



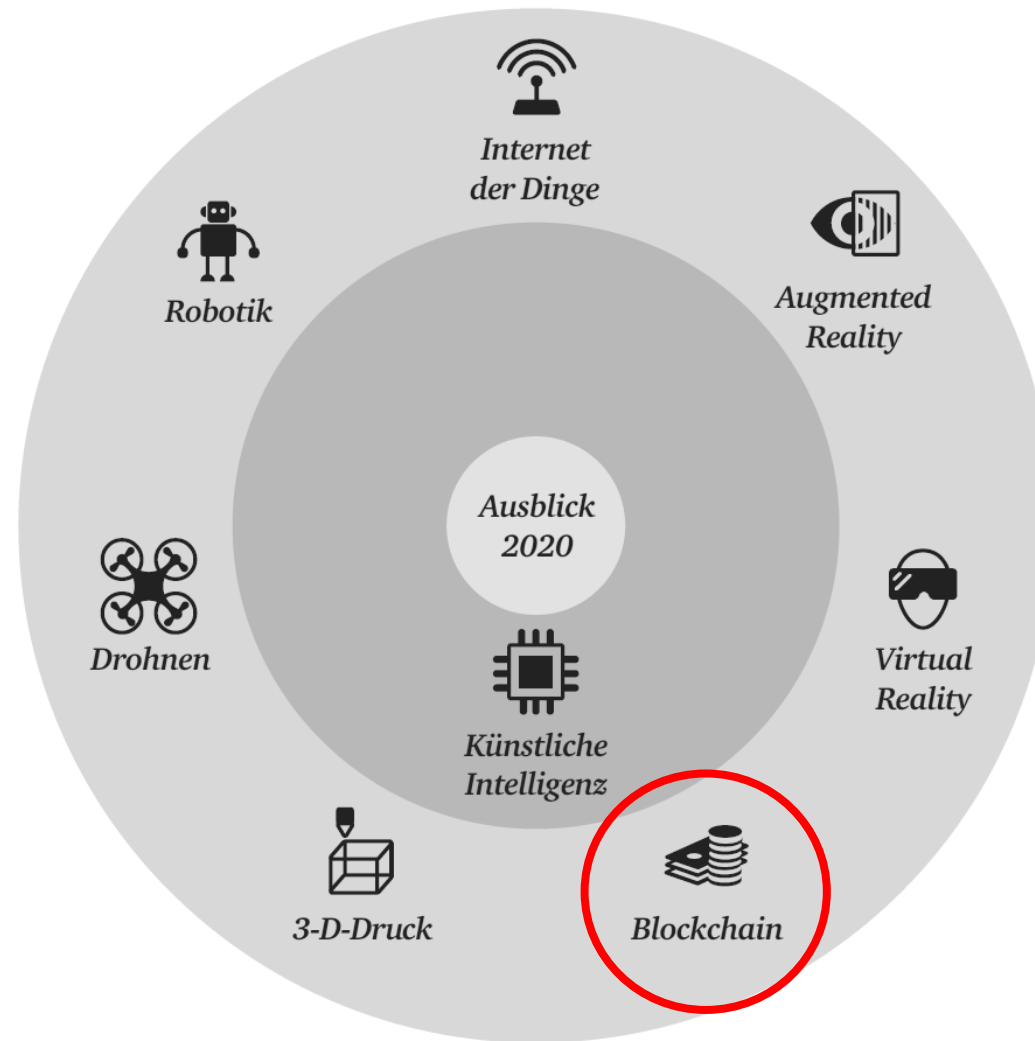
Einführung Blockchain

19. November 2019, Forum Blockchain for Business

Prof. Ernesto Turnes, CFA, M.A. HSG Banking & Finance, M.A. HSG Economics

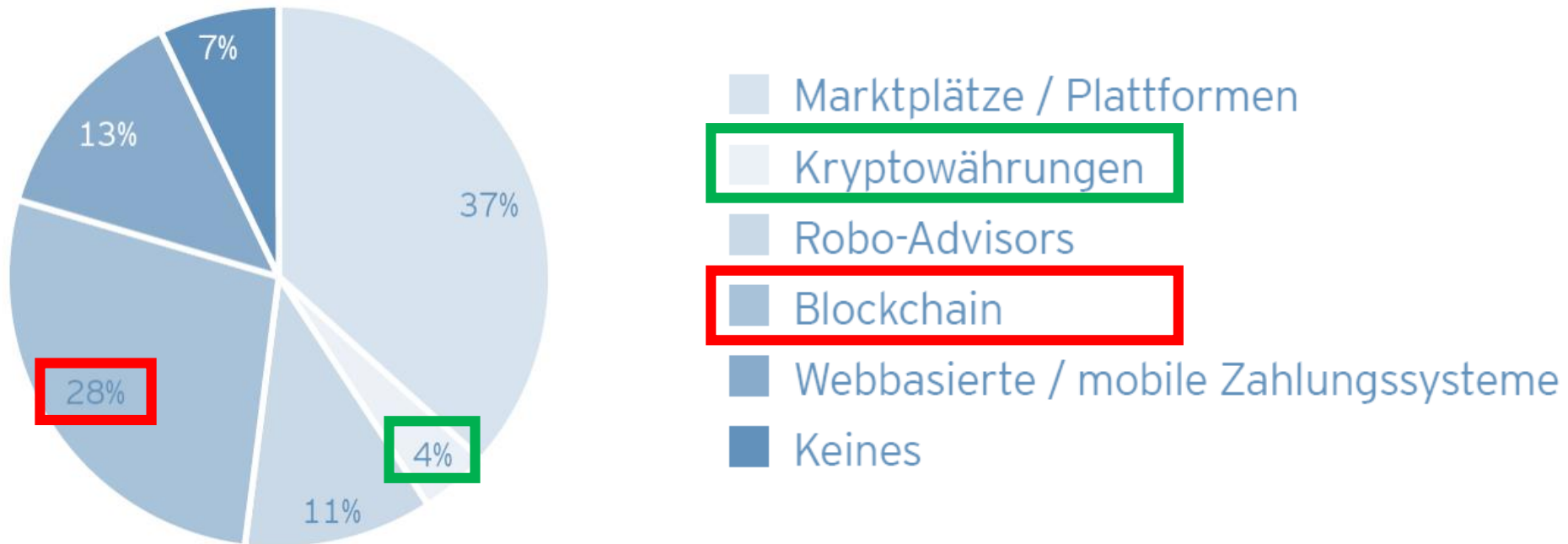


Technologische **Megatrends**



EY Bankenbarometer 2019

«In welchem der folgenden Phänomene / Entwicklungen sehen Sie am ehesten eine Bedrohung für etablierte Finanzinstitute?»





