Bitcoin

Prof. Dipl.-Ing. Klaus Knopper
Hochschule Kaiserslautern
<klaus.knopper@hs-kl.de>

Vortrag zur Veranstaltung
„Anwendungsorientierte Informatik“
vom 6.12.2017

Inhalt der Vorlesung

- Grundsätzlichen Aufbau digitaler „Krypto-Währungen“ kennen lernen: Adressen (public) vs. Keys (private), Transaktionsprotokoll (Blockchain),*)
- Sicherheitsaspekte: Verfügbarkeit, Integrität, Vertraulichkeit, Authentizität,
- Rolle in der Wertschöpfungskette und im Zahlungsverkehr,
- Aktuelle Gesetzeslage und Verfügbarkeit/Usability.

---

*) low-tech Version

Warum Krypto-Währungen?

- Satoshi Nakamoto (Pseudonym) 2008: ☞ White Paper zu einem **dezentralen Zahlungssystem** mit „Bargeld"-ähnlichen Eigenschaften, Open Source Implementierung (bitcoin core client),
- **Unabhängigkeit von zentralen Instanzen**, die den Wert des Geldes kontrollieren (Zentral-Banken, Währungsaufsicht etc.),
- **Vertrauen** eher in die **Zuverlässigkeit von technisch-mathematisch beweisbaren Verfahren** als in Vertrauenswürdigkeit von Einzelpersonen oder Institutionen,*)
- **Ziel: einfacher, schneller und sicherer Transfer von Geld**.

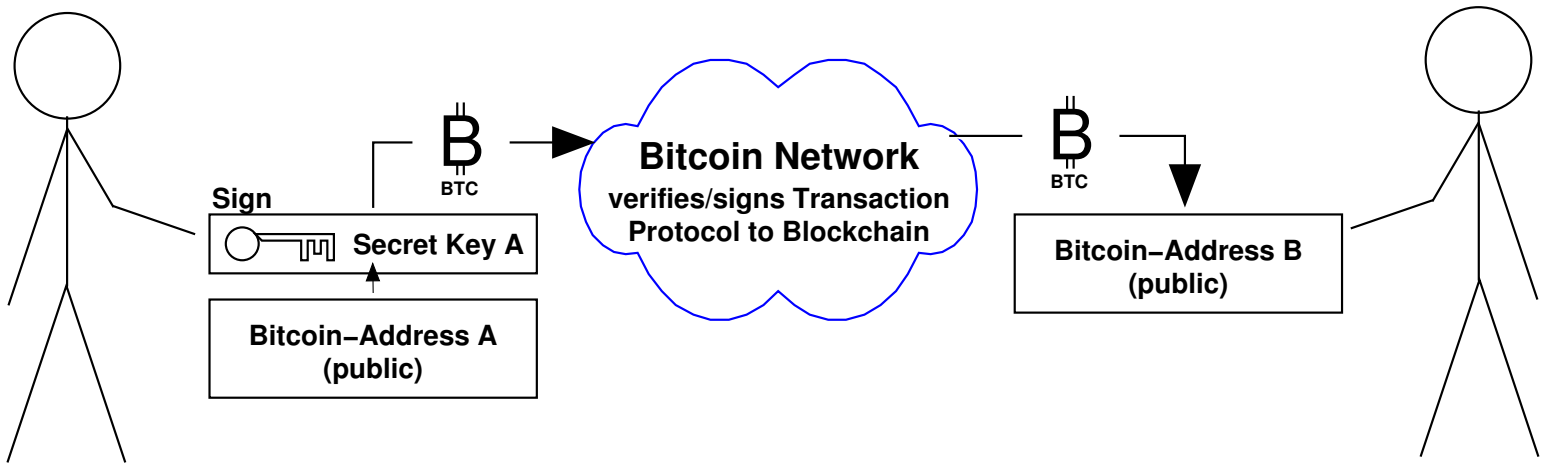
---

*) Transaktionsgebühren sind im Netzwerk möglich und dienen der Erhaltung der Infrastruktur, sind aber von Staatsgrenzen und Geldinstituten unabhängig.

