

# 21 Lektioner

## Hvad jeg har lært af at falde ned i Bitcoin-kaninhullet

Gigi

tioner

I har lært af at falde ned i Bitcoin-kaninhullet  
dgave. Ophavsret ©2018–2024 Gigi / @dergigi / dergigi.co



og og dens online version er distribueret under vilkårene f

*likeret til min kone, mit barn og alle  
nne verden. Må Bitcoin bringe jer  
en vision for en fremtid, der er væ-  
kæmpe for.*



mødte Gigi første gang i et af mine åndelige hjem - hjemstedet for *The Baltic Honeybadger* kom mest ivrige af de Bitcoin-troende valfarter til hvilken dyb samtale over frokost var det bånd, Gigi og jeg så mejslet i sten som en Bitcoin-transaktion afmørt, da vi gav hinanden hånden et par timer tidligere i åndelige hjem, Christ Church, Oxford, hvor jeg havde privilegie at studere til min MBA, var stedet, hvor jeg fandt minhuls"-øjeblik. Ligesom Gigi transcenderede jeg mine tekniske og sociale verdener og blev åndelig opnået. Efter at have „købt på toppen“ i november 2017, var der ekstremt hårde lektioner i det ubarmhjertigt kæmpende, vneladende uendelige 3-årige faldende marked. Det ville virkelig have tjent mig godt i den periode, men de lektioner er simpelthen naturlige sandheder, som ikke er skjult af en uigennemsigtig, skrøbelig film. Hvis man ikke læser denne bog vil facaden dog krakelere.

I en stjerneklar aften i Oxford i slutningen af august 2018, 10 dage efter at kniven igen var blevet stukket ind i Bitfinex-børsen blev hacket, sad jeg eftertænktsonen i en „Masters Garden“. Tiderne var hårde, og jeg var næsten mentale og følelsesmæssige bristepunkt efter,

kolthed fik et slag i ansigtet. Jeg havde endelig

tioner tager dig med på en ægte Bitcoin-rejse; ikke minden for filosofi, teknologi og økonomi, men også sjælen.

Men dykker dybere ned i den filosofi, der kortfattet beskrives i de 7 af de 21 lektioner, kan man med tilstrækkelige udtyk komme så langt som til at forstå alle facetterne af hans 7 lektioner om økonomi indfanger i enkle ord. Hvordan vi er taget til fange af en lille gruppe galere og hvordan det er lykkedes dem at sætte skylden på os, sind, hjerter og sjæle. De 7 lektioner om teknologi og bitcoins skønhed og teknologisk-darwinistiske perspektiver -teknisk bitcoiner giver lektionerne en god gennemgang af deres underliggende teknologiske natur, og endda teknologiens natur.

Det er en flygtige oplevelse, som vi kalder livet, lever, elsker, drømmer, sover. Men hvad er livet andet end en tidsstemplet række af begivenheder?

Det er ikke let at bestige Bitcoin-bjerget. Der er mange bjergrupperne er hårde. Revner og sprækker findes overalt, og det er ikke altid nemt at opsluge dig. Når du har læst denne bog, vil du

„Vil du være såd at fortælle mig, hvilken  
vej jeg skal gå herfra?“

„Det afhænger en hel del af, hvor du vil  
hen.“

„Jeg er ligeglads med, hvor –“

„Så er det ligegyldigt, hvilken vej du går  
– Lewis Carroll, *Alice i Eventyrland*“



randerlighed og forandring

aphedens knaphed

plikation og lokalitet

blemet med identitet

perfekt undfangelse

ngsfrihedens kraft

enserne for viden

konomi

ansiel uvidenhed

ation

rdi

ksioner over „Stor ikke, bekræft

tælle tid kræver arbejde

g dig langsomt, og undgå at ødelægge ting

livet er ikke dødt

erpunks skriver kode

orer for Bitcoins fremtid

ende tanker

danske udgave

er en lidt usædvanlig bog. Men hey, Bitcoin er en usædvanlig teknologi, så en usædvanlig bog om Bitcoin passer mig ikke sikker på, om jeg er en usædvanlig fyr (jeg kan tænke på mig selv som en *almindelig* fyr), men hvordan denne bog blev til, og hvordan jeg blev ført fortælle.

Det og fremmest er jeg ikke forfatter, men ingenior med uderet litteratur. Jeg har studeret kode og kodning, jeg havde aldrig til hensigt at skrive en bog, og selvfølgelig ikke om Bitcoin. Jeg skriver endda ikke om Bitcoin på mit mobilskærmbillede, bare en fyr, der blev bidt af Bitcoin-feberen. Hårdt at sige, for er jeg berettiget til at skrive en bog om Bitcoin? Et spørgsmål. Det korte svar er nemt: Jeg hedder Peter, og jeg er en bitcoiner.

En langt længere svar er en smule mere nuanceret.

I baggrund er inden for datalogi og softwareudvikling min liv var jeg en del af en forskningsgruppe, der brugte computere til at tænke og ræsonnerede. I et senere liv skrev jeg software til automatiseret pasbesparende software, hvilket er endnu mere skræmmende end det, jeg talte om i min bog.

. Og 21 Lektioner blev til denne bog. Så jeg er nu

årlig til at sammenfatte mine tanker i et enkelt twe

r skrive denne bog?", spørger du måske. Igen. Et langt svar. Det korte svar er, at jeg simpelthen var besat af Bitcoin. Jeg fandt det fascinerende. Jeg kan tilsyneladende ikke stoppe på det og de konsekvenser, det vil have for vores

Det lange svar er, at jeg tror, at Bitcoin er den vigtigste teknologi i vores tid, og flere mennesker skal forstå naturen af den. Bitcoin er stadig et af de mest misforståede teknologier i vores moderne verden, og det tog mig år at få alvoren af denne fremmede teknologi. At indse, hvordan det fungerer, og hvordan det fænomen vil ændre vores samfund og vores oplevelse. Jeg håber at plante frøene, der kan føre til denne erkendelse, i dit sind.

I dette afsnit har titlen „*Om denne bog (... og om mit værdighed)*“. Det betyder, at jeg ikke er den eneste i denne bog, hvem jeg er, og hvad jeg har gjort. Jeg er ikke rigtig noget. Jeg er bare et knudepunkt i en større bogstaveligt og billedligt talt. Og du skal altså være opmærksom på, hvad jeg siger. Som vi bitcoinere plejer at sige:

...forstået af dig, så snart *du* er klar, og jeg tror også at de brøkdele af en bitcoin vil finde dig, så snart du er klar. I bund og grund vil alle få Bitcoin på det hurtigt. I mellemtiden er Bitcoin, som den er, og det er ikke noget at forvirre sig over.



gesom mange andre, at jeg har lært mere i de  
at studere Bitcoin, end jeg har gjort i løbet af to å  
uddannelse.

Følgende lektioner er en sammenfatning af, hva  
e blev først udgivet som en artikelserie med titl  
“Learned From Bitcoin”. Det følgende kan ses som d  
e af den oprindelige serie.

Som Bitcoin er disse lektioner ikke statiske. Jeg pl  
jde på dem med jævne mellemrum og udgive op  
per og yderligere materiale i fremtiden.

Ansætning til Bitcoin behøver fremtidige versioner  
ikke at være bagudkompatible. Nogle lektioner  
t, mens andre kan blive omarbejdet eller erstattet.  
oin er en uudtømmelig læremester, og derfor på  
disse lektioner er altomfattende eller komplette.  
ng af min personlige rejse ned i kaninhullet. Der  
ktioner at lære, og enhver person vil lære noget  
æde ind i Bitcoins verden.

Håber, at du vil finde disse lektioner nyttige, og at  
ed at lære dem ved at læse, ikke vil være lige så b  
ertefuld som det var at lære dem alene.



# **21 Lektioner**



„Åh, din tåbelige Alice!“ sagde hun igen.  
hvordan kan du lære noget herinde? Den  
er jo næsten ikke plads til dig, og slet ikke  
nogen lærebøger!“

– Lewis Carroll, *Alice i Eventyrløkken*



*„Men jeg bryder mig ikke om at være blandt gamle mennesker,“ sagde Alice. „Åh, det kan du ikke undgå,“ sagde katten: „Her er vi tossede alle sammen. Jeg er tosset. Du er tosset.“ „Hvor dan ved du, at jeg er tosset?“ sagde Alice. „Det må du være,“ sagde katten, „ellers ville du ikke være kommet her.“*

– Lewis Carroll, *Alice i Eventyrland*

ober 2018 stillede Arjun Balaji det uskyldige spørsmål: *Hvor har du lært af Bitcoin?* Efter at have forsøgt at få svar på spørsmålet i et kort tweet, og uden held, indså jeg, at jeg ikke havde lært, er alt for mange til hurtigt at kunne besvare spørsmålet, hvis det overhovedet kan besvares.

Jeg, jeg har lært, handler naturligvis om Bitcoin - en teknologi, der ikke er direkte relateret til det. Men selvom nogle af Bitco

What have you learned from Bitcoin?

1,353 7:19 PM - Oct 10, 2018



511 people are talking about this



ektioner er struktureret i bundter af syv, hvilket res  
ler. Hvert kapitel betragter Bitcoin gennem en n  
ger, hvad man kan lære ved at inspicere dette mæ  
ra en anden vinkel.

udforsker den filosofiske lære om Bitcoin. Sam  
foranderlighed og forandring, begrebet ægte kn  
perfekte undfangelse, identitetsproblemet, mods  
eplikation og lokalitet, ytringsfrihedens kraft og gr  
en.

udforsker den økonomiske lære af Bitcoin. Dis  
handler finansiel uvidenhed, inflation, værdi, pe  
s historie, brøkreservebankvæsen og hvordan  
er stabile penge på en snedig, indirekte måde.

om en vis forhåndsviden om Bitcoin er gavnlig, h  
e lektioner kan fordøjes af enhver nysgerrig læse  
elaterer til hinanden, bør hver lektion kunne stå fo  
kan læses uafhængigt af hinanden. Jeg har gjort m  
ndgå teknisk jargon, selvom nogle domænespec  
dgælige.

Håber, at mine tekster kan inspirere andre til at e  
erfladen og undersøge nogle af de dybere spørgs  
rejser. Min egen inspiration kom fra en lang ræk  
indholdsskabere, hvem jeg er evigt taknemmelig  
, men ikke mindst: Mit mål med at skrive dette  
vise dig om noget som helst. Mit mål er at få dig til  
ise dig, at der er meget mere ved Bitcoin, end m  
skulle tro. Jeg kan ikke engang fortælle dig, hva  
hvad Bitcoin vil lære dig. Det bliver du nødt til se

„Herfra er der ingen vej tilbage. Du tager den  
ille - historien slutter, du vågner op i din seng og  
å, hvad du vil tro på. Du tager den røde pille<sup>3</sup>  
u forbliver i Eventyrland, og jeg viser dig, hvor d  
aninhullet når.“



k: Alt, hvad jeg tilbyder, er sandheden. Intet andet

**Del I.**

**Filosofi**



*Musen kiggede spørgende på hende. Det så ud, som om den blinkede med det ene af sine små øjne, men den sagde ikke noget.*

– Lewis Carroll, *Alice i Eventyrlandal*

man ser overfladisk på Bitcoin, kan man konkludere, at det er langsom, spild af ressourcer, unødvendigt reduktionistisk og event paranoid. Hvis man ser nysgerrigt på Bitcoin, kan man få et følelse af, at tingene ikke er, som de ser ud ved yderst.

Bitcoin har det med at tage dine antagelser og vendte dem på hovedet. Efter et stykke tid, lige når du er ved at finde din forståelse for Bitcoin, smidder Bitcoin igennem muren som en elefant i en kammeratik og knuser dine antagelser endnu en gang.

Bitcoin er et barn af mange discipliner. Som blinde mænd, der ikke ser en elefant, vil alle se denne nye teknologi fra forskellige vinkler. Og alle vil nå frem til forskellige konklusioner om, hvad der faktisk sker.

