ÖSTERREICHISCHE
FMA · FINANZMARKTAUFSICHT

DLT-TOKEN / CRYPTO-ASSETS: BASICS

Mag. Ralph Rirsch, BSc MBA
Dr. Stefan Tomanek, MBA
Wien am 21.10.2021

KRYPTOGRAFIE – HASH-FUNKTION

- Kryptografie beschäftigt sich mit der Verschlüsselung von Informationen
- Ursprung im alten Ägypten, vor ca. 3000 Jahren
- Seit 2006 computergestützte Hashfunktionen dominant
- Beispiele der SHA-256 Hashfunktion (Hashgenerator)

Text	Hash
Marc	88c3cf364123a25bbab687d4fe8ec6284836b9f00654eda361579d584a43343e
marc	4697c20f8a70fcad6323e007d553cfe05d4433f81be70884ea3b4834b147f4c1
mark	6201eb4dccc956cc4fa3a78dca0c2888177ec52efd48f125df214f046eb43138
mark" "	ded0ee5484d15c5bd403cd2d97d9c557179a93903c00fdea08a5820670bfd3d9

Quelle: eigene Darstellung

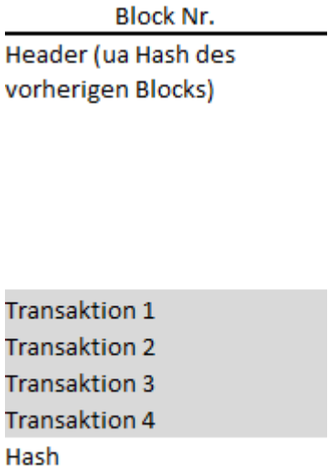
- FMA nutzt „Hash“ für Amtssignatur

Signaturwert	B9phfeKkqvMBhPx1eL+UBNpI1g2o+b6kjZHlRmDDSbRufsQS7Sq0tOly8Rv5TgyEPkvfi/6dOW64CbvXqgAy LU0vm0bmXLf2sgETeGlGBHcy44IgDwyFxaRr7pjA/lngxoXAc1slYZBNFpf6ZWTuXsbiD8PnKPOeYHF7PfI/ 0mM5iivJ1qjjDKnOlPT+EPCs2ggf1YKBf673xCGarP3znqpTdN2/jShke+g+ySvkAfOGx8MFeggvRzwpZVDQ Zp9/6ufx+TLVwD64n4veIeQ8NGVSVlGDGp0qm1L/juoGtPmPn/Uc/m2AC3RXDJfrBhW86Gu7DPPYcFRx8gl5 6ykmAg==	
FINANZMARKTAUFSICHT FMA ÖSTERREICH @ AMTSSIGNATUR	Unterzeichner	Österreichische Finanzmarktaufsichtsbehörde
	Datum/Zeit-UTC	2019-08-26T12:44:49Z
	Aussteller-Zertifikat	CN=a-sign-corporate-light-02,OU=a-sign-corporate-light-02,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serien-Nr.	532114608
	Methode	urn:pdfsigfilter:bka.gv.at:binaer:v1.1.0
Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: http://www.signaturpruefung.gv.at	
Hinweis	Dieses Dokument wurde amtssigniert. Auch ein Ausdruck dieses Dokuments hat gemäß § 20 E-Government-Gesetz die Beweiskraft einer öffentlichen Urkunde.	

