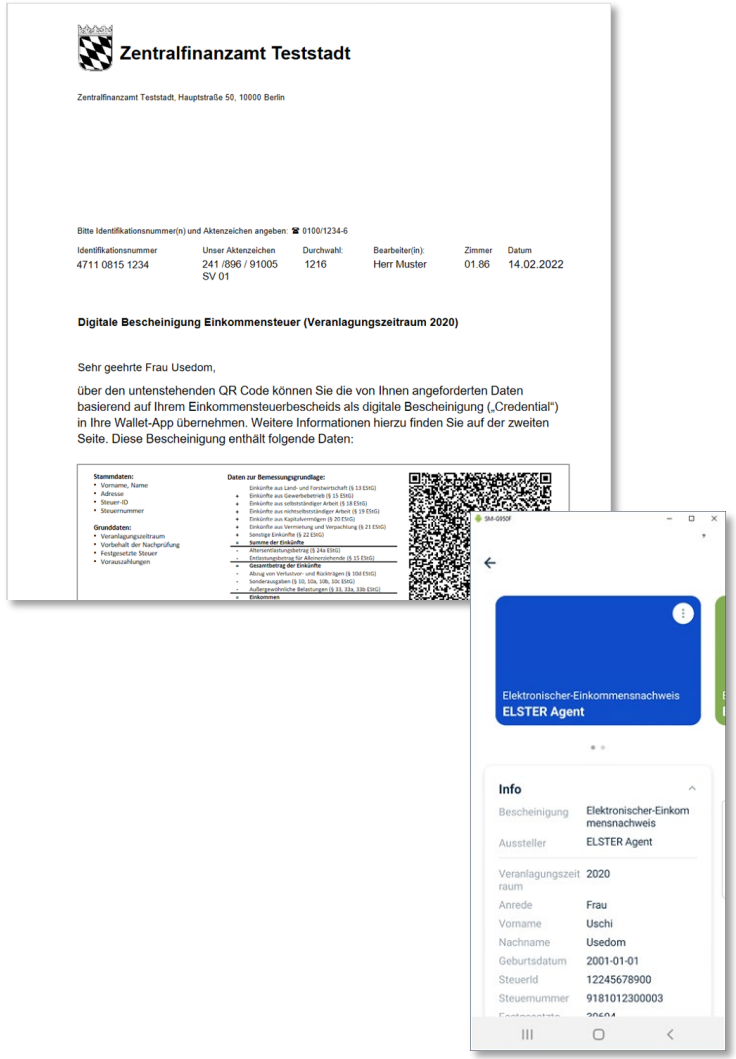
Die Hoheit über die Gültigkeit von Dokumenten ist im digitalen Raum herausfordernd