象  
衆



ur 0.1.: Blinde munke undersøger Bitcoin-elefante

roblemet med identitet

en perfekt undfangelse

Viringsfrihedens kraft

Grænserne for viden

on 5 udforsker hvordan Bitcoins oprindelseshistorie er fascinerende, men også helt afgørende for et. De sidste to lektioner i dette kapitel udforsker Bitcoins kraft og grænserne for vores individuelle vide. Det er af Bitcoin-kaninhullets overraskende dybde.

Jeg håber, at du vil finde Bitcoins verden lige så længe og underholdende, som jeg gjorde og stadig vil drage dig til at følge den hvide kanin og udforske det hemmelige kaninhul. Hold nu fast i dit lommeur, hop ned og n



*nu lidt - var jeg den samme, da jeg stod op morges? Jeg synes næsten, jeg kan huske, jeg var lidt anderledes. Men hvis ikke jeg var den samme, så er spørgsmålet jo: hvem i alverden er jeg da? Ja, det er det, der er så gådefuldt!"*

– Alice

in er i sagens natur svær at beskrive. Det er en r forslag på at drage en sammenligning med tidlig - om det så er ved at kalde det digitalt guld eller p t - vil utvivlsomt komme til kort. Uanset hvilken a kker, er der to aspekter af Bitcoin, som er helt es ralisering og uforanderlighed.

Håde at tænke på Bitcoin er som en automatise t<sup>1</sup>. Softwaren er kun en brik i puslespillet, og at ltre Bitcoin ved at ændre softwaren er en nyttelø iiver nødt til at overbevise resten af netværket o ndringerne, hvilket mere er en psykologisk indsaa reteknisk.

Følgende vil måske lyde absurd i begyndelsen

Bitcoins natur er sådan, at da version 0.1 blev fremlagt, blev kernedesignet mejslet i sten for resten af dets levetid.“

– Satoshi Nakamoto

mennesker har forsøgt at ændre Bitcoins natur. I det meste af tiden har de alle fejlet. Mens der er et endeløst hav af forgreninger og forkælvinger af Bitcoin (alternativer til Bitcoins), gør Bitcoin-netværket ikke noget ud af det. Det er ikke som det gjorde, da det første knudepunkt gik bort. Det er ikke noget, der vil ikke have betydning i det lange løb. Forgreningerne vil ikke overleve. De vil uddø. Bitcoin er det eneste, der virkelig betyder noget. Hvis der kom en ny teknologi, der kunne udnytte vores grundlæggende forståelse af matematik og kryptografi til at ændre sig, vil Bitcoin fortsætte uden bekymring.

Bitcoin er det første eksempel på en ny livsform, der lever og ånder på internettet. Den overlever, fordi den kan betale folk for at holde den i live. Den kan ikke ændres. Den kan ikke debatteres med. Den kan ikke pilles ved. Den kan ikke bestikkes. Den kan ikke ødeslages. Hvis atomkrig ødelagde halvdelen af vores netværk, ville den fortsætte med at leve ubeskadiget.

e er skørt, men alligevel sker det.

n har lært mig, at den ikke ændrer sig. Det gø



ser mere...

– Alice

erelt synes den teknologiske udvikling at gøre ting  
lige. Flere og flere mennesker er i stand til at nyde  
e har været luksusvarer. Snart vil vi alle leve som  
de fleste af os allerede gør. Som Peter Diamond  
ance [24]: „Teknologi er en ressourcefrigørende  
en kan forvandle det, som engang var knapt, til d  
igt.“

oin, som i sig selv er en avanceret teknologi, bry  
tendens og skaber en ny vare, som er virkelig knap  
da nogle, der hævder, at det er en af de mest knap  
et. Udbuddet af Bitcoins kan ikke øges, uanset h  
fter der anvendes på at skabe mere.

„Kun to ting er virkelig knappe: tid og bitcoin.“

– Saifedean Amm

doksalt nok gør den det ved hjælp af en kopiering.  
Transaktionerne sendes, blokkene distribueres, o  
e hovedbog (som er en logbog med alle transak  
du gættede det - distribueret. Alle disse ord bet  
den herekopiering. For nogle kan Bitcoin kopieres



Pal! Hvor er du?

– Lewis Carroll, *Alice i Eventyrlændet*

set fra kvantemekanik er lokalitet ikke et problem  
erden. Spørgsmålet „Hvor er X?“ kan let besvare.

X er en person eller et objekt. I den digitale verden  
målet om *hvor* allerede et vanskeligt spørgsmål,  
at besvare. Hvor er dine e-mails egentlig? Et datamaskine  
ere „skyen“, som bare er en andens computer.  
kede finde alle de harddiske, som dine e-mails er  
du i teorien finde dem.

bitcoin er spørgsmålet om „hvor“ *virkelig* vanskeligt  
bitcoins helt præcist?

„Jeg åbnede øjnene, så mig omkring og stillede  
et uundgåelige, traditionelle, beklageligt overbrudte  
spørgsmål, der stilles efter en operation: ‘Hvor  
er det?’“

– Daniel Dennett

I emnet er todelt: For det første er den distribuerede  
stribueret gennem fuld replikation, hvilket betyder  
den er overalt. For det andet er der ingen bitcoins,

ikke. De eksisterer ikke. Der er hovedbogsposten hovedbog, der er delt. De findes ikke på nogen sted. Hovedbogen findes stort set på alle fysiske steder. Geografi giver ikke mening - det vil ikke hjælpe dig med at forstå din politik her.“

– Peter Van Valkenburgh

d ejer du egentlig, når du siger „*Jeg har en bitcoin*“? Findes nogen bitcoins? Kan du huske alle de mængder du blev tvunget til at skrive ned af din bitcoin-tegning? Du ved dog godt, at disse magiske ord er, hvad du ejer: en tråd, som kan bruges til at tilføje poster til den offentlige blockchain. Og når du gør det, så kan du også overglænne til at „flytte“ nogle bitcoins. Det er derfor, at du ikke er den eneste i verden, der har praksis med at flytte bitcoins. Hvis du tror, at du er den eneste i verden, der har praksis med at flytte bitcoins, så er du velkommen til at sende mig dine bitcoins.

**Det er ikke et godt ide at have bitcoins i din taske.**

– Lewis Carroll, *Alice i Eventyrland*

Carter har i en hyldest til Thomas Nagels behandling af spørgsmål, i forbindelse med en flagermus, skrevet følgende artikel, der diskuterer følgende spørgsmål: Hvad er en bitcoin? Han viser på glimrende vis, hvordan blokkæder i almindelighed og Bitcoin i særdeleshed er den samme gåde som Theseus' skib<sup>1</sup>: Hvilket er den rigtige Bitcoin?

„Overvej, hvor lidt Bitcoins komponenter forbliver samme. Hele kodebasen er blevet omskrevet, ændret og udvidet, så den knap nok ligner sin oprindelige version. Registreringen af, hvem der ejer hvilke hovedbogen, er stort set netværkets eneste uedvarende træk. For at blive betragtet som virkelig uederløs, skal du opgive den nemme løsning det er at have én computer, der kan udpege den *rigtige* billede som den legitime.“

– Nic Carter

Det er ikke en overdrift, at teknologiens fremskridt fortsætter med at tage disse filosofiske spørgsmål alvorligt. Først vil selvkørende biler blive konfronteret med virkeligt

er den originale Bitcoin. Et år tidligere, den 25. oktober 2013, kom Ethereum sig i to lejre. Markedet besluttede, at den nye kæde er den oprindelige Ethereum.

Ildt decentraliseret, vil spørgsmålene stillet af *The Block* nu blive besvares igen og igen, så længe disse netværk og deres forskelle eksisterer.

**Det har lært mig, at decentralisering er i modstrid med centralisering.**

svar....

– Lewis Carroll, *Alice i Eventyrlændet*

Elsker en god oprindelseshistorie. Bitcoins oprindelse er fascinerende, og detaljerne i den er vigtigere, end man måske selbart skulle tro. Hvem er Satoshi Nakamoto? Var han en mand, eller en gruppe mennesker? Var han en kvinde, en rumvæsen eller en avanceret kunstig intelligens? Uanset fra de besynderlige teorier, vil vi nok aldrig få svar på det, da det er vigtigt.

Satoshi valgte at være anonym. Han plantede frøet til et nyt kryptovaluta, hvilket hængende længe nok til at sikre, at netværket var et fuldt fungerende system. Og så forsvandt han.

Det er et system, som kan se ud som et underligt anonymitetsstunt, men derimod et værdifuldt bidrag til et ægte decentraliseret system. Der er ingen centraliseret kontrol, ingen centraliseret autoritet og ingen, der kan tvinge til at retsforfølge, torturere, afpresse eller udnytte teknologien til sin egen undfangelse af teknologi.

„En af de største ting, Satoshi gjorde, var at forsøge at gøre teknologien til et værdifuldt værktøj, der kunne bruges til at løse problemer, der ikke kunne løses ved hjælp af traditionel politisk og økonomisk makt.“

– Jimmy Sonko

del for mere end 7.000 år siden. Guldets fængs  
de glans førte til, at det blev betragtet som en gav  
guderne.“

Münze Österreich

m guld i oldtiden, kan Bitcoin betragtes som en g  
I modsætning til guld er Bitcoins oprindelse ude  
eskelig. Og denne gang ved vi, hvem guderne b  
vedligeholdelse er: mennesker over hele verden  
er ej.

**Har lært mig, at fortællinger er vigtige.**

*men meget nødtigt, „talte du?“*

– Lewis Carroll, *Alice i Eventyrland*

in er en idé. En idé, som i sin nuværende form  
nen af et maskineri, der udelukkende drives af  
ekter af Bitcoin er tekst: Hvidbogen (whitepaper)  
ren, som køres af knudepunkterne, er tekst. How  
t. Transaktioner er tekst. Offentlige og private  
Alle aspekter af Bitcoin er tekst og svarer dermed

„Kongressen må ikke vedtage nogen lov, der v  
ører oprettelsen af en religion, eller forbud mod d  
rie udøvelse; eller indskrænker ytringsfriheden, e  
ressens frihed, eller folks ret til fredeligt at sam  
g at anmode staten om at få klagemål behandlet“

– Første tilføjelse til USA's forfatr

om det sidste slag i kryptokrigen<sup>1</sup> ikke er blevet u  
vil det være meget svært at kriminalisere en idé  
baseret på udveksling af tekstbeskeder. Hver gang  
er at forbyde tekst eller tale, glider vi ned ad en a  
undgåeligt fører til vederstyggeligheder såsom ulo

er tale. Det kan ikke reguleres i et frit land som  
et med umistelige garanterede rettigheder og en  
*ekte forfatningstilføjelse*, der udtrykkeligt udelukker  
givelseshandlinger fra statsligt tilsyn.“

– Beautyom

**ar lært mig, at ytringsfrihed og fri software er  
et frit samfund.**

---

igt primtal er et tal, der repræsenterer information, hvis b  
distribution er forbudt i visse jurisdiktioner. Et af de første

– Lewis Carroll, *Alice i Eventyrland*

egynde at arbejde med Bitcoin er en ydmygende troede, at jeg vidste ting. Jeg troede, at jeg var vug troede, at jeg i det mindste kunne min datalog et det i årevis, så jeg burde da vide alt om digitalashfunktioner, kryptering, driftssikkerhed og netvært.

er svært at lære alle de grundlæggende element til at virke. At forstå dem alle i dybden er på grulige.

„Ingen har fundet bunden af Bitcoin-kaninhullet – Jameson L

iste over bøger, jeg skal læse, bliver ved med at v end jeg kan nå at læse dem. Listen over aviser o al læses, er næsten uendelig. Der er flere podcasts emner, end jeg nogensinde ville kunne nå at lyttelig overvældende. Desuden udvikler Bitcoin sig, umuligt at holde sig sicur med den accelererende



Figur 7.1.: Bitcoin-kaninhullet er bundløst.

ar lært mig, at jeg ved meget lidt om næsten alt om mig, at dette kaninhul er bundløst.