Deloitte Global **Blockchain Survey** (2019, n = 1'386, GL-Stufe, alle Branchen)

Blockchain technology is broadly scalable and will eventually achieve mainstream adoption



Blockchain will disrupt our industry



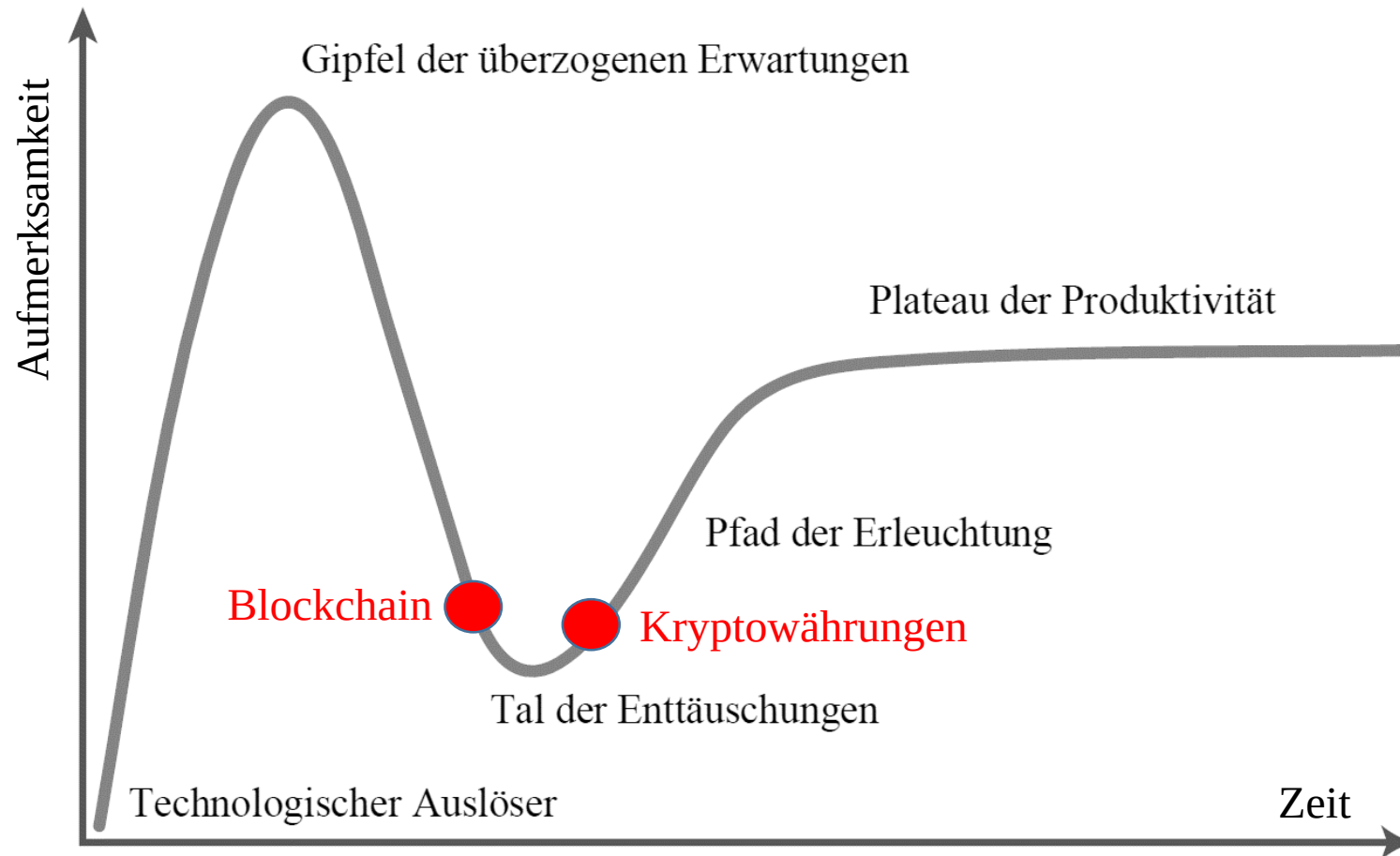
■ 2019 ■ 2018

Note: Percentages indicate respondents who strongly or somewhat agree with each statement.

Source: Deloitte's Global Blockchain Survey, 2018 and 2019.



Gartner Hype Cycle Blockchain (September 2019)

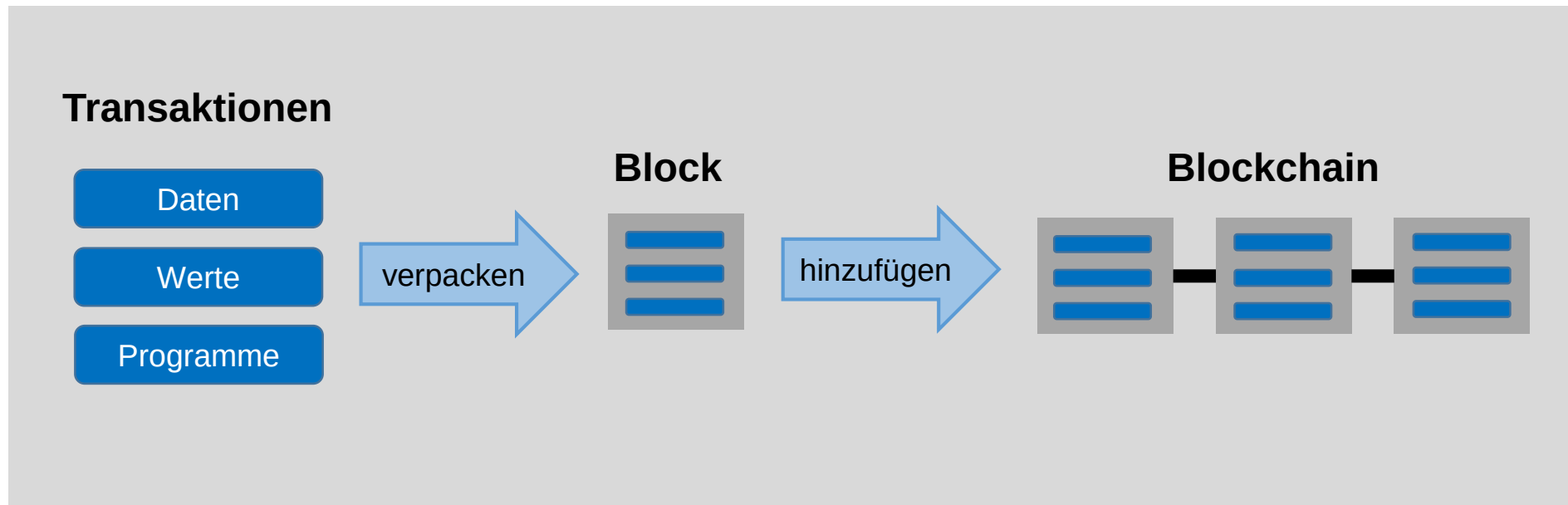


Definition Blockchain

Blockchain = **verteilte Transaktionsdatenbank** (Oberbegriff: **Distributed Ledger Technology, DLT**)

- **Datenbank:** Register, Liste oder Hauptbuch zur Erfassung von Transaktionen
- **Transaktionen:** Transfer von Daten, Werten und Programmen (z.B. Smart Contracts)
- **Verteilt:** Peer-to-Peer-Netzwerk (P2P) anstelle von zentralem Intermediär-System

