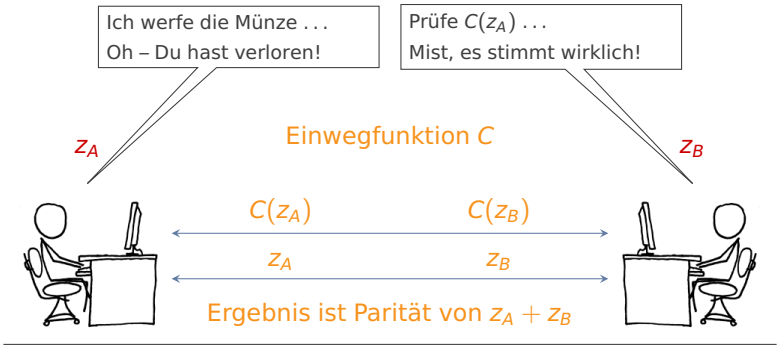
universität innsbruck

Prinzipien von Blockchain-Systemen

Einführung, Grundlagen, Schichtmodell

Rainer Böhme

Kryptographischer Münzwurf



Allgemeine Lösung: Kryptographische Commitments

Verallgemeinerung

Prinzip: Einigung auf einen Zustand ohne dritte Partei

1. Kryptographischer Münzwurf: ein Bit
2. Erweiterung des Zustandsraums: Kontensalden
3. Erweiterung des Teilnehmerkreises: Lotterie (Bsp.)
4. Hash-Verkettung: Einbezug der Vergangenheit – “Blockchain”
5. **“Money is memory”**

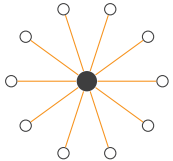
Geld als kollektives Gedächtnis

“Money may only be an imperfect substitute for high quality information storage and access. [. . .]

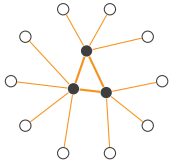
Government’s monopoly on seignorage might be in some jeopardy as information access and storage costs decline.”

Kocherlakota, N. R. *Money is Memory*. Research Department Staff Report 218, Federal Reserve Bank of Minneapolis, 1996.

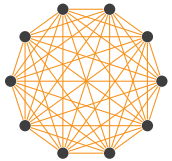
Topologien für verteilte Systeme



zentralisiert



föderal



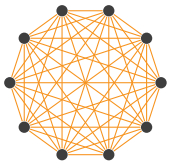
dezentralisiert

Verteilung der Kontrolle

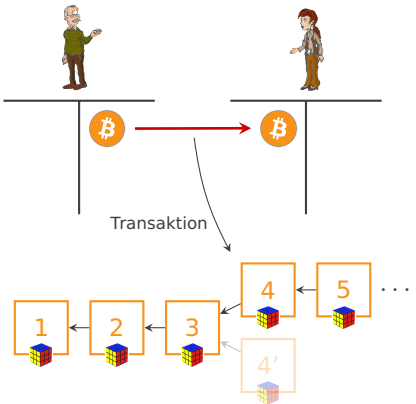
asymmetrisch ⟷ symmetrisch

Vgl. VO Rechnernetze und Internettechnik, Kapitel „Verteilte Systeme“, 8. Juni 2017, S. 6

Bitcoin auf einer Folie



P2P-Netz



Bitcoin-Blockchain

Vgl. VO Rechnernetze und Internettechnik, Kapitel „Verteilte Systeme“, 13. Juni 2019, S. 23

Konzept dieses Wahlmoduls

Ausgangspunkt Bitcoin als verteiltes System mit dezentraler Kontrolle (vgl. RNIT)

Wahl der Perspektive

- Designentscheidungen verstehen
- Zusammenspiel der Komponenten erklären
- Allgemeiner Zugang zu Blockchain-Systemen, Bitcoin nur als Beispiel
- Kryptographie als Blackbox – Vorsicht!

Schwerpunkte

- Prinzipien: Theorie in Vorlesung und praktische Übungen
- Analyse: Am Bsp. Bitcoin mit BlockSci
- Entwicklung: Am Bsp. Ethereum mit Solidity

Voraussetzung Alle Pflichtmodule der ersten vier Semester

Ziele der Veranstaltung

Lernergebnis
„Wie kann man das **Prinzip der verteilten (dezentralen) Kontrolle** für weitgehend frei programmierbare Informationstechnische Systeme realisieren?