**Del II.**

**Økonomi**



*„Der stod et stort rosentræ nær indgangen til haven. Roserne på det var hvide, men tre gartnere var ivrigt i færd med at male dem røde. Alice syntes, at det så mærkeligt ud. . . “*

– Lewis Carroll, *Alice i Eventyrlandalen*

ge vokser ikke på træerne. Det er tåbeligt at tro, vores forældre sørger for, at vi ved det, ved at brudsprog som et mantra. Vi bliver opfordret til at blæftigt, til ikke at bruge dem letsindigt, og til at spise de tider, så de kan hjælpe os gennem de dårlige tider, trods alt ikke på træerne.

Min far har lært mig mere om penge, end jeg nogensinde ville få brug for at vide. Gennem den blev jeg tilsyneladende med forskellige pengenes historie, bankvæsenet, forskellige skoler og mange andre emner. Min søgen efter kendskab førte mig ned ad et væld af stier, hvorfra jeg fik

go

## ogenes historie og undergang

viddet i brøkreserve-bankvæsenet

bile penge

jeg kun være i stand til at kradse i overfladen. Det er ambitiøst, men også bredt og dybt, hvilket gør det dække alle relevante emner i en enkelt lektion, der bog. Jeg tvivler på, at det overhovedet er muligt at er en ny form for penge, hvilket gør det afgørende økonomi for at forstå den. Økonomi handler om handlinger og samspillet mellem økonomiske aktører. sandsynligvis en af de største og mest uklare banebrydende spørsmål i økonomien.

disse lektioner en udforskning af de forskellige teknologier bag Bitcoin. De er en personlig afspejling af min rejsen med teknologi. Da jeg ikke har nogen økonomisk baggrund, er det et stort udbrud uden for min komfortzone og klar over, at enhver teknologi jeg måtte have, er ufuldstændig. Jeg vil gøre mit bedste for at få et godt overblik over teknologien, hvad jeg har lært, selv med risiko for at gøre fejl. Når alt kommer til alt, forsøger jeg stadig at blive opdateret med nyheder og udvikling i teknologien.

pige! Nej, jeg vil ikke spørge om det. Jeg kan  
måske læse navnet et eller andet sted.”“

– Lewis Carroll, *Alice i Eventyrland*

f de mest overraskende ting for mig var den mæn  
økonomi og psykologi, der kræves for at få en fors  
er ved første øjekast ser ud til at være et rent te  
et computernetværk. Som en lille fyr med behåre

„Det er en farlig forretning, Frodo, at træde ind  
en. Du læser hvidbogen, og hvis du ikke holder di  
det ikke til at vide, hvor du bliver ført hen.“

at forstå et nyt monetært system, er man nødt til  
mle. Jeg begyndte meget hurtigt at indse, at den  
el uddannelse, jeg havde fået i uddannelsessyste  
nul.

femårig begyndte jeg at stille mig selv en mass  
wordan fungerer banksystemet? Hvordan funge  
det? Hvad er fiat-penge? Hvad er *almindelige*  
er der så megen gæld?<sup>1</sup> Hvor mange penge  
g trykt, og hvem bestemmer det?

– Aaron

Jeg har lært mere om finans, økonomi, teknologi, kryptografi, menneskelig psykologi, politik, spilteori og givning og mig selv i de sidste tre måneder mere end jeg har i de sidste tre et halvt år på universitetet“

– Dunny

er blot to af de mange bekendelser, der florerer på min, som blev udforsket i Lektion 1, er en levende, bevægede, at økonomi også er en levende ting. Det er et ud fra personlig erfaring, er levende ting i sagen, forstå.

Et videnskabeligt system er blot en station i en endeløs søgen efter viden. Det er nødvendigvis påvirkeværdien utilstrækkelighed, der ligger i enhver menneskelig indsats. Men at anerkende disse fakta betyder ikke, at nutidens økonomi er bagud. Det betyder blot, at økonomi er et levende væsen - og at leve indebærer både ufuldkommenhed og forandring.“

videnhed om disse emner til systemisk, bevidst uv  
historie, fysik, biologi, matematik og sprog alle  
s uddannelse, bliver verdenen inden for penge o  
rraskende nok kun udforsket overfladisk, hvis over  
ekulerer på, om folk stadig ville være villige til at o  
gæld, som de gør i øjeblikket, hvis alle blev u  
konomi og i, hvordan penge og gæld fungerer. O  
jeg på, hvor mange lag aluminium der skal til f  
ktiv sølvpapirshat. Sandsynligvis tre.

„Disse nedbrud og redningspakker er ikke tilfæl  
eder. Og det er heller ikke et uheld, at der ikke  
ogen finansiel uddannelse i skolen. Det er overla  
igesom det før borgerkrigen var ulovligt at udda  
n slave, har vi ikke lov til at lære om penge i skole

– Robert Kiyosaki

som i Troldmanden fra Oz bliver vi bedt om ikke  
ærksomme på manden bag kulisserne. I modsætning  
manden fra Oz, har vi nu ægte trolddom<sup>7</sup>: et un  
ment grænseløst netværk af værdioverførsel. De



*re for at blive samme sted. Og hvis du vil nogensinde  
steder hen, må du løbe dobbelt så hurtigt.“*

– Hjerter Dame

rsøge at forstå den monetære inflation, og hvordan et nært system som Bitcoin kan ændre den måde, penge, var udgangspunktet for min rejse ind i økonomien. Jeg vidste, at inflation var den hastighed, hvori penge blev skabt, men jeg vidste ikke meget mere end det. Som nogle økonomer mener, at inflation er en god ting, når man har „hårde“ penge, som ikke let kan skabes - som guldstandardens dage - er afgørende for en sund økonomi, der har et fastsat udbud på 21 millioner, læner sig fra den nævnte lejr.

Hvad er effekten af inflation ikke umiddelbart indlyser. Det af inflationsraten (og andre faktorer) kan der gøre, er årsag og effekt. Ikke nok med det, men inflationen rammer ikke alle og ikke ensartet. Det er dog også forskellige grupper af mennesker mere end andre. Hazlitt påpeger i *Økonomi i én lektion*: „Økonomien er ikke et at se ikke blot på de umiddelbare, men også på de sekundære effekter af enhver handling eller politik; den består af venserne af denne politik ikke blot for én gruppe, men for alle.“

– Henry Hazlitt

Hens destruktive kraft bliver tydelig, så snart en øliver til *meget* inflation. Hvis der opstår hyperinflation, vil penge hurtigt slemme.<sup>2</sup> Når den inflationære valuta er i den, kan den ikke lagre værdi over tid, og folk vil derfor ikke investere i de varer, der kan.

Den konsekvens af hyperinflation er, at alle dem, der har sparet op i løbet af deres liv, reelt set forsættes i din tegnebog vil selvfølgelig stadig være deres værdiløst papir.

Det falder også i værdi med såkaldt „mild“ inflation. Det er somt nok til, at de fleste mennesker ikke lægger stor vægt på deres købekraft mindskes. Og når først seddelpriisen har fået udgangspunkt i hvad der før var mild inflation, med et tryk på en øjere inflation. Som Friedrich Hayek påpegede, er det dog usynligt, at det ved at føre mild inflation som regel til decideret inflation.

En mild, stabil inflation hjælper ikke - den kan kun hjælpe til med at dæmpe inflation.“

## 9.1.: Hyperinflation in the Weimar Republic (1923)

tion er især lusket, fordi den favoriserer dem, der har seddelpresserne. Det tager tid for de nyskabte værdier og priserne at tilpasse sig, så hvis du er i stand til at have mere penge, før alle penge devalueres, er du foran i tiden. Det er også derfor, at inflation kan ses som en skat, der staten i sidste ende tjener på det, mens alle andre betale prisen.

„Jeg tror ikke, det er en overdrivelse at sige, at historie i høj grad omhandler inflation, og som regel er det en inflation, der er skabt af stater for deres egen vind i skyld.“

– Friedrich Hayek

n ikke ske i mit land“ tænker du sikkert. Det tænker du er fra Venezuela, som i øjeblikket lider af høj en inflationsrate på over 1 million procent er værdiløse. [75]

Det måske ikke inden for de næste par år, eller måske bruges i dit land. Men et blik på listen over lande<sup>5</sup> viser, at det uundgåeligt vil ske over en tilstrækkelig periode. Jeg husker og brugte mange af de nævnte valutaer, schilling, den tyske mark, den italienske lire, den britiske sterling, det irske pund, den kroatiske dinar osv. Min bedste minde er dog den østrig-ungarske krone. Som tiden går, bliver de lande i øjeblikket bruges<sup>6</sup> vil langsomt, men sikkert ud af brug ved deres respektive kirkegårde. De vil opleve hypotekarkravene blive erstattet. De vil snart være historiske valuter, som de forældede.

– Historien har vist, at staterne uundgåeligt vil falde under presset fra inflationsprisen til at øge pengemængden.“

– Saifedean Ammous

t i første omgang - men den værdi, det har, vil i de samme størrelsesorden.

en monetær vare eller valuta er god til at fastholde over tid og rum, anses den for at være *hård*. Hvis en valuta ikke kan fastholde sin værdi, på grund af nem forringning, betragtes den som en *blød* valuta. Begrebet har her nævnt for at forstå Bitcoin og fortjener en grundigere analyse. Vi vil tage emnet op igen i den sidste økonomiske artikel om penge.

hånden som flere og flere lande rammes af hyperinflation og flere mennesker blive nødt til at forholde sig til en med hårde og bløde penge. Hvis vi er heldige, vil bankchefer måske endda blive tvunget til at revurdere deres økonomopolistiske strategier. Uanset hvad der måtte ske med Bitcoin, jeg har fået takket være Bitcoin, sandsynligvis været en del af en ny historisk udvikling uanset udfaldet.

**Nu har lært mig om den skjulte skat ved inflationsproffen forbundet med hyperinflation.**



som tilbage igen og sa sig ængsteligt omkring,  
som om den havde mistet noget. . . “

– Lewis Carroll, *Alice i Eventyrland*

di er på en måde paradoksal, og der er flere teorier at forklare, hvorfor vi værdsætter visse ting fremst. Dette paradoks har mennesker været opmærksomme på over hundre år. Som Platon skrev i sin dialog med Sokrates, værdsætter vi nogle ting, fordi de er sjældne, og andre af deres nødvendighed for vores overlevelse.

„Og hvis du er fornuftig, vil du også give dette råd til mine elever - at de aldrig skal konversere med nogen, der er helt ortset fra dig og hinanden. For det er det sjældne, som er dyrebart, mens vand er det billige, skønt det er det bedste, som Pindar sagde.“

– Platon

Detne paradoks af værdi<sup>3</sup> viser noget interessant om os: Det virker, som om vi værdsætter ting på et særdeleskag, men gør det med visse ikke-tilfældige kriterier. Noget kan være *dyrebart* for os af forskellige årsager, men ting kan også dele visse karakteristika. Hvis vi let kan kopiere

attes (en tabt privat nøgle er tabt for evigt) og gør os at udføre nogle ret nyttige ting. Det er udelebte værktøj til værdioverførsel på tværs af grænser, og tægtskabt over for censur og konfiskation i processen. Det er en selvstændig værdilager, der giver enkeltpersoner muligheden for at opbevare deres formue uafhængigt af banker og andre institutioner. Og det er ikke et værktøj til at nævne et par ting.

**Det er ikke et værktøj til at nævne et par ting.**

*Holdt jeg alle mine lemmer meget smilende,  
Ved brug af denne salve,  
Fem shillinger pr. æske –  
Tillad mig at sælge dig et par stykker.“*

– Den vise

I er penge? Vi bruger dem hver dag, men alligevel gsmål overraskende svært at besvare. Vi er afhængigt af dem, de er både store og små, og hvis vi har for få, bliver vores dage lidt uhyggelige. Alligevel tænker vi sjældent over den ting, der har gjort en stor forskel i verden til at dreje rundt. Bitcoin har tvunget mig til at tænke på det samme spørgsmål igen og igen: Hvad pokker er penge?

