kan m'n nonce niet vinden

Ethereum

Litecoin

Petro

wallet

Dash

aba128d3931e54ce63a69d8c2c1c705era9f39ca950df13655d92db662515eacf

Wat is een Bitcoin ?

Monero

Satoshi Nakamoto

Ripple

IOTA

Zcash

foute hash

Insanecoin

Geschiedenis van geld is geld

- Het begon allemaal in Italië
- Boekhouden
  - Luca Pacioli (franciscaner monnik en wiskundige), 1494 "Summa de Arithmetica Geometria Proportione et Proportionalita"b asis voor dubbel boekhouden
- Banken
  - Banco Medici (1397), eerste staatsbank Banco di San Giorgio (Genua), oudste Monte dei Paschi di Siena (1472)
- Vertrouwen
- Rechtszekerheid
- Essentiële voorwaarde voor handel, economische ontwikkeling en welvaart
- Vinger in de pap door overheden, risico's en bureaucratie, (verborgen) kosten

Nadelen van huidige systeem

- Internationale handel / barrières
- Valuta, kosten en risico's
- Snelheid
- Security
- Privacy, (de overheid weet alles)
- invloed van de politiek, of het gebrek daarvan
- Alle transacties gaan via tussenpersonen

Blockchain Technologie

- transactie vrij van tussenpersonen
  - geen invloed van overheden
- met absolute betrouwbaarheid
  - cryptografie als basis
  - volledige decentralisatie van de operatie en consensus onder de deelbemers
- met volledige privacy
- zonder kosten
  - shared network, gedeelde kosten, iedereen draagt bij
- niet alleen betaalmiddel maar ook voor andere transacties,
  - onroerend goed / kadaster, Bill of Lading, stemmen, verzekeringen, etc.

Het Blockchain Paradigma

- Nu
  €100 overboeking
  1. maak overboeking
  2. de bank rekent een fee voor de kosten
  3. de bank verifieert dat ik kredietwaardig ben
  4. mijn bank checks met jouw bank of de intermediair of jouw rekening bestaat
  5. Mijn bank updates zijn grootboek
  6. Jouw bank updates zijn grootboek

- De Blockchain heeft slechts één grootboek
  1. Ik maak de overboeking
  2. De naastbijzijnde computers in het netwerk checken of de transactie valide is
  3. Als de transactie OK is wordt die verstuurd naar alle computers in het netwerk
  4. Iedere computer verifieert de transactie totdat de transactie aan alle ledgers is toegevoegd.

- Belangrijk voordeel is internationale bereik
  daarnaast een toegenomen productiviteit / efficiency

- Maar hoe wordt dit netwerk veilig?

Cryptografie en Encryptie

- de 1e beveiligingslaag is is de encryptie van de transactie
  - transactie ID, tijd, bedrag, afzender adres, ontvangstadres worden samengevoegd tot één nummer
    bv een bitcoin transactie van October 20, 2017
    aba128d3931e54ce63a69d8c2c1c705era9f39ca950df13655d92db662515eacf
  - dit verkort de data die worden verstuurd, maakt de transactie efficienter en verbergt de inhoud, maar
  - de encryptie standaard is publiek dus de data kunnen zichtbaar worden gemaakt,
    public keys van zender en ontvanger + bedrag
- de 2e beveiligingslaag is de "Distributed Ledger"
  - Omdat er duizenden kopieën zijn is het praktisch onmogelijk m veranderingen aan te brengen
- anonimiteit, de "Private Key"
  - de ledger moet openbaar zijn om te kunnen werken. Daarom zijn de gebruikersgegevens anoniem iedere "wallet" is alleen toegankelijk via een "private key"die alleen bekend is aan de gebruiker. Gebruikers kunne meer dan één "wallet"hebben

Block

- Block is een lijst van transacties over een bepaalde tijdsperiode, dus alle informatie die in die periode (een paar minuten) in het netwerk is geprocessed. Er wordt één blok tegelijk aangemaakt

- Chain, ieder blok krijgt een time-stamp en wordt in chronologische orde gekoppeld aan het vorige blok, via een cryptografisch algoritme. De algoritmes zijn moeilijk te berekenen en kosten minuten rekentijd voor snelle computers. Als de puzzle is opgelost wordt het block in de chain vastgelegd en is dan (in principe) niet meer te wijzigen.

- Als het block is vastgelegd wordt e.e.a. geverifieerd door de computers in het netwerk.

Bitcoin

- De bitcoin is geen object, de bitcoin is alleen een transactie record. Het bewijs dat je 30 bitcoins hebt is alleen de geschiedenis van de transacties waarmee je ze kreeg.
    - de ledger houdt 3 zaken bij; een input (Karel heeft de bitcoin gisteren ontvangen van Anna), een hoeveelheid (hoeveel wil Karel aan Maria sturen) en een output (Maria's adres waar de output naar toe moet)

Het maken van een Block

- Niet iedere computer in het netwerk maakt een blok. Dit is gespecialiseerd werk dat door een beperkte groep wordt gedaan. Maken en verifiëren van een blok levert een beloning op.

