Ideen und Konzepte der Informatik

Elektronische Währung

Bitcoins und Blockchains

Antonios Antoniadis

11. Dec. 2017

Was ist eine Währung?

Was ist eine Währung?

- Mittel zum Austausch von Gütern
- Ein „Geldsystem“
- Werden in der Regel von Regierungen herausgegeben und kontrolliert.
- Konzept existiert seit mehr als 5000 Jahren.

Überblick

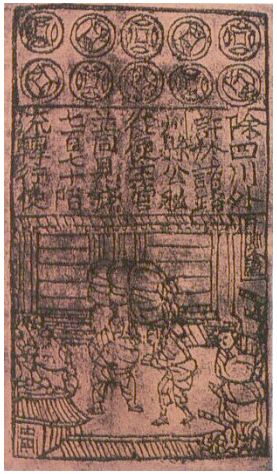
- Geschichte und Grundlagen
- Dezentrale Währung Vor- und Nachteile
- Bitcoins
- Blockchains
- Weitere Anwendungen

Geschichtlicher Rückblick

- Früher mit Gütern direkt gehandelt:
  - Sehr unpraktisch wegen u.a. (i) Transport, (ii) zeitlicher Aspekt, z.B. was, wenn ich meine im Winter geernteten Äpfel am kommenden Spätsommer gegen Trauben eintauschen möchte? (iii) Nur direkter Austausch möglich.

Geschichtlicher Rückblick

- Früher mit Gütern direkt gehandelt:
  - Sehr unpraktisch wegen u.a. (i) Transport, (ii) zeitlicher Aspekt, z.B. was, wenn ich meine im Winter geernteten Äpfel am kommenden Spätsommer gegen Trauben eintauschen möchte? (iii) Nur direkter Austausch möglich.
- Später, Metalle die den Wert von gelagerten Gütern representierten.
- Münzen. Der „Stempel“ auf der Münze hat garantiert, dass die Münze das richtige Metall und richtige Gewicht hat.
- Scheine. Einfacher zu produzieren und zu transportieren.



Grundlagen

Eine Währung funktioniert nur mit **Vertrauen**.

- Man tauscht sein Gut oder seine Arbeit für Münzen und Scheine aus, nur wenn man darauf vertraut, dafür etwas zurückzubekommen.

Grundlagen

Eine Währung funktioniert nur mit **Vertrauen**.

- Man tauscht sein Gut oder seine Arbeit für Münzen und Scheine aus, nur wenn man darauf vertraut, dafür etwas zurückzubekommen.
- Dies wird in der Regel durch den König, Regierung, Armee usw. gebürgt.

Grundlagen

Eine Währung funktioniert nur mit **Vertrauen**.

- Man tauscht sein Gut oder seine Arbeit für Münzen und Scheine aus, nur wenn man darauf vertraut, dafür etwas zurückzubekommen.
- Dies wird in der Regel durch den König, Regierung, Armee usw. gebürgt.
- Wenn das Vertrauen verloren geht, verliert die Währung ihren Wert. Dann entstehen meistens Parallelwährungen, z.B. Zigarettenwährung in Deutschland nach dem Zweiten Weltkrieg.

Digitale Währungen

- Früher hat jedes Land Gold- und Silberreserven gelagert, was den Wert der Scheine und Münzen im Umlauf widerspiegelte.

Digitale Währungen

- Früher hat jedes Land Gold- und Silberreserven gelagert, was den Wert der Scheine und Münzen im Umlauf widerspiegelte.
- Heute nicht mehr der Fall. Ein großer Teil des Geldes im Umlauf existiert nur als ein Eintrag in der Datenbank eines Finanzinstituts.

Digitale Währungen

- Früher hat jedes Land Gold- und Silberreserven gelagert, was den Wert der Scheine und Münzen im Umlauf widerspiegelte.
- Heute nicht mehr der Fall. Ein großer Teil des Geldes im Umlauf existiert nur als ein Eintrag in der Datenbank eines Finanzinstituts.
- In dem Sinne kann man sagen, dass jede übliche Währung auch eine **Digitale Währung** ist. Allerdings zentral kontrolliert von Regierungen/Finanzinstituten.