Det er et spørgsmål, som „moderne“ verden vil de fleste nok tænke på på en anden måde end de taler om penge, selvom de fleste af vores penge er opbevaret i en bankkonto. Vi bruger allerede nuller og ettedekomminalt penge, så hvordan er Bitcoin anderledes? Bitcoin er anderledes, fordi det i sin kerne er en meget anderledes type penge, vi bruger i øjeblikket. For at forstå dette skal vi se nærmere på, hvad penge er, hvordan de har fungeret i historien og hvordan guld og sølv blev brugt i det meste af handelshistorien.

nnesker brugt alle mulige ting som penge: perle  
e materialer som elfenben, skaller eller særlige k  
e slags smykker og senere sjældne metaller so

den forstand minder den (Bitcoin) mere om en  
elmetal. I stedet for at udbuddet ændrer sig for  
holde værdien den samme, er udbuddet forudbe  
mt, og værdien ændrer sig.“

– Satoshi Nakamoto

de dogne væsener vi er, tænker vi ikke så meget  
bare fungerer. For de fleste af os fungerer penge  
som med vores biler eller computere er de fleste  
get til at tænke over disse tings indre funktion, i  
ammen. Folk, der har set deres livsopsparing forv  
af hyperinflation, kender værdien af stærke peng  
der har set deres venner og familie forsvinde på  
nhederne i Nazityskland eller Sovjetunionen forst  
ivatliv.

erlige ved penge er, at de er altomfattende. Pe

– Ron Pa

in fjerner denne magt på fredelig vis, da den fjerner  
af penge uden brug af magt.

gene gennemgik flere iterationer. De fleste iterationer  
De forbedrede vores penge på den ene eller anden måde.  
r ganske nylig blev vores penges indre funktioner  
r næsten alle vores penge simpelthen skabt ud af magthaverne. For at forstå, hvordan det kunne ske,  
at lære om pengenes historie og efterfølgende unngå det vil kræve en række katastrofer, eller blot en encesindsats for at rette op på denne korruption,  
eg beder til guderne for stabile penge om, at det

**n har lært mig, hvad penge er.**



venner havde givet dem, sasom at hvis man går ind i ilden, vil den brænde en, og at hvis man skærer sig meget dybt i fingeren med en kniv, bløder det som regel, og hun havde aldrig glemt, at hvis man drikker af en flaske, hvorfra der står 'gift', er det næsten sikkert, at det giver problemer før eller siden.“

– Lewis Carroll, *Alice i Eventyrland*

ge mennesker tror, at penge er understøttet af guld i store bankbokse, beskyttet af tykke mure. Det har været sandt for mange årtier siden. Jeg er ikke selv tænkte dengang, for jeg var i meget større problem omkring, hvordan et land med et hovedstørstort set ingen forståelse af guld, papirpenge, eller et andet værditegn, kunne være understøttet af noget.

El af processen med at lære om Bitcoin er at få et overblik over, hvad de betyder, hvordan de opstod, og hvorfor de er vigtige. Og hvordan den bedste idé, vi nogensinde har haft. Så hvad er der egentlig? Og hvordan endte vi med at bruge dem? De er ikke noget, der er pålagt ved *fiat*, betyder det blot, at det er et teknologisk løsning, der er en formel godkendelse eller et forslag. Således er de ikke penge, blot fordi *nogen* siger, at de er penge. Da er de ikke penge.

kammerater.

n af fiat-penge stammer ikke fra deres indby  
per. Hvor gode en bestemt type fiat-penge er, h  
nen med den politiske og skattemæssige ustabil  
drømmer dem frem. Deres værdi pålægges ved

r nylig brugte man to typer af penge: **varepenge**  
ulde *ting*, og **repræsentative penge**, som blot  
den værdifulde ting, for det meste på skrift.

allerede været inde på varepenge ovenfor. Foll  
e knogler, muslingeskaller og ædelmetaller som  
lev det især mønter lavet af ædelmetaller som g  
blev brugt som penge. Den ældste mønt, der ind  
et fundet, er fremstillet af en naturlig blanding af g  
lev produceret for mere end 2700 år siden.<sup>1</sup> Hvis  
I Bitcoin, er det ikke konceptet *coin* (mønt).

2.2.: Lydisk mønt. Billedet er licenseret under Commons Attribution Share-Alike 4.0 af Numismatic Group, Inc.

viser sig, at hamstring af mønter, eller *hodling*, for sprogs sprog, er næsten lige så gammelt som mønter. Nønhamstrer var en person, der lagde næsten alle mønter i en krukke og begravede den i fundamentet, som først blev fundet 2.500 år senere. Det er en opbevaring, hvis du spørger mig.

af ulempene ved at bruge ædelmetalmønter er, at de er afklippet, hvilket effektivt forringes møntens værdi. Mønterne kan ikke blive præget af de afklippede mønter, hvilket øger deres værdi over tid og devaluerer hver enkelt mønt i pris. Det harberede bogstaveligt talt så meget af deres værdi, at de kunne slippe afsted med.

Stater kun er glade for inflation, hvis det er dem, der har gjort det. Men, blev der gjort en indsats for at stoppe denne udvikling. På klassisk politi-og-røver-manér blev mønterne



## 12.3.: Sølv mønter med varierende grad af afklipning

en stadig kan ses den dag i dag. Tiden med nem var forbi.

med disse metoder til devaluering af mønter<sup>2</sup> holdt adig andre problemer. De er klodsede og ikke at transportere, især når der skal ske store været er ikke særlig praktisk at dukke op med en størs, hver gang du vil købe en Mercedes.

aler om tyske ting: Hvordan den amerikanske dollar har en anden interessant historie. Ordet „dollar“ er et ikke ord *Thaler*, en forkortelse for *Joachimsthaler*. Joachimsthaler var en mønt, der blev præget i byen Joachimsthal. Thaler er simpelthen en forkortelse for nogen, der kommer fra dalen, og fordi Joachimsthal var en møntproduktion, omtalte folk simpelthen disse sølv mønter. Thaler (tysk) blev til daalders (hollandsk) og



2.4.: Den oprindelige „dollar“. Sankt Joachim er med sin kappe og troldmandshat. Billedet er af Wikipedia-bruger Berlin-George

reelsen af repræsentative penge indvarslede d  
s undergang. Guldcertifikater blev introduceret i  
g femten år senere blev sølvdollaren også langs  
erstattet af gældsbeviser: sølvcertifikatet. [99]

tog omkring 50 år fra introduktionen af de fø  
ater, til disse stykker papir blev forvandlet til no  
ville genkende som en amerikansk dollar.

ærk, at den amerikanske sølv-dollar fra 1928 i t  
går under navnet *sølvcertifikat*, hvilket indikerer  
blot et dokument, der angiver, at indehaveren  
papir har krav på et stykke sølv. Det er interessant,  
at teksten, der indikerer dette, er blevet mindre  
over tid. Sporet af „certifikat“ forsvandt helt efter  
en kort tid, således at man nu bare har et



5.: En amerikansk sølv dollar fra 1928. „Betales til dehaveren på forespørgsel.“ Billede cc-by-sa National Numismatic Collection ved the Smithsonian Institution

Det kunne indløses til guldmønter, var sandsynligvis forbedring. Papir er mere praktisk, lettere, og da det er vilkårligt blot ved at printe et mindre tal, er det let at udskifte mindre enheder.

Det minde indehaverne (brugerne) om, at disse certifikater var representative for ægte guld og sølv, blev de farvet i orange hermed, og det fremgik tydeligt af selve certifikatet, da skriften flydende fra top til bund.

Dette bekræfter, at der er deponeret et hundredtals guld i guldmønt i USA's skatkammer, som kan udskiftes til ihændehaveren på forespørgsel.“

Det blev ordene „PAYABLE TO THE BEARER ON DEMAND“



2.6.: Dette er et amerikansk 100 dollars guldchein fra 1928. Billedet er cc-by-sa fra National Numismatic Collection, National Museum of American History.

var papiret og dermed statens mulighed for at udskifte sedler, som den ønsker.

Affelsen af guldstandarden i 1971 fuldendte en rede-lange trick. Penge blev forvandlet til den i kongemandoen over en hær og driver fængsler, siger, som man tydeligt kan læse på enhver dollarseddel i dag: „DENNE SEDDEL ER LOVLIGT BETALINGEN“. Med andre ord: Den har værdi, fordi sedlen siger,

at der er en anden interessant lektion i nutiden skjult i det åbne. På den anden linje står der, at



7.: En 20-dollarseddel fra 2004-serien, der bruger  
‘DENNE SEDDEL ER LOVLIGT BETALING  
DEL’

har set, blev guld og sølv brugt som penge i årtusinderne. Men da man blev mønter lavet af guld og sølv erstattet af papir, var det ikke længere accepteret som betaling. Denne accept skal dog ikke overvirke os om, at papiret i sig selv har værdi. Det er dog ikke helt at afbryde forbindelsen mellem repræsentation og værdi. Det er dog et politisk ønske: at afskaffe guldstandarden og overbevise os om, at papiret i sig selv er værdifuldt.

**Har lært mig om pengenes historie og det største økonomiens historie: fiat-valuta.**

*ved med at vokse og vokse, og snart matte hun knæle ned på gulvet. Men lidt efter var der ikke engang plads til det, og hun prøvede nu at lægge sig helt ned, med den ene albue mod dører og den anden under hovedet. Hun blev imidlertid ved med at vokse, og til sidst havde hun ingen anden udvej end at stikke den ene arm ud ad vinduet og fodden op i skorstenen. Så sagde hun: „Nu kan jeg ikke gøre mere, hvad der end sker. Hvor skal der dog blive af mig?“*

– Lewis Carroll, *Alice i Eventyrland*

di og penge er ikke trivielle emner, især ikke i vores samfund. At få penge i handlen med at skabe penge i vores banksystem er heller ikke et nyt koncept. Og jeg kan ikke slippe følelsen af, at det er blevet mere komplikerede end nogensinde. Det er dog ikke kun er stødt på i akademiske og juridiske tekster, men også i almindelig praksis i finansverdenen. Det er ikke enkle vendinger, ikke fordi det virkelig er kompleks, men fordi det er skjult bag lag på lag af fagsprog og teknik. Det er ikke kompleksitet. „Ekspansiv pengepolitik, kvantitativ finanspolitiske stimuleringer af økonomien.“ Publikum er ikke kendende, hypnotiseret af de fancy ord.

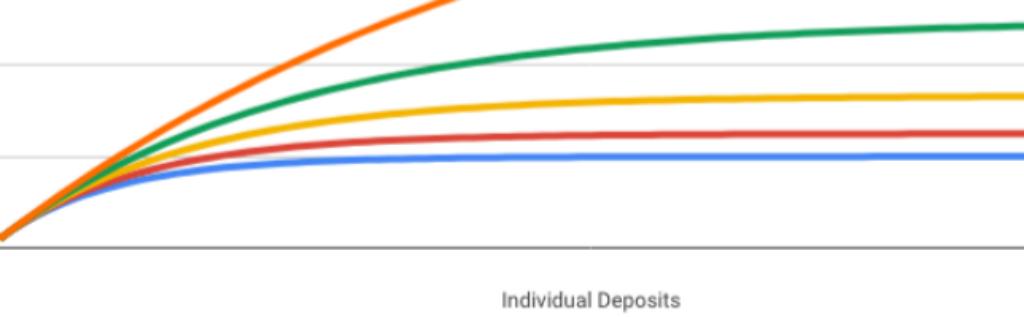
reservebankvæsen, hvilket betyder, at bankerne låne penge ud, som de faktisk ikke har! Det er en stor skandale, og den har stået på alt for længe. Det er falskmøntneri - nogle gange kaldet kvantitativt opspil - et andet navn for falskmøntneri. Den kunne være trykning af penge, som, hvis den var foretaget af en almindelig person, ville sende dem i fængsel et par dage - og det ville tage lang tid og indtil vi begynder at sende banknoter tilbage til landet - og jeg inkluderer centralbankfolk og politikere - fængsel for denne skændsel, vil den fortsætte.“

– Godfrey Bloom

Det er vigtigt at gentage den vigtigste del: Banker kan udlåne penge, selvom de faktisk ikke har.

Hvis man ikke ønsker at være brøkreservebankvæsen, behøver en bank bare en lille *brøkdel* af hver krone, der bliver sat ind. Det kan være 0 eller 10%, som regel i den lave ende, hvilket er altid bedre end nu værre.