Adressen vs. Keys

- **Grundlage** ist die **asymmetrische Verschlüsselung und Signatur** wie bei **SSL/TLS** mit öffentlichen Zertifikaten und privaten Schlüsseln, welche auch im WWW für sichere Transaktionen (Shopping, Online-Banking) eingesetzt wird.
- Die **Bitcoin-Adresse** ist die **„öffentliche Kontonummer“**, die Zahlungen **empfangen** kann, (entspricht **„public key“**).
- Der zu dieser Adresse passende **private key** (bzw. **secret key**) dient zur Autorisierung von Zahlungen (**Senden** von Bitcoins), er ist **nur dem Eigentümer** bekannt,

Schematische Darstellung einer Transaktion



Die Bitcoin-Adresse ist in der Blockchain öffentlich, während der damit verbundene geheimen Schlüssel, mit dem Transaktionen durchgeführt werden können, nur dem Besitzer bekannt ist.

Bitcoin-Überweisungen sind daher auch nicht anonym sondern pseudonym: Alle Transaktionen sind lückenlos öffentlich dokumentiert, jedoch gibt es keine öffentliche Zuordnung zu den Besitzern der geheimen Schlüssel.

Verfügbarkeit von Bitcoin-Adressen

- Mathematisch gesehen existiert eine **riesige Menge von Bitcoin-Adressen** und dazu passenden privaten Schlüsseln,
- Es ist **theoretisch möglich**, einen zu einer Bitcoin-Adresse gehörenden privaten Schlüssel (vergl. Zugangspasswort beim Online-Banking) durch Ausprobieren zu **erraten**, die **Wahrscheinlichkeit hierfür ist aber „astronomisch“ gering** (im Mittel $2^{255} \approx 10^{77}$ Versuche bei einer Schlüssellänge von 256 Bit),
- Schlechte Zufallszahlen-Generatoren reduzieren allerdings die Anzahl der Bits, die bei einem brute-force-Angriff ausprobiert werden müssen.

Bitcoin Codes (1)

Die **Codes** für öffentliche Adresse und privaten Schlüssel lassen sich als **Zahlen- oder Buchstabenfolge** (oft im ☞ Base58-Format) sowie als ☞ **QR-Code** darstellen und somit **leicht** einscannen und **elektronisch verarbeiten**, zur einfachen Nutzung per Multiplattform **Bitcoin-Applikation oder App**: ☞ Mycelium, Electrum, Bitcoin Core (komplette Blockchain-Kopie).

bitcoin:1Knoppix PjYgK52P3
dnuSmp1u FP2A3LuGW

Bitcoin Codes (2)

Der **Besitzer des private Key** einer Bitcoin-Adresse kann das Bitcoin-Guthaben **ohne Widerrufsmöglichkeit**, auch für den eigentlichen Eigentümer, transferieren oder ausgeben (d.h. ein „Diebstahl“ ist möglich, wenn der private Key unzureichend geschützt ist!).
Wer um die Sicherheit seines ggf. sehr hohen Bitcoin-Guthabens fürchtet, muss den für den **Transfer** seiner Bitcoins notwendigen **private Key** allerdings nicht zwangsläufig auf einem Computer im Netzwerk oder überhaupt digital speichern.*)

- **Paper-Wallet:** Ausdruck des Public+Private-Keypaar auf Papier, anschließend Zerstören aller elektronischen Exemplare des *Private Key* (Überschreiben / sicheres Löschen),
- **Brain-Wallet:** Auswendig merken (!) des Private Key, z.B. als ☞ Base58-Zeichenkette oder kodiert als „Gedicht“.

---

*) Man bezeichnet ausschließlich „offline“ gespeicherte geheime Schlüssel auch als „Cold Wallet“.

Transaktionsprotokoll: Die Blockchain

- **Alle Transaktionen** werden in Form einer Liste **kontinuierlich protokolliert** und von den Teilnehmern am Bitcoin-Netzwerk **durch elektronische Signatur bestätigt**,
- erst nach einer **hinreichenden Anzahl von Bestätigungen** durch die Netzwerk-Teilnehmer **ist eine Transaktion bestätigt**,
- das **Transaktionsprotokoll** ist in sog. **Blöcke** aufgeteilt, die vollständig oder teilweise von allen Netzwerk-Teilnehmern gespeichert werden,
- bei **„core"**-Clients für das Bitcoin-Netzwerk werden **alle bestätigten Transaktionsblöcke** gespeichert (derzeit 20GB), bei „light"-Clients hingegen nur die den Teilnehmer betreffenden (z.B. Smartphone-Clients),
- um Transaktionen zu fälschen bzw. Beträge doppelt auszugeben müsste ein Teilnehmer mehr als 50% des Bitcoin-Netzwerkes bzw. der Rechenleistung aller Teilnehmer besitzen.