BLOCKCHAIN BEISPIEL

Ein Block besteht vereinfacht aus:

- Header (ua Hash des vorherigen Blocks)
- Transaktionen 1 bis n
- Hashwert von Header und Transaktionen



Quelle: eigene Darstellung

BLOCKCHAIN BEISPIEL

Block 0 aka „Genesis Block“:

- Grundausstattung der ersten Teilnehmer
- Jede Person bekommt von dem Algorithmus je 5 Token
- Header und Transaktionen 1 bis 3 werden „verhasht“

Block Nr.	Block 0
Header (ua Hash des vorherigen Blocks)	
Transaktion 1	Marc 5
Transaktion 2	Eva 5
Transaktion 3	Jutta 5
Transaktion 4	
Hash	9fb5d8cd25711a609e6d5de30ee13321ea4e4b9bb9b422c80de9d7416a471ae6

Quelle: eigene Darstellung

BLOCKCHAIN BEISPIEL

Block Nr.	Block 0	Block 1
Header (ua Hash des vorherigen Blocks)		9fb5d8cd25711a609e6d5de30ee13321ea4e4b9bb9b422c80de9d7416a471ae6
Transaktion 1	Marc 5	Marc 2
Transaktion 2	Eva 5	Eva 6
Transaktion 3	Jutta 5	Jutta 7
Transaktion 4		
Hash	9fb5d8cd25711a609e6d5de30ee13321ea4e4b9bb9b422c80de9d7416a471ae6	467cd92c9735968903c0457d3dcac6c3824ee260c3a193307eb9c616c5937aab

Quelle: eigene Darstellung

Block 1 - erste tatsächliche Transaktionen finden statt:

- Hash aus Block 0 wird als Header in Block 1 eingefügt und somit verkettet
- Marc überträgt Eva 1 Token
- Marc überträgt Jutta 2 Token
- Marc erhält 0 Token
- Header und Transaktionen 1 bis 3 werden „verhasht“

BLOCKCHAIN BEISPIEL

Block 2 – laufende Transaktionen:

- Hash aus Block 1 wird als Header in Block 2 eingefügt und somit verkettet
- Jutta überträgt Stefan 4 Token
- Guthaben von Eva und Marc bleibt gleich
- Header und Transaktionen 1 bis 4 werden „verhasht“

Block Nr.	Block 0	Block 1	Block 2
Header (ua Hash des vorherigen Blocks)		9fb5d8cd25711a609e6d5de3 0ee13321ea4e4b9bb9b422c8 0de9d7416a471ae6	467cd92c9735968903c0457d3 dcac6c3824ee260c3a193307e b9c616c5937aab
Transaktion 1	Marc 5	Marc 2	Marc 2
Transaktion 2	Eva 5	Eva 6	Eva 6
Transaktion 3	Jutta 5	Jutta 7	Jutta 3
Transaktion 4			Stefan 4
Hash	9fb5d8cd25711a609e6d5de3 0ee13321ea4e4b9bb9b422c8 0de9d7416a471ae6	467cd92c9735968903c0457d3 dcac6c3824ee260c3a193307e b9c616c5937aab	d6976edbc2624973d808d136 e9e245b11ed0a215f45831e4 948aee32e3833509

Quelle: eigene Darstellung

BLOCKCHAIN BEISPIEL

Block 3 – laufende Transaktionen:

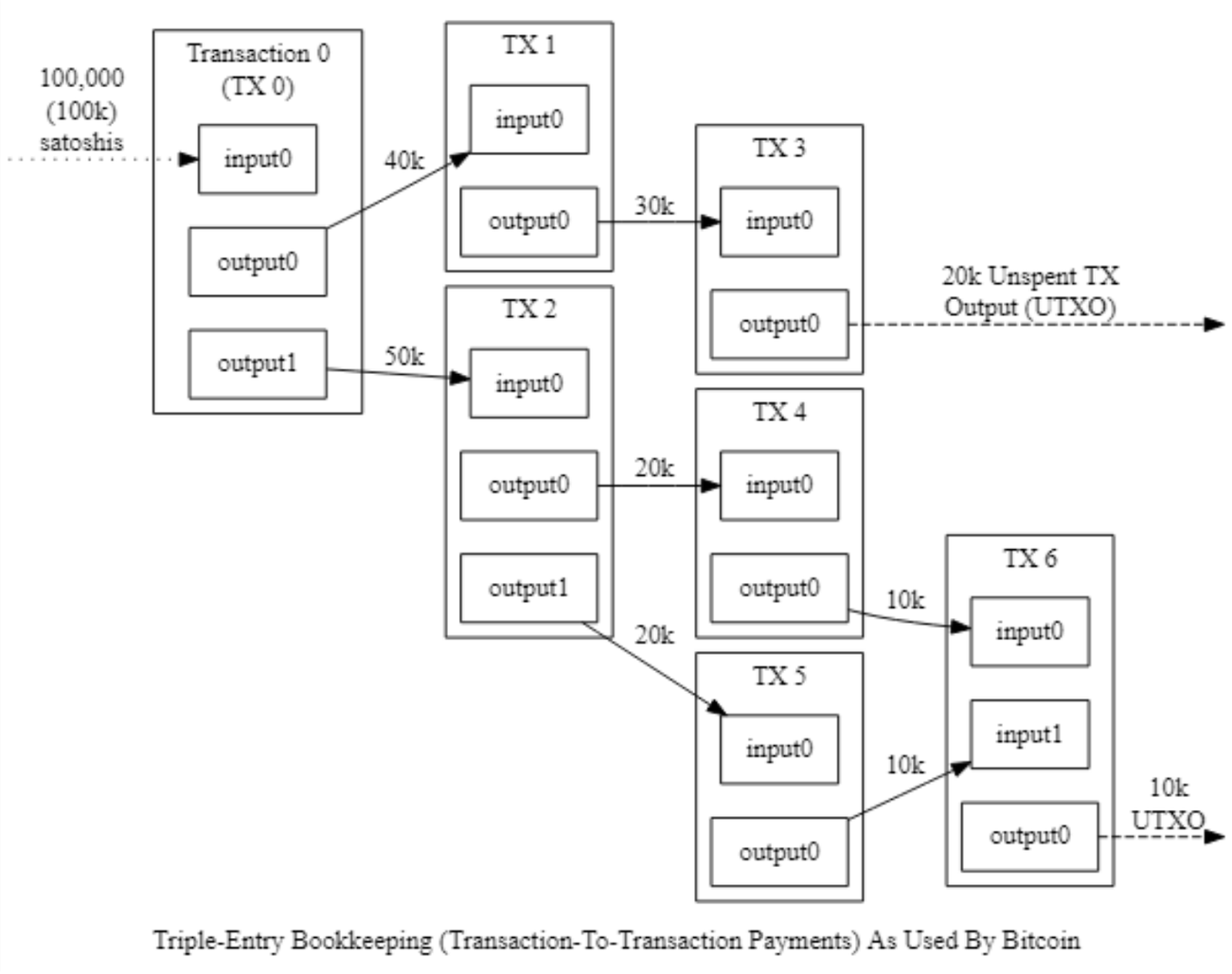
- Hash aus Block 2 wird als Header in Block 3 eingefügt uns somit verkettet
- Weitere Transaktionen werden ähnlich der vorhergehenden Blöcke stattfinden…
- Header und jene Transaktionen werden „verhasht“ werden

Block Nr.	Block 0	Block 1	Block 2	Block 3
Header (ua Hash des vorherigen Blocks)		9fb5d8cd25711a609e6d5de30ee13321ea4e4b9bb9b422c80de9d7416a471ae6	467cd92c9735968903c0457d3dcac6c3824ee260c3a193307eb9c616c5937aab	d6976edbc2624973d808d136e9e245b11ed0a215f45831e4948aee32e3833509
Transaktion 1	Marc 5	Marc 2	Marc 2	
Transaktion 2	Eva 5	Eva 6	Eva 6	
Transaktion 3	Jutta 5	Jutta 7	Jutta 3	
Transaktion 4			Stefan 4	
Hash	9fb5d8cd25711a609e6d5de30ee13321ea4e4b9bb9b422c80de9d7416a471ae6	467cd92c9735968903c0457d3dcac6c3824ee260c3a193307eb9c616c5937aab	d6976edbc2624973d808d136e9e245b11ed0a215f45831e4948aee32e3833509	