Det er vigtigt at bruge et konkret eksempel til bedre at forstå den. Hvis en bank har en brøkdel af 10% er tilstrækkeligt, og vi bør være sikre på at tage alle beregningerne i vores hoved. Så hvis du har 100 dollars i banken - fordi du ikke vil gemme dem



Figur 13.1.: Pengenes multiplikatoreffekt

wad gør bankerne med resten af pengene? Hvad  
ne 90 dollars? De gør, hvad banker gør, de låner  
mennesker. Resultatet er en pengemultiplikatoref-  
engemængden i økonomien enormt (figur 13.1).  
e indskud på \$100 vil snart blive til \$190. Ved  
de nyoprettede \$90, vil der snart være \$271 i øk-  
43,90 derefter. Pengemængden øges rekursivt, t-  
gstaveligt talt låner penge, som de ikke har. [93]  
abra cadabra forvandler bankerne på magisk vis  
1.000 dollars eller mere. Det viser sig, at en ti-fo-  
n er nemt. Det tager kun nogle få lånerunder.

S&P 500  
2,440.99 ↑0.64%

BREAKING  
NEWS

YELLEN: I'M STRONGLY OPPOSED TO  
AUDIT THE FED

2.: Yellen (direktør for den amerikanske centralbank) er en stærk modstander af en revision af den amerikanske centralbank (Federal Reserve), mens *Sign Guy* i baggrunden stærkt argumenterer for bitcoin.

Hansiel regulering, delvist offentlige, delvist private med noget, der påvirker os alle og som er en del af vores samlede civilisation, og gør det skamløst. De er kunderne i den nærmeste fremtid, og tilsyneladende uden ansvarlighed eller mulighed for revision (se figur 1).

Bitcoin stadig er inflationær, vil den snart ikke være det? Det strengt begrænsede udbud på 21 millioner bøger vil dog ende helt fjerne inflationen. Vi har nu to mon-

nomer der følger den østrigske skole) og bitcoins  
slutte sig til det stadig voksende internet af pen-  
oppe dem, hvis de vælger at gøre det.

**n har lært mig, at brøkreservebankvæsen er**



*selv, mens hun vandrede rundt i skoven, „er at vokse til min rette størrelse, og det andet er at finde vej ind i den dejlige have. Jeg tror, at det vil være den bedste plan.“*

– Lewis Carroll, *Alice i Eventyrlandalen*

vigtigste lektion, jeg har lært fra Bitcoin, er, at stabeligheden lange bane er overlegne i forhold til svaghepenge, også omtalt som *stabile penge*, er enhver valuta, der fungerer som et pålideligt værdilagelse. Følgelig er Bitcoin stadig ung og volatil. Kritikere vil ikke lagrer værdi pålideligt. Volatilitetsargumentet. Volatilitet er forventeligt. Det vil tage markedet nedsænke ud af, hvad den rette pris er for disse nye penge. Det ofte påpeges i spøg, er det baseret på en målestokker i dollars, vil du ikke være i stand til at se, at der er en være én bitcoin værd.

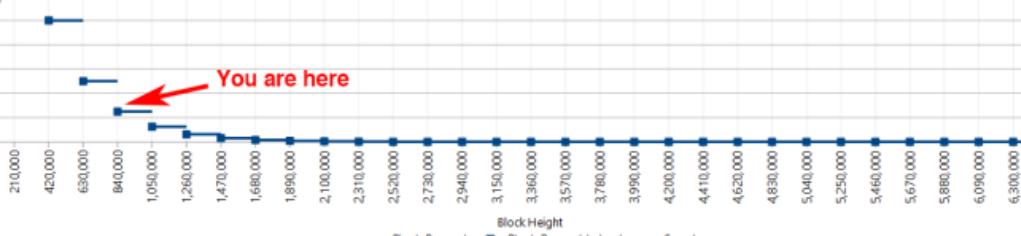
„En fast pengemængde, eller en pengemængde, der kun ændres i overensstemmelse med objektivt beregnelige kriterier, er en nødvendig betingelse for en meningsfuld og retfærdig prisfastsættelse af penge.“

n hurtig tur gennem de glemte valutaers kirkegård, der kan trykkes, blive trykt. Indtil nu har været i stand til at modstå denne fristelse.

håndterer fristelsen til at trykke penge på en gen? Han var bevidst om vores grådighed og fejlbarlighed, han noget mere pålideligt end menneskelig tilbagematematik.

Denne formel er nyttig til at beskrive Bitcoins opfindelse. I virkeligheden ikke findes nogen steder i koden. Udstedelsen sker på en algoritmisk kontrolleret måde ved at give en belønning, der udbetales til minedriverne hver gang. Formlen ovenfor bruges til hurtigt at opsummere alt, der sker under overfladen. Hvad der virkelig sker, kan bedre beskrives på ændringerne i blokbelønningen, belønningen, der tilføjes til den, der finder en gyldig blok, hvilket sker cirka

hver 10 minutter. Logaritmfunktioner og eksponentiale er ikke lidt svært at forstå. Begrebet *soliditet* er måske lettere at forstå.



Figur 14.2.: Bitcoins kontrollerede udbud

heden af en fiat-valuta afhænger af, hvem der har de respektive trykpresser. Nogle stater kan være i stand til at trykke større mængder valuta end andre, hvilket gør dem i svagere valuta. Andre stater kan være mere respektive pengetrykning, hvilket resulterer i en hårdere valuta.

„Et vigtigt aspekt af denne nye virkelighed er, at institutioner, som den amerikanske centralbank, ikke kan gå konkurs. De kan trykke alle de penge, de ønsker. De har brug for til sig selv, stort set uden omkostninger.“

– Jörg Guido Hülsmann

Vi havde fiat-valutaer, blev pengenes soliditet bestemt af de egenskaber ved de ting, vi brugte som penge.

computer.

pet, der er skitseret ovenfor, kan udtrykkes mere om forholdet mellem „lager“ og „produktion“. Kort sagt, hvor meget der er af noget i øjeblikket. Til ved at holde den et mål for den aktuelle pengemængde. Det er, hvor meget der produceres over en periode. Og til gengengen til at forstå stable penge ligger i at forstå forholdet mellem lager og produktion.

Det er svært at beregne forholdet mellem lager og produktion, da mængden af penge afhænger af, hvordan man regner det. [94] Man kan nøjes med at tælle pengesedler (M0), tilføje rejsechecks og indlån (M1), inkludere bankkontoer og investeringsforeninger samt nogle andre ting, og tilføje indskudsbeviser til det hele (M3). Desuden varierer det fra land til land, hvordan alt dette defineres og hvad der inkluderes. Da den amerikanske centralbank stoppede med at offentliggøre tal for M3, må vi nøjes med den monetære form. Jeg ville elske at få bekræftet disse tal, men jeg tror, at jeg har nødt til at stole på den amerikanske centralbank. Guld er et af de sjældneste metaller på jorden, og forholdet mellem lager og produktion. Ifølge US Geologisk Survey er der i verden omkring 160.000 ton guld.

har et højere forhold mellem lager og produktion  
grundens til, at guld indtil nu har været de hårdes  
des. Det siges ofte, at alt det guld, der er udvun-  
ne kunne være i to svømmebassiner af olympisk  
størrelse beregninger<sup>3</sup>, ville vi have brug for fire. Så m-  
øget opdateres, eller også er svømmebassiner i  
verden blevet mindre.

Gejstet til Bitcoin. Som du nok ved, har bitcoin-mining blivt populært i de seneste år. Dette skyldes, at vi stadig har en række af det, der kaldes *belønnings-æraen*, hvor minerne bliver belønnet med *en masse* bitcoin for deres beregningssats. Vi er i øjeblikket i belønnings-æra nummer 3, der begyndte i 2016 og vil slutte i begyndelsen af 2020, sandsynligvis. Da den totale bitcoin-forsyningen er forudbestemt, tillader Bitcoin-satsen kun omkostninger, der fungerer som funktioner kun omkostninger. Ikke desto mindre kan man ikke forudsige med sikkerhed, hvor høj Bitcoins forhold mellem produktion vil være. Spoiler alert: det vil være højt. Hvor højt? Det viser sig, at Bitcoin vil blive uendeligt dyrt (se figur 4.4).

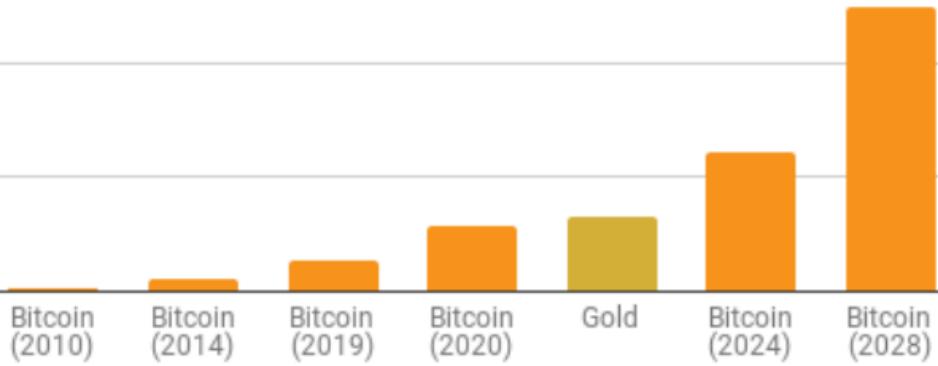
Det er grund af en eksponentiel nedgang i minedriftbeløb, når produktionen af nye bitcoin aftager, hvilket resulterer i en

#### 4.: Visualisering af forholdet mellem lager og produktion for USD, guld og Bitcoin

Ere eksponentialfunktionens kraft vil antallet af udvundet per år, falde til under 100 bitcoin om 50 år, til 100 guld om 75 år. Den globale vandhane, som er i gang, vil tørre ud omkring året 2140 og effektivt stoppe produktionen af bitcoin. Dette er et langt spil. Hvis du læser denne artikel nu, er det stadig tidligt på den.

Bitcoin nærmer sig et uendeligt forhold mellem lager og produktion, vil den være de mest stabile penge, der findes. Det er en realitet, men svært at få overbevisning om.

Med økonomiske briller er Bitcoins *vanskelighedsjustering* den vigtigste komponent. Hvor svært det er at udvindende nye bitcoins afhænger af, hvor hurtigt nye bitcoins bliver udvundet.<sup>4</sup> Denne teknologiske justering af netværkets minedrifts-sværhedsgrad er muligt for os at forudsige dens fremtidige udvikling. Denne justeringsalgoritmen for sværhedsgrad kan ikke ændres ved at ændre virksomheden fra dens dybde, men justeringen af sværhedsgraden kan ændres ved at ændre algoritmen af sværhedsgraden.



#### 4.5.: Stigende forhold mellem lager og produktion af bitcoin sammenlignet med guld

edrift, vil Bitcoins kontrollerede udbud ikke blive forvetning til enhver anden ressource, uanset hvor meget en vil lægge i at mine bitcoin, vil den samlede lade.

Som at  $E = mc^2$  dikterer den universelle hastighed i vores univers, dikterer Bitcoins vanskelighedsjustering den **suelle pengegrænse** i bitcoin.

det ikke var for denne vanskelighedsjustering, der allerede være blevet udvundet. Hvis det ikke var for vanskelighedsjustering ville Bitcoin sandsynligvis ikke

et du prøver.

**Har lært mig, at stabile penge er essentielle.**

**Del III.**

**Teknologi**



„...og jeg ville også have sagt  
at hun til sig selv. Så tog hun den lille guldnøgle og  
åbnede døren ud til haven

– Lewis Carroll, *Alice i Eventyrland*

ne nøgler, ure, der kun virker ved et tilfælde, k  
mærkelige gåder og bygherrer uden ansigter ell  
er lyder som eventyr fra Eventyrland, er dagligdag  
en.

vi undersøgte i kapitel II, Store dele af det nu  
elle system er systematisk ødelagt. Ligesom Alice  
be på at klare os bedre denne gang. Men takket  
onym opfinder har vi en utrolig sofistikeret teknologi  
os denne gang: Bitcoin.

se problemer i et radikalt decentraliseret og fjendtlig  
unikke løsninger. Hvad der ellers ville være trivende  
at løse, er alt andet end det i denne mærkelige  
punkt. Bitcoin er afhængig af stærk kryptografi  
ninger, i hvert fald hvis man ser på det med teknisk  
Hvor stærk denne kryptografi er, vil blive udforske  
ende lektioner.

væg dig langsomt, og undga at ødelægge ting

watlivet er ikke dødt

opherpunks skriver kode

metaforer for Bitcoins fremtid

næste lektioner udforsker den teknologiske udvikling som uden tvivl er lige så vigtig som selve teknologi. Det er ikke den næste skinnende app på din telefon. Det er et for en ny økonomisk virkelighed, og derfor bør vi se som finansiel software af atomreaktor-kvalitet. Hvor finder vi os i denne økonomiske, samfundsma- logiske revolution? Fortidens netværk og teknologien metaforer for Bitcoins fremtid, der udforskes i de næste kapitler i dette kapitel.

