bitcoin

Ein kritischer Blick

Claus Diem

23. Oktober 2017

bitcoin

Idee:

bitcoin

Idee:

Alice will Bob 100 Münzen schicken / übereignen.

bitcoin

Idee:

Alice will Bob 100 Münzen schicken / übereignen.

Sie schreibt: “Alice schickt / gibt Bob 100 Münzen. Alice”

bitcoin

Idee:

Alice will Bob 100 Münzen schicken / übereignen.

Sie schreibt: “Alice schickt / gibt Bob 100 Münzen. Alice”

Es wird dezentral

- überprüft, ob Alice 100 Münzen hat,
- festgehalten, dass die Transaktion stattgefunden hat.

bitcoin

Idee:

Alice will Bob 100 Münzen schicken / übereignen.

Sie schreibt: “Alice schickt / gibt Bob 100 Münzen. Alice”

Es wird dezentral

- überprüft, ob Alice 100 Münzen hat,
- festgehalten, dass die Transaktion stattgefunden hat.

Hierbei sind “Alice” und “Bob” keine Personen, sondern Adressen.

bitcoin

Durchführung der Transaktionen:

Offene Transaktionen werden alle etwa 10 Minuten von einem Benutzer zu einem Block zusammengefasst.

Dieser Block wird an die bestehende Kette von Blöcken angehängt.

bitcoin

Hierzu macht ein Benutzer dies:

bitcoin

Hierzu macht ein Benutzer dies:

- Er sammelt Transaktionen ein

bitcoin

Hierzu macht ein Benutzer dies:

- Er sammelt Transaktionen ein
- Überprüft, ob diese gültig sind

bitcoin

Hierzu macht ein Benutzer dies:

- Er sammelt Transaktionen ein
- Überprüft, ob diese gültig sind
- Er bildet einen Hash-Baum (Merkle-Baum)

bitcoin

Hierzu macht ein Benutzer dies:

- Er sammelt Transaktionen ein
- Überprüft, ob diese gültig sind
- Er bildet einen Hash-Baum (Merkle-Baum)
- Er wählt eine Zufallszahl (Nonce)

bitcoin

Hierzu macht ein Benutzer dies:

- Er sammelt Transaktionen ein
- Überprüft, ob diese gültig sind
- Er bildet einen Hash-Baum (Merkle-Baum)
- Er wählt eine Zufallszahl (Nonce)
- Er berechnet einen Hash-Wert des Baums (= Blocks) und des vorherigen Blocks

bitcoin

Hierzu macht ein Benutzer dies:

- Er sammelt Transaktionen ein
- Überprüft, ob diese gültig sind
- Er bildet einen Hash-Baum (Merkle-Baum)
- Er wählt eine Zufallszahl (Nonce)
- Er berechnet einen Hash-Wert des Baums (= Blocks) und des vorherigen Blocks
- Wenn dieser "schön" ist, gibt er das Ergebnis bekannt.

bitcoin

Hierzu macht ein Benutzer dies:

- Er sammelt Transaktionen ein
- Überprüft, ob diese gültig sind
- Er bildet einen Hash-Baum (Merkle-Baum)
- Er wählt eine Zufallszahl (Nonce)
- Er berechnet einen Hash-Wert des Baums (= Blocks) und des vorherigen Blocks
- Wenn dieser "schön" ist, gibt er das Ergebnis bekannt.

Für diese Arbeit erhält er bitcoins.

bitcoin

Hierzu macht ein Benutzer dies:

- Er sammelt Transaktionen ein
- Überprüft, ob diese gültig sind
- Er bildet einen Hash-Baum (Merkle-Baum)
- Er wählt eine Zufallszahl (Nonce)
- Er berechnet einen Hash-Wert des Baums (= Blocks) und des vorherigen Blocks
- Wenn dieser "schön" ist, gibt er das Ergebnis bekannt.

Für diese Arbeit erhält er bitcoins.