Blockchain als verteilte Transaktionsdatenbank



Blockchain als **verteilte** Transaktionsdatenbank

Centralized

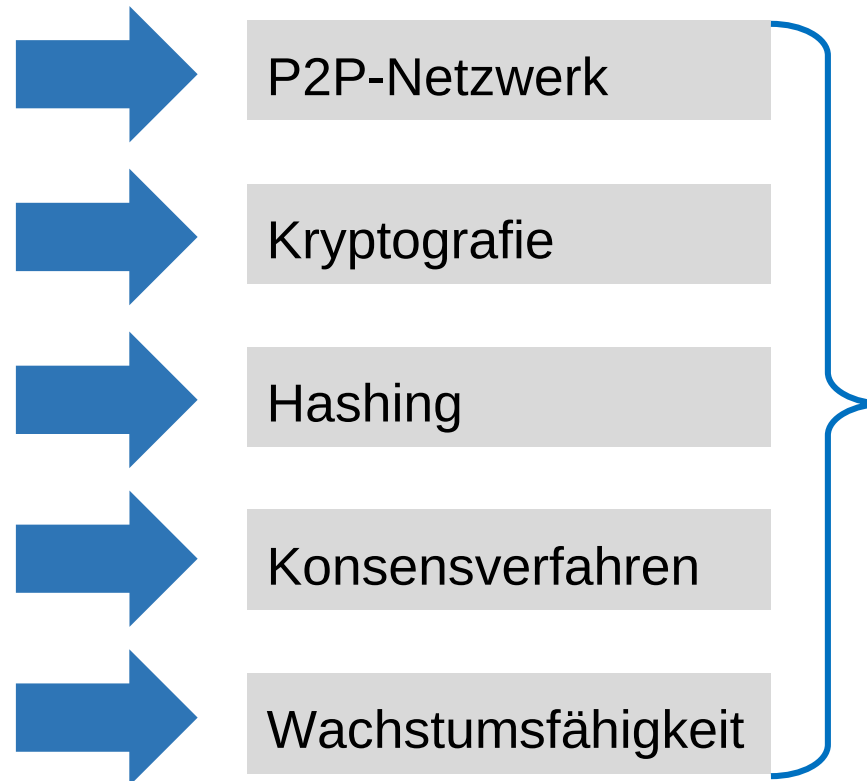


Distributed



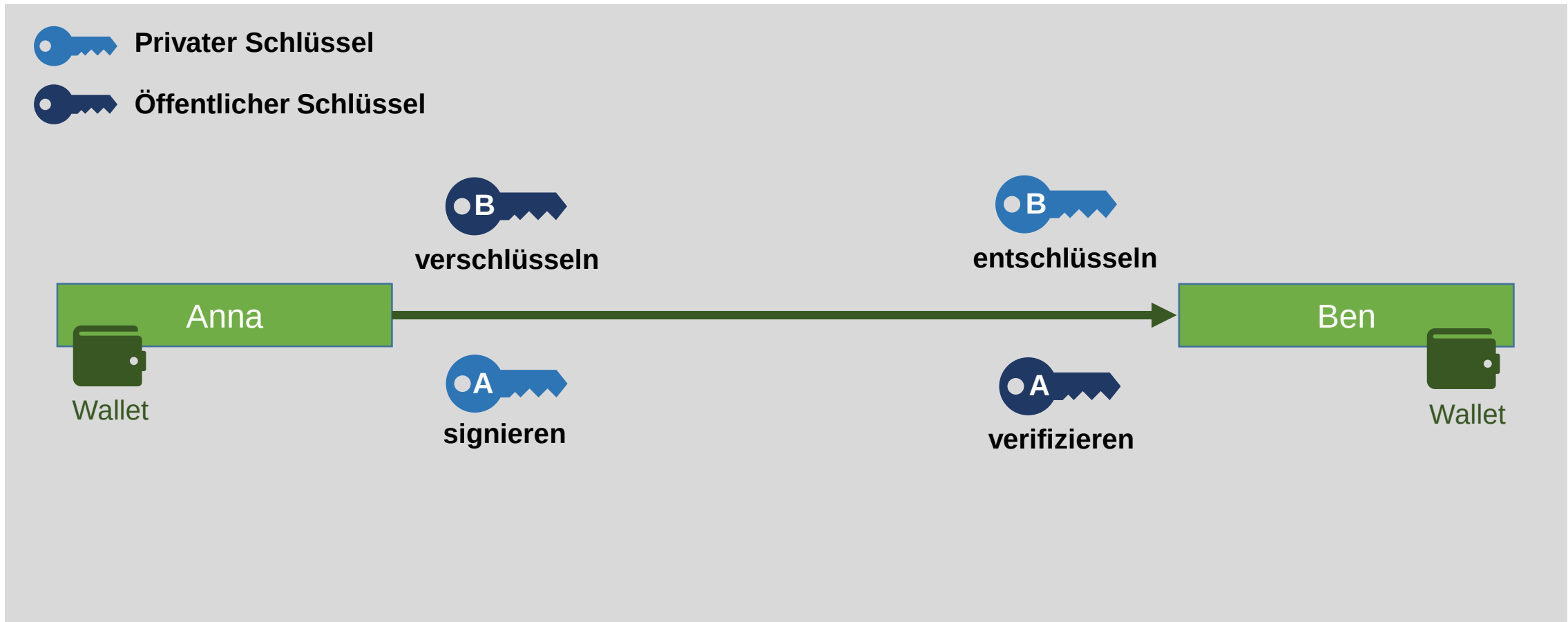
- ✓ Kein Intermediär
- ✓ Sicherheit
- ✓ Transparenz

Anforderungen an ein Transaktionssystem



Vertrauen

Eigentumssicherung durch Kryptografie (Verschlüsselung)



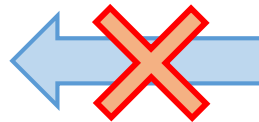
Eigentumssicherung durch Kryptografie (Verschlüsselung)

Privater Schlüssel



- Ist **privat**, geheim, vertraulich
- Darf auf keinen Fall geteilt werden (z.B. PIN-Code, Schlüssel Briefkasten)
- **Entschlüsselung** von Transaktionen
- **Digitale Signatur** für Transaktionen

Aus dem Private Key
wird der Public Key
erzeugt



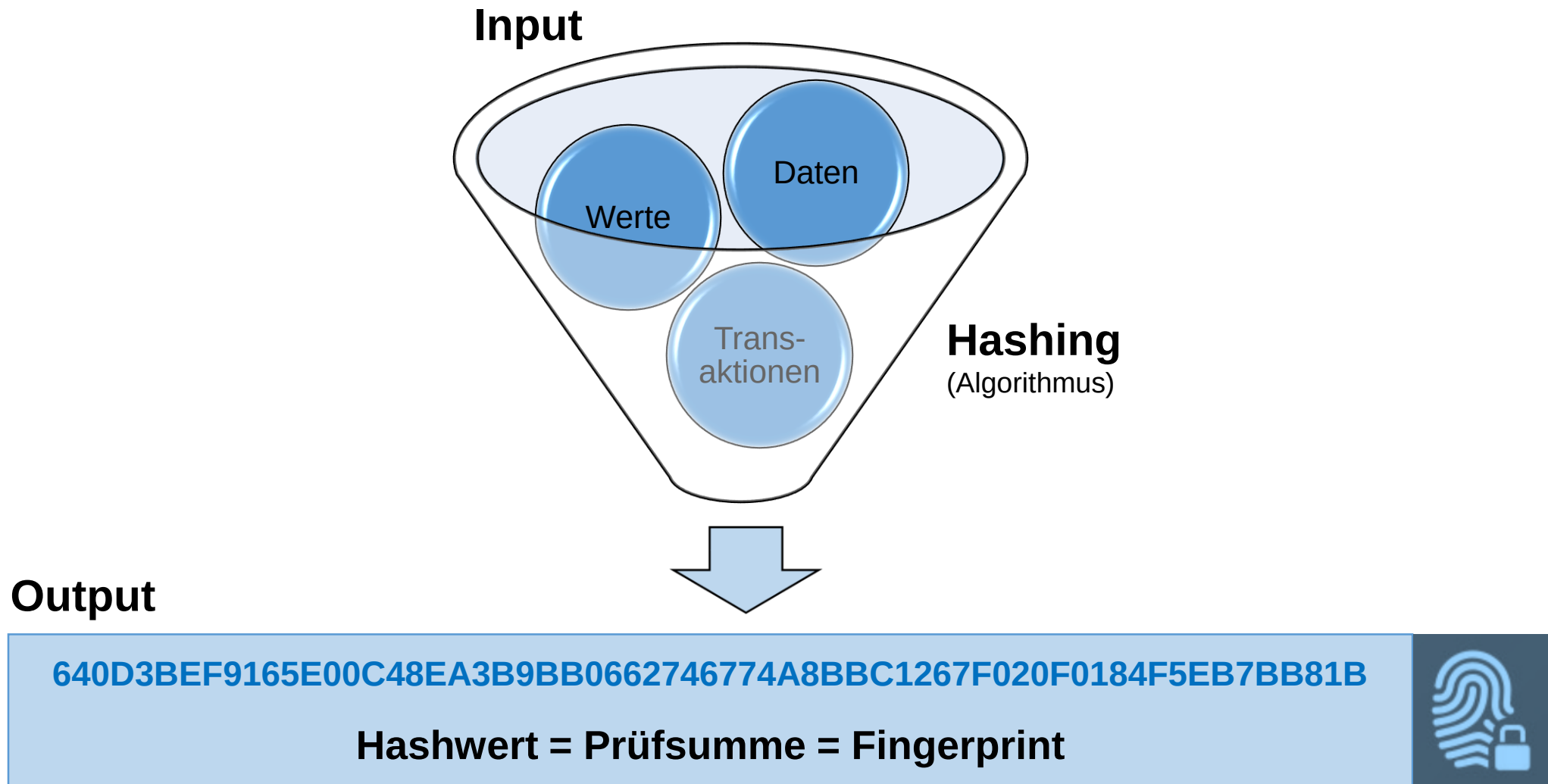
Aus dem Public Key
kann der Private Key
nicht erzeugt werden

