

Parldigi MasterClass

Grosser Rat Bern

Kryptowährungen und Blockchain

Bern, 4. Dezember 2023

Prof. Dr. Kai Brännler, Institute for Cybersecurity and Engineering, BFH

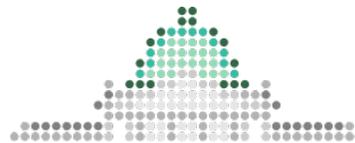
Prof. Dr. iur. Corinne Zellweger-Gutknecht, Rechtswissenschaftlerin, UNIBAS/UZH

Eine Veranstaltung von:



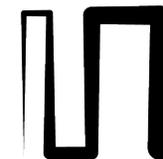
**Universität
Zürich** UZH

Digital Society Initiative



Parldigi

Unterstützt durch:



**Stiftung
Mercator
Schweiz**

Welches Problem löst die Blockchain?

Kai Brännler

Berner Fachhochschule



What is Bitcoin?

- An open-source software
- A peer-to-peer network
- A payment network
- A currency

What is Bitcoin?

- An open-source software
- A peer-to-peer network
- A *decentralized* payment network
Like cash, unlike Paypal
- A *decentralized* currency
Like gold, unlike the US Dollar

What is Bitcoin?

- An open-source software
- A peer-to-peer network
- A *decentralized* payment network
Like cash, unlike Paypal
- A *decentralized* currency
Like gold, unlike the US Dollar