Dezentrale Währung

Wie wäre es mit einer Währung, bei der die Nutzer selbst bestimmen. Ohne Autoritätspartei.

Vorteile:

- Mehr Anonymität
- Wird nicht „gesteuert“
- Kann jedem Zugang zur globalen Ökonomie ermöglichen
- Eröffnet viele Möglichkeiten Geschäfte zu machen
- Günstigere Transaktionen da keine Vermittler

Nachteile:

- Sicherheit?
- Kann einfacher als konventionelle Währungen für illegale Aktivitäten verwendet werden.
- An wen wendet man sich, wenn etwas schiefgeht?
- Man kann nicht den Wechselkurs manipulieren, z.B. um Exporte zu fördern.

Bitcoins und Blockchains

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

- Bitcoins/Blockchains
- Eingeführt unter Pseudonym „Satoshi Nakamoto“ in 2008
- Zurzeit sehr oft in den Medien, unter anderem weil:

Größte Hürde: Vertrauen erzeugen, ohne vertrauenswürdige Drittpartei

(Struktur folgt grob Michael Nielsen)

Jeder führt eine eigene Kopie der Kontoführung für **alle Konten**!

Größte Hürde: Vertrauen erzeugen, ohne vertrauenswürdige Drittpartei

(Struktur folgt grob Michael Nielsen)

Jeder führt eine eigene Kopie der Kontoführung für **alle Konten**!

1. Versuch: Alice schickt eine signierte Nachricht an alle Teilnehmer „Ich, Alice, schicke Bob einen Wert von 1 Münze.“

Da mit privaten Schlüssel signiert:

- wissen alle, dass Die Nachricht von Alice stammt und jeder kann das Kontobuch aktualisieren.
- Alice kann die Transaktion nicht abstreiten.

Größte Hürde: Vertrauen erzeugen, ohne vertrauenswürdige Drittpartei

(Struktur folgt grob Michael Nielsen)

Jeder führt eine eigene Kopie der Kontoführung für **alle Konten**!

1. Versuch: Alice schickt eine signierte Nachricht an alle Teilnehmer „Ich, Alice, schicke Bob einen Wert von 1 Münze.“

Da mit privaten Schlüssel signiert:

- wissen alle, dass Die Nachricht von Alice stammt und jeder kann das Kontobuch aktualisieren.
- Alice kann die Transaktion nicht abstreiten.

Allerdings:

- Was, wenn Alice versucht, bevor ihre Nachricht alle Teilnehmer erreicht, schnell das Geld nochmal bei einer anderen Transaktion auszugeben? (**double spending**)

Mögliche Lösung

- Alice kontaktiert vertrauenswürdige Drittpartei (z.B. Bank), sagt dass Sie eine Münze an Bob vergibt.
- Drittpartei verifiziert, dass Alice eine Münze hat und erzeugt die Seriennummer 12345 für diese Transaktion und schickt an alle Teilnehmer die Nachricht, „Alice kann eine Transaktion mit Bob mit Seriennummer 12345, für eine Münze ausführen“
- Alice schickt die signierte Nachricht und alle aktualisieren das Kontobuch.
- Eine weitere Transaktion ist nur durch eine neue Seriennummer möglich.

Allerdings:

- Wir möchten eine **dezentrale Währung**, also kommt keine vertrauenswürdige Drittpartei in Frage!

Was, wenn alle Teilnehmer zusammen die Rolle der Bank übernehmen?

Idee: Man kann vielleicht nicht in einzelne Teilnehmer vertrauen, aber schon in die „Mehrheit“ der Teilnehmer. Sollte die Mehrheit schummeln, geht Vertrauen in die Währung verloren und alle Teilnehmer haben Verluste.