Öffentlicher Schlüssel

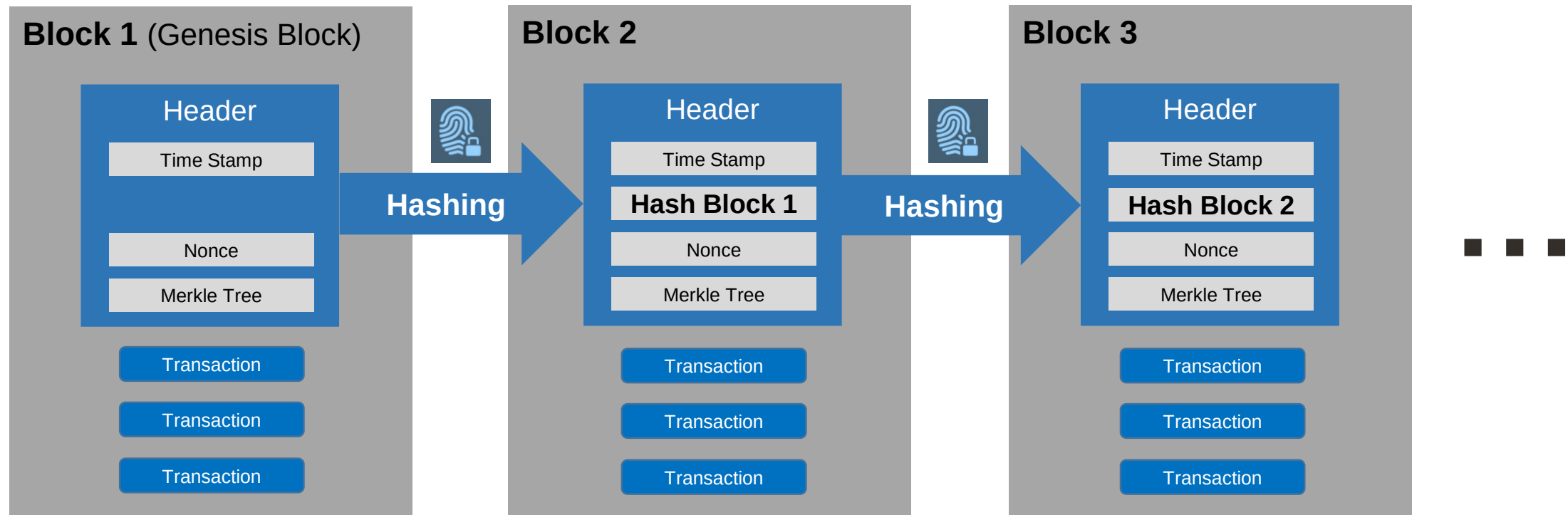


- Ist **öffentlich**, nicht vertraulich
- Kann problemlos geteilt werden (z.B. Kontonummer, Briefkasten)
- **Verschlüsselung** von Transaktionen
- **Verifizierung** von Transaktionen

Fälschungssicherheit durch Hashing



Fälschungssicherheit durch Hashing



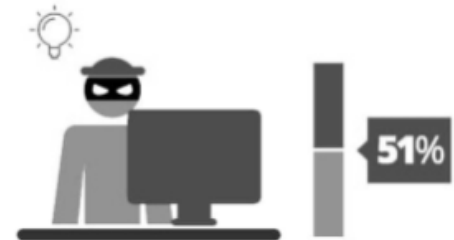
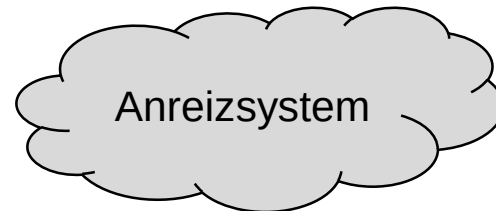
Validierung mit dem Konsens-Mechanismus «Proof of Work»



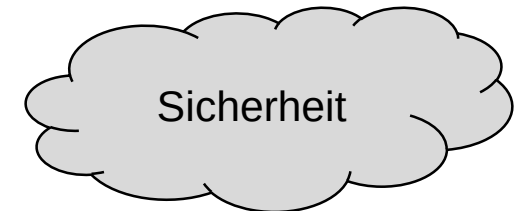
Um einen neuen **Block** an die **Blockchain** anhängen zu dürfen, müssen die **Miners** versuchen, schnellstmöglich ein **mathematisches Rätsel** zu lösen.



Der **erste Miner**, der die **Aufgabe** gelöst hat, erhält eine **Entschädigung** sowie alle **Transaktionskosten** des betreffenden Blocks.



Um die Blockchain erfolgreich **anzugreifen**, müsste ein **Hacker** über mehr als **50%** der **gesamten Rechenleistung** des Netzwerkes verfügen.



Arten von Blockchains

	Public (alle können teilnehmen und Transaktionen lesen)	Private (nur autorisierte Nutzer können teilnehmen und Transaktionen lesen)
Permissionless (alle können schreiben und Transaktionen validieren)	 	selten
Permissioned (nur autorisierte Nutzer können schreiben und Transaktionen validieren)	 	 HYPERLEDGER 

Public versus Private Blockchains

	Public Blockchain  	Private Blockchain (Konsortium)   
Partizipation	Meist ohne Zugangsbeschränkung (permissionless)	Meist mit Zugangsbeschränkung (permissioned)
Skalierbarkeit	Meist (noch) eingeschränkt	Hoch
Privatsphäre	Hoch	Sehr hoch
Native Kryptowährung	Ja	Nicht unbedingt notwendig