Quelle: eigene Darstellung

=> Eine simple Blockchain entsteht

BETRACHTUNG EINES „BITCOIN”

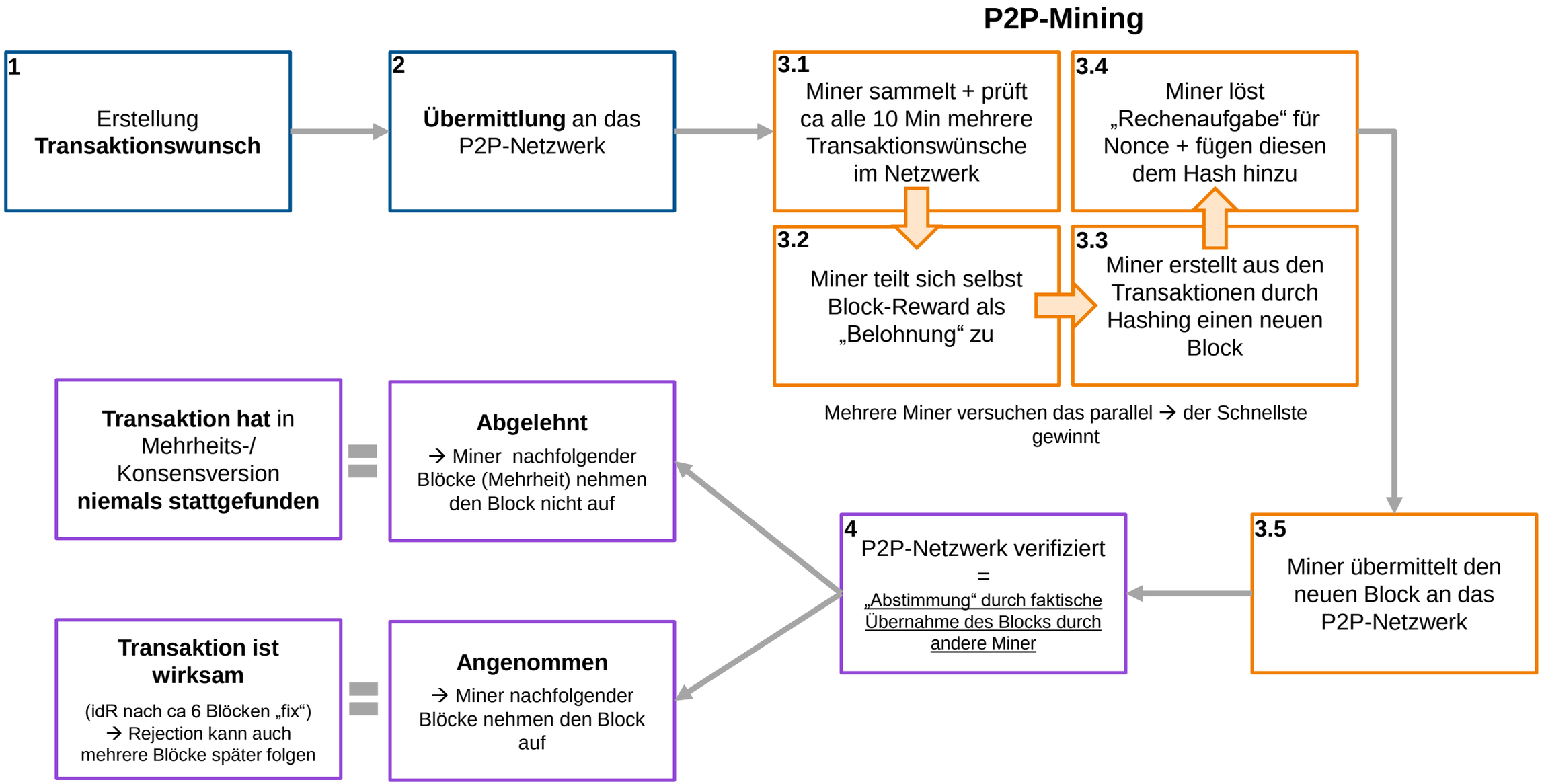


Triple-Entry Bookkeeping (Transaction-To-Transaction Payments) As Used By Bitcoin