BankCoin

Alice

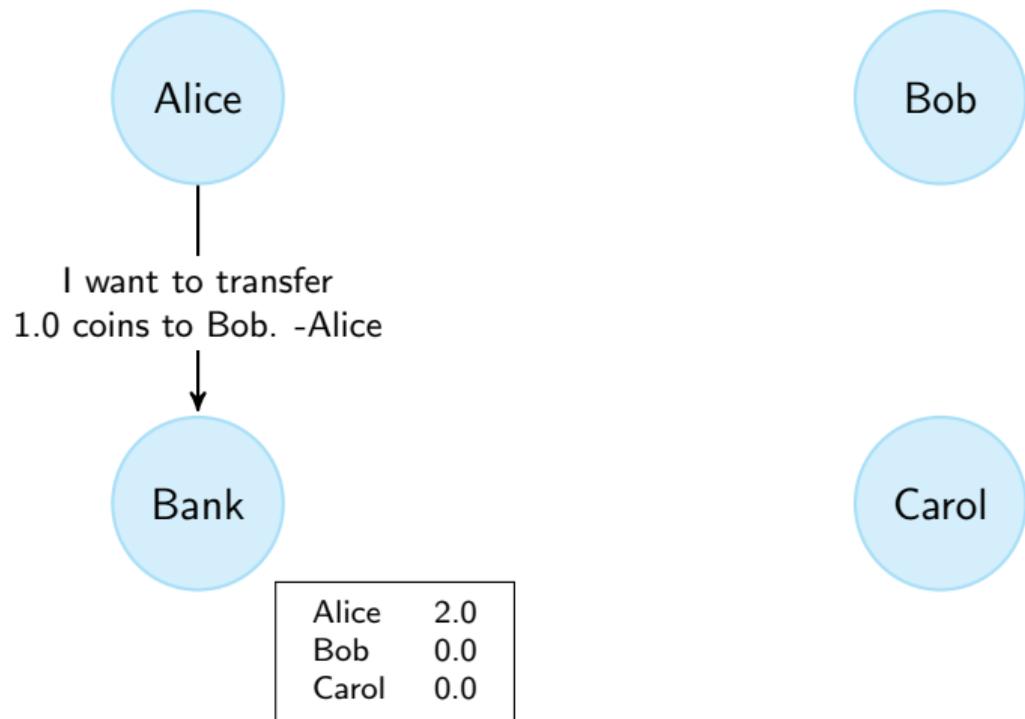
Bob

Bank

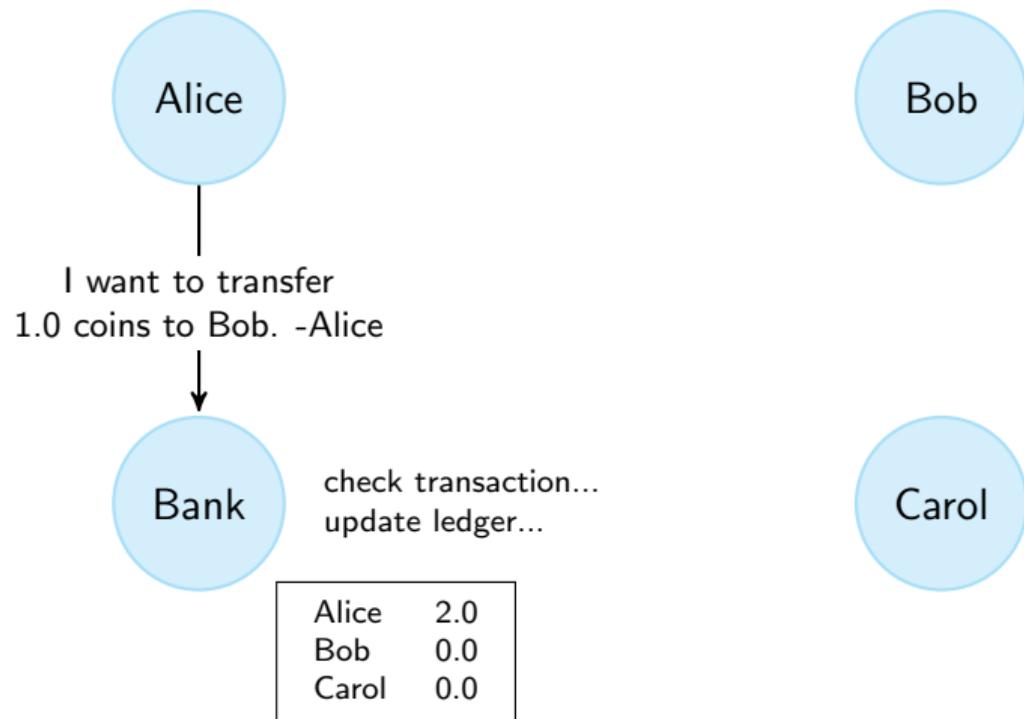
Carol

Alice	2.0
Bob	0.0
Carol	0.0

BankCoin



BankCoin



BankCoin

Alice

Bob

Bank

Carol

Alice	1.0
Bob	1.0
Carol	0.0

BankCoin Rules

- The bank has the ledger
- The bank accepts all valid transactions it receives and updates its ledger
- Everybody sends transactions to the bank

Problem

- The bank can censor transactions, create money, etc.
- Can we design a protocol without a central intermediary?
- In such a protocol, who would maintain the ledger?