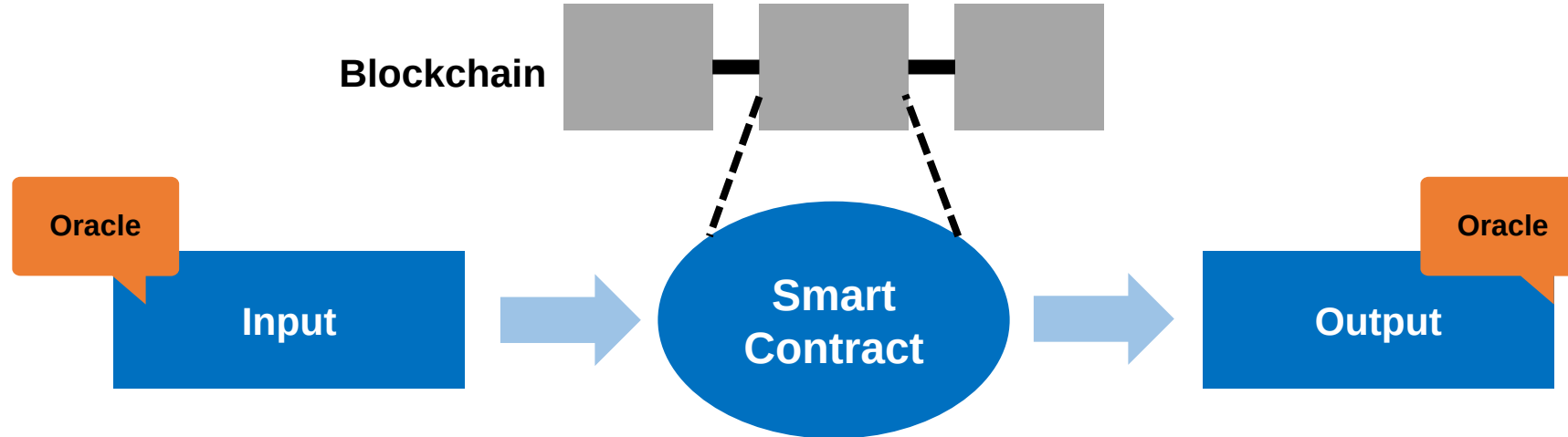
Smart Contracts und Anwendungsbeispiele der Blockchain



Smart Contracts

- Smart Contracts sind **Computerprogramme**, die bei Erfüllung bestimmter **Bedingungen automatisch** ausgeführt werden.
- Bei der automatischen Ausführung ist **keine zentrale Gegenpartei** involviert.
- Bei Smart Contracts werden **Inputs und Outputs** definiert. Dabei handelt es sich um eine **"Wenn-Dann"-Beziehung**.
- **Beispiel:** Flugverspätungsversicherung Fizzy der Axa (auf Ethereum-Blockchain)

Smart Contracts und Oracles



Anwendungsbeispiele der Blockchain



Herkunfts-/Echtheitsnachweis: z.B. Lebensmittel, Markenartikel, Diamanten, Kunst



Gesundheitswesen: z.B. Patientendossier



Bildungswesen: z.B. Diplome, Forschungsergebnisse



Identitätsnachweis: z.B. Pass/ID, Führerschein



Versicherungen: z.B. Flugverspätung, Ernteauffälle



Banking: z.B. Zahlungsverkehr, Finanzierung (ICO/STO), Trade Finance



Börsen: z.B. Wertpapierabwicklung (Settlement)

Anwendungsbeispiele der Blockchain



Öffentliche Verwaltung: z.B. Grundbuch, Wahlen, Betreibungs- / Handelsregister



Logistik/Lieferkette: z.B. internationaler Handel



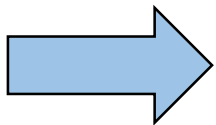
Autohandel: z.B. Occasionsmarkt



Energiebranche: z.B. Eigenverbrauchsgemeinschaften



Sportwetten: z.B. Fussball



Ersetzen eines Intermediärs, Prozessoptimierungen, neue Geschäftsmodelle, Kooperationen (Ökosysteme), ...



Kryptowährungen und Tokens

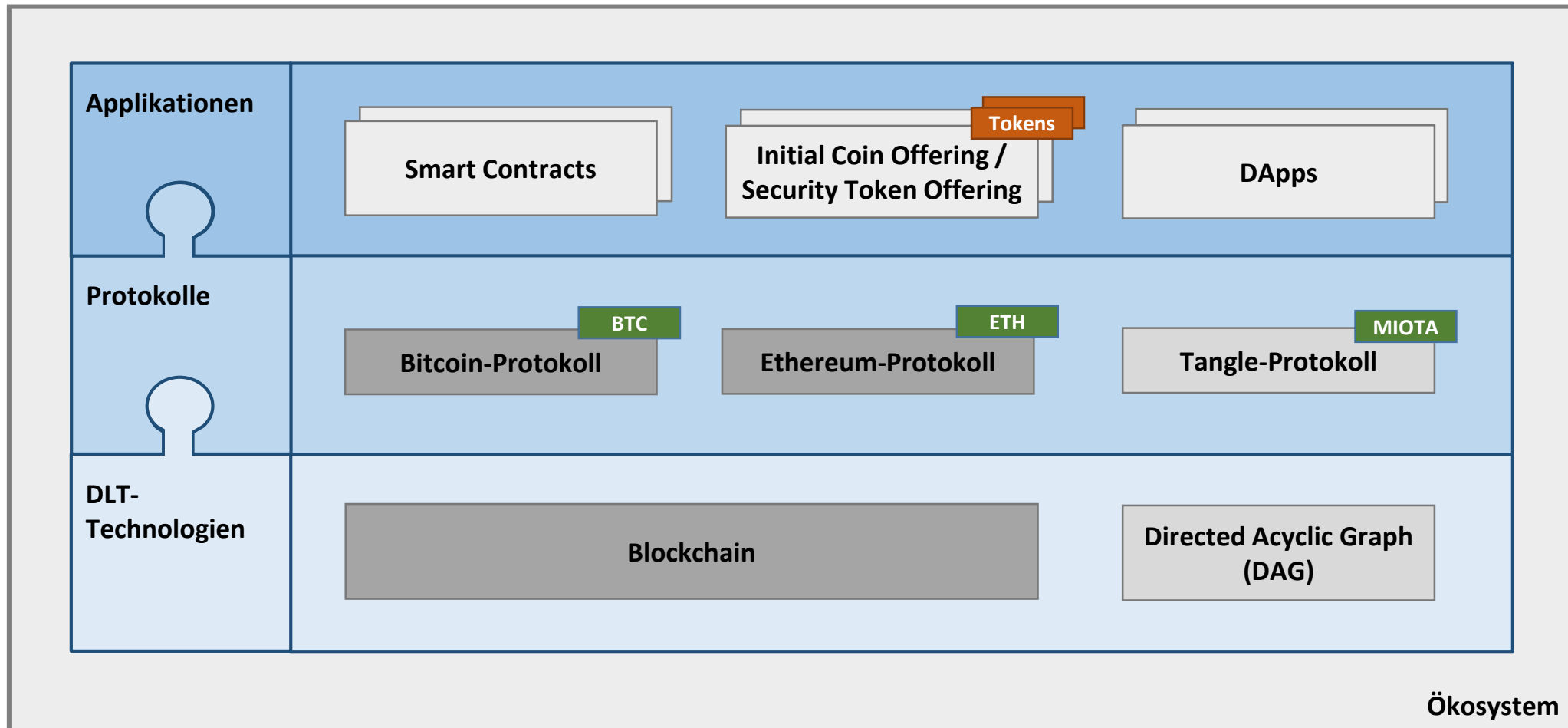


Marktkapitalisierung aller Kryptowährungen/Tokens



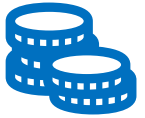
Quelle: www.coinmarketcap.com

Arten von Tokens/Kryptowährungen



Arten von Tokens/Kryptowährungen

Kategorisierung nach Schweizer Finanzmarktaufsicht (FINMA):