- maken van een block

- toevoegen van nieuwe transacties
  verifiëren van de geldigheid van alle transacties en alleen de geldige toevoegen aan het block, dit zullen er zo'n 1500-2000 zijn

- vaststellen en verkorten van de ledger
  dit is een lijst van alle transacties in één lijst
  [Input1][Hoeveelheid1][Output adres1],[Input2][Hoeveelheid2][Output adres2],[Input3][Hoeveelheid3][Output adres3], ...

- maak van deze string één getal (hashing) bv
  aba128d3931e54ce63a69d8c2c1c705ea9f39ca951df13655d92db662515eacf

- geef het block een timestamp en ID

- voeg het block toe in de keten
  dit vereist weer een hashing operatie zodat de voorafgaande blokken onderdeel worden van dit laatste blok

Hashing

- gestandaardiseerd, iedere text levert een 64 digit getal op
- uniek, iedere tekst levert een ander getal op
- deterministisch, hetzelfde origuineel levert altijd dezelfde hash
- het werkt enkelzijdig, de hash is direct gekoppeld aan de input, van de output de input terugrekenen is (practisch) onmogelijk
- Hacken van de ledger leidt altijd tot een andere hash en leidt dus tot verificatiefouten
- Hashing van het block in de keten maakt het hacken van een voorafgaand block onmogelijk omdat daarmee de hash verandert
- Hashing is niet zo moeilijk, de meeste computers kunnen dat snel.
- Toegevoegde complicatie voor block creatie om security te verhogen; "Proof of Work"

Proof of Work

- Maakt hacken moeilijker
- geeft de 'eerlijke' partijen tijd voor verificatie
- Consensus en beloning
- in eenvoudige vorm een moeilijke puzzle, de eerste computer die de puzzle oplost krijgt de beloning en het nieuwe block wordt geaccepteerd als het geldige block in de keten
- 'Block Reward' was in nov 2017 - 12.5 BC, toen $ 82 500
- Er zijn nu tienduizenden 'verifiers' die allemaal proberen om de reward te bemachtigen
- Het grote aantal garandeert de security van het systeem

Mining

- Fundamenteel is "raden-en-controleren" guess-and-check
  dat is niet moeilijk als je maar genoeg tijd hebt .... of een hele snelle computer

- Hoe werkt het?
  Toevoegen van een stukje de "nonce" aan het block zodat de oplossing wordt gevonden, bv de hash moet beginnen met een '0

Input	Output
Hello	eb5c7f52857a294c3f5925b1d66cbf9dd4760ca1f7e047453636c661fc093e8e
Hello0	80878c5b013ba72c0d2b7e8f65868649cbdb1e7e7a8c8a07537d6b3619c4e32f
Hello1	948edbe7ede5aa7423476ae29dcd7d61e7711a071aea0d83698377effa896525
Hello2	be98c2510e417405547facb89399582fc499c3de4452b3014857f92e6baad9a9
Hello3	0945f30798c23800c64afeb4bd218873fa7a2ad2e97ee68db067b2eb63cb0e9c

- Dit is een simpele, de huidige eis is 18 startnullen
  [000000000000000000.....]
  Dit kost de snelste computers meer dan 10 minuten

- Hacken vereist meer dan 51% computing power in het newerk, dit is practisch onmogelijk

Kosten

- Proof of work is effectief maar vreet energie
  inschatting is in 2020 gelijk aan de energieconsumptie van Denemarken

- Alternatief is proof of stake (Ethereum)
  - één partij wordt gekozen om het Block samen te stellen
  - de kans op uitverkiezing is evenredig aan het percentage van de coins die je bezit
  - de beloning is de transactie fees van het block
  - toevogen van neptransacties leidt tot het verliezen van al je coins

  de energiebesparing hiervan is enorm

Geschiedenis

- Oorsprong is stuk geschreven in 2009 door ***Satoshi Nakamoto***
- Grote onbekende en lead developer voor de Bitcoin tot 2011
- leiderschap overgedragen aan Gavin Andresen / Bitcoin Foundation
- (Ver)kopen van Bitcoin loopt via een Bitcoin exchange
- In 2014 Mt. Gox was de grootste die 70% van de wereldwijde transacties afhandelde.
- In 2014 ging Mt Gox failliet door een hack waarbij $450.000.000 is verdwenen
- Bitcoin mining is nu een professionele operatie met gespecialiseerde hardware
- Capaciteitsprobleem, gemiddeld 310 000 transacties per dag maar dat is onvoldoende om aan de vraag te beantwoorden. De oorzaak is de beperking van de Block-size (1MB). Wachttijden kunnen minuten tot uren zijn