Also: Neuen Block erzeugen = Minen

Problematische Aspekte

Problematische Aspekte

- Kosten pro Transaktion

Problematische Aspekte

- Kosten pro Transaktion
- Wartezeit, Unsicherheit bei Transaktionen

Problematische Aspekte

- Kosten pro Transaktion
- Wartezeit, Unsicherheit bei Transaktionen
- Hoher Speicherbedarf durch Blockkette

Problematische Aspekte

- Kosten pro Transaktion
- Wartezeit, Unsicherheit bei Transaktionen
- Hoher Speicherbedarf durch Blockkette
- (Möglicherweise) notwendiges Speichern der Blockkette durch Benutzer

Problematische Aspekte

- Kosten pro Transaktion
- Wartezeit, Unsicherheit bei Transaktionen
- Hoher Speicherbedarf durch Blockkette
- (Möglicherweise) notwendiges Speichern der Blockkette durch Benutzer
- Fragwürdige Skalierbarkeit

Problematische Aspekte

- Kosten pro Transaktion
- Wartezeit, Unsicherheit bei Transaktionen
- Hoher Speicherbedarf durch Blockkette
- (Möglicherweise) notwendiges Speichern der Blockkette durch Benutzer
- Fragwürdige Skalierbarkeit
- Tendenz zu Zentralisierung durch Mining-Pools, dadurch Gefahr einer “feindlichen Übernahme”

Problematische Aspekte

- Kosten pro Transaktion
- Wartezeit, Unsicherheit bei Transaktionen
- Hoher Speicherbedarf durch Blockkette
- (Möglicherweise) notwendiges Speichern der Blockkette durch Benutzer
- Fragwürdige Skalierbarkeit
- Tendenz zu Zentralisierung durch Mining-Pools, dadurch Gefahr einer “feindlichen Übernahme”
- Ein Benutzer (mit einer Adresse) ist nur pseudoanonym

Problematische Aspekte

- Kosten pro Transaktion
- Wartezeit, Unsicherheit bei Transaktionen
- Hoher Speicherbedarf durch Blockkette
- (Möglicherweise) notwendiges Speichern der Blockkette durch Benutzer
- Fragwürdige Skalierbarkeit
- Tendenz zu Zentralisierung durch Mining-Pools, dadurch Gefahr einer "feindlichen Übernahme"
- Ein Benutzer (mit einer Adresse) ist nur pseudoanonym
- Bösewichte sind sehr schwer überwachbar

Problematische Aspekte

- Kosten pro Transaktion
- Wartezeit, Unsicherheit bei Transaktionen
- Hoher Speicherbedarf durch Blockkette
- (Möglicherweise) notwendiges Speichern der Blockkette durch Benutzer
- Fragwürdige Skalierbarkeit
- Tendenz zu Zentralisierung durch Mining-Pools, dadurch Gefahr einer "feindlichen Übernahme"
- Ein Benutzer (mit einer Adresse) ist nur pseudoanonym
- Bösewichte sind sehr schwer überwachbar
- Unklare Entscheidungsfindung

Was man gerne hätte

Was man gerne hätte

- Schutz gegenüber Dieben u.a.

Was man gerne hätte

- Schutz gegenüber Dieben u.a.
- instantaner und kosteneffizienter Transfer

Was man gerne hätte

- Schutz gegenüber Dieben u.a.
- instantaner und kosteneffizienter Transfer
- Langfristige Speichereffizienz

Was man gerne hätte

- Schutz gegenüber Dieben u.a.
- instantaner und kosteneffizienter Transfer
- Langfristige Speichereffizienz
- Sehr viel höheres Transaktionsvolumen

Was man gerne hätte

- Schutz gegenüber Dieben u.a.
- instantaner und kosteneffizienter Transfer
- Langfristige Speichereffizienz
- Sehr viel höheres Transaktionsvolumen
- “Leichtgewicht”-Lösungen für Benutzer

Was man gerne hätte

- Schutz gegenüber Dieben u.a.
- instantaner und kosteneffizienter Transfer
- Langfristige Speichereffizienz
- Sehr viel höheres Transaktionsvolumen
- “Leichtgewicht”-Lösungen für Benutzer
- Weltweit benutzbares System

Was man gerne hätte

- Schutz gegenüber Dieben u.a.
- instantaner und kosteneffizienter Transfer
- Langfristige Speichereffizienz
- Sehr viel höheres Transaktionsvolumen
- “Leichtgewicht”-Lösungen für Benutzer
- Weltweit benutzbares System
- Klare Entscheidungsfindung

Was man vielleicht gerne hätte

Was man vielleicht gerne hätte

- Klare, automatisch verfolgte Regeln der “Geldpolitik” ?