Zahlungs-Tokens (Payment Tokens) dienen als Zahlungsmittel



Nutzungs-Tokens (Utility Tokens) dienen zur Nutzung von Plattformen und Applikationen



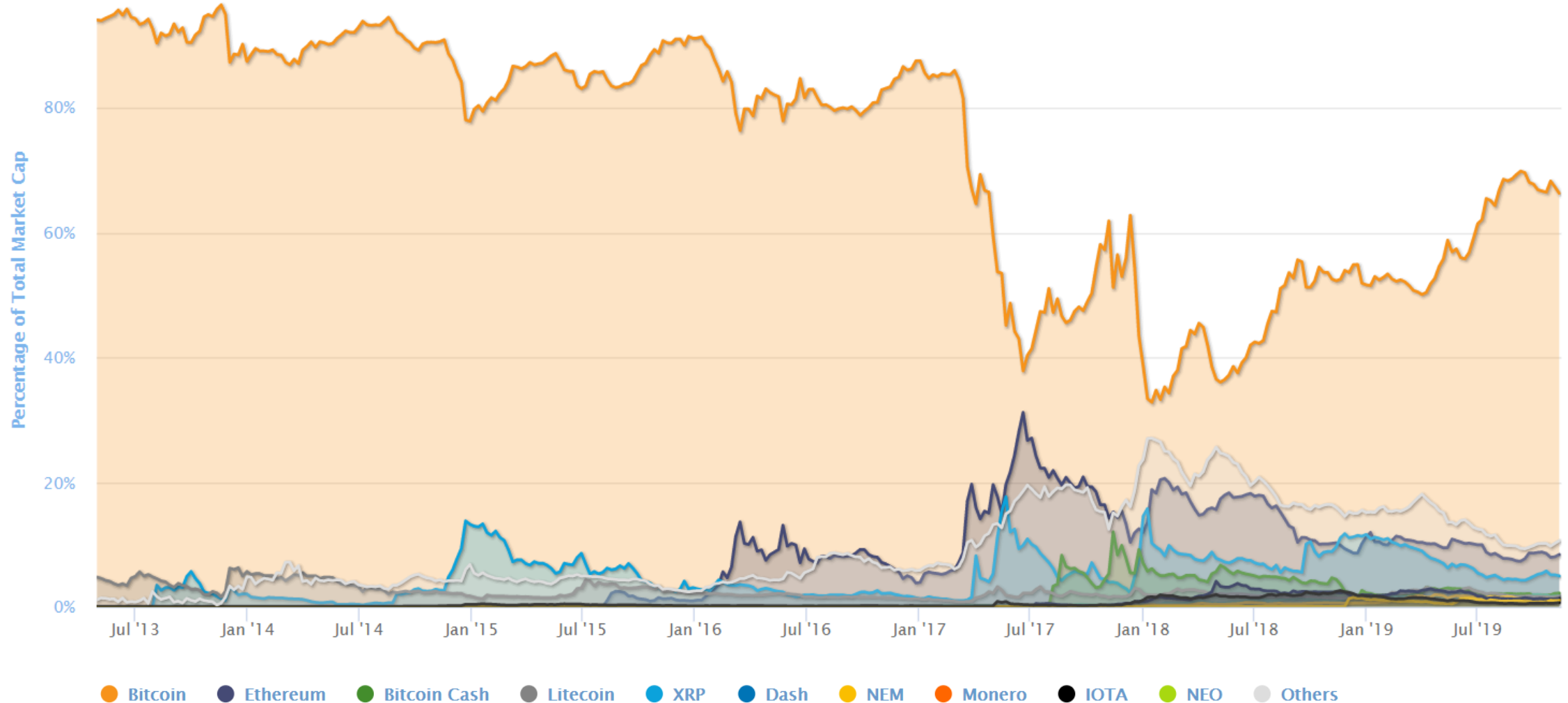
Anlage-Tokens (Security Tokens) repräsentieren Vermögenswerte wie Aktien, Anleihen oder Immobilien → Tokenisierung von Assets (Tokenomics)

Top 5 Kryptowährungen/Tokens (Stand: 14/11/2019, gerundet)

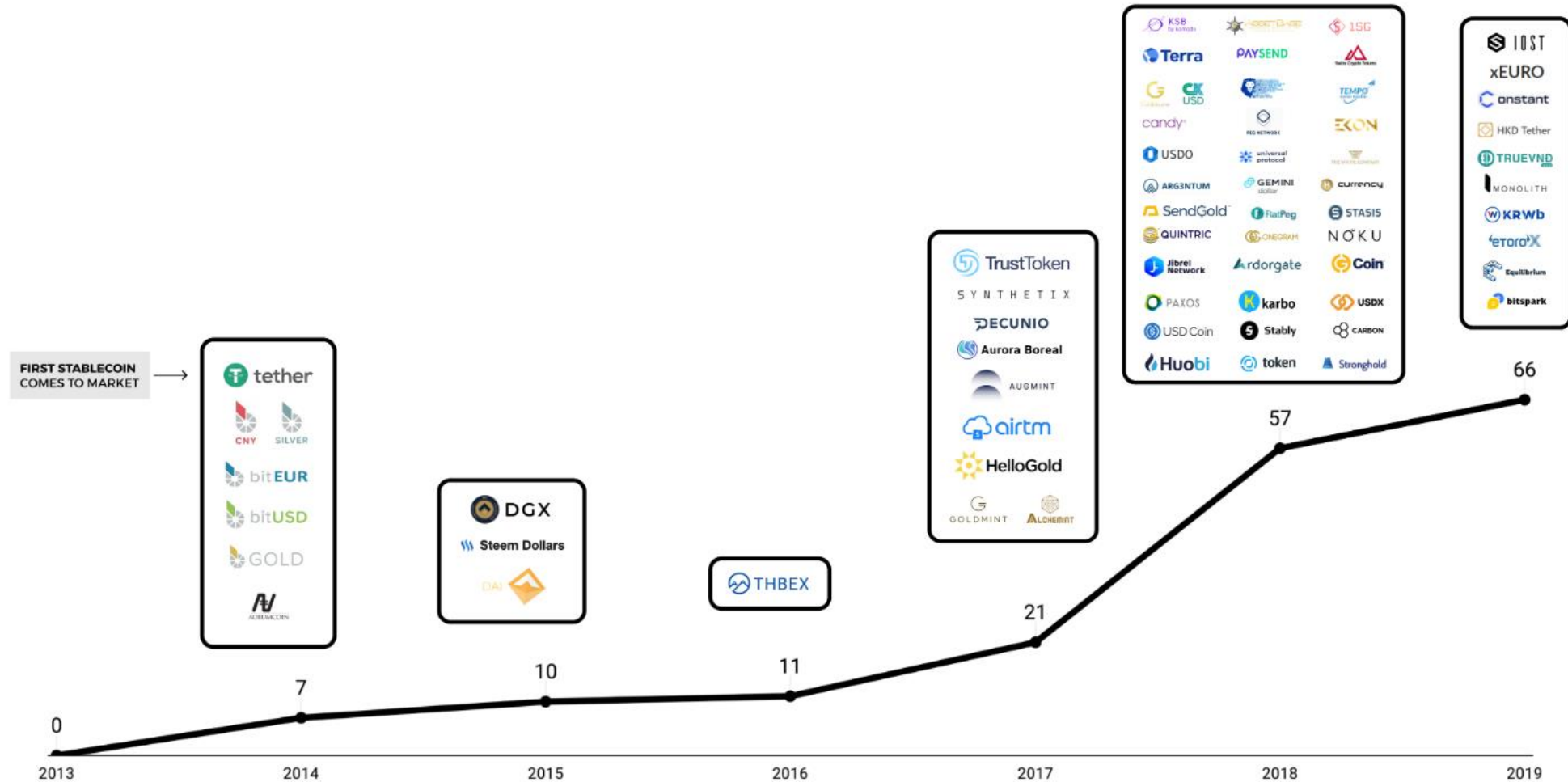
#		Name	Ticker	Gründung	Market Cap. (\$)	# ausstehend	# maximal
1		Bitcoin	BTC	2009	157 Mrd.	18 Mio.	21 Mio.
2		Ethereum	ETH	2015	20 Mrd.	109 Mio.	-
3		Ripple	XRP	2012	12 Mrd.	43'300 Mio.	100'000 Mio.*
4		Bitcoin Cash	BCH	2017	5 Mrd.	18 Mio.	21 Mio.
5		Tether	USDT	2015	4 Mrd.	4'000 Mio.	-