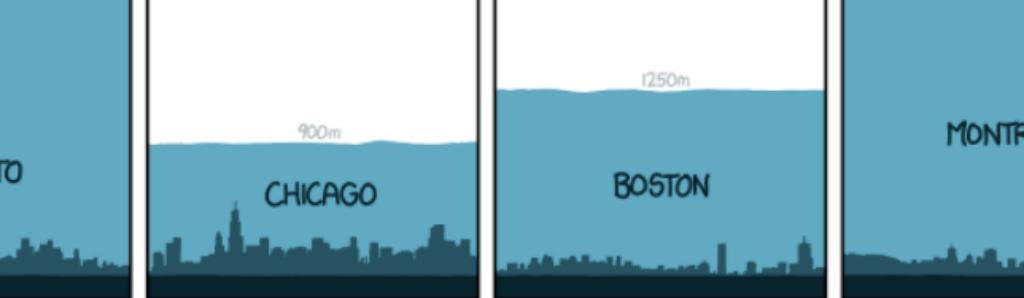
Den gang skal du spænde dig fast og nyde turen. Eksponentielle teknologier, er vi på vej mod himlen?

ge seks er tretten, og fire gange syv er fjorten  
- åh nej! Jeg når aldrig op på tyve med den ha-  
stighed!"

– Lewis Carroll, *Alice i Eventyrland*

er en vigtig del af vores hverdag. Store tal er dog ikke noget, som de fleste af os er fortrolige med. De største transaktioner, vi har i hverdagen, er i størrelsesordenen millioner, ikke milliarder eller billioner. Vi kan læse om millioner af mennesker i fællesskab med et par hundrede tusind dollar af dollars brugt på redningspakker til banker og andre institutioner i statsgæld. Selvom det er svært at finde hovedtal i de større overskrifter, er vi nogenlunde fortrolige med størrelsesordningen.

Hvorfor er det dog, at vi måske er fortrolige med milliarder og billioner, men vores intuition allerede at svigte når vi arbejder med størrelsesordenen. Har du en fornemmelse af, hvor lang tid der tager på, at der går en million/milliard/trillion sekunder? Hvis du ikke gæsos mig, er du fortapt uden faktisk at regne på det. Lad os nærmere på dette eksempel: Forskellen mellem et sekund og en millionsekund er næsten udtørlende. Det er dog ikke tilstigning på tre størrelsesordener:  $10^6$ ,  $10^9$ ,  $10^{12}$ . Det er derfor meget nyttigt at tænke i sekunder, så lad os omsætte de store tal:



1.: For omkring 1 billion sekunder siden. Kilde  
1225

2: For en billion sekunder siden var Manhattan et tykt lag is.<sup>1</sup>

Det vi bevæger os ind i den moderne kryptografis ære, svigter vores intuition katastrofalt. Bitcoin er et store tal og den næsten umulige opgave, der. Disse tal er langt, langt større end noget, vi kan til dag. Mange størrelsesordener større. At disse tal i virkeligheden er, er afgørende for alt om helhed.

Kigge nærmere på SHA-256<sup>2</sup>, en af hash-funktiones i Bitcoin, som et konkret eksempel. Det er kun ikke på 256 bits som „to hundrede og seksoghalv

„SHA-256 er meget stærk. Det er ikke som det f  
ise skridt fra MD5 til SHA1. Den kan holde i f  
rtier, medmindre der opstår et massivt gennembr  
angreb.“

– Satoshi Nakam

os skære det ud i pap.  $2^{256}$  er lig med følgende ta

115 kvattuordecillioner 792 tredecillioner 89 du  
illioner 237 undecillioner 316 decillioner 195 nove  
cillioner 423 oktodecillioner 570 septendecillio  
85 sexdecillioner 8 quindecillioner 687 quattuo  
illioner 907 tredecillioner 853 duodecillioner 269  
ecillioner 984 kvintilliard 665 kvintillion 640 kvad  
rd 564 kvadrillion 39 trilliard 457 trillion 584 billion  
illioner 913 miliarder 129 millioner 639 tusind 93

er mange kvintillioner! Det er stort set umuligt at f  
Der er intet i det fysiske univers at sammenligne  
langt større end antallet af atomer i det observer  
en menneskelige hjerne er simpelthen ikke skab

# 4 Billion



2.: Illustration af SHA-256-sikkerhed. Original g  
Grant Sanderson også kendt som 3Blue1Brown

e bedste visualiseringer af den sande styrke i SH  
eo af Grant Sanderson. Den hedder meget pas  
ure is 256 bit security?“<sup>5</sup> Den viser på smukke  
et 256-bit rum er. Gør dig selv en tjeneste og br  
på at se den. Som alle andre 3Blue1Brown-vide  
bare fascinerende, men også usædvanligt god

Du falder måske ned i et matematisk kaninhul.

Schneier [65] brugte de fysiske grænser for bereg  
lette tal i perspektiv: Selv hvis vi kunne bygge en  
, som ville bruge al energi til rådighed, til at flip  
7], bygge en Dyson-sfære<sup>6</sup> rundt om vores sol  
i 100 milliarder milliarder år, ville vi stadig kun h

er svært at overdrive betydningen af dette. Stærke vrede kan ender op og ned på magtbalancen i den fysiske verden, og der er så vant til. Ubrydelige ting findes ikke i denne verden. Hvis du bruger tilstrækkelig kraft, vil du kunne ødelægge en dør, kasse eller skattekiste.

En bitcoins skattekiste er meget anderledes. Den er sikret med et kryptografisk system, som ikke giver plads til brute force. Og så langt som de gældende matematiske antagelser holder, er brute force-angreb, vi har. Bevares, der er også risikoen for et globalt kollaps ved 215 skruenøgler (figur 15.3) Men tortur vil ikke virke, da der ikke findes enkeltin-adresser, og bitcoins kryptografiske vægge vil ikke falde under brute force-angreb. Selv hvis du angriber med en supercomputer, vil det være en sole, bogstaveligt talt.

Det er dog ikke kendsgerningen og dens implikationer blev gribet i opfordringen til at benytte kryptografiske vægge. *“Kunne man ikke komme ud af et system, hvis man ikke har nøglen? Eller hvordan kan man få nøglen tilbage, hvis man har mistet den?”* Således skrev Bruce Schneier i et brev til den amerikanske præsident i 1993.

„Det er ikke indlysende, at verden skulle fungere på denne måde, men på én eller anden måde smidte jeg ikke mit håndkugle ud i en vægtskål.“



### 15.3.: \$Angreb med 5\$ skruenøgle. Kilde: xkcd 5

ved endnu med sikkerhed, om universets smil er et muligt, at vores antagelse om matematiske forkert og at vi finder ud af, at P faktisk er lig med at vi overraskende finder hurtige løsninger på smer [79] som vi i øjeblikket antager, er svære at skulle være tilfældet, vil kryptografi, som vi kendt at eksistere, og konsekvenserne vil højst sandsynligvis til ukendelighed.

"Vires in Numeris" = „Styrke i tal“<sup>9</sup>

*Vires in numeris* er ikke kun et fængende motto, der bruges. Erkendelsen af, at der er en ufattelig styrke i det ubetygående. Forståelsen af den omvending af den magtbalance, som det muliggør, ændrede mit syn på den fremtid, der ligger foran os.

Det eneste resultat af dette er det faktum, at du ikke behøver

## 5.4.: Eksempler på elliptiske kurver. Grafik cc-by manuel Boutet.

hed, man skal sende ansøgningsskemaer til. Du  
re et stort tal, og så er du stort set klar. Den cent  
for kontooprettelse er matematik. Og kun Gud v  
ansvarlig for det.

vin er bygget på vores bedste forståelse af virke  
n der stadig er mange åbne problemer inden for  
og matematik, er vi dog ret sikre på visse ting. At  
etri mellem at finde løsninger og validere korrek  
øsninger er en af disse ting. At beregning kræv  
inden. Med andre ord: Det er sværere at finde e  
end at tjekke, om den spidse ting i din hånd fak  
r ej. Og det kræver arbejde at finde nålen.

enorme omfang af mulige bitcoin-adresser er virk  
nde. Antallet af private nøgler er endnu højere. I  
nde, hvor meget af vores moderne verden, der k  
usandsynligheden af at finde en nål i en ubegri  
Jeg er nu mere bevidst om dette faktum end no



– Lewis Carroll, *Alice i Eventyrland*

...in sigter mod at erstatte eller i det mindste give op om konventionel valuta. Konventionel valuta er burde baseret myndighed, uanset om vi taler om lovlige valutaer som den amerikanske dollar eller moderne moneder som Fortnites V-Bucks. I begge eksempler er du tvunget til at tåle, at den centrale myndighed udsteder, administrerer og kontrollerer dine penge. Bitcoin løser denne binding, og dermed løser det også problemet, Bitcoin løser, er spørgsmålet om *tillid*.

„Det grundlæggende problem med konventionel valuta er al den tillid, der kræves for at få det til at fungere. Det, der er brug for, er et elektronisk betalingsystem baseret på kryptografiske beviser i stedet for tillid“

– Satoshi Nakamoto

...in løser tillidsproblemet ved at være fuldstændig transparent, uden en central server eller betroede parter. Ikke med tredjeparter, men betroede parter, punktum. Unikt er, at prioriteten er der simpelthen *ingen* at stole på. Ingen.

introduktionen og konklusionen af Bitcoins hvid

Konklusion: Vi har foreslået et system til elektron  
transaktioner uden at være afhængig af tillid.“

– Satoshi Nakamoto

rk, at *uden at være afhængig af tillid* bruges i en sammenhæng her. Vi taler om betroede tredjepartsheder, som du stoler på til at producere, opbevare dine penge. Det antages for eksempel, at du kører din computer.

en Thompson demonstrerede i sin Turing Award Lecture, at der er tillid et ekstremt vanskeligt koncept i beregningsteori. Når man kører et program, er man nødt til at stege op i forskellige former for software (og hardware), som i teorien kan skade det program, man forsøger at køre, på en ondsindet måde. Thompson opsummerede i sin *Reflections on Trusting Trust*, at ”Denne moralen er indlysende. Du kan ikke stole på kode, som du selv har skabt.“ [70]

Thompson demonstrerede, at selv hvis du har adgang til din computer - eller ethvert andet program, der er programmet eller hardwaren - blive kompromitteret.

To what extent should one trust a statement that a program is from horses? Perhaps it is more important to trust the people who write software.

(lines deleted)

ing s is a  
otation of the body  
rogram from '0'  
nd.

```
tif("char\ts[ ] = |\n");  
=0; s[i]; i++)  
printf("\t%d, \n", s[i]);  
if("%s", s);
```

ome simple transliterations to allow  
C programmer to read this code.

gment  
al to .EQ.  
equal to .NE.  
ement  
le character constant  
iple character string  
at to convert to decimal  
at to convert to string  
character  
line character

FIGURE 1.

mission of the Association for Computing Machinery

## 6.1.: Uddrag fra Ken Thompsons artikel 'Reflections on Trusting Trust'

```
...  
c = nextf( );  
if(c != '\n')  
    return(c);  
c = nextf( );  
if(c == '\n')  
    return('\n');  
if(c == 'n')  
    return('\n');  
...
```

FIGURE 2.2.

```
...  
c = nextf( );  
if(c != '\n')  
    return(c);  
c = nextf( );  
if(c == '\n')  
    return('\n');  
if(c == 'n')  
    return('\n');  
if(c == 'v')  
    return('v');  
...
```

FIGURE 2.1.

```
...  
c = nextf( );  
if(c != '\n')  
    return(c);  
c = nextf( );  
if(c == '\n')  
    return('\n');  
if(c == 'n')  
    return('\n');  
if(c == 'v')  
    return('v');  
...
```

FIGURE 2.3.