NaiveCoin

Alice

Alice	2.0
Bob	0.0
Carol	0.0

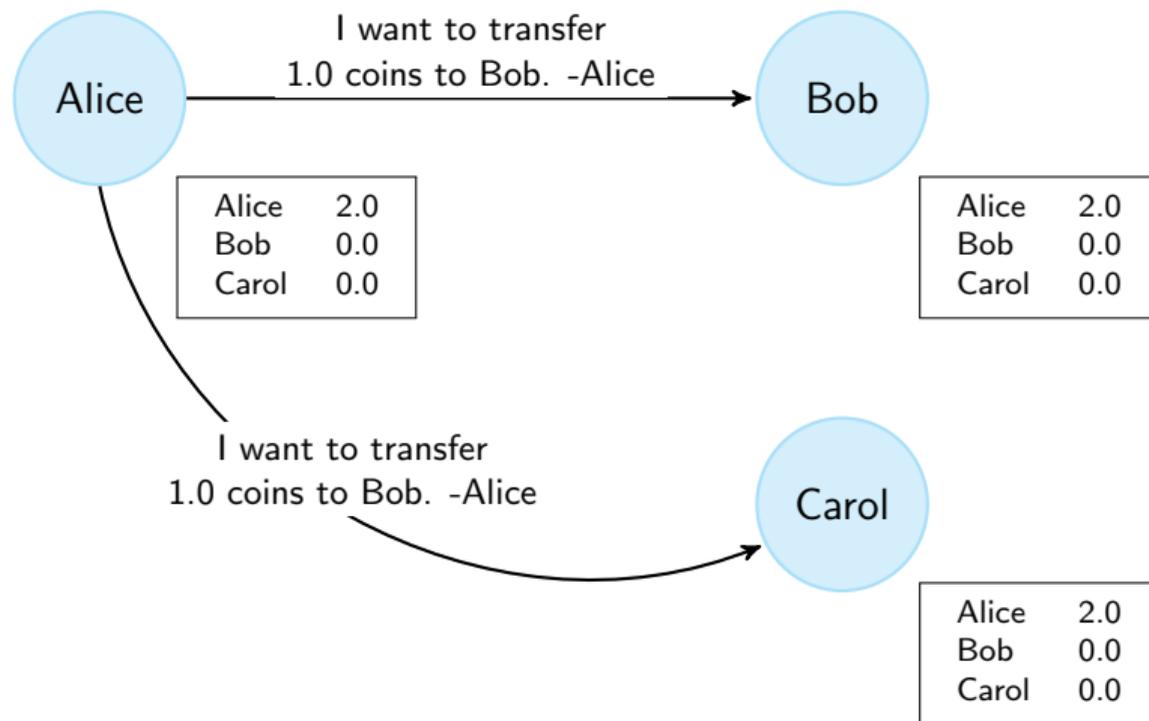
Bob

Alice	2.0
Bob	0.0
Carol	0.0

Carol

Alice	2.0
Bob	0.0
Carol	0.0

NaiveCoin



NaiveCoin

Alice

Alice	1.0
Bob	1.0
Carol	0.0

Bob

Alice	1.0
Bob	1.0
Carol	0.0

Carol

Alice	1.0
Bob	1.0
Carol	0.0

NaiveCoin

NaiveCoin Rules

- Each node has a copy of the ledger
- Each node accepts all valid transactions it receives and updates its ledger
- Each node broadcasts its transactions to all nodes

Problem solved

- No more bank!