Blockchain-Systeme erreichen dieses Ziel unter bestimmten Voraussetzungen.

Sie ermöglichen neue Anwendungen wie

- **Zahlungssysteme**, die unabhängig von konventionellen Währungssystemen sind, oder
- **Verträge**, die ohne Rekurs auf ein Rechtssystem technisch durchgesetzt werden.

Dieser Kurs vermittelt **Grundwissen** über elementare Techniken, die in modernen Blockchain-Systemen zum Einsatz kommen.

Zur Analyse der Technik sowie ihrer gesellschaftlichen Konsequenzen werden **ausgewählte Aspekte** der Rechts-, Sozial- und Wirtschaftswissenschaften für InformatikerInnen aufbereitet vermittelt.“

Syllabus

05.03.20	1. Einführung und Grundlagen	
12.03.20	2. Infrastruktur für Blockchain-Systeme	
19.03.20	3. Transaktionslogik in Bitcoin und Ethereum	
26.03.20	Übung: Blockchain-Analyse mit BlockSci	(Martin Plattner)
02.04.20	Übung: Besprechung der Übungsaufgaben	
23.04.20	4. Datenschutz und Sicherheit	
30.04.20	5. Skalierbarkeit, Off-Chain-Transaktionen, Governance	
07.05.20	Übung: Ethereum-Programmierung mit Solidity	(Michael Fröwis)
14.05.20	Übung: Besprechung der Übungsaufgaben	
28.05.20	6. Wiederholung, Fragestunde	
04.06.20	Klausur	

Änderungen vorbehalten.

Ansprechpartner

Professor

Univ.-Prof. Dr.-Ing.
Rainer Böhme

Sekretärin

Jenifer
Payr

Techniker

Manuel
Knoflach-Schrott

WissenschaftlerInnen

Dr. Svetlana
Abramova

Dr. Cecilia
Pasquini

Dr. Daniel
Woods

Michael
Fröwis

Maximilian
Hils

Patrik
Keller

Alexander
Schlögl

Organisatorisches

Die **Vorlesung+Übung** ist dreistündig und hat 5 ECTS-AP.

Der Lernerfolg wird zu 75 % in einer schriftlichen Klausur und zu 25 % durch Bewertung der Übungszettel überprüft. Um das Modul positiv abzuschließen, muss jede Teilleistung mindestens mit der Note 4 bewertet worden sein.

Der Lehrende entscheidet, ob Wiederholungsprüfungen bei Bedarf mündlich abgenommen werden.

Formell besteht Anwesenheitspflicht. Wir werden diese mit Rücksicht auf die Covid-19-Situation bis auf Weiters nicht überprüfen. Jedoch müssen alle Übungszettel fristgerecht abgegeben werden.

Es gibt kein Lehrbuch, das die Inhalte in dieser kompakten und vereinfachten Form vermittelt.

Verpassen Sie nach Möglichkeit keine einzige Veranstaltung.

Literatur

Bücher

- Narayanan, A., Bonneau, J., Felten, E., Miller, A., and Goldfeder, S. *Bitcoin and Cryptocurrency Technologies*. Princeton University Press, 2016.
- Wattenhofer, R. *Distributed Ledger Technology: The Science of the Blockchain*. CreateSpace Independent Publishing Platform, 2. Auflage, 2017.

Aufsätze (haupts. Bitcoin)

- Nakamoto, S. *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2008. Mimeo.
- Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J., and Felten, E. SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. In *IEEE Symposium on Security and Privacy*. San Jose, CA, USA, 2015, pp. 104–121.
- Tschorsch, F. and Scheuermann, B. Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies. *IEEE Communications Surveys and Tutorials*, 18, 3 (2016), 2084–2123.
- Zohar, A. Bitcoin: Under the Hood. *Communications of the ACM*, 58, 9 (2015), 104–113.

Relevante Literatur ist breit gestreut. Schreiben und denken Sie mit!