* Alle XRP sind bereits geschürft

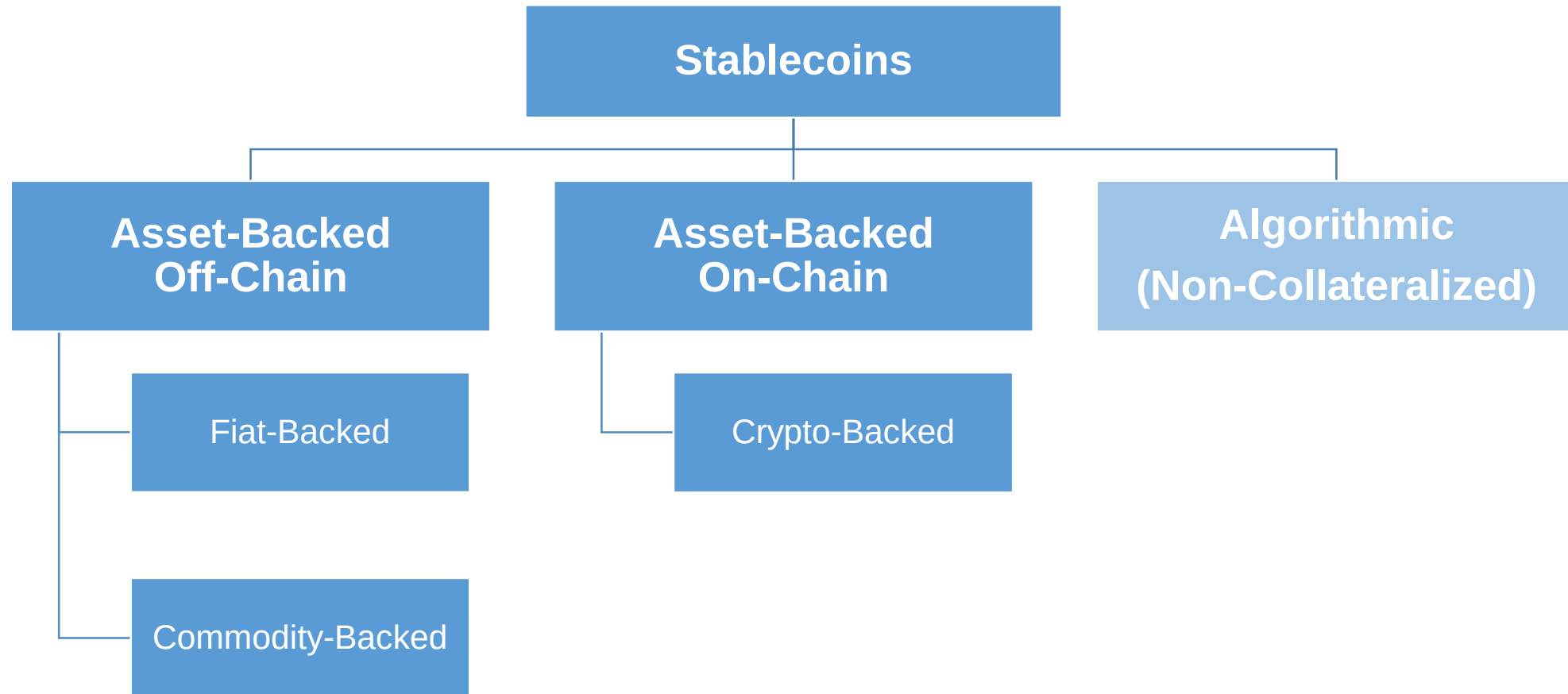
Marktanteil von Kryptowährungen/Tokens



Stablecoins



Arten der Besicherung von Stablecoins

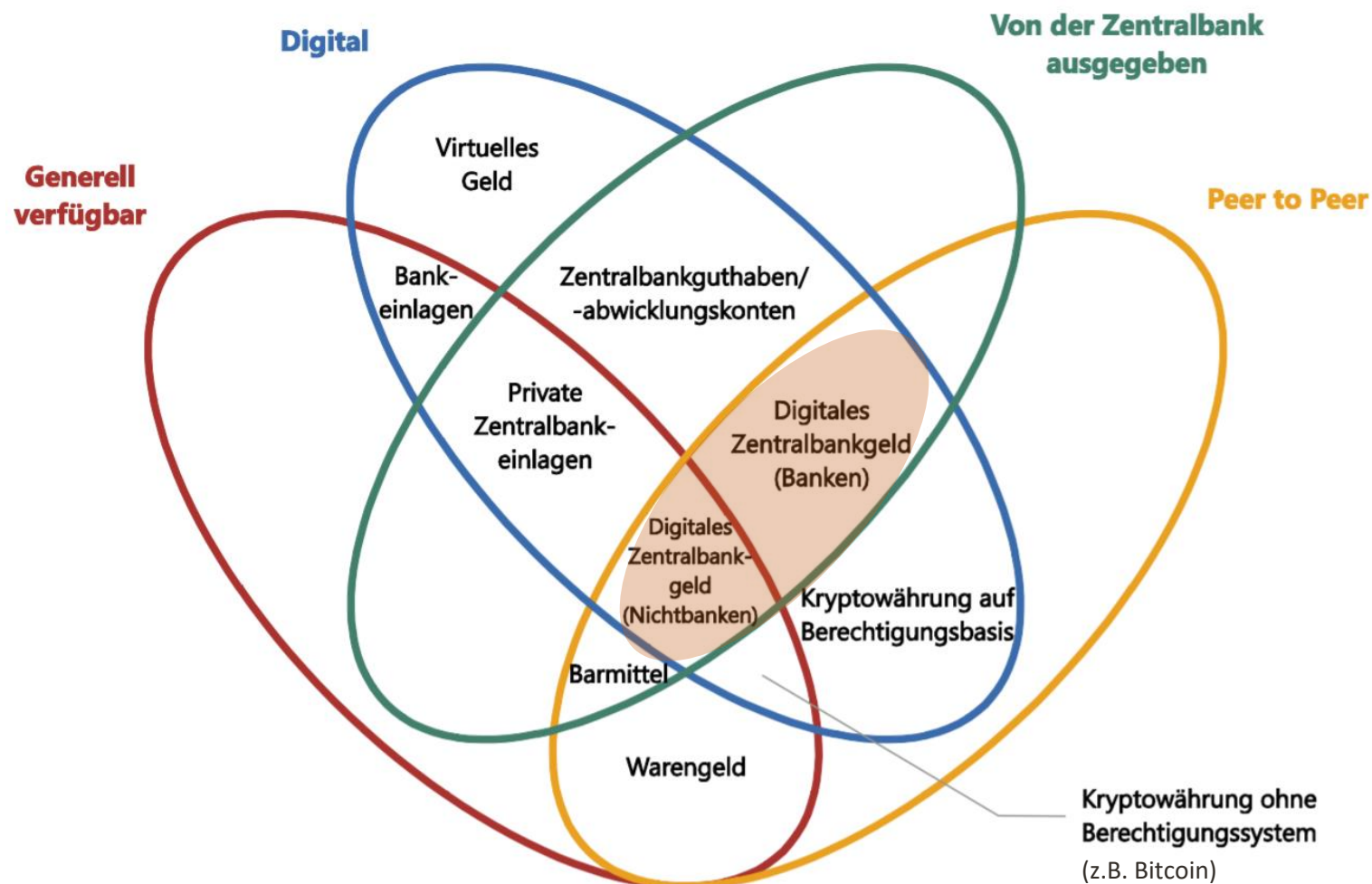




Globaler Stablecoin (in Planung)