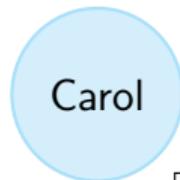
New Problem

- The Double Spending Problem

The Double Spending Attack

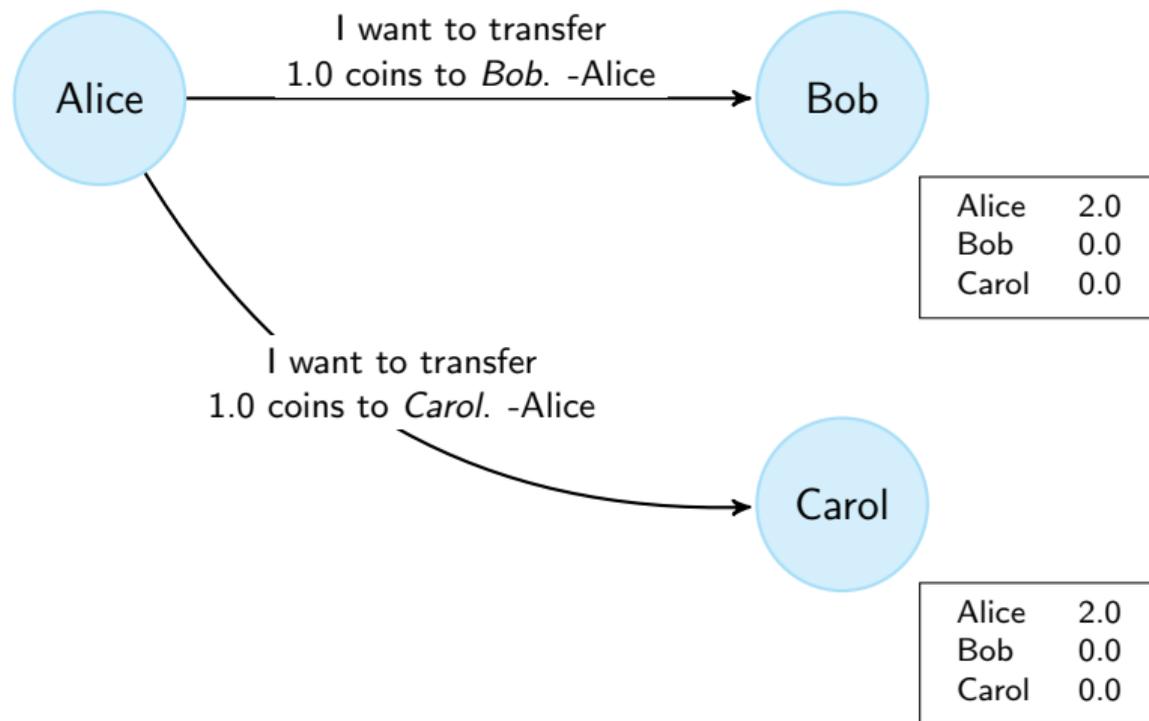


Alice	2.0
Bob	0.0
Carol	0.0



Alice	2.0
Bob	0.0
Carol	0.0

The Double Spending Attack



The Double Spending Attack

Alice

Bob

Alice	1.0
Bob	1.0
Carol	0.0

Carol

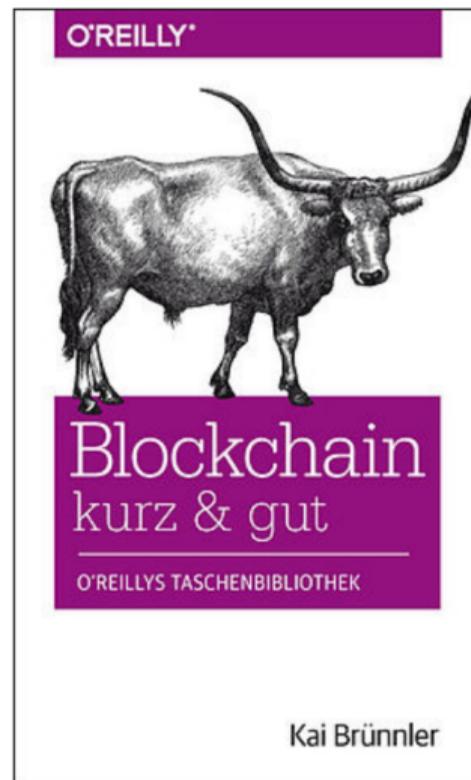
Alice	1.0
Bob	0.0
Carol	1.0

The Double Spending Attack

- Both Bob and Carol think they have been payed
- Bob will have trouble when he later tries to pay Carol
- The network is not in *consensus* anymore
- The problem of how to avoid this attack is the famous *double spending problem*
- This problem has only recently been solved by Satoshi Nakamoto in the Bitcoin whitepaper

Kai Brännler. *Blockchain kurz & gut*.
O'Reilly, 2018.

You can download a draft [here](#).