Weitere Quellen

Blockchain-Systeme und Gesellschaft

- Böhme, R., Christin, N., Edelman, B., and Moore, T. Bitcoin: Economics, Technology, and Governance. *Journal of Economic Perspectives*, 29, 2 (2015), 213–238.
- Pesch, P. and Böhme, R. Datenschutz trotz öffentlicher Blockchain? Chancen und Risiken bei der Verfolgung und Prävention Bitcoin-bezogener Straftaten. *Datenschutz und Datensicherheit*, 41, 2 (2017), 93–98.
- Böhme, R. and Pesch, P. Technische Grundlagen und datenschutzrechtliche Fragen der Blockchain-Technologie. *Datenschutz und Datensicherheit*, 41, 8 (2017), 473–481.

Sammlung wissenschaftlicher Aufsätze

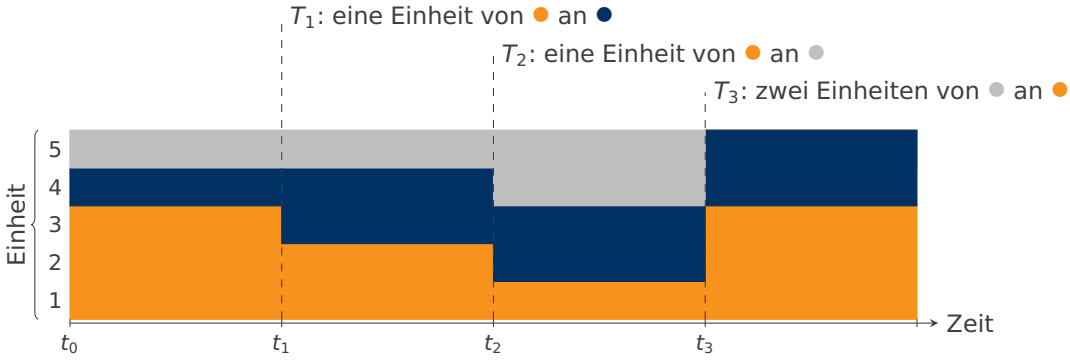
- CABRA – Comprehensive Academic Bitcoin Research Archive
  `https://cdecker.github.io/btcresearch/`

News, „graue Literatur“, Daten

- coindesk.com, bitcointalk.org, Reddit, div. Whitepaper, . . .
- blockchain.info, bitcoincharts.com, etherscan.io, coinmarketcap.com, . . .

Verwaltung eines virtuellen Gutes

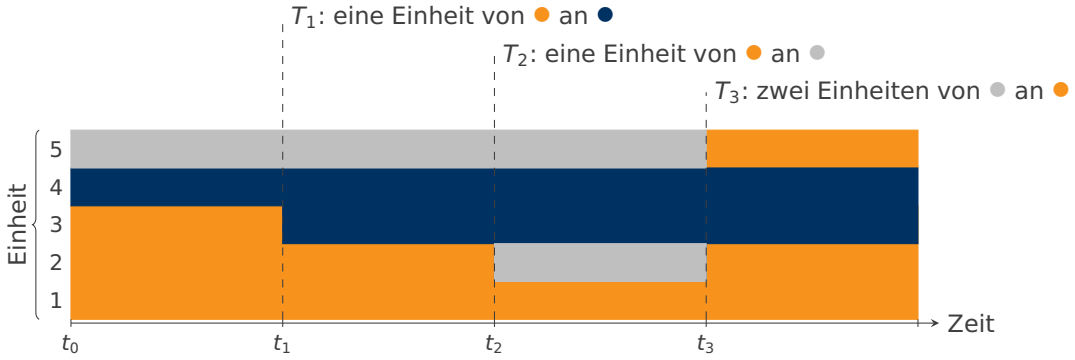
- Differenzkodierung durch Transaktionen
- Einhaltung von Nebenbedingungen
  - 1. Summe aller Konten konstant
  - 2. Kein Konto negativ
- Sichere Aufzeichnung



Verwaltung eines virtuellen Gutes

- Differenzkodierung durch Transaktionen
- Einhaltung von Nebenbedingungen
- Sichere Aufzeichnung

Variante ohne Fungibilität



Transaktionen als Zustandsübergänge

Beispiel Zustandsraum R kodiert den „Besitz“ von ≤ 5 virtuellen Einheiten

Jede Transaktion T beschreibt formal

- Menge A der Ausgangzustände
- Eindeutige Abbildung von A auf gültige Zielzustände $Z \subset R$

Verifikation von Transaktionen

1. Prüfung der syntaktischen Korrektheit
2. Prüfung, ob aktueller Systemzustand in A enthalten ist
3. Ermessensspielraum des (ersten) Prüfers: Ist der Zielzustand wünschenswert?

