Bitcoin & Blockchain

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

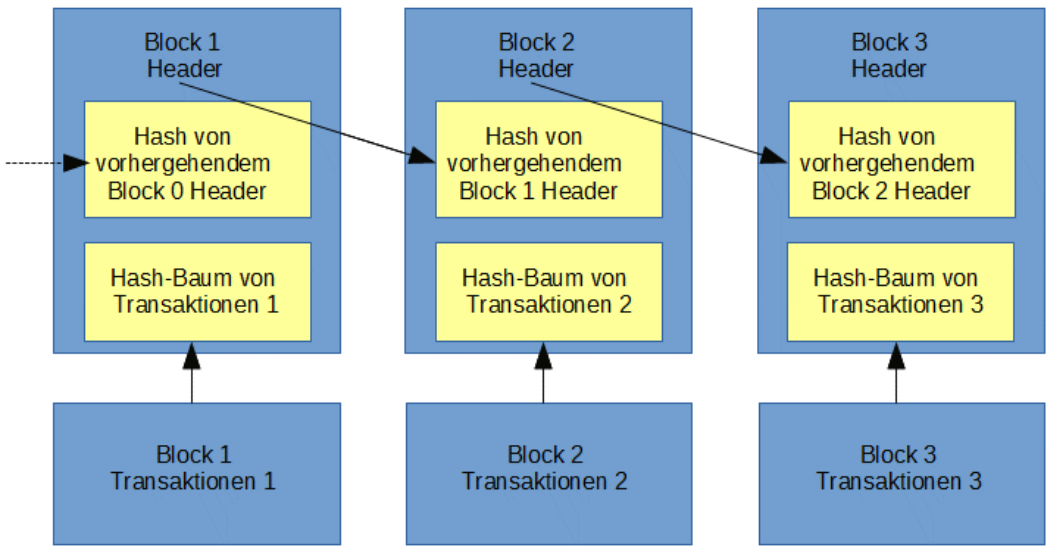
Vortrag für die 17. Knoppixtage 2018
in Anger am 30.8.2018

Inhalt der Vorlesung

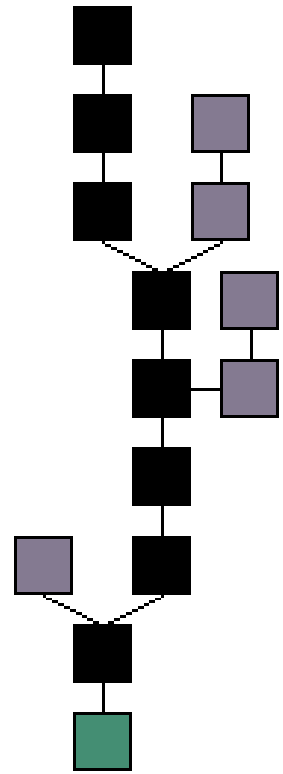
- Das Blockchain-Prinzip,
- Grundsätzlicher Aufbau digitaler „Krypto-Währungen“ am Beispiel Bitcoin: Adressen (public) vs. Keys (private), Transaktionsprotokoll in der Blockchain,*)
- Sicherheitsaspekte: Verfügbarkeit, Integrität, Vertraulichkeit, Authentizität,
- Rolle und Anwendungen von Bitcoin als Wertaufbewahrung, Spekulationsobjekt und im Zahlungsverkehr,
- Aktuelle Gesetzeslage und Verfügbarkeit/Usability,
- andere Krypto-Währungen und Blockchain-Anwendungen.

*) „low-tech“ Version

Blockchain (Skizzen)



Verkettete Blöcke



Längste gültige Sequenz

Blockchain (Paradigma)

Durch das Verfahren der Blockchain, in jedem neuen Block durch eine Prüfsumme den jeweils vorhergehenden **Festzuschreiben**, wird die zentrale Eigenschaft der **Unveränderlichkeit gespeicherter Daten** und die **Fälschungssicherheit** gewährleistet.