- Bitcoin-Whitepaper: “*We define an electronic coin as a chain of digital signatures.”*
- Transaktionen
- Inputs and Outputs
- Block
- Kette von Transaktionen/Blöcken – Blockchain

Keine virtuelle Münze –
vielmehr eine Rechnungseinheit

BTC-TRANSAKTION EINFACH



PROOF OF WORK VS. PROOF OF STAKE

≠

Computing Power

Requires high amount of computing power in order to provide trust and security to the network.

Wealth

Users with the highest stakes (Coins/Token) in the system have the most interest to maintain a secure network.

≠

Energy inefficient

High amounts of electricity must be used to power the hardware in order to mine competitively.

Energy efficient

Compared to Proof of Work low amounts of electricity are used to run the network.

=

Task of the miner

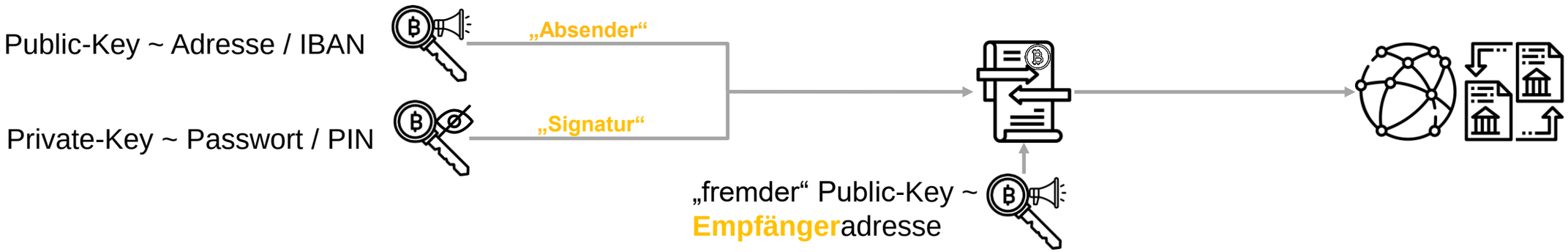
Verification and validation of (payment-) transactions as well as the execution and routing of these transactions.

Task of the miner

Verification and validation of (payment-) transactions as well as the execution and routing of these transactions.

„ECHTE“ DLT-WALLET SYSTEME

- Speichern ein **Schlüsselpaar**
- Bieten eine Oberfläche zur Erstellung von **Transaktionswünschen**
- **Führen Transaktionen nicht selbst aus**!
  → Ausführung durch Konsens im Netzwerk