Interpretieren Sie die aus DBMS bekannten AKID-Eigenschaften für Blockchain-Transaktionen.

Von Transaktionen zum Distributed Ledger

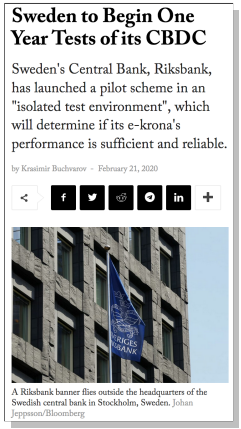
Die meisten Blockchain-Systeme realisieren eine verteilte, öffentliche Datenbank, welche Transaktionen entgegennimmt und erfolgreich verifizierte Transaktionen in definierter Reihenfolge persistent speichert (*append only*).

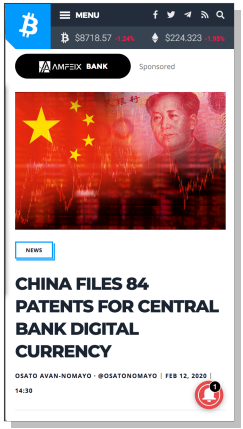
Somit entsteht eine Folge gültiger Zustände, die stetig fortgeschrieben wird.

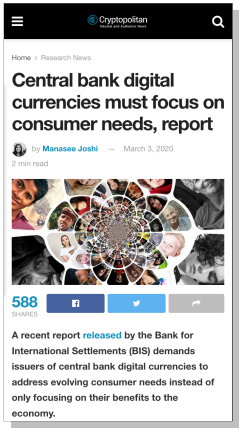
Verbleibende Probleme definieren Gestaltungsspielraum für Lösungen:

1. Kompakte Kodierung von Transaktionen für große Zustandsräume
2. Bei „Besitz“-Interpretation: Autorisation der Weitergabe
3. Identifikation der Parteien
4. Konfliktlösung: Einigung auf einen gemeinsamen Zustand

Pause







bitcoinist.com, chainbulletin.com, cointelegraph.com, cryptopolitan.com (Abruf: 4. März 2020)

Kryptographische Commitments

Kryptographie ist viel mehr als Verschlüsselung.

Definition (vereinfacht)

- Probabilistischer Algorithmus

$$\text{Commit}(\boldsymbol{m}) \to (c, r)$$

- Algorithmus

$$\text{Open}((c, r), \boldsymbol{m}) \to \{\text{wahr}, \text{falsch}\}$$

Sprachgebrauch:

- $\boldsymbol{m}$ ist eine Nachricht (*message*)
- c heißt *commitment*
- r heißt *reveal value* oder *opening*

Eigenschaften

1. **Korrektheit**

$$\text{Open}(\text{Commit}(\boldsymbol{m}), \boldsymbol{m}) = \text{wahr}$$

2. **Hiding** (informell): c enthält keine Information über $\boldsymbol{m}$.
   $\to$ schützt i.d.R. den **Sender**
3. **Binding** (informell): Der Sender kann c nicht für eine andere Nachricht $\boldsymbol{m'} \neq \boldsymbol{m}$ öffnen.
   $\to$ schützt i.d.R. den **Empfänger**

Autorisation allein mit Commitments

Idee

- Besitzzuweisende Transaktion enthält frisches c (gibt neuer Besitzer bekannt)
- Weitergabe-Transaktion ist nur gültig, wenn sie ein passendes r enthält.

$\rightarrow$ Kopplung von Besitz i. S. v. Verfügungsgewalt an Kenntnis von r.