Was ist eine Blockchain eigentlich?

- Zentrales (z.B. Finanzmarktwerkzeug) oder verteiltes (z.B. Bitcoin) **Datenbank-Management-System**,
- Ein Block enthält Nutzdaten und signierte Prüfsummen, mit denen die Daten verifiziert werden können,
- Jeder neue Block enthält die signierte Prüfsumme des vorhergehenden Blocks. Dadurch ist es unmöglich, einen früheren Block zu manipulieren, ohne dass die ganze darauf folgende Kette „ungültig" wird, (s. zentrale Eigenschaft der Unveränderlichkeit),
- Jeder Besitzer einer Blockchain-Kopie kann die enthaltenen Blöcke vom ersten bis zum letzten anhand im Protokoll festgelegter Regeln verifizieren,
- Existieren zwei konkurrierende Versionen einer Blockchain, so gilt die - unter Beachtung der Regeln - längste Version (und damit die am schwersten zu fälschende) als die gültige,
- Ein **neuer Block** wird nach bestimmten Regeln durch ein **Konsensverfahren** erzeugt ☞ Proof-of-Work, ☞ Proof-of-Stake, ☞ Proof-of-Burn, ☞ Proof-of-Activity.

Blockchain-Header

Die sog. **Meta-Daten** eines Blocks:

1. kryptographisch sicherer **Hash des vorhergehenden Blocks**,
2. **Zeitstempel**,
3. Transaktions- oder Nutz**daten mit eigenen Hashes** (s.a. ☞ Merkle Tree)

stellen die eigentliche Stärke des Blockchain-Systems dar (s. nächste Folien). Hier spielen vor allem kryptographische Hash- und Signaturfunktionen eine Rolle, mit denen die **Unveränderlichkeit und Authentizität** garantiert wird. ☞ Beispiel „digital signiertes Dokument“. (Demo)

Blockchain-Daten

Die in der Blockchain **gespeicherten Nutzdaten** können, wie bei relationalen- und anderen Datenbanken, grundsätzlich beliebiger Natur sein, z.B. könnte die Wikipedia-Datenbank in Form einer Blockchain gespeichert werden, was auch ein **lückenloses Nachvollziehen jeder Änderung** erlaubt.

Allerdings ist es aus praktischen Überlegungen *nicht* sinnvoll, die Blockchain für *beliebige* Daten als „Universal-Datenbank-System“ zu nutzen...

Eigenschaften einer Blockchain

Vorteile:

- **Transparenz**: Nachvollziehbarkeit von Transaktionen/Verträgen,
- **Festschreiben** von Buchungen (alte Werte **nicht nachträglich änderbar**),
- **Fälschungssicherheit**, kaum manipulierbar bzw. Aufwand immens hoch (51%-Attacke),
- bei verteilter/redundanter Variante: hohe **Verfügbarkeit**, sicher vor Datenverlust,
- bei verteilter/redundanter Variante: **Kein Vertrauen in zentrale Instanz** (Webseite/Anbieter) **erforderlich**, nur Vertrauen zu **beweisbarer Sicherheit mathematischer Algorithmen**.

Eigenschaften einer Blockchain

Nachteile:

- **Ständiges Wachstum**: Alle Blöcke bis zum allerersten müssen dauerhaft gespeichert werden, um Nachvollziehbarkeit zu sichern, daher sind langfristg nur „kleine“ Datenmengen in jedem Block sinnvoll (Prüfsummen und Signaturen anstelle kompletter Dokumente),
- Proof-of-Work **„Belohnungs“-Konzept** für das Signieren von Daten und Generieren neuer Blöcke ist **sehr aufwändig** („Stromverbrauch einer Kleinstadt“ bei Bitcoin), s.a. ☞ Mining (S. 17),
- Algorithmische Umsetzung muss flexibel genug, aber fehlerfrei sein, da eine ggf. erforderliche **Änderung am Protokoll** im Regelfall eine **neue, inkompatible Version der Blockchain erzeugt** ☞ Fork
- Durch Konzentration von Rechenleistung in wenigen Pools (bei Proof-of-Work) kann eine **gefährliche 51%-Situation** entstehen.