Universität
Basel

MasterClass

Kryptowährungen & Blockchain

Prof. Dr. iur. Corinne Zellweger-Gutknecht, 04.12.2023

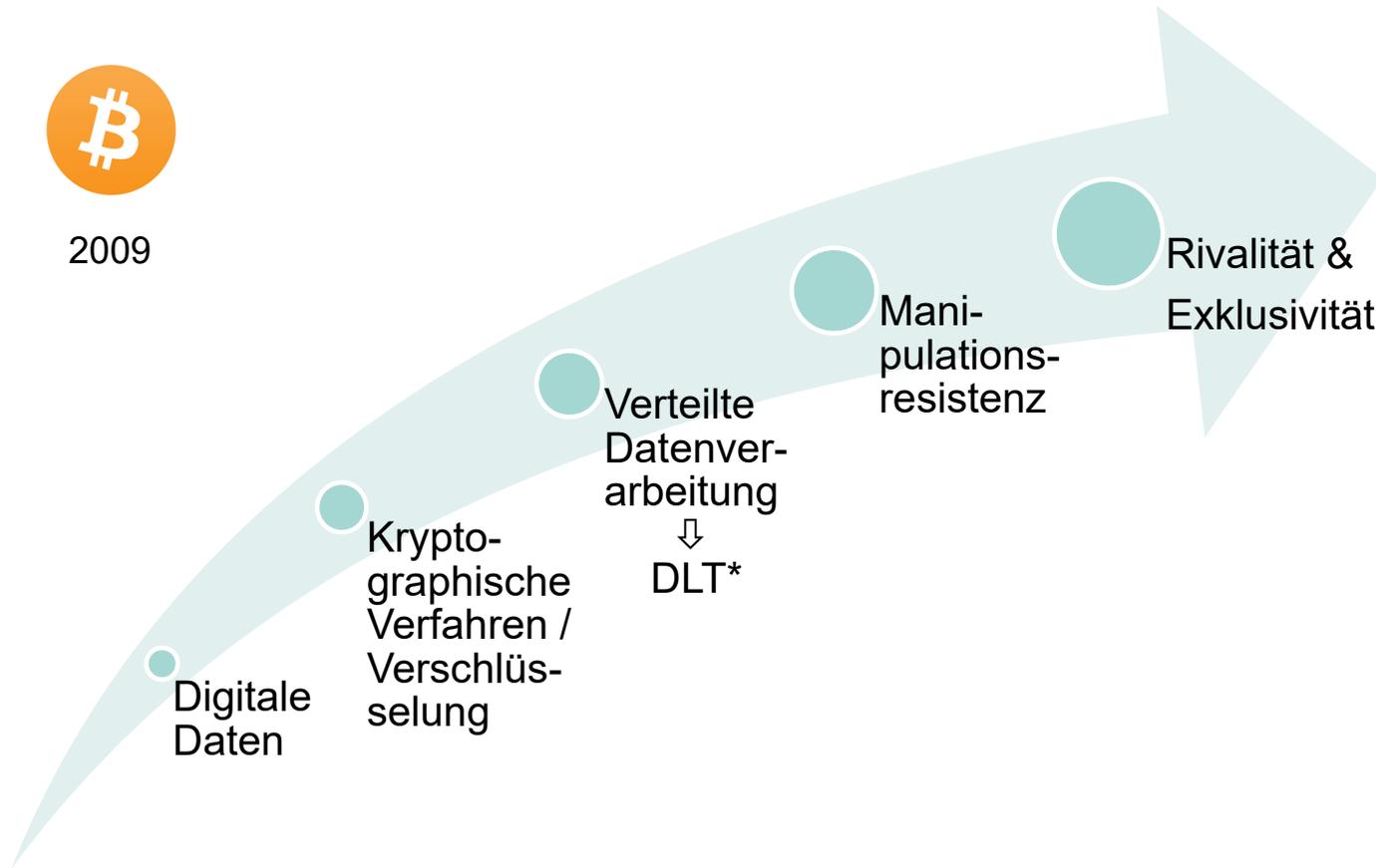
Agenda

-
- 1 Kryptowerte – die Vorgeschichte
 - 2 Kryptowährungen – eine erste rechtliche Annäherung
 - 3 Kryptowährungen Schweiz
 - 4 Gesetzgebung, Regulierung (Schweiz)
 - 5 Digitaler Schweizer (Retail) Franken?
 - 6 Gesetzgebung, Regulierung (EU)
-

Kryptowerte – die Vorgeschichte



2009



➤ **Angebot und Nachfrage können entstehen (Preisbildung → Wertdaten)**

➤ Je nach Funktion / Verwendung

- Anlagetoken («**Tokenisierung**»)
- Nutzungstoken
- Zahlungstoken («**Kryptowährung**») → Abwicklung auf derselben Techn.
- Mischung

* distributed ledger technology («Streuregistertechnologie»)

Kryptowährungen - eine erste rechtliche Annäherung



Privat ausgegeben
& keine/wenig Regulierung, da

- **Dezentral**
 - Kein identifizierbarer Emittent
 - Kein rechtlicher Anspruch

Stattdessen:

- Regulierung/Restriktion
 - On-/off-**Ramps** (Börsen..)
 - Lizenzierte **Halter** (Eigenmittel..)
- Verfahren gegen **Akteure**

Privat ausgegeben
& staatlich reguliert



- Lizenzierung
 - Emittenten
 - Banken u.a. Finanzinstitute und Infrastrukturen
 - Dienstleister (CH ohne VASP-Lizenz)



- Privatrecht: Natur, Transfer...
- Verhaltensregeln
 - Prospekt, Information
 - Geldwäsche
 - Marktintegrität
 - ..