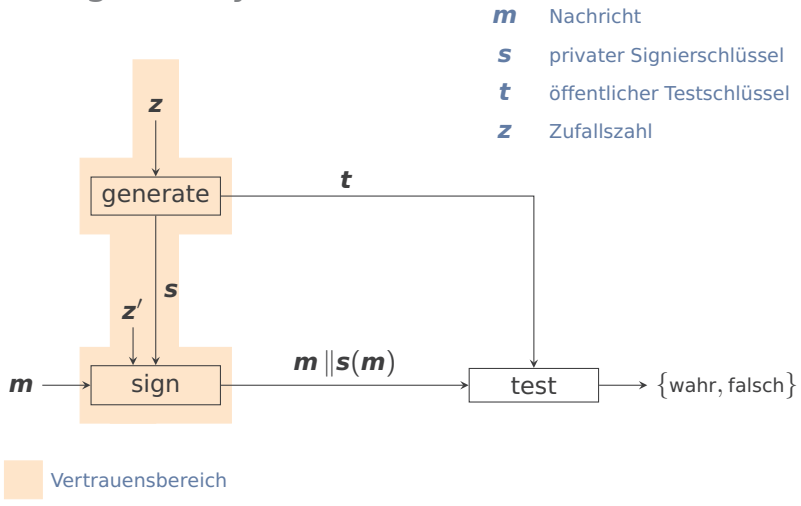
Typische Kodierung Transaktion enthält Referenz auf Besitzzuweisung mit c (*funding transaction*)

$$T_i = (\bullet \text{ an } \bullet, j, r(\bullet \text{ an } \bullet), c(\bullet \text{ an } \bullet))$$

Nachteil Veröffentlichung von r gibt vollständiges Geheimnis preis.

Vorsicht, es gibt noch weitere Nachteile dieser Konstruktion!

Digitales Signatursystem



Vgl. VO Rechnernetze und Internettechnik, Kapitel „Sicherheit“, 6. Juni 2019, S. 28

Autorisation mit digitalen Signaturen

Idee

- Besitzzuweisende Transaktion enthält Testschlüssel ***t*** (gibt neuer Besitzer bekannt)
- Weitergabe-Transaktion ist nur gültig, wenn sie korrekt digital signiert ist.

→ Kopplung von Besitz i. S. v. Verfügungsgewalt an Kenntnis von ***s***.

„Öffentliche Schlüssel sind Kontonummern“

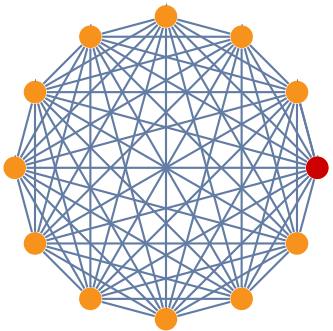
Kodierung bei Bitcoin Statt ***t*** wird ein Commitment zu ***t*** verwendet.
Der Testschlüssel wird erst bei der Weitergabe offengelegt.

Vorteil Geheimnisse mehrfach verwendbar: ***s***(● an ●) gibt nicht ***s*** preis.

Nachteil Transaktionen mit gleichem ***t*** sind verkettbar → Datenschutz am 23.04.20.

Schwache Identitäten

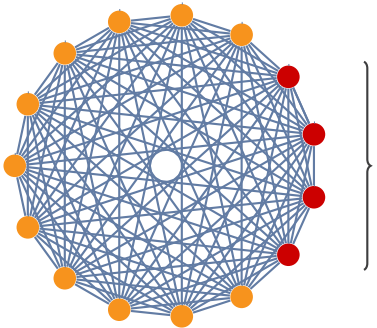
Offene Systeme ohne zentrale Identifizierung von Parteien



Vgl. Douceur, J. R. The Sybil Attack. In P. Druschel, F. Kaashoek and A. Rowstron, eds., *Peer-to-peer Systems*. LNCS 2429, Springer, Berlin Heidelberg, 2002, pp. 251–260.