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**.

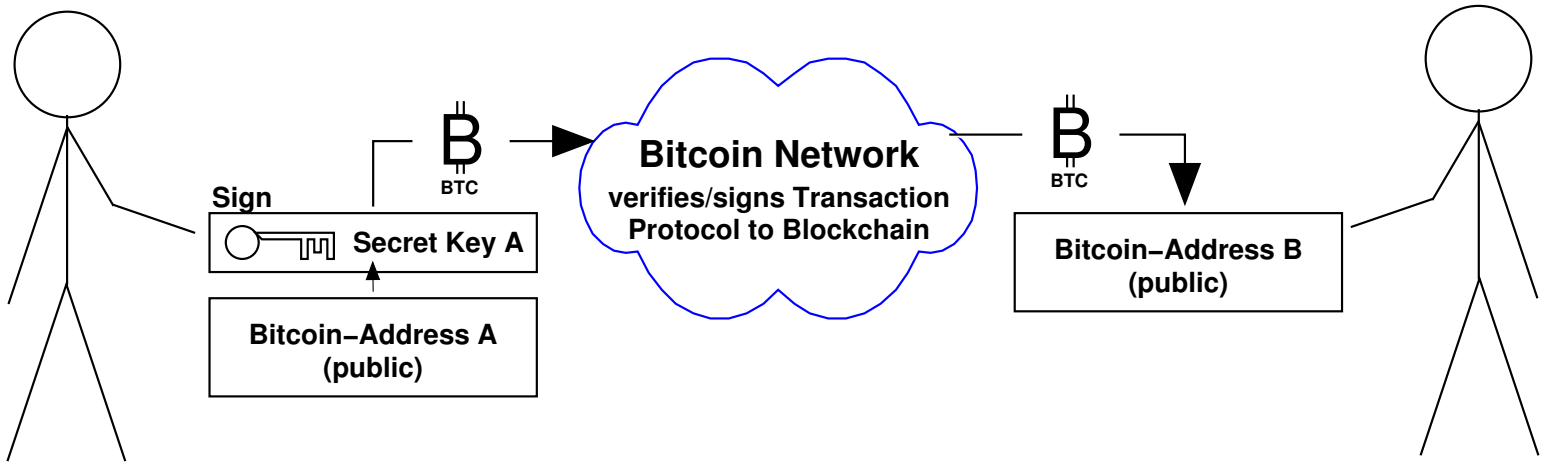
---

*) 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.
- Beispiel Generator (Javascript): **`https://www.bitaddress.org/`**

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 **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 auch hier in **Blöcke** aufgeteilt, die die Transaktionen und weitere Protokolldaten enthalten, und die (bei Bitcoin) alle 10 Minuten erzeugt und dann vollständig oder teilweise von allen Netzwerk-Teilnehmern gespeichert werden,
- bei **„core“**-Clients für das Bitcoin-Netzwerk werden **alle bestätigten Transaktionsblöcke** gespeichert (derzeit 150GB), bei „light“-Clients hingegen nur die den Teilnehmer betreffenden (z.B. Smartphone-Clients) sowie Links zu speziellen Servern,
- 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 (Proof-of-Work)** für dem Netzwerk zur Verfügung gestellte Rechenleistung gelöst, wobei alle 10 Minuten ein neuer Block generiert wird, für den es - derzeit 12,5 - Bitcoins als Belohnung für die Lösung einer sehr rechenintensiven kryptographischen Aufgabe - nämlich das Generieren passender Daten zu einem teil vorgegebenen Block-Hash, gibt (☞ Demo: Vanity-Adressen-Berechnung).

Je mehr Rechenleistung im Netz verfügbar ist, desto rechenintensiver wird die kryptographische Aufgabe und 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 Miner vom Sender eine **Transaktionsgebühr variabler Größe** angeboten werden kann, um diese Transaktion möglichst priorisiert/schneller bestätigt zu bekommen.