5 Minuten Pause: Evaluation

Blockchain

- Jeder Teilnehmer führt schon ein Kontobuch. Nennen wir das von jetzt an **Blockchain** (Kette von Blocks).
- Neue Transaktionen werden in einem Block gesammelt und der Block wird der Blockchain beigefügt. Das formt eine Kette von Blocks in der sich alle Transaktionen befinden.
- Alle Transaktionen zu speichern ist ausreichend um den Betrag, den jeder Nutzer zur Vefügung hat, zu erzeugen.

- Alice schickt an Bob die Nachricht „Ich, Alice sende Bob 1 Münze mit Seriennummer 12345“
- Bob kann in seiner Kopie der Blockchain verifizieren, dass Alice diese Münze besitzt.
- Bob sendet an alle Teilenhmer die Nachricht von Alice, und er sagt Bescheid, dass er die Transaktion annehmen möchte.
- Jeder Teilnehmer sammelt solche offene Transaktionen die zulässig sind, in einem neuen Block.
- Wenn die „Mehrheit“ mit so einem Block einverstanden ist, hängt jeder Teilnehmer diesen Block am Ende seiner Blockchain. Nur dann ist die Transaktion bestätigt!
- Das Ganze geht noch mal von vorne los.

- Alice kann nicht gleichzeitig die Münze mit der gleichen Seriennummer an zwei Personen senden, das würde anderen Teilnehmern auffallen und die Transaktion würde nicht in den neuen Block kommen.
- Aber wie wird beschlossen, mit welchem Block die Mehrheit einverstanden ist, so dass die Blockchain um diesen verlängert wird?
- Das ist die **Neuerung:** *Proof of work Konzept.*

Proof of Work

- Jeder Teilnehmer darf an seiner Blockchain seinen letzten Block mit Transaktionen anhängen, solange:
  - Das die längste zulässige Blockchain ist, die er kennt
  - Er zuerst ein sehr rechenintensives mathematisches Rätsel löst.
- Wenn zwei Teilnehmer gleichzeitig das Rätsel lösen und jeder seine Version des letzten Blocks an seiner Blockchain anhängt dann gibt es kurzfristig zwei unterschiedliche Versionen der Blockchain. Diese wird zu einer Version zurückgeführt sobald das nächste oder übernächste Rätsel gelöst wird.
- Es ist extrem unwahrscheinlich, dass beide Versionen gleichzeitig weiterwachsen und jeder Teilnehmer muss die längste Blockchain benutzen, die er kennt.

Kryptographische Hashing-Funktion

- Eine Funktion, die Eingabe/Daten von beliebiger Größe einem Text fester Größe zuordnet.
- Diese Funktion sollte einfach zu berechnen, aber praktisch unmöglich Rückgängig zu machen sein.

Kryptographische Hashing-Funktion

- Eine Funktion, die Eingabe/Daten von beliebiger Größe einem Text fester Größe zuordnet.
- Diese Funktion sollte einfach zu berechnen, aber praktisch unmöglich Rückgängig zu machen sein.

Beispiel:

Ideen der Informatik:

2864c9ef03f5fd8090c09f2cefe62e5d44fb8b84ed99c1500225db6572a2fef5

Ideen der Informatik.:

0f8dbd48fd128a55773323b272eb5b9c14c01d019f74a6aa70ae71aba038bde0

Kryptographische Hashing-Funktion

- Eine Funktion, die Eingabe/Daten von beliebiger Größe einem Text fester Größe zuordnet.
- Diese Funktion sollte einfach zu berechnen, aber praktisch unmöglich Rückgängig zu machen sein.