De Basis

- Slechts 8 pagina's
- Voor kenners met een goede basis in wiskundige statistiek en theoretische en praktische cryptografie
- zie https://bitcoin.org/bitcoin.pdf

Bitcoin: A Peer-to-Peer Electronic Cash System

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

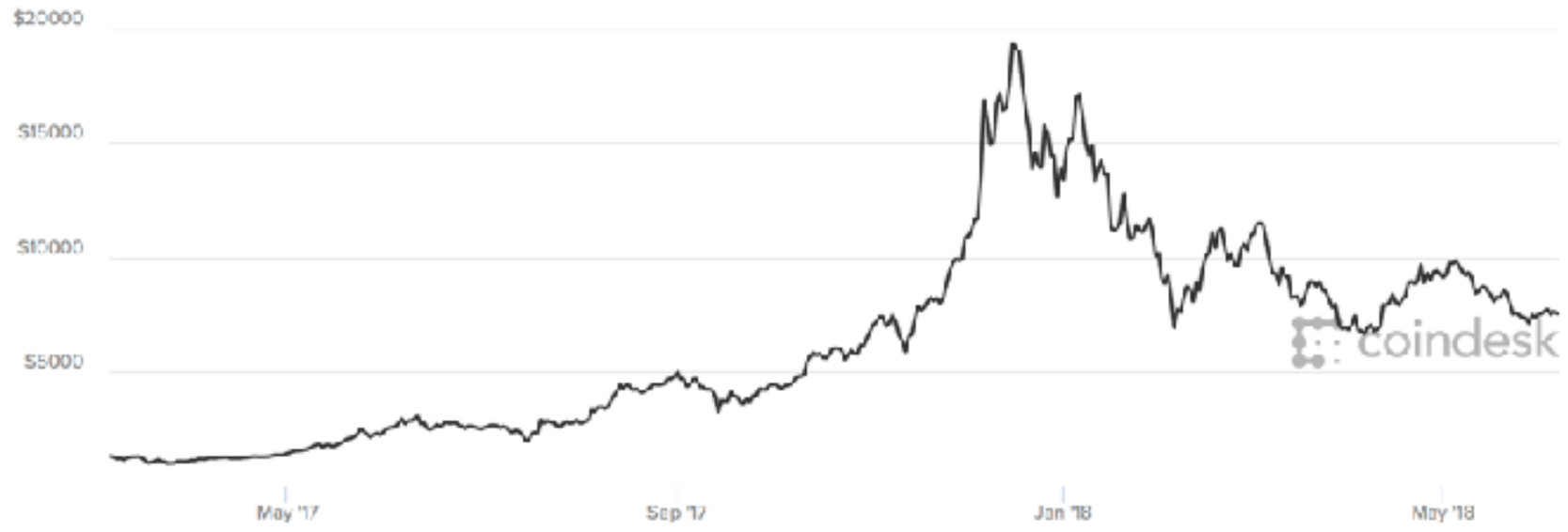
Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required 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.