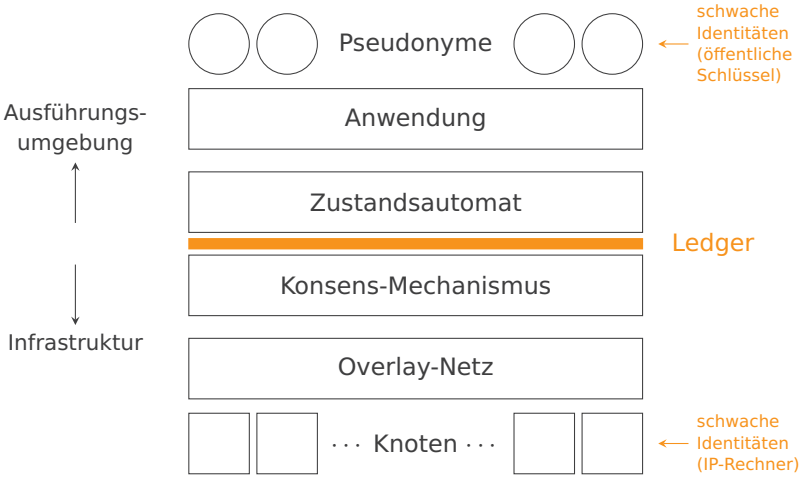
Schwache Identitäten

Offene Systeme ohne zentrale Identifizierung von Parteien



Vgl. Douceur, J. R. The Sybil Attack. In P. Druschel, F. Kaashoek and A. Rowstron, eds., *Peer-to-peer Systems*. LNCS 2429, Springer, Berlin Heidelberg, 2002, pp. 251–260.

Schichtmodell für Blockchain-Systeme



Von Transaktionen zum Distributed Ledger

Die meisten Blockchain-Systeme realisieren eine verteilte, öffentliche Datenbank, welche Transaktionen entgegennimmt und erfolgreich verifizierte Transaktionen in definierter Reihenfolge persistent speichert (*append only*).

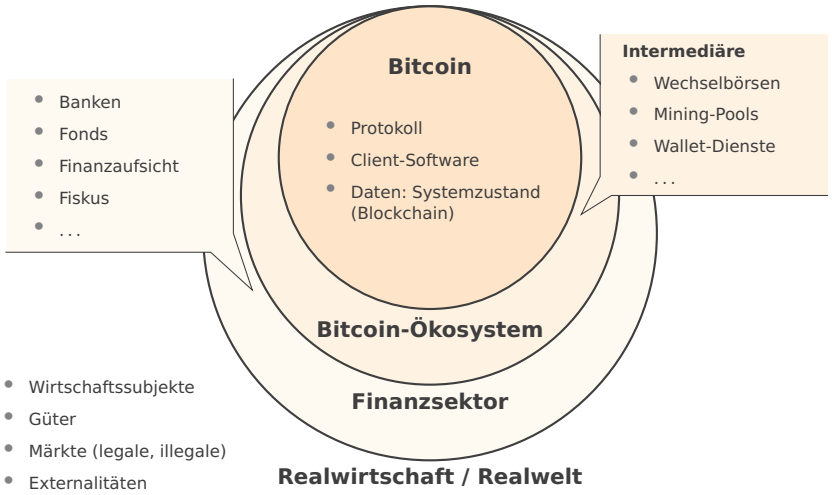
Somit entsteht eine Folge gültiger Zustände, die stetig fortgeschrieben wird.

Verbleibende Probleme definieren Gestaltungsspielraum für Lösungen:

1. Kompakte Kodierung von Transaktionen für große Zustandsräume
2. Bei „Besitz“-Interpretation: Autorisation der Weitergabe
3. Identifikation der Parteien
4. Konfliktlösung: Einigung auf einen gemeinsamen Zustand

Blockchain-Systeme sind spezielle Formen von Distributed Ledgers. Warum viele Systeme Blöcke als „Hilfsstruktur“ brauchen, lernen Sie nächste Woche.

Bitcoin im Kontext



Syllabus

05.03.20	1. Einführung und Grundlagen	
12.03.20	2. Infrastruktur für Blockchain-Systeme	
19.03.20	3. Transaktionslogik in Bitcoin und Ethereum	
26.03.20	Übung: Blockchain-Analyse mit BlockSci	(Martin Plattner)
02.04.20	Übung: Besprechung der Übungsaufgaben	
23.04.20	4. Datenschutz und Sicherheit	
30.04.20	5. Skalierbarkeit, Off-Chain-Transaktionen, Governance	
07.05.20	Übung: Ethereum-Programmierung mit Solidity	(Michael Fröwis)
14.05.20	Übung: Besprechung der Übungsaufgaben	
28.05.20	6. Wiederholung, Fragestunde	
04.06.20	Klausur	

Änderungen vorbehalten.

Einladung zum Vortrag

Heute, 12:15 Uhr, SR1, ICT-Gebäude.

Does digitalization require Central Bank Digital Currencies for the general public?

Dr. Martin Summer
Österreichische Nationalbank
Leiter der Abteilung für volkswirtschaftliche Studien