The moral is obvious. You can't not totally create yourself. (Especially companies that employ people like source-level verification or scrubbers from using untrusted code.)

```
compile(s)  
char *s;  
|  
|  
|
```

FIGURE 3.

```
compile(s)  
char *s;  
|  
if(match(s, "pat")  
compile();  
return;  
|  
|  
|
```

FIGURE 3.

```
compile(s)  
char *s;  
|  
if(match(s, "pat")  
compile();  
return;  
|  
if(match(s, "pat")  
compile();  
return;  
|  
|  
|
```

FIGURE 3.

## 2.: Fra *Stealthy Dopant-Level Hardware Trojans* af er, Regazzoni, Paar, Burleson

...e al din software og al din hardware (assemblerede  
kere osv.) fra bunden uden hjælp fra eksterne  
ware-understøttet maskineri.

„Hvis du ønsker at lave en æbletærete helt fra buren,  
, skal du først opfinde universet.“

– Carl Sagan

*Thompson hack* er en særlig genial bagdør der er svær at opdage, så lad os tage et hurtigt kig på en bagdør, der er svær at opdage, som fungerer uden ændringer i softwaren. Forskere har udviklet en metode til at kompromittere sikkerhedskritisk hardware ved at ændre polariteten af urenheder i silicium. [9] Basert på de fysiske egenskaber af det materiale, som computeren er lavet af, var de i stand til at kompromittere en krysalldrevet tilfældig talgenerator. Da denne ændring ikke er synlig uden bagdør ikke opdages ved optisk inspektion, hvilket er en af de vigtigste mekanismer til afsløring af manipuleringer.

„Stol ikke. Bekræft.“

– Bitcoinere over

Instående eksempler burde illustrere, at *tillidslosning* er utopisk. Bitcoin er nok det system, der kom nærmest denne utopi, men det er stadig *tillidsminimeret*. Det er ikke muligt at fjerne tillid, hvor det er muligt. Man kan sige, at det er uundgåeligt, da du også bliver nødt til at stole på, at du har brugt den rette mængde energi, at P ikke er lig med NP, og at du faktisk har en mulighed for at få adgang til kryptologisk kærligheden og ikke er fanget i en simulation af omgivelserne.

Det er dog muligt at udvikle mere sikre protokoller, der bygger på værktøjer og procedurer for at øge tilliden. Et eksempel på et slikt system er Gitian<sup>4</sup>, som er en softwaredistribution, der genererer deterministiske builds. Ideen er, at hvis flere uafhængige personer kan reproducere identiske binære filer, reduceres risikoen for at være blevet manuelt manipuleret. Fancy bagdøre er ikke den eneste teknologi, der kan bruges til dette formål. Simpel afpresning eller pengeafpresning er også teknikker, der kan bruges til at øge tilliden. Som i hovedprotokollen, bruges decentralisering til at øge tilliden.

## Figur 16.3.: Hvad kom først, hønen eller ægget?

er funktionelt erklæret pakkehåndtering, hvilket  
er reproducerbare bit-for-bit. Resultatet er, at du  
behøver at stole på nogen softwareleverende siste  
bekræfte, at den serverede binære fil ikke er  
ret ved at genopbygge den fra bunden. For nylig  
er godkendt til at integrere Guix i Bitcoins byggeplattform.  
vis er Bitcoin ikke afhængig af en enkelt algoritme  
stykke hardware. En effekt af Bitcoins radikale design  
er en distribueret sikkerhedsmodel. Selvom man ikke  
å de bagdøre, der er beskrevet ovenfor, er det usandsynligt  
e software-tegnebøger, alle hardware-tegnebøger,  
fiske biblioteker, alle knudepunkts-implementeringer  
ilere i alle sprog er kompromitterede. Det er muligt  
andsynligt.

rk, at du kan generere en privat nøgle, uden at vælge  
f computerhardware eller -software. Du kan slå på  
et par gange, men afhængigt af din mønt og kastet  
de til tilfældighed måske ikke tilstrækkeligt tilfælde  
nd til, at lagringsprotokoller som Glacier<sup>7</sup> råder over  
ninger af konsistensitet som en af to kilder til kontrollert





siges ofte, at bitcoins udvindes, fordi tusindvis af ejder på at løse *meget komplekse* matematiske problemer skal løses, og hvis du beregner det rigtige "priser" du bitcoins. Selvom denne forenklede optælling med minder mørke om at løse bestemte matematiske problemer. Matematikken er heller ikke særlig kompleks, men det mest komplekst, er *at fortælle tiden* i et decentraliseret system. Beskrevet i hvidbogen er bevis-for-arbejde-systemet (det mineredrift eller mining) en måde at implementere et tidsstempelsystem på.

Når jeg først lærte, hvordan Bitcoin fungerer, tænkte jeg, at arbejde-for-bevis er ineffektivt og spild af tid. Efter et par timer i et koldt værelse i et teknisk laboratorium, hvor jeg satte sammen et computerprogram til at løse de matematiske problemer, så jeg kunne få et beløb i bitcoins, fandt jeg ud af, at arbejde-for-bevis ikke var et spild af tid, men et godt eksempel på, hvordan teknologi kan løse et teknisk problem.

A peer-to-peer version of electronic cash would allow online payments directly from one party to another without going through a bank. Digital signatures provide part of the solution, but the main trusted third party is still required to prevent double-spending. To solve the double-spending problem using a peer-to-peer network, transactions by hashing them into an ongoing chain of work, forming a record that cannot be changed without redoing the longest chain not only serves as proof of the sequence of events but also proves that it came from the largest pool of CPU power. As the power of CPU power is controlled by nodes that are not cooperating to

### 3. Timestamp Server

The solution we propose begins with a timestamp server. A timestamp is a hash of a block of items to be timestamped and widely published in a newspaper or Usenet post [2-5]. The timestamp proves that the data existed in a particular format at a certain time, obviously, in order to get into the hash. Each timestamp includes its hash, forming a chain, with each additional timestamp reinforcing the previous ones.



### 4. Proof-of-Work

ge  
or-arbejde er et system, hvor alle kan validere, hvilken rækkefølge det skete. Denne uafhængighed, der fører til konsensus, en enighed mellem dem, hvem der ejer hvad.

Ikalt decentraliseret miljø har vi ikke den luksus at have en central administrator. Ethvert ur ville introducere en betroet tredje punkt i systemet, som man skulle stole på, og som

„Timing er det grundlæggende problem,“ som Satoshi Nakamoto påpeger [72]. Dette problem løste Satoshi genialt ved at implementere et decentraliseret ur via en blokkæde, der opbygges på bevis-for-arbejde. Alle er på forhånd enige om, at den mest akkumulerede arbejde er kilden til sandhed. Det er definition det, der faktisk skete. Denne aftale er det, der definerer Nakamoto-konsensus.

Netværket tidsstempler transaktioner ved at hashere dem ind i en løbende kæde, der fungerer som bevis for ændelsesforløbet“

– Satoshi Nakamoto

oin efter forgodtbefindende, og alle kan validere s  
ikter. Ikke nok med det, men alle kan validere s  
*individuelt* uden at skulle stole på nogen andre f

tager tid at forstå bevis-for-arbejde. Det er ofte  
og selvom reglerne er simple, fører de til ret k  
ener. For mig hjalp det at ændre mit perspektiv  
yttigt, ikke ubrugeligt. Validering, ikke beregning.

**n har lært mig, at det er svært at fortælle hvad  
r hvis man er decentraliseret.**



*Sådan sejlede båden langsomt af sted, under den lyse sommerdag, med sin muntre besætning og dens musik af stemmer og latter...*

– Lewis Carroll, *Alice i Eventyrland*

er måske et forældet mantra, men „bevæg dig i ting“ er stadig måden hvorpå en stor del af teknologien arbejder. Ideen om, at det er ligegyldigt, hvis du ikke gør noget i første omgang, er en grundlæggende søjle i *fejl tidligt, fejl altid*. Succes måles i vækst, og så længe du vokser, vil du altid kunne prøve igen. Hvis noget ikke virker i første omgang, skifter du fokus og prøver igen. Med andre ord: kast lort mod væggen, og se, hvad der bliver hængende.

Denne er meget anderledes. Den er anderledes på grund af teknologien.

Den er anderledes af nødvendighed. Som Satoshi Nakamoto har e-valuta blevet forsøgt mange gange før, og alle forsøgene mislykkedes, fordi der var et hoved, der kunne stoppe dem. Det nye ved Bitcoin er, at det er et dyr uden hovedet.

„Mange mennesker afviser automatisk e-valuta, fordi de husker om en tabt sag på grund af alle de virksomheder, der har fejlet siden 1990’erne. Jeg håber, det er ikke et argument, der kan stoppe os.“

Bitcoins natur er sådan, at når version 0.1 er fr  
et, er kerneldesignet mejslet i sten resten af den  
etid.“

– Satoshi Nakamoto

en af de mange paradoksale egenskaber ved Bitcoin er en tendens til at tro, at alt, der er software, nemt kan ændres. Men dyrets natur gør det forbandet svært at ændre. Asu smukt viser i *Unpacking Bitcoin's Social Layer*, at det er kun muligt at ændre reglerne for Bitcoin ved at få en konsensus om ændring og derefter overbevise alle brugerne om at benytte denne ændring. Dette gør Bitcoin meget ustabilt over for ændringer, selvom det er software. Tidsdygtighed er en af Bitcoins vigtigste egenskaber. Softwaresystemer skal være anti-skrøbelige, hvilket samspillet mellem Bitcoins sociale lag og dets teknologier. Monetære systemer er i deres natur fjendtlige. Et vidst i tusindvis af år, er et solidt fundament afgørende miljø.

Og skybruddet kom, og floderne steg, og stormene  
viste sig og ramte det hus. Men det holdt ikke, før det

relsen af *pay to script-hash*<sup>3</sup> og *adskilt vidne*<sup>4</sup> er. Bitcoins regler kan ændres, hvis nok brugere er enighed om det. Denne ændringen er til fordel for netværket. Sidstnævnte er en del af udviklingen af Lightning-netværket<sup>5</sup>, som er et alternativ til Bitcoin. Det er bygget på Bitcoins solide fundament. Fremtidige teknologier som Schnorr-signaturer [60] vil forbedre effektiviteten samt scripts (intelligente kontrakter), som ikke er almindelige transaktioner takket være Taproot [38]. Disse teknologier bygger på solide fundamenter.

Satoshi Nakamoto var ikke kun en klog bygherre rent teknologisk, men også, at det ville være nødvendigt at træffe kloge ideologisk.

„At Bitcoins programkode er open source betyder, at alle uafhængigt kan gennemgå koden. Hvis den var closed source, kunne ingen kontrollere sikkerheden. Jeg mener, det er vigtigt for et program af denne type at være open source.“

– Satoshi Nakamoto

---

script hash-transaktioner (P2SH) blev standardiseret i BIP 173. Det muliggør at sende transaktioner til en script-hash (en adresse, der består af en hash af en hash af en offentlig nøgle (en adresse, der består af en hash af en hash af en offentlig nøgle (en adresse,

Bitcoins radikalt decentraliserede natur, der gør, sig langsomt og velovervejet. Et netværk af knuder er især drives af et suverænt individ, er i sage standsdygtigt over for ændringer - ondsindede er lighed for at tvinge opdateringer ned over brugte måde at indføre ændringer på langsomt at dreneste af disse individer om at benytte en ærke-centrale proces med at introducere og implementere er det, der gør netværket utroligt modstandsindsindede ændringer. Det er også det, der gør de parere ødelagte ting end i et centraliseret miljø, en til, at alle forsøger ikke at ødelægge ting til at

**Har lært mig, at det at bevæge sig langsomt er funktioner, ikke en fejl.**

vente, til det var deres tur, og de skændtes hele tiden og sloges om pindsvinene. Det varede derfor ikke længe før dronningen var så rasende at hun mindst én gang i minuttet stampede jorden og råbte: „af med hans hoved!“ eller: „af med hendes hoved!“

– Lewis Carroll, *Alice i Eventyrlandalen*

man skal tro på eksperterne, har privatlivets fridom været under angreb i mere end en årti. Den pseudonyme opfindelse af Enigma og den anonyme udgiver af WikiLeaks viser, hvordan teknologi kan give et nyt udslag for det. Privatlivet lever, på trods af, at det på ingen måde kan slippe overvågningsstaten.

