Bitcoin und virtuelles Geld

Gliederung

- 1. Allgemeines
  - 1.1.Entstehung
  - 1.2. Verbreitung und Kurs
  - 1.3.Eigenschaften
  - 1.4.Anonymität vs Pseudonymität
  - 1.5.Erwerb von Bitcoin
- 2. Welche Idee steht dahinter?
  - 2.1. Kritik am Kapitalismus

Gliederung

- 2.2.Was soll dieses Geld umsetzen?
  - 2.2.1.Realisierung des Eigentumswechsels
  - Exkurs: Die Sache mit dem Tausch
  - 2.2.2.Verhindern von Mehrfachausgaben
- 2.3.Der Wert der Bitcoins
- 2.4.Begrenzte Geldmenge
- Exkurs: Wachstum und Kredit
- Exkurs: Sicherheit und Zentralbanken

- 3.Kontroversen und Diskussion
  - 3.1.Kontroversen
  - 3.2.Diskussion

1. Allgemeines

1.1.Entstehung

- Konzept 2008 von Satoshi Nakamoto
- Idee einer digitalen, dezentral organisierten Währung
- Bitcoin-Netzwerk entstand 3. Januar 2009 mit Berechnung des ersten Blocks, der 50 ersten Bitcoins erzeugt hat
- Einige Tage später Veröffentlichung von Bitcoin-Client
- Später stieß Open Source Community dazu

1.2. Verbreitung und Kurs

- März 2014 3.303 Orte die Bitcoin annehmen (Geschäfte, Hotels, Pizzalieferdienste etc.)
- Internetseiten: Mega, Wordpress, Reddit...
- Spenden: z.b. Wikileaks
- Heftige Kursschwankungen: teilweise bis zu 20% am Tag
- Bspw. November 2013 von 200$/BTC auf 1200$/BTC
- Heutzutage unter anderem diverse andere Cryptowährungen wie Litecoin, Peercoin, aber auch scheinbar als Witz gedachte wie: Dogecoin, Coinye(gibt es nicht mehr)

Coinye und Dogecoin

1.3.Eigenschaften

- Fälschungssicherheit:
  - Durch asymmetrische kryptographische Verfahren digitale Signaturen (geprüft)
  - Doppeltes Ausgeben mittels Proof-of-Work verhindert
- Kosten und Geschwindigkeit:
  - Da Peer-to-Peer kaum Gebühren, nur Bestätigung einer Transaktion
  - Bestätigung dauert ca 10 Min., jede weiter erhöht Wahrscheinlichkeit der Dauerhaftigkeit
  - Nach 6 Bestätigungen gilt Zahlung als verbindlich

1.3.Eigenschaften

- Dezentralität:
  - Verwirklicht durch P2P
  - Einflussnahme nur möglich falls Mehrheit der Mining Rechenleistung mit veränderter Software erfolgt
- Irreversibilität von Transaktion:
  - Aufgrund der Dezentralität

1.4.Anonymität vs Pseudonymität

- Weder IP-Adressen noch Bitcoin-Adressen können Personen zugeordnet werden → höherer Schutz als konv. Zahlungen
- Anonymität begrenzt, da Transaktionen zwischen 2 Adressen öffentlich
- Ermöglicht weitreichendere Verfolgung als Bargeld
- Tauschbörsen sind Bestimmungen zur Bekämpfung von Geldwäsche unterworfen
- Anonymität von Bitcoin-Transaktionen über Tor-Netzwerk möglich

1.5.Erwerb von Bitcoin

- Über Tauschbörsen
- Verschiedene Internetdienste offerieren kleine Beträge, wenn Einkäufe gemacht, Umfragen ausgefüllt werden, oder Ähnliches
- Mining

2. Welche Idee steht dahinter?

2.1. Kritik am Kapitalismus

- Ideal des freien Marktes als gegenseitiger Nutzen, Kooperation und Harmonie
- Seine negativen Eigenschaften werden dem staatlichen Eingreifen und/oder der Monopolstellung der Banken zugeschrieben
- Beispielweise wird im staatlichen Gelddrucken ein Verstoß gegen Prinzip des freien Marktes gesehen, da dies aus seiner Monopolstellung rührt und nicht aus freiem Wettbewerb

2.2.Was soll dieses Geld umsetzen?