Staatlich ausgegeben
«digitales Zentralbankgeld»
(central bank digital currency CBDC)

- Retail vs. wholesale
- Retail
 - lanciert (Nigeria, Bahamas, Jamaica),
 - Pilot (Südkorea, Indien, Russland, Ghana, Karibik)
 - Konzept (Euro, Schweden, China, UK ...)



Staatlich gedeckt

- Synthetische CBDC (privater Emittent, Deckung mit Zentralbankgeld)

Kryptowährungen Schweiz

grün = Projekt/Pilot



• XCHF (Swiss Crypto Franc)

- Bitcoin Suisse AG (SRO Mitglied)
- 1 CHF = 1 XCHF
- Garantie Sygnum Bank AG (ehem. Anleihe mit Prospekt)
- 1.765 Mio. XCHF
- Zahlungstoken auf Ethereum BC

• CCHF (Centi Franc)



- Centi AG
- 1 CHF = 100 CCHF
- Garantie Dukascopy Bank SA
- 20 Mio. CCHF / 200K CHF
- Mikrozahlungen (v. Händler [277] automatisch auf Bankkonto), unwiderruflich
- **jCHF (Jarvis Franc)** gegen USDC

• DCHF (Digital Franc)



- Sygnum Bank AG
- Banklizenz
- Gegenwert als Sichtguthaben bei SNB (kein Insolvenzprivileg)
- Zahlungstoken auf Sygnums Handelssystem SygnEx

• tCHF & tEUR (SDX Coin)



- SDX AG (Tochter der SIX AG)
- Lizenz als Zentralverwahrer (bzw. SDX Trading AG als Börse)
- Gegenwert als Sichtguthaben bei SNB (kein Insolvenzprivileg)
- Zahlungstoken auf SDX Plattform

• CHFD (Digitalfranken)

- Swiss Stablecoin AG
- Testumgebung Postfinance

• BGT (Buchgeld-Token)

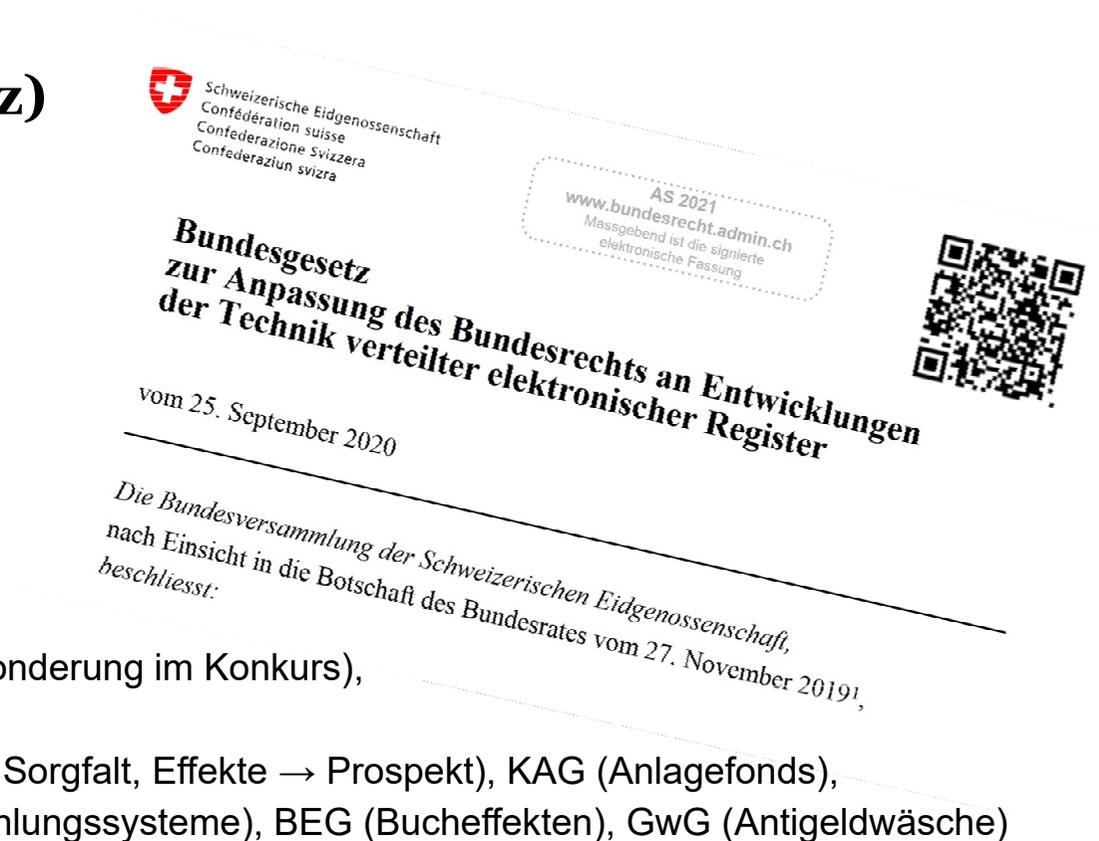
- SBVg (White Paper)
- 3 Varianten
 - Standardised (pro Bank; Deckung und Technologie normiert)
 - Joint (SPV)
 - Coloured (pro Bank, Deckung und Technologie individuell)