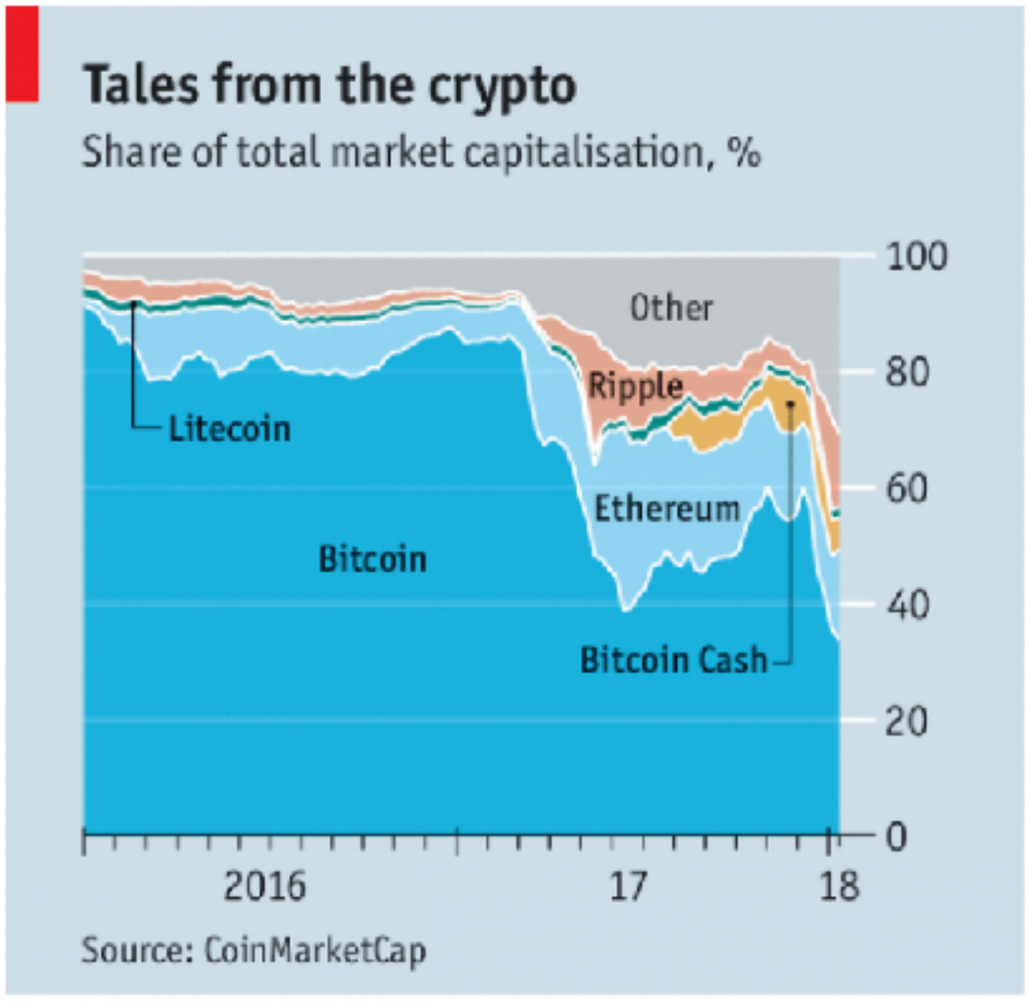
Wat is de waarde van de Bitcoin ?



- Volgens artikel in de FT zeggen economen Jackman & Savouri dat de Botcoin over gewaardeerd is en dat de echte waarde makkelijk te berekenen is.
  De bitcoin is een betaalmiddel en op die basis is de waarde simpelweg te berekenen

- De redenering is als volgt:
  - er zijn 15 m bitcoins (limiet)
  - het gebruik voor betalingen is ongeveer $ 1.200 m per jaar
  - als iedere bitcoin 4x per jaar voor een betaling wordt gebruikt zijn er 60m betalingen per jaar
  - 60m betalingen voor $ 1.200 m aan waarde betekent $20 /bitcoin

Bitcoin - The only game in town ?



Economist.com

- Iedere dag een nieuwe crypto munt
- D*ogecoin* , een Japanse parodie gebaseerd op een cartoon gelanceerd in 2013, totaal in circulatie nu $2B
- 1400 verschillende coins, *UFOcoin, Putincoin, Sexcoin, Insanecoin* (nu $7m waard)
- 40 hebben een waarde van meer dan $1B
  - *Ethereum* $137B
  - *Cardano* $20B
  - *Neo* @8B
- nog te komen
  - *Petro*, een cryptovaluta die geen cryptovaluta is, gedekt door reserves die er niet zijn, uitgegeven door een overheid zonder geld
  - *cryptoroebel*
  - *e-kroon*

Wat kan ik er mee

- Gebruik Bitcoin als een investering

  alternatief, koop goud en hang het om de hals van je vrouw,
  daar heb je meer plezier van

- Gebruik Bitcoin als betaalmiddel

  alternatief, telebankieren bij KNAB of de RABO,
  dat is makkelijker en minder riskant

Investeren in / kopen van Bitcoin

- Ga naar een broker / bitcoin exchange
  b.v.
  Anycoin Direct, Bitcoin.de, BitPanda, BL3P, Paymium,
  The Rock Trading

- Gebruik een Bitcoin ATM
  Bitcoins4me, Your Sun in Deventer Binnensingel 2
  BGST, Shell benzinestation in Enschede, Gronausestraat 1000

- Zoek iemand in de omgeving
  zie localbitcoins.com

Ale info beschikbaar via www.bitcoin.org

Bitcoin als betaalmiddel

- Kies een wallet

- 4 mogelijkheden:
  - Desktop, beschikbaar voor Linux, Mac en Windows

  - Hardware

  - Mobile, Android, IOS of Windows Phone
  - Web

Aan de gang met Cryptomunten

- Bestudeer goed hoe het werkt
  (en besluit dan om toch maar niet met Bitcoins te gaan werken...?)

- Koop een wallet ($100-150)

- Kies een exchange

- Koop Bitcoin

- Geef de Bitcoin uit en ontvang uw salaris/pensioen in Bitcoin
  of.....
  Verkoop de Bitcoin met winst/verlies

De Bitcoin vandaag

Bitcoin Price / Euro