☞ **http://blockchain.info**

Bitcoin Mining (1)

Die von Satoshi Nakamoto vorgeschlagene Lösung zum Initialproblem der Währungsverfügbarkeit wurd durch den Ansatz einer Belohnung für dem Netzwerk zur Verfügung gestellte Rechenleistung gelöst, wobei alle 10 Minuten ein neuer Block generiert wird, für den es - derzeit 25 - Bitcoins als Belohnung für die Lösung einer rechenintensiven kryptographischen Aufgabe gibt. Je mehr Rechenleistung im Netz verfügbar ist, desto höher wird gleichzeitig der Rechenaufwand für den nächsten Block (die „Difficulty“ steigt).

Bitcoin Mining (2)

Waren zu Beginn noch schnelle Prozessoren oder Grafikkarten ausreichend, um den SHA256-basierten Rechenalgorithmus zum „Schürfen“ von Bitcoins und Gewinnen im Wettbewerb um die schnellste Lösung als „Solo Miner“ durchzuführen, so ist es inzwischen nur noch mit Hilfe von ☞ ASICs und im Zusammenschluss mit anderen „Pool Minern“ möglich, einen signifikanten Anteil an den 10-minütlich vergebenen Bitcoins zu erhalten. Hier übersteigt, je nach Tauschkurs, der finanzielle Aufwand für den Betrieb (Strom, Kühlung) mitunter den erzielten Profit, wodurch das Mining in den meisten Ländern unrentabel geworden ist.

Bitcoin Mining (3)

Nach Berechnung aller 21 Millionen Bitcoins wird eine gewisse Rechenleistung weiterhin für die Signatur der Transaktionen benötigt, wofür dem Netzwerk vom Sender eine Transaktionsgebühr variabler Größe angeboten werden kann, um diese Transaktion möglichst schnell bestätigt zu bekommen.