• wCBDC (Buchgeld-Token)

- SNB (Projekt Helvetia III Dez-Jun); UBS, BCV, BSKB, ZKB, Commerzbank, Hypothekbank Lenzburg; SDX, SIC, SIX Repo, SIX SIS
- Für Anleihen (1.12.: BKB emittiert für BS 105 Mio. Anleihe, mit digitalen Franken erworben)
- Für Repo-Geschäfte

Gesetzgebung, Regulierung (Schweiz)

- **Rahmengesetz**
passt zehn bestehende Gesetze an
- **In Kraft Feb/Aug 2021**
 - Privatrecht, insb. OR (Wertpapierrecht, Gesellschaftsrecht)
 - IPRG = Kollisionsrecht
 - Insolvenz- und Finanzmarktrecht, z.B. SchKG (Aussonderung im Konkurs),
 - Finanzmarktgesetze:
BankG (Lizenzpflicht), FIDLEG (Finanzinstrument → Sorgfalt, Effekte → Prospekt), KAG (Anlagefonds), FINIG (Wertpapierhaus), FinfraG (Handelsplätze, Zahlungssysteme), BEG (Bucheffekten), GwG (Antigeldwäsche)
- **Ziel:**
rechtlich sichere und flexible Basis für Handel von Rechten mittels DLT
- **Nicht:** Kryptowährungen (Stablecoins vs. Prospektpflicht), NFTs, Zentralbankgeld



(Beeple, © Christie's)

Digitaler Schweizer (Retail) Franken?

TA Swiss Studie 2023/2024 (HSLU, Observatoire de la Finance Genf, Uni BS, FHNW)

Fokus

- Wirtschaftliche Aspekte in der Schweiz
- Technische Aspekte
- Ökologische Auswirkungen
- Politischer und rechtlicher Aspekt in der Schweiz
- Gesellschaftliche Aspekte (inkl. Bevölkerungsumfrage)