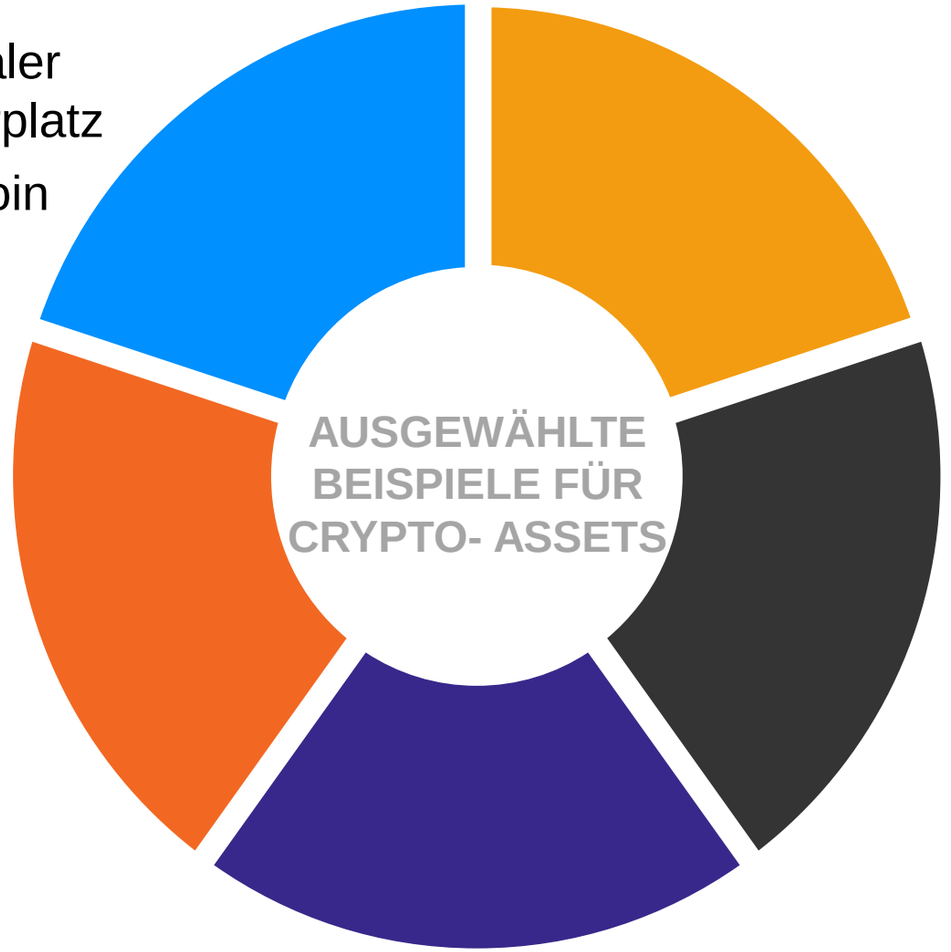


- „enthält“ nie lokal gespeicherte Token-Instanzen (auch „custodial wallets“)
- IdR keine Verwendung der Kunden-Token-Instanzen durch Wallet(-Dienstleister) → Unterschied zu klassischem Einlagengeschäft
- **Dieselben Keys** können **auf unendlich vielen Wallets gleichzeitig** gesichert werden! → keine „Duplikation“ der Token-Instanzen

SMART CONTRACTS

- sind grds simple Computerprotokolle basierend auf „WENN-DANN Funktionen“
- Können schriftliche Verträge in manchen Fällen ersetzen
- Eher geeignet für standardisierte vertragliche Leistungspflichten
- Erstellbar auf bspw. Ethereum-, Cardano-, Stellar-Blockchain
- Verwendung von Smart Contracts bspw für
  - Beauftragung und Entlohnung von Dienstleistern entlang der Wertschöpfungskette
  - Abbildung von Miet- oder Kaufverträgen

VIELFÄLTIGE ANWENDUNGSFÄLLE



- Dezentraler Speicherplatz
  zB Filecoin
- Intendierte dezentrale Zahlungssysteme
  zB Bitcoin
- Privacy Coins
  zB Monero
- Dezentrale digitale Plattform als Basis für andere Token
  zB Etherum
- Stable Coins
  zB Diem/Libra

Quelle: Libra und Diem Logo aus https://libra.org/en-US/ bzw https://www.diem.com/en-us/ entnommen; Bitcoin, Ethereum, Filecoin und Monero Logo entnommen aus https://coinmarketcap.com/;

MARKTÜBERBLICK

Viele dieser Akteure sind aktuell unreguliert oder nur AML-reguliert

Der Kryptomarkt Teilt sich grob auf in:

- **„Gatekeeper“** = Dienstleister für Transaktionen von Fiat-Geld zu Crypto (und zurück), insb Crypto-Broker
- **Fiat-Zahlungsdienstleister** (inkl Banken), die selbst Gatekeeper sein können oder die Fiat-Zahlungsströme von Gatekeepern erledigen
- **Emittenten** = Primärmarkt (ICO, ITO, IEO, TGE uVm)
  - Teilweise kein Emittent vorhanden (zB Bitcoin)
  - Teilweise zentraler Betreiber eines (Öko-)Systems
- **Wallet-Provider** = Dienstleister, die Verwaltung von (kryptographischen) Keys und Erstellung von Transaktionswünschen erleichtern

  Sonderform: Custodial Wallet Provider, die DLT-Token selbst in fremdem Namen halten
- **Exchanges** = Sekundärmarkt (zentral / dezentral organisiert)
- **Andere Dienstleister** = diverse DL ua „Anlage“-Beratung und Portfolioverwaltung, Research und IT-Dienstleistungen (bspw DLT-Analytics zur Nachverfolgung von Transaktionen)
- **Diverse „Interessenvertretungen“** und Vereine zur allgemeinen Förderung des Marktes

DEFINITIONEN

Im Zusammenhang mit DLT-Token wird eine Vielzahl unterschiedlichster Begrifflichkeiten verwendet:

- die meisten davon sind ungenau, falsch und/oder irreführend
- einige davon sind legaldefiniert und daher mit Rechtsfolgen versehen
- Wortwahl idZ von erheblicher Bedeutung für differenzierten Diskurs

Einige Negativbeispiele

- Kryptowährung, Kryptogeld, Kryptodevisen etc → kein staatliches Fiat-Geld; Währungsbezug ist zu vermeiden
- Virtuelle Währung = konkret in AML-Regulierung definiert (unglückliche Wortwahl)
- Kryptowert, Rechnungseinheit = konkret im deutschen Aufsichtsrecht definiert (spezifische Definitionen → kein „Auffangbegriff“, zukünftig „Kryptowert“ (=„Crypto-Asset“) europäisch in MICAR definiert)

Empfehlung

- **DLT-Token** = technischer und unbelasteter Begriff
- **Crypto-Asset** = breiter Auffangbegriff zukünftiger Regulierung für die meisten bekannten DLT-Token

DEFINITIONEN

Oft wird unterschieden zwischen

- **Coin =** streng genommen nur Bitcoin als erstes DLT-Token
- **Altcoin =** streng genommen alle DLT-Token, deren Code sich unmittelbar von Bitcoin ableitet („Alternative Coins“)
- **Token =**
  - Technisch auch für Coins zutreffend
  - Von Teilen des Marktes / Lehre nur für DLT-Token verwendet, die auf einer bestehenden Blockchain „aufsetzen“, also nicht die primäre „Verrechnungseinheit“ des Systems sind. Abgrenzung aber problematisch – Beispiel:
    - Ethereums Code geht weit über BTCs Funktionalitäten hinaus (zB Smart Contracts, Mining-Mechanismus)
    - ETH ist die primäre Verrechnungseinheit des Ethereum-Netzwerks → Altcoin oder Token?

Diese Unterscheidung ist finanzmarktaufsichtsrechtlich in aller Regel nicht relevant. Der Begriff „Token“ ist jedenfalls korrekt.