- Ein Konsortium rund um Facebook plant im **Juni 2020** die Lancierung des **globalen Stablecoins "Libra"**. Eine **Massenadaption** wird durch die **hohe Anzahl Nutzende** von Facebook (> 2 Mrd.) begünstigt (WhatsApp und Instagram gehören auch zu FB).
- Libra basiert auf einer **Permissioned Blockchain** und wird mit **Reserven** gedeckt (Korb aus Währungen und Staatsanleihen; Varianten: ein Libra pro Land oder nur noch Facebook Pay?)
- Libra ermöglicht eine **hohe Skalierbarkeit** (1'000 TPS) und **geringe Transaktionskosten** (Validierung durch Members statt Mining/PoW)
- **Libra Association** mit Sitz in Genf (unabhängig von Facebook) übernimmt die **Koordination** zwischen den Validatoren und das **Management** der **Libra-Reserven**. Die Mitglieder zahlen **USD 10 Mio.**, partizipieren an den **Erträgen** der Libra-Reserven und haben ein **Stimmrecht** im Libra Association Council (bei geplanten 100 Mitgliedern → 1% Stimmanteil)

Digitales Zentralbankgeld (Central Bank Digital Currencies, CBDC)



Wallets als Schlüsselbund

- Für **Transaktionen** und **Handel** von Kryptowährungen bzw. Tokens wird ein **Wallet** benötigt.
- Im **Wallet** werden die **privaten und öffentlichen Schlüssel** (Schlüsselbund) gespeichert und der **Betrag an Tokens** angezeigt (Tokens werden auf der Blockchain gespeichert).
- **Arten von Wallets** (<https://bitcoin.org/de/wallets/web/>):
 - **Online Wallet** (Online in der Cloud)
 - **Exchange Wallet** (Online an der Börse)
 - **Mobile Wallet** (App auf dem Smartphone)
 - **Desktop Wallet** (Software auf dem Desktop)
 - **Paper Wallet** (Ausdruck auf Papier)
 - **Hardware Wallet** (physisches Gerät) →





Krypto-Börsen (nicht abschliessend)

Name	Domizil	Webseite
Binance	Tokio	www.binance.com
Bitcoin.de	Deutschland	www.bitcoin.de
Bitfinex	Hong Kong	www.bitfinex.com
Bitpanda	Österreich	www.bitpanda.com
Bitstamp	GB	www.bitstamp.com
Bittrex	USA	www.bittrex.com
Coinbase	USA	www.coinbase.com
Huobi	China	www.huobi.com
Kraken	USA	www.kraken.com
Poloniex	USA	www.poloniex.com



Initial Coin Offering (ICO) und Security Token Offering (STO)

Definition ICO und STO

- Bei **ICOs** und **STOs** werden zur **Finanzierung** von **Projekten** und **Unternehmen** neue Tokens ausgegeben (Crowdfunding).
- Beim **ICOs** werden **Nutzungs-Token** (ohne Rechte) ausgegeben, bei **STOs** dagegen **Security Tokens** (Eigentumsrechte). Die Tokens sind jedoch **nicht** automatisch an der Börse handelbar.
- Die neuen Tokens werden gegen **Fiatwährung** (USD, EUR) oder **Kryptowährungen** wie BTC (Bitcoin) und ETH (Ether) emittiert.
- Aufgrund von **Betrugsfällen** sind **ICOs** in Verruf geraten. **STOs** gelten daher als **ICO 2.0** bzw. als **regulierte Version** von ICOs. In jüngster Vergangenheit gibt es auch einige **IEOs** (Initial Exchange Offerings).



Definition ICO und STO

- Sämtliche Details zum **ICO/STO** werden im **White Paper** festgehalten und veröffentlicht.
- Die **ICO/STO-Unternehmen** benötigen nicht nur die **Unterstützung** von Anwälten, IT-Experten und Marketing-Spezialisten, sondern auch eine **Bankbeziehung**. Die Banken sind jedoch meist (noch) sehr zurückhaltend.
- Die **Schweizer Börse** plant die Lancierung einer eigenen **STO- und Digital-Assets-Handelsplattform** (SIX Digital Exchange, SDX) mit einem **eigenen Stablecoin** (zusammen mit SNB).



Motive für ICO/STO-Finanzierungen

- (Einfacherer) Zugang zu Kapital
- Tiefere Kosten?
- Breite Investorenbasis
- Kleine Stückelung
- Handelbarkeit (erst nach Börsenkotierung)
- Sammeln von Erfahrungswerten
- Digitale Ausübung von Stimmrechten (z.B. Equity Tokens)
- ...

Die 15 grössten ICO/STO seit 2016

#	Name		Total Raised Amount (USD mn) ¹⁾	End of ICO (month)	Focus	Industry	Country
1	EOS²⁾	1 Year ICO	4'100	06.2018	Blockchain infrastructure for decentralized apps	BC infrastructure	Cayman Islands
2	Telegram		1'700	03.2018	Tokens to enhance messenger ecosystem	Social media	British Virgin Islands
3	TaTaTu	NEW ICO	575	06.2018	Social entertainment on the Blockchain	Entertainment	Cayman Islands
4	Dragon		320	03.2018	Decentralized currency for casinos	Gambling	British Virgin Islands
5	Huobi Token		300	02.2018	Coin for South Korean crypto exchange	FinTech	Singapore
6	HDAC		258	12.2017	IOT platform backed by Hyundai BS&C	Internet of things	Switzerland
7	Filecoin		257	09.2017	Decentralized market for data storage	Data storage	USA
8	Tezos		232	07.2017	Blockchain infrastructure for decentralized apps	BC infrastructure	Switzerland
9	Sirin Labs		158	12.2017	Secure open source consumer electronics	Consumer electronics	Switzerland
10	Bancor		153	06.2017	Enabling direct conversion between tokens	FinTech	Switzerland
11	Bankera		151	03.2018	Banking for the Blockchain era	FinTech	Lithuania
12	Polkadot		145	10.2017	Interoperability protocol across multiple Blockchains	BC infrastructure	Switzerland
13	The DAO		143	05.2016	Decentralized autonomous organization	Venture Capital	Switzerland
14	Polymath		139	01.2018	Security token platform	FinTech	Barbados
15	tZERO	NEW STO	134	08.2018	Security token trading platform	FinTech	USA



Zitat von Roy Amara:

«Wir tendieren dazu, **Technologien** kurzfristig zu überschätzen und langfristig zu unterschätzen.»