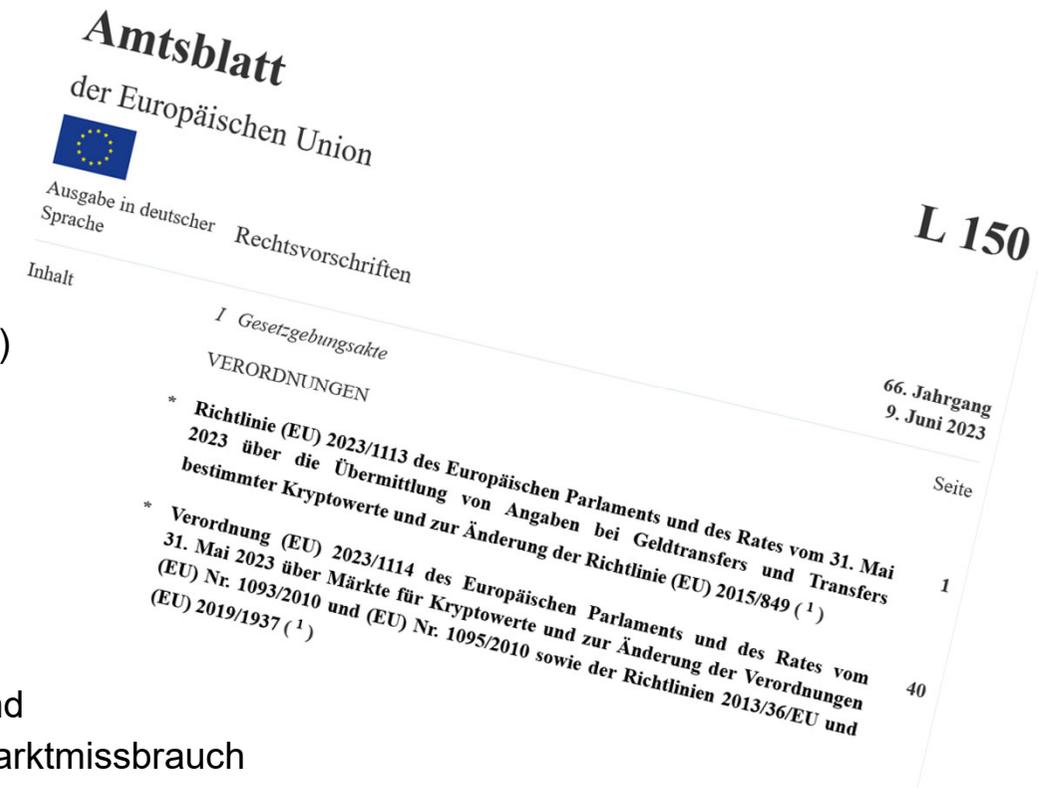
Rechtliche Aspekte

- **Verfassungsstufe:**
Systematische Auslegeordnung (Konfliktfelder und Lösungsansätze)
- **Gesetzesstufe:** insb. Anpassungsbedarf (Identifikation und Begründung)
 - Währungsrecht: Rechtsnatur, Zugang, Funktionalitäten, Schranken; internationale Bezüge
 - Zivilrecht: Rechtsnatur, Inhaberschaft, Transfer, Abgrenzungen zu anderen Vermögenswerten
 - Finanzmarktrecht: Abgrenzungen (insb. zu Effekten), Akteure, Pflichten, Rulebooks, AML/CFT



Gesetzgebung, Regulierung (EU)

- **MICA** (VO über Märkte für Kryptowerte)
 - Reaktion auf **ICOs** & globale Stablecoins (**Libra/Diem**)
 - Ergänzt Finanzmarktrichtlinie II (**MiFID II**) & -verordnung (**MiFIR**)
 - Vollständig in Kraft per 30.12.2024; schon per 30.06.2024 für **vermögenswertreferenzierte Tokens** und **E-Geld-Tokens**
 - Transaktionsobergrenze EUR 200 Mio. pro Tag (?)
 - Grandfathering für bestehende CASPs max. 18 Monate
- Einheitlicher Rechtsrahmen für Kryptowerte & -Dienstleister, die **nicht** durch **traditionelle** Finanzmarktregulierung erfasst sind zu Emission, Verwahrung & Verwaltung, Handelsplattformen, Marktmissbrauch
- **Digitaler Euro**
 - Juli 2023: drei **Verordnungsentwürfe** (Einführung des **digitalen** Euro; **Bargeld** als gesetzliches Zahlungsmittel; digitale **Euro-Dienste** durch Zahlungsdienstleister mit Sitz in einem Mitgliedstaat, dessen Währung nicht der Euro ist)
 - Oktober 2023: Ende Untersuchungsphase; EZB-Rat startet **Vorbereitungsphase** bis 2025
 - **Motive**: paneuropäischer Zahlungsraum; «Dollarization»; xBP



Parldigi MasterClass

Grosser Rat Bern

nächste Veranstaltung am 11. März 2024

Cybersecurity

Prof. Dr. Endre Bangerter

Co-Leiter Institute for Cybersecurity and Engineering, BFH

Dr. Melanie Knieps

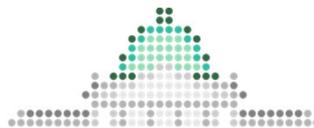
Forscherin Digital Society Initiative, UZH

Eine Veranstaltung von:



**Universität
Zürich** UZH

Digital Society Initiative



Parldigi

Unterstützt durch:



**Stiftung
Mercator
Schweiz**