# Unser Projekt mit dem Bayerischen Landesamt für Steuern

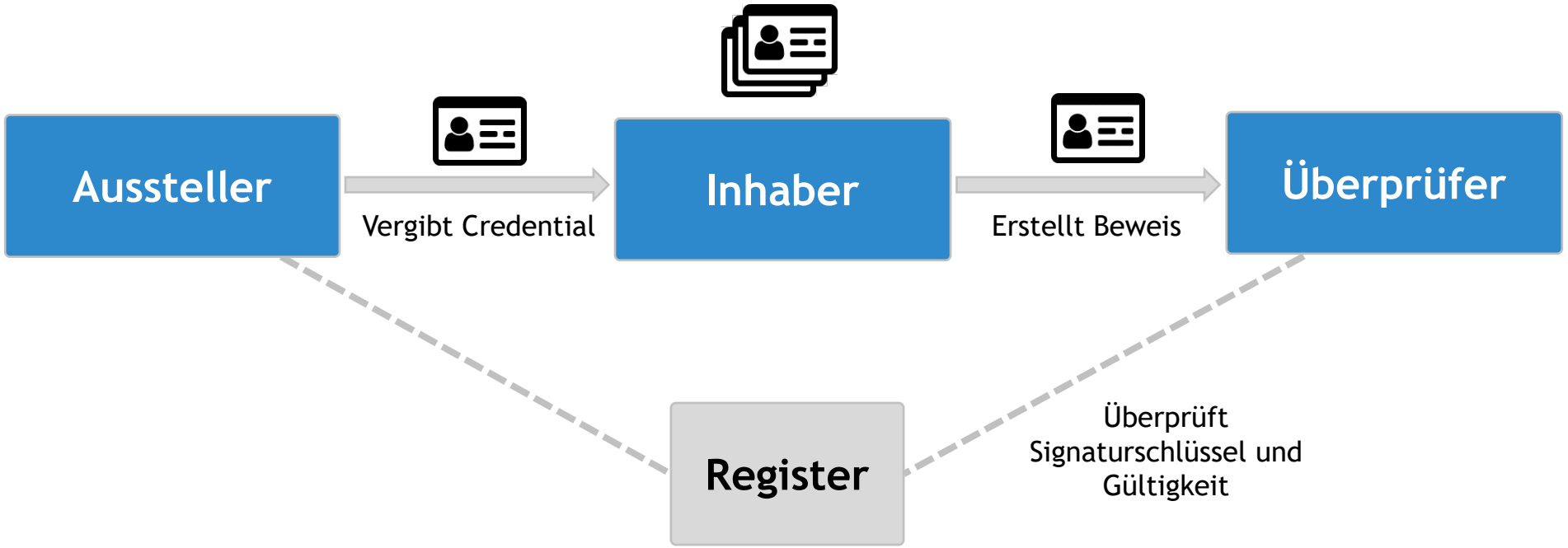
Bayerisches Staatsministerium für Digitales

Bayerisches Landesamt für Steuern

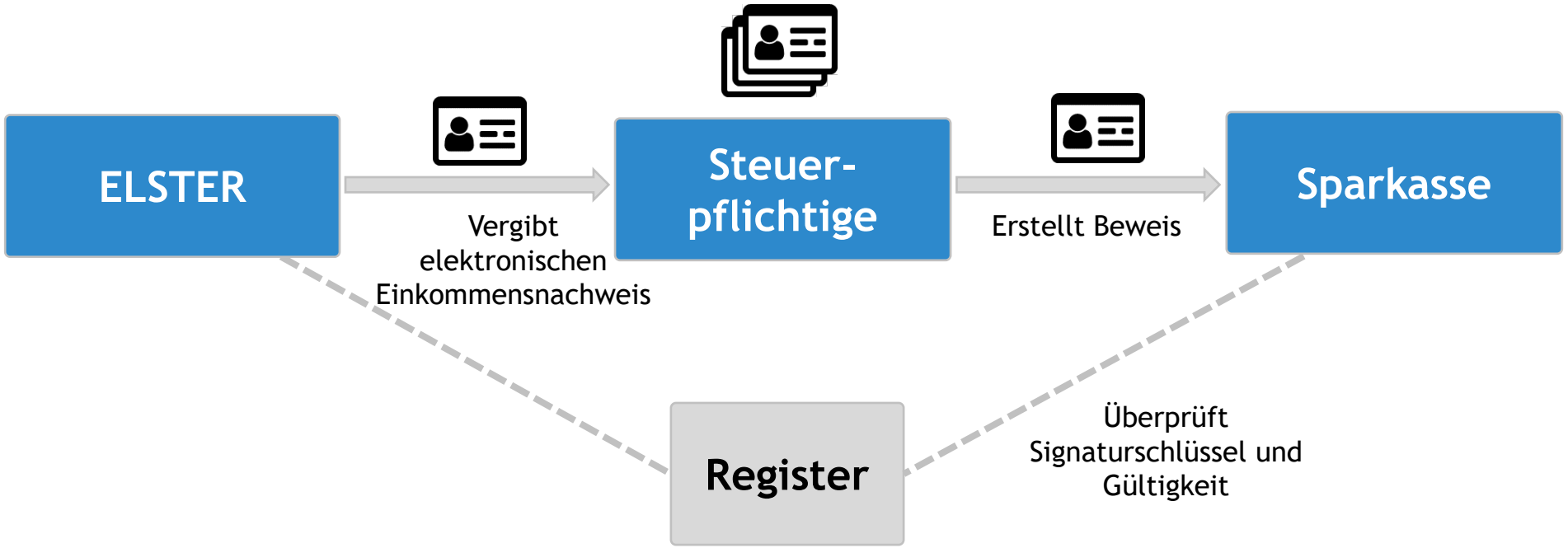
**Lösungsansatz:** Elektronische Einkommensnachweise