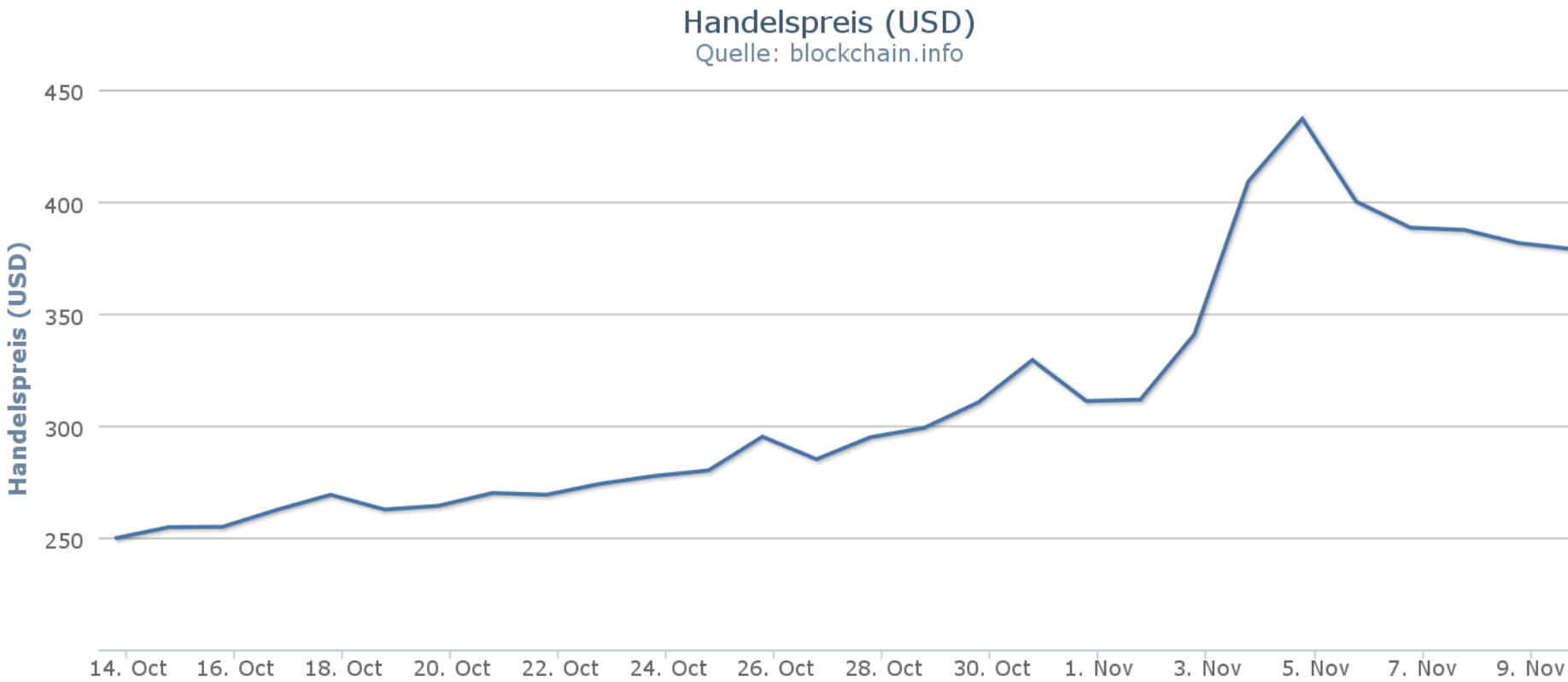
Rechtliche Aspekte von Bitcoin

- In einigen Ländern ist der Zahlungsverkehr mit bzw. Umtausch zwischen Landeswährung (☞ „**Fiatgeld**“) und nicht staatlich kontrollierbaren Digitalwährungen (Bitcoin, Altcoins etc.) den regulierten Banken untersagt, z.B. in Russland und China (kurioserweise nach wie vor die Länder mit dem größten Nutzerbestand),
- in Deutschland gilt Bitcoin derzeit als **„Rechnungseinheit“** und der Handel als „(privates) Veräußerungsgeschäft“, d.h. ☞ kurzfristige Spekulationsgewinne oder -Verluste ($<$ 1 Jahr Haltezeit) aus Währungsvolatilität/Börsenhandel **unterliegen zum aktuellen Kurs in € der Einkommensteuer**, die Umsatzsteuer auf Bitcoin-Transaktionen selbst wurde vom EUGh jedoch abgeschafft,
- die Regelungen des **Geldwäschegesetz**es etc. bezüglich Fiat-Währungen finden auf Bitcoin ebenfalls Anwendung, sind aber je nach Transaktionsart und Anonymisierungsgrad des Teilnehmers teils mehr, teils weniger kontrollierbar (Transaktionsprotokoll ist öffentlich, die Eigentümer der jeweiligen Adressen aber grundsätzlich nicht zuzuordnen).

Statistik: Bitcoin/USD-Tauschwert (1)

Statistik: Bitcoin/USD-Tauschwert (2)

Statistik: Bitcoin/USD-Tauschwert (3)