Beispiel:

Ideen der Informatik:

2864c9ef03f5fd8090c09f2cefe62e5d44fb8b84ed99c1500225db6572a2fef5

Ideen der Informatik.:

0f8dbd48fd128a55773323b272eb5b9c14c01d019f74a6aa70ae71aba038bde0

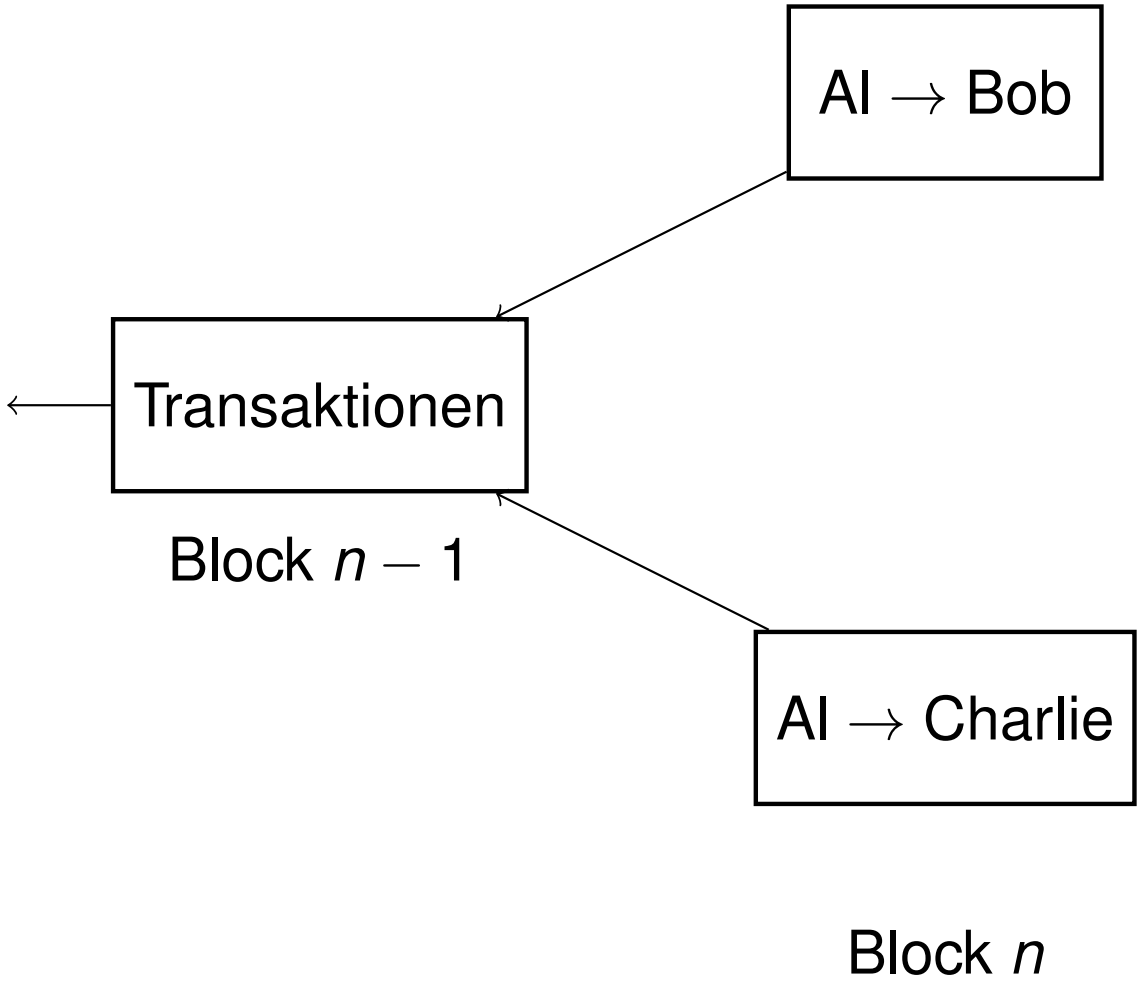
Ein Punkt Unterschied und die Ausgaben sind ganz anders!