Was man vielleicht gerne hätte

- Klare, automatisch verfolgte Regeln der “Geldpolitik” ?
- Sicherheit gegenüber staatlichen Zugriff ?

Was man vielleicht gerne hätte

- Klare, automatisch verfolgte Regeln der “Geldpolitik” ?
- Sicherheit gegenüber staatlichen Zugriff ?
- Besteuerbarkeit ?

Was man vielleicht gerne hätte

- Klare, automatisch verfolgte Regeln der “Geldpolitik” ?
- Sicherheit gegenüber staatlichen Zugriff ?
- Besteuerbarkeit ?
- Automatische Besteuerung ?

Was man vielleicht gerne hätte

- Klare, automatisch verfolgte Regeln der “Geldpolitik” ?
- Sicherheit gegenüber staatlichen Zugriff ?
- Besteuerbarkeit ?
- Automatische Besteuerung ?
- Volle Anonymität per default ?

Was man vielleicht gerne hätte

- Klare, automatisch verfolgte Regeln der “Geldpolitik” ?
- Sicherheit gegenüber staatlichen Zugriff ?
- Besteuerbarkeit ?
- Automatische Besteuerung ?
- Volle Anonymität per default ?
- Anonymität nur für den Käufer ?

Was man vielleicht gerne hätte

- Klare, automatisch verfolgte Regeln der “Geldpolitik” ?
- Sicherheit gegenüber staatlichen Zugriff ?
- Besteuerbarkeit ?
- Automatische Besteuerung ?
- Volle Anonymität per default ?
- Anonymität nur für den Käufer ?
- Zugriff nach Richterbeschluss ?

Was man vielleicht gerne hätte

- Klare, automatisch verfolgte Regeln der “Geldpolitik” ?
- Sicherheit gegenüber staatlichen Zugriff ?
- Besteuerbarkeit ?
- Automatische Besteuerung ?
- Volle Anonymität per default ?
- Anonymität nur für den Käufer ?
- Zugriff nach Richterbeschluss ?
- Dezentralität ??

Einige Zahlen

bitcoin

Einige Zahlen

bitcoin

- Blockkette: 260 mio Transaktionen, 160 GB

Einige Zahlen

bitcoin

- Blockkette: 260 mio Transaktionen, 160 GB
- limitiert auf 7 Transaktionen pro Sekunde

Einige Zahlen

bitcoin

- Blockkette: 260 mio Transaktionen, 160 GB
- limitiert auf 7 Transaktionen pro Sekunde
- Ausgebene bitcoins für das Minen:
  z.Z. ca. 660.000 pro Jahr (4% der Geldmenge) $\hat{=}$ 3,1 mrd. €

Einige Zahlen

bitcoin

- Blockkette: 260 mio Transaktionen, 160 GB
- limitiert auf 7 Transaktionen pro Sekunde
- Ausgebene bitcoins für das Minen:
  z.Z. ca. 660.000 pro Jahr (4% der Geldmenge) $\hat{=}$ 3,1 mrd. €
- pro Transaktion: ca. 35 Euro, etwa 1 % des durchschnittlichen Transaktionswertes

Einige Zahlen

bitcoin

- Blockkette: 260 mio Transaktionen, 160 GB
- limitiert auf 7 Transaktionen pro Sekunde
- Ausgebene bitcoins für das Minen:
  z.Z. ca. 660.000 pro Jahr (4% der Geldmenge) $\hat{=}$ 3,1 mrd. €
- pro Transaktion: ca. 35 Euro, etwa 1 % des durchschnittlichen Transaktionswertes

  (Das sind keine Transaktionskosten, da der Großteil der Kosten nicht für die Transaktion von Käufer und Verkäufer getragen wird. Es sind aber nichtsdestoweniger Kosten, die alle Benutzer von bitcoin zusammen tragen. Es beinhaltet aber auch direkte Übertragungsgebühren.)