- Eigenschaften von Bargeld:
  - Anonymität
  - Unmittelbarkeit
  - Geringe bzw. keine Transaktionsgebühren
- Alles ohne „vertrauenswürdige Dritte“ wie Staat und Zentralbanken

2.2.1.Realisierung des Eigentumswechsels

- Mit physischem Geld ist dieser ersichtlich
  - Gebe ich jemandem Geld habe ich dies nicht mehr
  - Ich kann also auch nicht behaupten ich hätte dieses nicht übergeben
- Bei Bitcoin:
  - Tauschen von Zeichenketten
  - Problem: Diese können kopiert werden
  - Lösung: Unterschreiben eines digitalen Vertrages, welcher Zeichenkette erst gültig macht

Exkurs: Die Sache mit dem Tausch

- Waren werden nicht für Bedürfnisbefriedigung produziert sondern für einen Gewinn
- Die Bedürfnisse kommen hier nur als Hebel gegen den jeweils anderen ins Spiel
- Im Tausch stehen sich gegensätzliche Interessen gegenüber: Verkäufer will möglichst hohen Preis, Käufer möglichst geringen Preis
- Geld vermittelt diesen Gegensatz, löst diesen Konflikt aber nicht
- Diese dauernd auftretende Situation benötigt das staatliche Gewaltmonopol

  → So sehr manche Marktradikalen den Staat und seine Einmischung verabscheuen, ihre Wirtschaft benötigt ihn

2.2.2.Verhindern von Mehrfachausgaben

- Theoretisch besteht Möglichkeit digitale Verträge mehrfach zu unterschreiben
- Lösung: Alle Verträge sind öffentlich
- Anschließend unterschreibt Software eines anderen diesen Vertrag (er fungiert quasi als Notar)
- Diese „Zeugen“ werden zufällig ausgewählt um Missbrauch zu verhindern
- Die potentiellen Zeugen konkurrieren mit anderen um dieses Recht, indem sie Rechenzeit zur Verfügung stellen und mathematische Rätsel lösen

Mining von Bitcoins

2.3.Der Wert der Bitcoins

- Wie kommt neues Kryptogeld in die Welt?
- Wieso sollten Menschen Rechenzeit aufwenden um Verträge zu beglaubigen?
- Das erste Problem wird mit dem zweiten gelöst:
  - Überprüfer von Transaktion erhalten Bitcoins dafür, wenn sie gezogen werden + Transaktionsgebühren
  - So kommen auch neue Coins in die Welt. Sie werden „abgebaut“ (Mining)

2.4.Begrenzte Geldmenge

- Die Gesamtmenge an BTC ist auf 21 Millionen begrenzt
- Deshalb wird die Anzahl an BTC die man als Zeuge verdient auch immer geringer, bis sie irgendwann 0 beträgt (Wenn alle BTC abgebaut sind)
- Grund für diese Grenze ist die Annahme, dass begrenzte Geldmenge zu einer besseren Wirtschaft führen würde
- Diese Idee wird den gängigen Währungen entgegengesetzt, die Kreditgeld sind (neues Geld kann einfach von Zentralbank gedruckt werden)

Exkurs: Wachstum und Kredit

- Unternehmen investieren Geld um mehr Geld zu verdienen
- Sie kaufen, produzieren, verkaufen
- Je schneller das geht, desto schneller ist der Profit gemacht, desto schneller können neue Investitionen getätigt werden
- Da hier Geld nur ein Mittel zum Zweck ist, soll ein Mangel daran, kein Grund gegen seine Vermehrung sein
- Durch Kredite kann man ersteinmal losproduzieren (lassen), mit der Erwartung, dass man später mehr hat

Exkurs: Wachstum und Kredit

- Wenn es um Wachstum geht ist es schlauer Geld für Zinsen zu verleihen, statt es einfach herumliegen zu lassen
- Diese einfache Form des Kredites entwickelt sich spontan unter den Bedingungen des freien Marktes
- So gab es bspw. auch schon 2011 mehrere Bestrebungen Bitcoin-Kreditgenossenschaften zu gründen
- Wert von geliehenem Geld ist für Kreditgeber, von ökonomischem Erfolg des Schuldners abhängig

Exkurs: Sicherheit und Zentralbanken

- Um sich vor Ausfall zu schützen, verlangen Kreditgeber Sicherheiten
- Heißt Kredit aber durchschnittlich ein erfolgreiches Geschäft, kann ein Schuldschein wie Vermögen fungieren
- So können sich regelrechte Kreditketten bilden
- Das Problem: In einer Kreditkrise oder Rezession zerstört ein bankrotter Schuldner das „Geld“ derer, die nach ihm in der Kette kommen
- Hier kommt die Zentralbank ins Spiel: Mit einem Geld, dessen Wert durch das Wachstum garantiert ist, dass es anschiebt

3.Kontroversen und Diskussion

3.1.Kontroversen

- Finanzielle Risiken aufgrund von Kursschwankung
- Vorwurf der Nutzung für illegale Geschäfte
- Legitimität einer nicht-zentralen Geldschöpfung
- Rechtliche Fragen
- Inflationäre Risiken durch allgemeine Akzeptanz
- Reputationsrisiken der Zentralbank

3.2.Diskussion

- Können Bitcoins unser Geld ersetzen?
- Was für Auswirkungen hätte das?
- Was ist dran an der Kapitalismuskritik der Bitcoin-Gemeinde?