# Hierfür verwenden wir das Konzept der Self-Sovereign Identities (SSI)



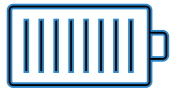
# Mithilfe des elektronischen Einkommensnachweises können beispielsweise Kredite beantragt werden



# Welche Charaktereigenschaften der Blockchain-Technologie spielen eine besondere Rolle?

**Unveränderbarkeit**
Eine *rückwirkende Veränderung* der Transaktionen ist aufgrund des notwendigen Rechenaufwands unwahrscheinlich.

***und***



**Verfügbarkeit**
Durch den Einsatz eines verteilten Netzwerks werden Transaktionen redundant ausgeführt, was zu einer Verfügbarkeit auch bei Ausfall einzelner Knoten führt.

***und***

**Neutralität**
Stakeholder müssen sich nicht auf zentrale Infrastruktur einigen, sondern können sich am Netzwerk *selbst beteiligen*.

# Welche Herausforderungen der öffentlichen Verwaltung werden hier adressiert?



**Förderale Strukturen**

Förderale Verantwortlichkeiten verhindern die zentrale Speicherung von Daten

**Fälschungsgefahr**

Die Vervielfältigung von digitalen Dokumenten & Bescheinigungen ist leicht

**Hoheitsverlust**

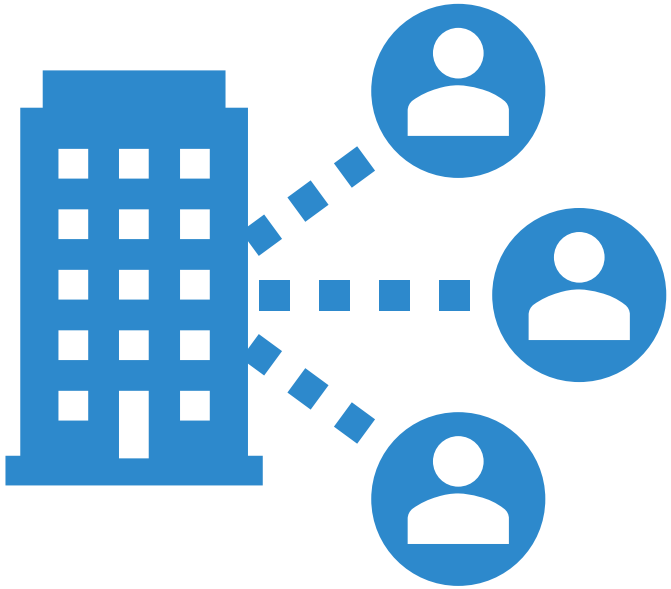
Kontrolle über die Hoheit von Dokumenten ist im Digitalen Raum herausfordernd

Self-Sovereign Identities sollten im Sinne eines Ökosystems verstanden werden, in dem es eine Vielzahl von Ausstellern, Nutzern und Verifizierern gibt

# 05

# Abschluss & Zusammenfassung

# Die Herausforderung, die öffentliche Verwaltung zu digitalisieren, ist enorm



Die Blockchain-Technologie kann dabei helfen, mit einer neutralen Infrastruktur föderale Hürden zu bewältigen

SSI kann dabei unterstützen, ein Ökosystem für fälschungsresistente, digitale Nachweise zu schaffen

In der öffentlichen Verwaltung müssen noch zahlreiche weitere Hürden der Digitalisierung bewältigt werden

# Das Research Lab for Digital Innovation & Transformation (ditlab) in Frankfurt

FRANKFURT UNIVERSITY OF APPLIED SCIENCES

dit lab
Research Lab for Digital Innovation & Transformation

FRANKFURT UNIVERSITY OF APPLIED SCIENCES

**Wir arbeiten und forschen an innovativen Projekten u.a. in den Bereichen:**

- Digitale Transformation
- Blockchain-Technologie
- Künstliche Intelligenz
- Digitales Identitätsmanagement
- Machine Economy