Einige Zahlen

bitcoin

- Blockkette: 260 mio Transaktionen, 160 GB
- limitiert auf 7 Transaktionen pro Sekunde
- Ausgebene bitcoins für das Minen:
  z.Z. ca. 660.000 pro Jahr (4% der Geldmenge) $\hat{=}$ 3,1 mrd. €
- pro Transaktion: ca. 35 Euro, etwa 1 % des durchschnittlichen Transaktionswertes

  (Das sind keine Transaktionskosten, da der Großteil der Kosten nicht für die Transaktion von Käufer und Verkäufer getragen wird. Es sind aber nichtsdestoweniger Kosten, die alle Benutzer von bitcoin zusammen tragen. Es beinhaltet aber auch direkte Übertragungsgebühren.)
- Energieverbrauch: ca. 22 TWh pro Jahr $\rightarrow$ 2,5 GW

https://digiconomist.net/bitcoin-energy-consumption,
https://bitinfocharts.com

Einige Zahlen

Kosten für das Minen aktuell

Einige Zahlen

Kosten für das Minen aktuell (T = Tausend) durch Geldausgabe (= Einnahme der Miner):

Einige Zahlen

Kosten für das Minen aktuell (T = Tausend) durch Geldausgabe (= Einnahme der Miner):

	pro Tag	Trans. pro Tag	Kosten pro Trans.
bitcoin	11.000 T €	310 T	35 €

Einige Zahlen

Kosten für das Minen aktuell (T = Tausend) durch Geldausgabe (= Einnahme der Miner):

	pro Tag	Trans. pro Tag	Kosten pro Trans.
bitcoin	11.000 T €	310 T	35 €
ethereum	4.700 T €	460 T	10 €

Einige Zahlen

Kosten für das Minen aktuell (T = Tausend) durch Geldausgabe (= Einnahme der Miner):

	pro Tag	Trans. pro Tag	Kosten pro Trans.
bitcoin	11.000 T €	310 T	35 €
ethereum	4.700 T €	460 T	10 €
bitcoin cash	170 T €	8,3 T	20 €

Einige Zahlen

Kosten für das Minen aktuell (T = Tausend) durch Geldausgabe (= Einnahme der Miner):

	pro Tag	Trans. pro Tag	Kosten pro Trans.
bitcoin	11.000 T €	310 T	35 €
ethereum	4.700 T €	460 T	10 €
bitcoin cash	170 T €	8,3 T	20 €
litecoin	620 T €	25 T	25 €

Einige Zahlen

Kosten für das Minen aktuell (T = Tausend) durch Geldausgabe (= Einnahme der Miner):

	pro Tag	Trans. pro Tag	Kosten pro Trans.
bitcoin	11.000 T €	310 T	35 €
ethereum	4.700 T €	460 T	10 €
bitcoin cash	170 T €	8,3 T	20 €
litecoin	620 T €	25 T	25 €
Dash	(?) 450 T €	6,0 T	75 €

Einige Zahlen

Kosten für das Minen aktuell (T = Tausend) durch Geldausgabe (= Einnahme der Miner):

	pro Tag	Trans. pro Tag	Kosten pro Trans.
bitcoin	11.000 T €	310 T	35 €
ethereum	4.700 T €	460 T	10 €
bitcoin cash	170 T €	8,3 T	20 €
litecoin	620 T €	25 T	25 €
Dash	(?) 450 T €	6,0 T	75 €
Monero	320 T €	3,4 T	80 €

Einige Zahlen

Kosten für das Minen aktuell (T = Tausend) durch Geldausgabe (= Einnahme der Miner):

	pro Tag	Trans. pro Tag	Kosten pro Trans.
bitcoin	11.000 T €	310 T	35 €
ethereum	4.700 T €	460 T	10 €
bitcoin cash	170 T €	8,3 T	20 €
litecoin	620 T €	25 T	25 €
Dash	(?) 450 T €	6,0 T	75 €
Monero	320 T €	3,4 T	80 €
ethereum classic	260 T €	38 T	6,9 €

Einige Zahlen

Kosten für das Minen aktuell (T = Tausend) durch Geldausgabe (= Einnahme der Miner):

	pro Tag	Trans. pro Tag	Kosten pro Trans.
bitcoin	11.000 T €	310 T	35 €
ethereum	4.700 T €	460 T	10 €
bitcoin cash	170 T €	8,3 T	20 €
litecoin	620 T €	25 T	25 €
Dash	(?) 450 T €	6,0 T	75 €
Monero	320 T €	3,4 T	80 €
ethereum classic	260 T €	38 T	6,9 €
Zcash	1200 T €	5,7 T	220 €