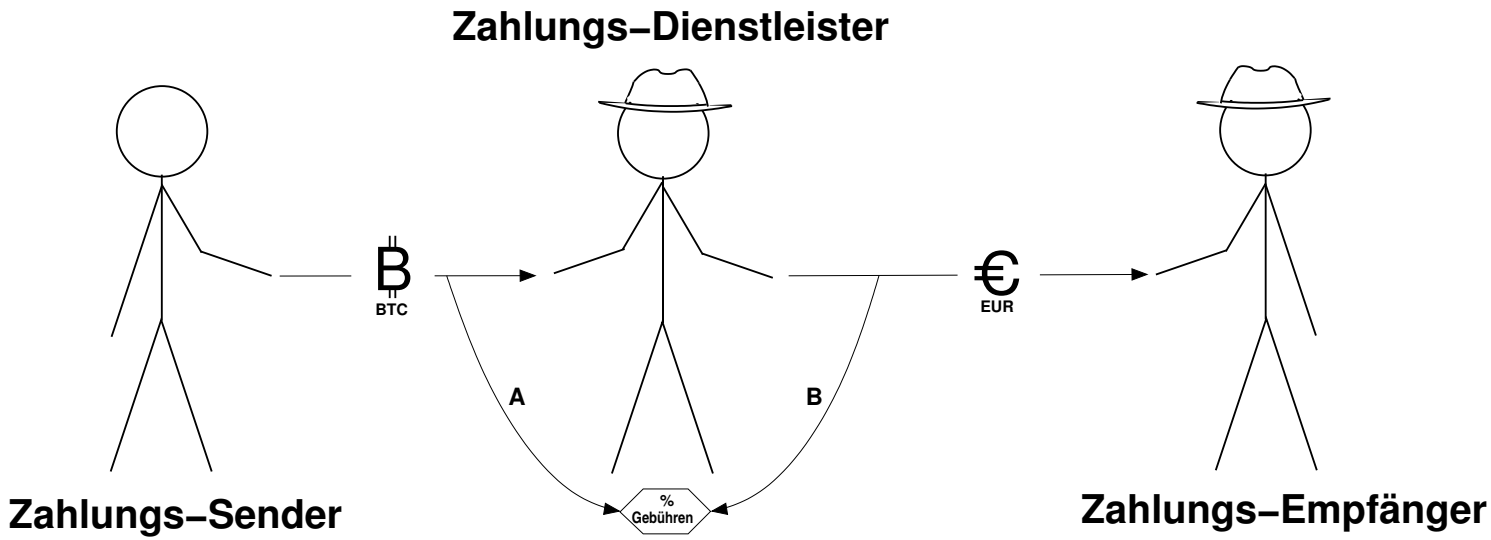
Bitcoin-Akzeptanzstellen

- Oktober 2015: 7223 in ☞ **OpenStreetMap** eingetragene Akzeptanzstellen weltweit
- Grundsätzlich keine „Registrierung“ notwendig (z.B. Bitcoin-Adresse einfach auf Rechnung drucken), aber: landesspezifische Regeln zur Besteuerung und Währungshandel müssen beachtet werden
- **Öffentliche Bitcoin Akzeptanzstellen** (stündlich aktualisiert): ☞ **`http://coinmap.org`**

Bitcoin akzeptieren, € empfangen

- Zahlungsakzeptanz in **Bitcoin parallel zu Fiatgeld**, aber
- **Sofort-Umtausch** eingenommener Bitcoin in € über **Zahlungsdienstleister** (z.B. Bitpay, ChainPay, GoCoin), dadurch
- **Minimierung** des Risiko durch **Kursschwankungen**.
- **Vorteil** der **Zuverlässigkeit und Finalisierung beim Geldtransfer**, **Vereinfachung** des **internationalen** Geldempfangs,
- **Nachteil** der **Abhängigkeit vom Zahlungsdienstleister**, **Gebühren**, umgetauschtes **Fiatgeld** € unterliegt **ebenfalls Wertschwankungen**.

Bitcoin akzeptieren, € empfangen - Schema



Der Dienstleister erhebt für den transparenten Umtausch i.d.R. Gebühren in Höhe von 1...2% vom Zahlungsempfänger.

Bitcoin nativ akzeptieren, pro und contra (1)

- **Pro: Kein Zwischenhandel** (außer geringe Transaktionskosten des Bitcoin-Netzwerks),
- **Pro:** Langfristig zu erwartende **Rendite** durch **inhärente Deflation der Bitcoin-Währung** (Mengenbegrenzung auf 21 Mio. Grundeinheiten), steuerlich günstiges Langzeit-Investitionsobjekt (1 Jahr halten = spekulationssteuerfrei),
- **Contra: Stark schwankende Wechselkurse** zu Fiat-Währungen,
- **Contra: Risiko** bis zum Totalverlust durch fehlgeleitete **Regulierungen** oder **„Zocken“**.

Bitcoin nativ akzeptieren, pro und contra (2)