Rechtliche Aspekte von Bitcoin (1)

- 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),

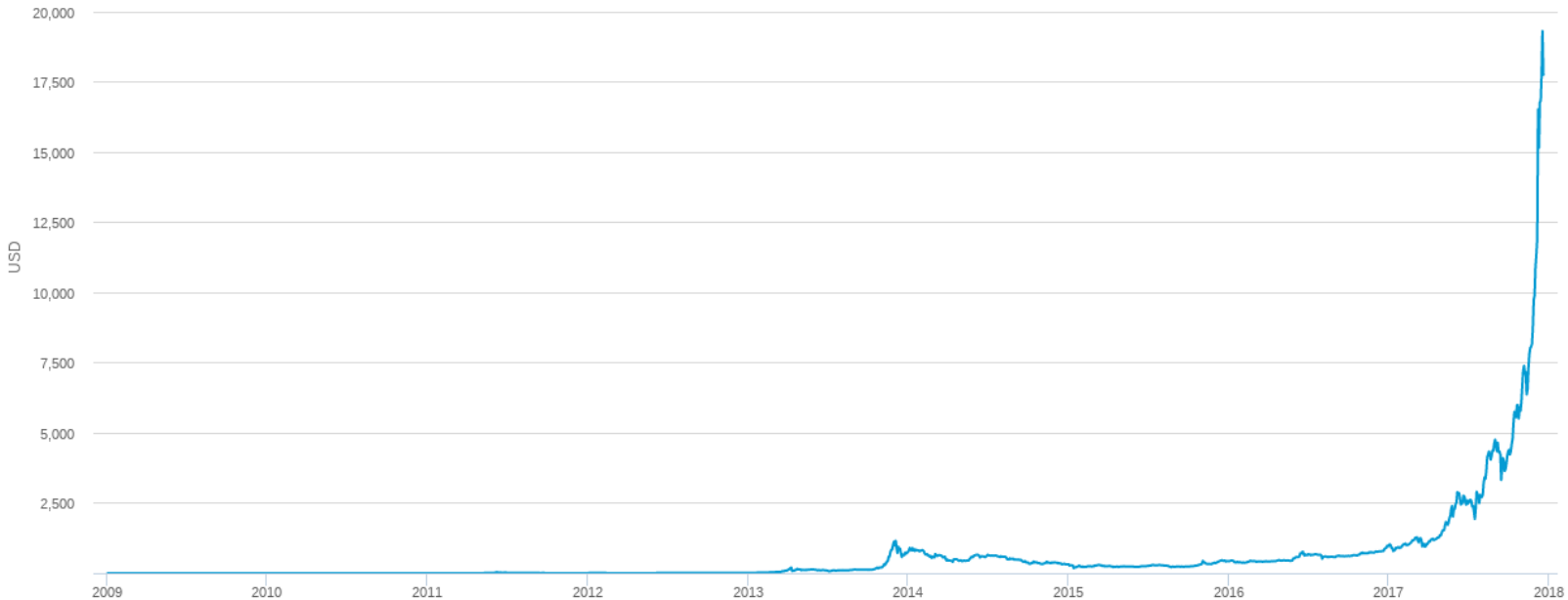
- in Deutschland gilt Bitcoin derzeit als **„Rechnungseinheit“** und der Handel nur bei **langfristigen Anlagen** als **steuerfreies „(privates) Veräußerungsgeschäft“**, während ☞ kurzfristige Spekulationsgewinne oder -Verluste (< 1 Jahr Haltezeit) aus Währungsvolatilität/Börsenhandel **zum aktuellen Kurs in € der Abgeltungssteuer (25%) unterliegen**. Eine von manchen Finanzämtern postulierte Umsatzsteuer auf Bitcoin-Transaktionen wurde vom EUGh jedoch abgeschafft,

Rechtliche Aspekte von Bitcoin (2)

- 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 unmittelbar zuzuordnen).