Das Mathematische Rätsel

- Setze zu deinem neuen Block eine ganze Zahl (Nonce) hinzu, sodass der Wert der Hashing-Funktion mit einer bestimmten Anzahl von Nullen begint.
- Kann eigentlich **nur** durch Ausprobieren von allen möglichen Zahlen gelöst werden.
- Je mehr Nullen, desto mehr muss man ausprobieren. Die Anzahl der Nullen wird so angepasst, dass im Durchschnitt jede 10 Minuten ein Teilnehmer die Lösung findet.
- Wenn ein Teilnehmer so eine Zahl (Nonce) findet, hängt er seinen Block an seine Blockchain (und schreibt sich auch eine feste Anzahl Münzen gut für seine Mühe). Dann teilt er seinen Block und Nonce mit allen Teilnehmern.
- Diese können einfach verifizieren, ob der Block zulässig ist und ob die Nonce zu der gewollten Anzahl Nullen führt und nehmen den an.

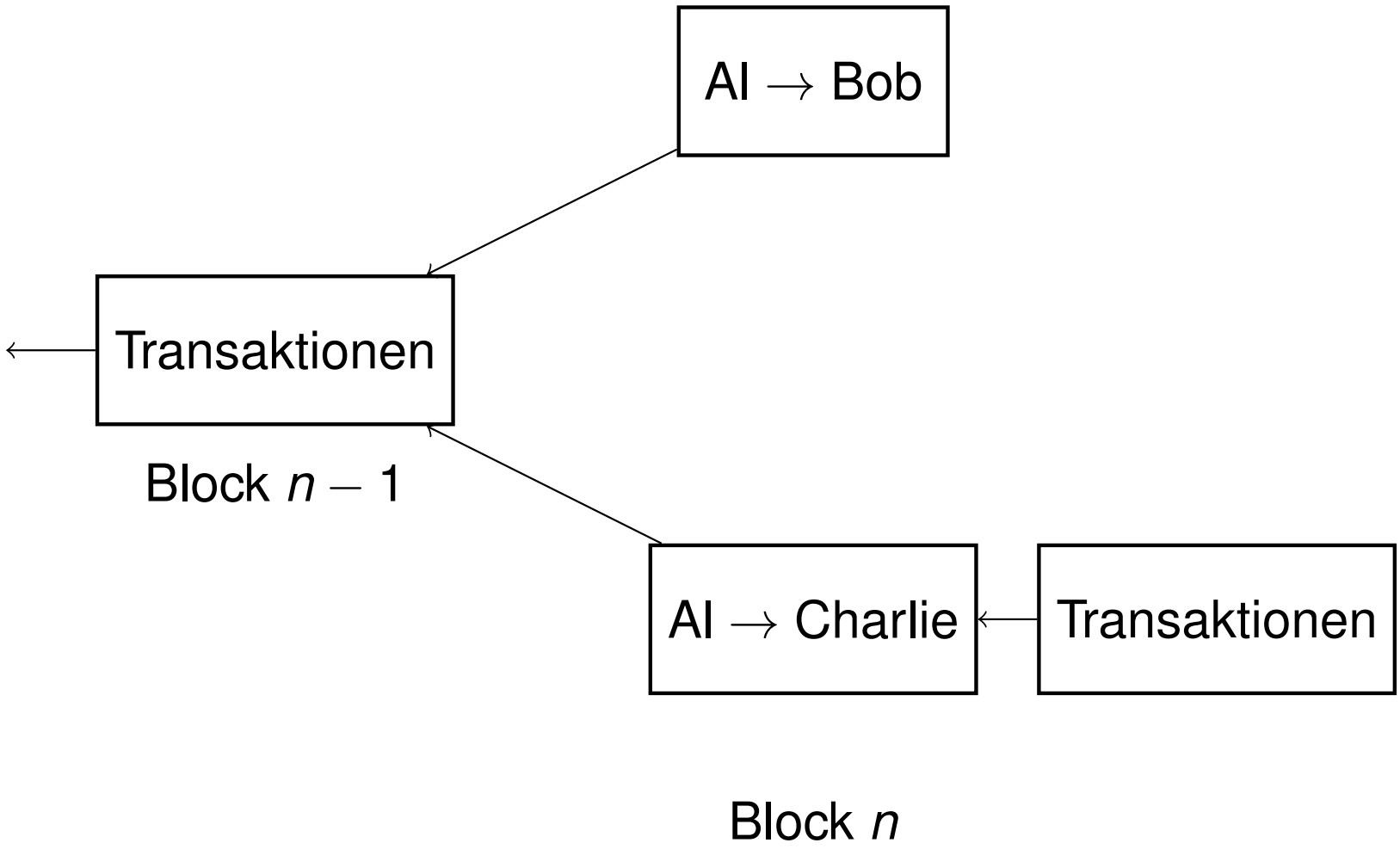
Gamblers ruin

- Was, wenn zwei Teilnehmer jeweils ihr Rätsel gleichzeitig lösen? Kann Alice das ausnutzen um zu betrügen?



Gamblers ruin

- Was, wenn zwei Teilnehmer jeweils ihr Rätsel gleichzeitig lösen? Kann Alice das ausnutzen um zu betrügen?



Gamblers ruin

- Während alle Teilnehmer an der oberen Kette arbeiten, versucht Alice an der unteren Kette zu überholen.
- Wenn Sie das schafft, dass Ihre Abzweigung länger wird, dann hat Bob ein Problem!
- Auch wenn Alice eine Wahrscheinlichkeit von $p = 0.1$ hat ihr Rätsel schneller zu lösen (welches ein Zehntel der ganzen Rechenkraft benötigt), wird sie mit Wahrscheinlichkeit

$$\left(\frac{p}{1-p}\right)^z = \left(\frac{1}{9}\right)^z,$$

  z Kettenglieder aufholen können.
- Man rät dazu bei großen Transaktionen zu warten bis die Kette um 6 Glieder länger wird (also circa eine Stunde) bis man die Transaktion als anerkannt betrachtet. Für $z = 6$ ist die obere Wahrscheinlichkeit 0.0000019.

Weitere Details