**Unsere Partner:**

fim Kernkompetenzzentrum Finanz- & Informationsmanagement

Fraunhofer FIT

**Förderungen:**

Bundesministerium für Bildung und Forschung

HESSEN

ZE Zentrum
VE verantwortungsbewusste
DI Digitalisierung
*Centre Responsible Digitality*

Fraunhofer FIT

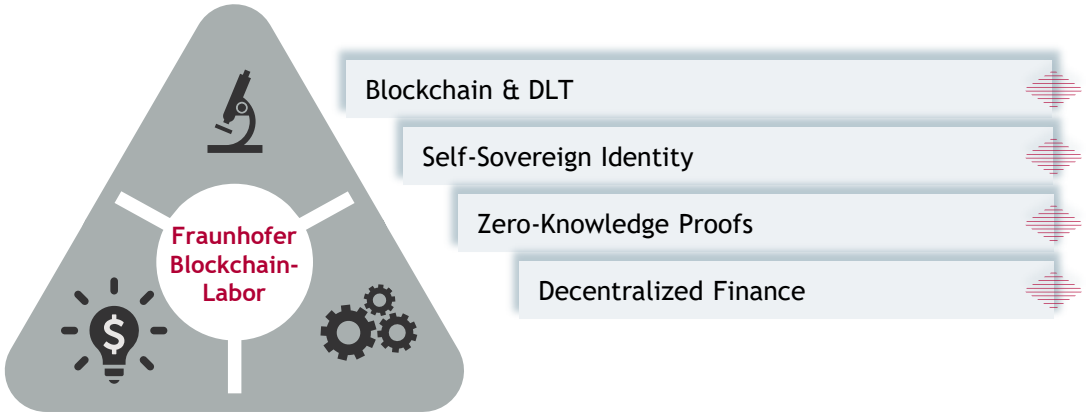
hessian.AI

fim Finanz- & Informationsmanagement GmbH

# Das Fraunhofer Blockchain-Labor – Forschung mit Zukunftspotential

## Fraunhofer Blockchain-Labor

- Das Fraunhofer Blockchain-Labor ist eine multidisziplinäre Einrichtung zur **Konzeption, Entwicklung** und **Evaluation** von **Blockchain-Lösungen** und **dezentralen Systemen**.
- Wir bieten **nachhaltige, innovative** und **wertstiftende IT-Lösungen** für **alle Branchen**.




Workshops, Vorträge & Schulungen

Konzepte, Analysen & Studien

Prototypen, MVPs & Netzwerkaufbau

Publikationen & Wissenschaftliche Community

## Unser Leistungsspektrum

### WISSENSCHAFTLICHE BEGLEITUNG

- Anwendung wissenschaftlicher Methoden im interdisziplinären Umfeld
- Überführung aktueller Erkenntnisse aus der Forschung in praxistaugliche, integrative Anwendungen

#State-of-The-Art

### GESCHÄFTSMODELLENTWICKLUNG

- Begleitung aus rechtlicher, ökonomischer und technischer Perspektive
- Anforderungs- und Potentialanalysen neuer Technologien
- Einordnung und Entwicklung von disruptiven Geschäftsmodellen

#Value-Driven

### TECHNOLOGIE-IMPLEMENTIERUNG

- Konzeptionierung technischer Systeme aufbauend auf Blockchain und anderen dezentralen Lösungen
- Implementierung von Prototypen mit Hilfe agiler Methoden sowie deren technische Evaluierung

#Cutting-Edge

FRANKFURT UNIVERSITY OF APPLIED SCIENCES

dit lab
Research Lab for Digital Innovation & Transformation

fim
Kernkompetenzzentrum
Finanz- & Informationsmanagement

Fraunhofer FIT

# Vielen Dank für Ihre Aufmerksamkeit

## Kontakt:


**Prof. Dr. Nils Urbach**
Frankfurt University of Applied Sciences & Fraunhofer FIT

nils.urbach@fim-rc.de
+49 69 1533-3849
https://www.linkedin.com/in/nurbach/
@nilsurbach