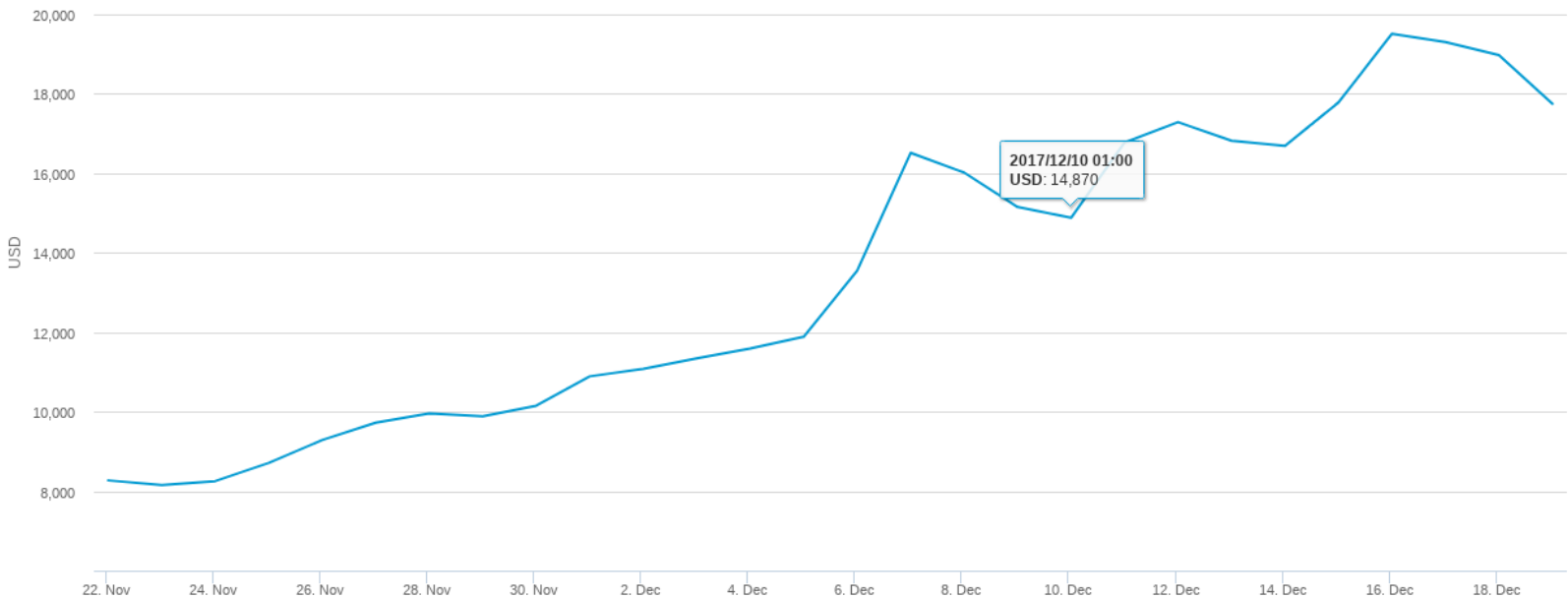
☞ Anonymisieren von Bitcoin-Transaktionen per „Mixer“

Statistik: Bitcoin/USD-Tauschwert (1)



Statistik: Bitcoin/USD-Tauschwert (2)

Statistik: Bitcoin/USD-Tauschwert (3)