Sein und soll

Wünschenswert wäre:

Sein und soll

Wünschenswert wäre:

ein System für $\gg 1$ mrd Transaktionen pro Tag

Sein und soll

Wünschenswert wäre:

ein System für $\gg 1$ mrd Transaktionen pro Tag

also: Faktor von mindestens 1.000, besser 10.000 zu bitcoin.

Sein und soll

Wünschenswert wäre:

ein System für $\gg$ 1 mrd Transaktionen pro Tag

also: Faktor von mindestens 1.000, besser 10.000 zu bitcoin.

1 mrd Transaktionen $\rightarrow$ 600 GB für die Blockkette

Sein und soll

Wünschenswert wäre:

ein System für $\gg$ 1 mrd Transaktionen pro Tag

also: Faktor von mindestens 1.000, besser 10.000 zu bitcoin.

1 mrd Transaktionen $\rightarrow$ 600 GB für die Blockkette

bei 1 mrd Transaktionen / Tag: 200 TB pro Jahr für die Blockkette

Blockkette speichern?

Es wird nahegelegt, dass Clients die gesamte Blockkette speichern.

Blockkette speichern?

Es wird nahegelegt, dass Clients die gesamte Blockkette speichern.

Aber es gibt Alternativen:

- Weglassen von nicht mehr relevanten Transaktionen
- Oder: Nur speichern von Headern
- Oder: Einfach immer online nachschauen

Blockkette speichern?

Es wird nahegelegt, dass Clients die gesamte Blockkette speichern.

Aber es gibt Alternativen:

- Weglassen von nicht mehr relevanten Transaktionen
- Oder: Nur speichern von Headern
- Oder: Einfach immer online nachschauen

Durch Speichern der Kette wird das System stabilisiert.

Alternativen

- Kontostände speichern statt Transaktionen

Alternativen

- Kontostände speichern statt Transaktionen
  - Ripple
  - Mini-Blockchain Projekt = Cryptonite
  - Peercoin ...

Alternativen

- Kontostände speichern statt Transaktionen
  - Ripple
  - Mini-Blockchain Projekt = Cryptonite
  - Peercoin ...
- Proof of stake statt proof of work

Alternativen

- Kontostände speichern statt Transaktionen
  - Ripple
  - Mini-Blockchain Projekt = Cryptonite
  - Peercoin ...
- Proof of stake statt proof of work
  - Casper in Ethereum
  - Peercoin, Blackcoin ...

Alternativen

- Kontostände speichern statt Transaktionen
  - Ripple
  - Mini-Blockchain Projekt = Cryptonite
  - Peercoin ...
- Proof of stake statt proof of work
  - Casper in Ethereum
  - Peercoin, Blackcoin ...
- Lightweight-Clienten für Benutzer ohne Speichern der gesamten Blockkette
  - schon beschrieben von Satoshi Nakamoto

Alternativen

- Kontostände speichern statt Transaktionen
  - Ripple
  - Mini-Blockchain Projekt = Cryptonite
  - Peercoin ...
- Proof of stake statt proof of work
  - Casper in Ethereum
  - Peercoin, Blackcoin ...
- Lightweight-Clienten für Benutzer ohne Speichern der gesamten Blockkette
  - schon beschrieben von Satoshi Nakamoto
- Anonymität bei der Überweisung
  - verwirklicht in Zcash
    mittels Zero-Knowledge Beweisen.

Alternativen

- Kontostände speichern statt Transaktionen
  - Ripple
  - Mini-Blockchain Projekt = Cryptonite
  - Peercoin ...
- Proof of stake statt proof of work
  - Casper in Ethereum
  - Peercoin, Blackcoin ...
- Lightweight-Clienten für Benutzer ohne Speichern der gesamten Blockkette
  - schon beschrieben von Satoshi Nakamoto
- Anonymität bei der Überweisung
  - verwirklicht in Zcash
    mittels Zero-Knowledge Beweisen. Was ist das?