MICAR - HINTERGRUND

- **EU-Verordnung**
  - reguliert Emission & Dienstleistungen iZm DLT-Token (=„Crypto-Assets“ bzw „Kryptowerte“)
  - Teil des EU-Pakets zur Digitalisierung des Finanzsektors
  - soll durch Vollharmonisierung den Binnenmarkt stärken und Innovation durch Rechtssicherheit fördern

- **Zeitplan:**
  - 24.09.2020 Veröffentlichung des Proposals (COM/2020/593 final)
  - **Verhandlungen laufen noch** → alle Angaben in dieser Präsentation vorbehaltlich Änderungen:
    - Letzte Kompromissversion vom 07.06.2021
    - Wechsel der Ratspräsidentschaft → Zeitplan aktuell offen
    - **Anwendbarkeit (Art 126 MICAR)**
      - 24 Monate nach Inkrafttreten
      - Titel 3 (ART) & Titel 4 (EMT) schon 12 Monate nach Inkrafttreten
    - **Übergangsregime** für bereits national zugelassene / registrierte Dienstleister (Art 123 MICAR) → weitere 24 Monate

Entwurf der EK: MiCA-VO – Übersicht Anwendungsbereich

Anwendungsbereich von MiCA

Anwendungsbereich:	***Personen, die in der Union Crypto-Assets ausgeben oder Dienstleistungen iZm Crypto-Assets erbringen***
Ausnahmen – **Crypto-Assets**:	MiFID-Finanzinstrumente, E-Geld (sofern nicht EMT), (strukturierte) Einlagen, Verbriefungen iSd VO (EU) 2017/2402
Ausnahmen – **Entitäten**:	Vollumfänglich: EZB / NB, (R)VU, Liquidatoren / Verwalter im Insolvenzverf., konzerninterne Erbringung von Crypto-Dienstleistungen, Europäische Investitionsbank, EFSF, ESM und internationale Organisationen des öffentlichen Rechts Bestimmungen nur zT anwendbar: Kreditinstitute und Wertpapierfirmen

Emittenten

Zulassung und Beaufsichtigung von Emittenten von ***ART*** / ***EMT***

Vorschriften iZm ***Betrieb, Organisation und Unternehmensführung*** von ***ART*** / ***EMT*** – Emittenten

Verbraucherschutzvorschriften für Ausgabe, Tausch und Verwahrung von Crypto-Assets sowie den Handel

Transparenz- und Offenlegungspflichten für die ***Ausgabe*** von Crypto-Assets und ihre ***Zulassung zum Handel***

Crypto-Asset Service Provider

Zulassung und Beaufsichtigung von ***CASP***

Vorschriften iZm ***Betrieb, Organisation und Unternehmensführung*** von ***CASP***

Verbraucherschutzvorschriften für Ausgabe, Tausch und Verwahrung von Crypto-Assets sowie den Handel

Marktmissbrauch

Maßnahmen zur ***Verhinderung von Marktmissbrauch*** mit dem Ziel, die Integrität der Märkte für Crypto-Assets zu gewährleisten

Crypto-Asset Service Providers (CASP)

- Juristische Personen mit Sitz in EU
- Mindestkapitalanforderungen
- Zulassung als CASP ist in der gesamten EU gültig (im Rahmen der Dienst- und Niederlassungsfreiheit)
- Crypto-Asset Dienstleistungen (Art 67 bis 73 MiCA) – angelehnt an MiFID II
  - Verwahrung und Verwaltung von Crypto-Assets für Dritte
  - Betrieb einer Handelsplattform für Crypto-Assets
  - Tausch Crypto-Assets gegen Nominalgeldwährung oder Tausch Crypto-Assets gegen andere Crypto-Assets
  - Ausführung von Aufträgen über Crypto-Assets für Dritte
  - Platzierung von Crypto-Assets
  - Annahme und Übermittlung von Aufträgen für Dritte
  - Beratung zu Crypto-Assets

FRAGEN/DISKUSSION

Kontakt:

- Ralph Rirsch, ralph.rirsch@fma.gv.at, Tel.+43 (0)1 249 59 – 4312.
- Stefan Tomanek, stefan.tomanek@fma.gv.at, Tel.+43 (0)1 249 59 – 3412.

FINANZMARKTAUFSICHT ÖSTERREICH

Kompetenz Kontrolle Konsequenz