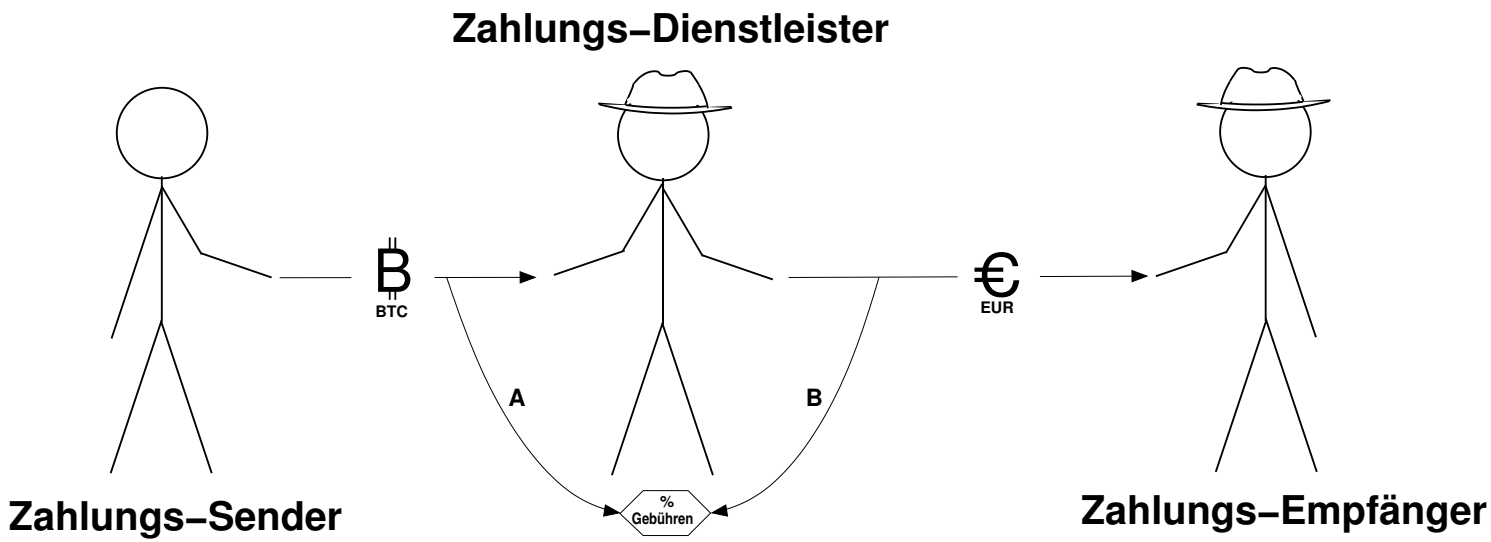
Bitcoin-Akzeptanzstellen

- Dezember 2017: 11279 in ☞ **OpenStreetMap** eingetragene Akzeptanzstellen weltweit ☞ **`http://coinmap.org`**
- Grundsätzlich keine „Registrierung“ notwendig (z.B. Bitcoin-Adresse ☞ generieren und einfach auf die Rechnung drucken), aber: landesspezifische Regeln zur Besteuerung und Währungshandel müssen beachtet werden

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)

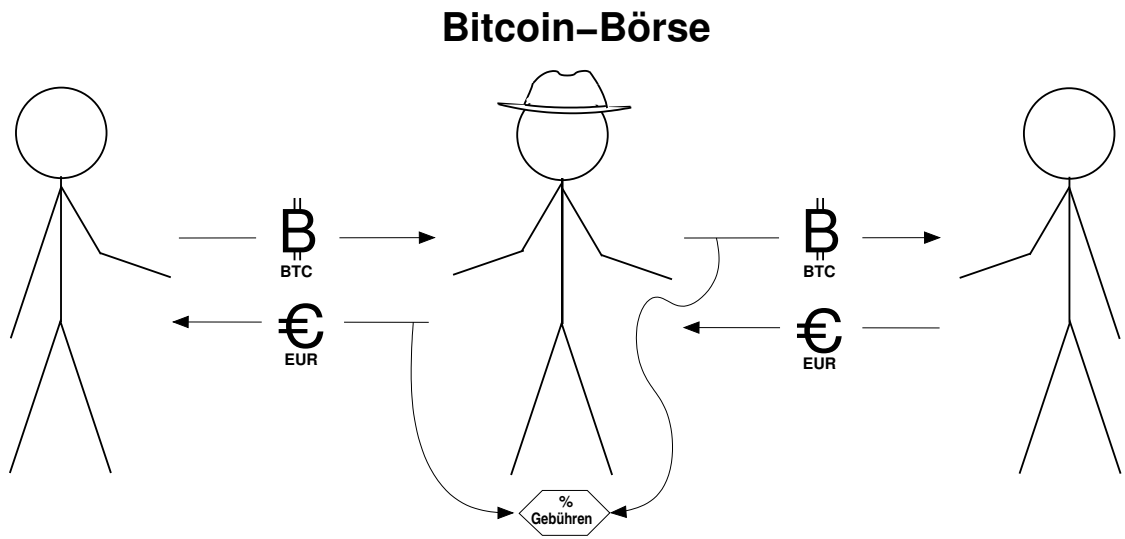
- **Pro: Kein Zwischenhandel** (außer geringe Transaktionskosten des Bitcoin-Netzwerks),
- **Pro:** Langfristig zu erwartende **Rendite** durch **inhärente Deflation der Bitcoin-Währung** (Mengenbegrenzung auf 21 Mio. Grundeinheiten), steuerlich günstiges Langzeit-Investitionsobjekt (1 Jahr halten = 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)