- **Anonymität:** Jeder Nutzer ist in der Blockchain durch einen öffentlichen Schlüssel gelistet. Keiner muss wissen, wem der öffentliche Schlüssel gehört, und er kann durch den privaten Schlüssel Transaktionen ausführen.

Weitere Details

- **Anonymität:** Jeder Nutzer ist in der Blockchain durch einen öffentlichen Schlüssel gelistet. Keiner muss wissen, wem der öffentliche Schlüssel gehört, und er kann durch den privaten Schlüssel Transaktionen ausführen.
- Allerdings, wenn der private Schlüssel verloren geht, kann keiner mehr die Bitcoins benutzen.

06.12.2017

Der Schatz auf der Müllkippe

32-Jähriger sucht seine Bitcoin-Millionen

Eine erste Suche im September 2013 blieb erfolglos. Das infrage kommende Areal ist so groß wie ein Fußballfeld.

(Foto: Twitter/@howelzy)

James Howells ist Multi-Millionär - und irgendwie auch nicht. Auf seiner Festplatte schlummern Tausende Bitcoins, die inzwischen 75 Millionen Euro wert sind. Der Haken: Die F vergraben auf einer Müllkippe. Jetzt rückt Howells mit schwerem Gerät an.

Weitere Details & Fragen

- Eigentlich muss nicht jeder Nutzer versuchen, die Kette zu verlängern, aber jeder darf.
- Es braucht sehr viel Rechenkraft/Energie um ein Rätsel zu lösen. Macht es Sinn? Aber traditionellere Währungen verlangen auch nach viel Aufwand: Drucken, Verteilen, Banken, vor Fälschung schützen...
- Es wird insgesamt nur circa 21 Millionen Bitcoins geben. Was bedeutet das für die Währung? Warum würden Leute weiterhin versuchen die Rätsel zu lösen und die Kette zu verlängern?
- Wie können Staaten Steuern für anonyme Transaktionen verlangen?

Blockchain: Weitere Anwendungen

Währungen sind nur ein Teil der Anwendungen von Blockchains. Da Blockchains verteilte/dezentrale Datenbanken sind deren Korrektheit auf das Vertrauen aller Teilnehmer ruht. Ein Paar Beispiele:

- Klevere Verträge
- Gesundheitsdatenbanken