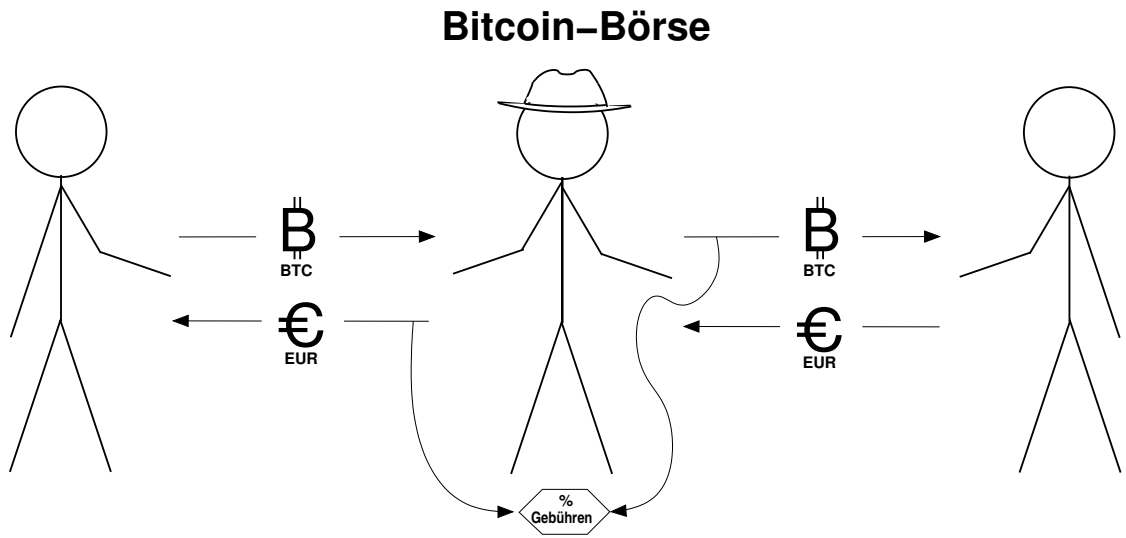
Mischform wird oft empfohlen: nur so viel Bitcoin „halten“, dass Verlust verkraftet werden kann, den Rest umtauschen oder als Direktzahlungsmittel für Zulieferer mit Bitcoin-Akzeptanz verwenden, sofern möglich.

In jedem Fall ist die sorgfältige Sicherung der privaten Schlüssel gegen Diebstahl oder Verlust Pflicht, wie bei Zugangscodes zum Online-Banking oder Kreditkartennummern! (s.a. Presse-Meldungen über „Börsen-Hacks“ in Japan und USA)

Altcoins: durchaus innovative „Nachahmer“

- Litecon, Dogecoin, nationale Cryptowährungen wie Auroracoins, ...
- Funktionsprinzip ähnlich Bitcoin-Transaktionsprotokoll, unterschiedliche Mengenbegrenzung und Initialverteilung, andere Algorithmen zum „Mining“ und Transaktionsbestätigungen,
- derzeit, außer im Insiderhandel, sehr geringe wirtschaftliche Bedeutung, Akzeptanz und Marktkapitalisierung gegenüber der Leitwährung Bitcoin.

Handeln mit Bitcoins - Banken und Börsen



Die Börse behält für jeden Trade i.d.R. Gebühren in Höhe von 1...2% ein.

Beispiel: ☞ Bitcoin.DE (ein Unternehmen der Fidor-Bank)

Probleme der Bitcoin-Implementation

- Die aktuelle Blockgröße limitiert die Anzahl von möglichen Transaktionen pro Zeiteinheit, was zu einem Skalierungsproblem führen kann.
- Änderungen am Bitcoin-Protokoll bedingen einen **Hard Fork** der Blockchain, wobei die Mehrheit der Miner das neue Protokoll verwenden müssen, wodurch der alte Zweig der Blockchain ungültig wird.
- Inhärente Deflation,
- verlorengegangene Bitcoins werden nicht ersetzt.

Andere Blockchain-Währungen lösen diese Probleme bereits, Bitcoin als „Leitwährung“ ist gerade durch die große Verbreitung aber inflexibel.

Neue Entwicklungen - Blockchain statt Bitcoin?

Neben ☞ **„Krypto-Geld“** hat das Prinzip der von jedermann verifizierbaren ☞ **Blockchain** als **öffentliches Transaktions-protokoll** weitere Anwendungsmöglichkeiten, die auch von erklärten Gegnern elektronischer Währungen als **wirtschaftlich zukunftsweisend** bewertet werden.

- Notar-äquivalente **Beglaubigungen**: Einfügen von Dokumenten-Prüfsummen mit Datum per Transaktion in die Blockchain,
- **Programme**, **Algorithmen** und **Meta-Informationen** in der Blockchain: **ethereum**,
- **Belohnungssysteme** mit Nachweis („proof-of-work“): **gridcoin**.

Fragen & Antworten