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 ☞ Bitcoin Group SE in Kooperation mit der Fidor-Bank)

Wertaufbewahrung und Spekulation

Konträr zur ursprünglichen Absicht eines Bargeld-ähnlichen Zahlungsmittels, wird Bitcoin auch als „digitales Gold“ gehandelt.

- Der **Tauschwert** von Bitcoin wird im wesentlichen durch Angebot und Nachfrage bestimmt, und hat, abgesehen vom Resourcenverbrauch beim Mining, keinen „realen Gegenwert“. Letzteres trifft allerdings durchaus auch auf Fiat-Bargeld („Papiergeld“, „Münzen“) zu.
- Durch den deflationären Charakter wäre bei steigender oder auch gleichbleibender Nachfrage langfristig eine Wertsteigerung vorprogrammiert.
- Keine Beeinflussung durch Zinspolitik, keine willkürliche Änderung der Geldmenge: Vertrauensvorschuss.
- Vertrauen in Marktmechanismen und Regulierungen?

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.

Probleme der Bitcoin-Implementation (1)

- Die **geringe Blockgröße** limitiert die Anzahl von Transaktionen pro Sekunde, was zu einem ☞ Skalierungsproblem führt ☞ Viele unbestätigte Transaktionen im Mempool, Transaktionsgebühren sehr hoch. Bitcoin wird als *Zahlungsmittel* für „kleine" Käufe gerade bei hohem Interesse immer weniger brauchbar.
- Änderungen am Bitcoin-Protokoll bedingen eine **Hard Fork** der Blockchain, oder es muss spontan die Mehrheit der Miner und Anwender das neue Protokoll verwenden.
- Inhärente Deflation durch die Mengenbegrenzung: Zu wertvoll zum Ausgeben.
- ☞ Verlorengegangene Bitcoins (private Schlüssel zerstört oder nicht mehr zugänglich) werden nicht ersetzt.

Probleme der Bitcoin-Implementation (2)

Andere Blockchain-Währungen lösen einige dieser Probleme bereits durch entsprechende Protokollmechanismen.

Bitcoin als „Leitwährung“ ist gerade durch die große Verbreitung aber unflexibel; eine technische Änderung des Protokolls zieht eine Fork nach sich, wodurch eine neue Währung entsteht. Dies wurde bereits mit ☞ bislang mäßigem Erfolg („Bitcoin Cash“) versucht.

Neue Entwicklungen - Blockchain ohne Bitcoin?

Neben ☞ **„Krypto-Geld“** hat das Prinzip der von jedermann verifizierbaren ☞ **Blockchain** als **öffentliches Transaktionsprotokoll** 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** für Teilnahme an wissenschaftlichen Projekte mit Nachweis („proof-of-work“): **gridcoin**.

Fragen & Antworten