Satoshi gjorde sig store anstrengelser for at skjule sin identitet. Ti år senere er det stadig uvist, om han var en enkelt person, en gruppe mennesker, en organisation eller en tidsrejsende kunstig intelligens, som snart vil overtage verdensherredømmet. Lægger vi vores forventninger til side, ser vi, at Satoshi valgte at identificere sig som en japansk mand, og derfor antager jeg ikke, men satser på, at han valgte køn og omtaler ham som *han*.

Det er ikke klart, hvad hans virkelige identitet måtte være, havde han ikke været en pseudonym.

Kryptering virker. Korrekt implementerede, stærke kryptosystemer er en af de få ting, du kan stole på.”

– Edward Snowden

i var ikke den første pseudonyme eller anonyme person, der bliver heller ikke den sidste. Nogle har direkte benyttet denne pseudonyme publikationsstil, blandt andet den pseudonyme redaktør fra MimbleWimble [71] , mens andre har ofte udgivet encerede matematiske beviser, mens de har forblydt sig selv under pseudonymet [3].

Det er en mærkelig ny verden, vi lever i. En verden, hvor alle kan være tilgængelige, og bidrag accepteres på baggrund af fortjenten om, at de er korrekte. Folk kan samarbejde og handle frit. Det vil kræve lidt tid at blive fortrolig med disse nye paradigmer, men det er et stort om, at alt dette har potentialet til at ændre verden.

Det er vigtigt at alle huske, at privatliv er en grundlæggende mening i vores samfund. Så længe folk udøver og forsvarer disse rettigheder, vil vi beholde privatlivets fred langt fra slut.

– Lewis Carroll, *Alice i Eventyrland*

... som mange andre gode idéer, opstod Bitcoin ikke alene. Det blev gjort muligt ved at benytte og kombinere viden fra en række forskellige discipliner og opdagelser inden for matematik, fysik, datalogi, teknologi, økonomi, politik, filosofi, litteratur, kultur og andre områder. Satoshi var utvivlsomt et genialt menneske, men det er også muligt at han ikke have været i stand til at opfinde Bitcoin, hvis han ikke havde været en del af den teknologiske udvikling, der skete i hans tid.

„Den, der kun ønsker og håber, blander sig ikke ind i begivenhedernes gang og i udformningen af deres egen skæbne.“

– Ludwig von Mises

En af disse giganter er Eric Hughes, en af grundlæggerne af den cypherpunk-bevægelsen og forfatter til *A Cypherpunk Manifesto*. Det er svært at forestille sig, at Satoshi ikke var påvirket af Hughes' manifest. Det indbefatter mange ting, som Bitcoin har i sin natur.

anonymt transaktionssystem er ikke et hemmeligt transaktionssystem. Vi Cypherpunks er dedikerede til at bygge anonyme systemer. Vi forsvarer vores rettigheder med kryptografi, med anonyme systemer til oversendelse af e-mail, med digitale signaturer og elektroniske penge. Cypherpunks skriver kode.

– Eric Hughes

Cypherpunks finder ikke trøst i håb og ønsker. De griber på begivenhedernes gang og former deres egen skæbne. Cypherpunks skriver kode.

En cypherpunk-manér satte Satoshi sig derfor ned og skrivede koden. Denne kode tog en abstrakt idé og gav den til verden, at den faktisk virkede. Denne kode plantede den konomisk virkelighed. Takket være denne kode kan man nu se, at dette nye system rent faktisk fungerer, og hvem der har beviser Bitcoin over for verden, at den stadig er sikre, at hans innovation overgik fantasien og blev realitet. Satoshi skrev koden til at implementere sin idé, i en udgivningsbogen. Han sørgede også for ikke at forsinke udgivningen. Når alt kommer til alt, er der altid en ting man kan gøre.

```
return nSubsidy + nFees;

    int GetNextWorkRequired(const CBlockIndex* pindexLast)

const unsigned int nTargetTimespan = 14 * 24 * 60 * 60; // two weeks
const unsigned int nTargetSpacing = 10 * 60;
const unsigned int nInterval = nTargetTimespan / nTargetSpacing;

Genesis block
(pindexLast == NULL)
return bnProofOfWorkLimit.GetCompact();
```

Figur 20.1.: Kodeuddrag fra Bitcoin version 0.1

„Jeg måtte skrive hele koden, før jeg kunne overbevis mig selv om, at jeg kunne løse alle problemer. Derefter skrev jeg hvidbogen.“

– Satoshi Nakamoto

idens verden af endeløse løfter og tvivlsom udforskeres desperat brug for en udøvelse af dedikeret opbygning, overbevis dig selv om, at du faktisk kan løse problemet. Implementér løsningerne. Vi bør alle stræbe efter at være cypherpunk.



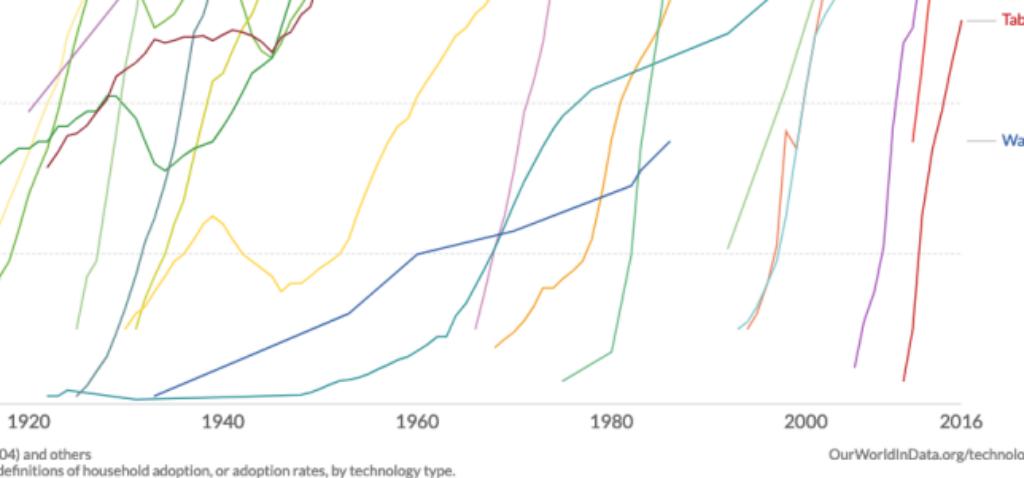
essant...

– Lewis Carroll, *Alice i Eventyrland*

sidste par årtier er det tydeligt, at teknologisk innovationer har en lineær trend. Uanset om man tror på den singulæritet eller ej, er det ubestrideligt, at fremtidige områder er eksponentielle. Ikke alene det, men også hvormed teknologier bliver taget i brug, accelererer ved af det, er busken i den lokale skolegård vækten bruger Snapchat i stedet. Eksponentielle kurver er til at give dig en forskrækkelse, længe før du ser.

Bitcoin er en eksponentiel teknologi, der bygger på eksponentielle teknologier. *Our World in Data*<sup>1</sup> viser smukt den stigende trend i teknologisk adoption, startende i 1903 med installationen af fastnettelefoner (se Figur 21.1). Fastnettelefoner, computere, internettet og smartphones følger alle et eksponentielt væksttrend i pris, ydeevne og udbredelse. Bitcoin [23].

Bitcoin har ikke kun én, men flere netværkseffekter<sup>2</sup>, der opfører sig i eksponentielle vækstmønstre inden for deres forskellige områder: pris, brugere, sikkerhed, udviklere, markedsandelser som globale penge.



## 1.1.: Bitcoin er bogstaveligt talt helt uden for skala

kke nået sin modenhed endnu. Den befinner sig  
sårene. Men hvis teknologien er eksponentiel, er  
værkethed til allestedsnærværende kort.

ED Talk fra 2003 valgte Jeff Bezos at bruge ele-  
metafor for nettets fremtid.<sup>3</sup> Alle tre fænomener -  
ernettet og Bitcoin - er *aktiverende* netværksteknologi-  
gør andre ting. De er infrastrukturer, der skal lave  
og deres natur er at være grundlaget for andre teknolo-

citet har eksisteret i lang tid nu. Vi tager den for-  
t er betydeligt yngre, men de fleste tager det os

## Figur 21.2.: Mobiltelefon, ca. 1965 vs. 2019.

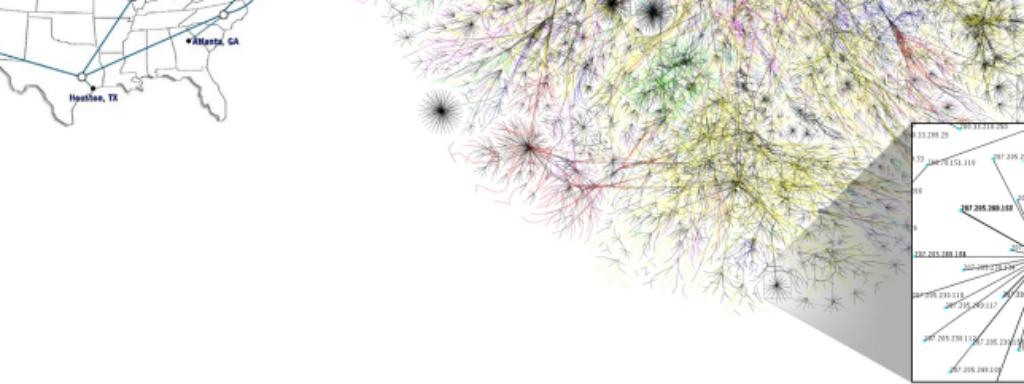
nde Bitcoin som noget, der bare er.<sup>4</sup> I 1994 var internettet stadig forvirrende og det var ikke almindeligt at se denne gamle optagelse af *Today Show*<sup>5</sup> fra 1994, at det, der føles naturligt og intuitivt nu, faktisk ikke var det i 1994. Bitcoin er stadig forvirrende og fremmed for mange, men nu er det naturligt for dem, som internettet er naturligt for den digitalt indfødte. Det er også en logisk følge af, at et stabile sats<sup>6</sup> være en selvfølge for fremtiden.

„Fremtiden er allerede her - den er bare ikke jævnligt udordnet.“

– William Gibson

I 2015 brugte omkring 15% af voksne amerikanere internettet hver dag. Denne procentdel viser, hvordan teknologien har vævet sig ind i alle vores liv. Ifølge en forbrugertastatistik fra det russiske foretaget af Kaspersky Lab [41], har 13% af de amerikanske voksne kendt som *Lindy-effekten*. Lindy-effekten er en teori om, at teknologier med en lang historie har en lidt længere forventede levetid for ikke-forgængelige fænomener som teknologi.

Denne teori er kendt som *Lindy-effekten*. Lindy-effekten er en teori om, at teknologier med en lang historie har en lidt længere forventede levetid for ikke-forgængelige fænomener som teknologi.



3.: Internettet, 1982 vs 2005. Kilde: cc-by Merit Network Inc. og Barrett Lyon, Opte Project

coin og dens kloner til at betale for varer i 2018. Så der ikke er det eneste anvendelsesområde for bitcoin. I likation af, hvor vi befinner os i internettid: Vi er i midten af 90'erne.

udtalte Jeff Bezos i et brev til aktionærerne [11] at "Det er ikke et for internettet", og han erkendte det store uudnyttede potentiale for både internettet og sin virksomhed. Uanset om man er for Bitcoin, er de enorme mængder uudnyttet på netværket ikke tilgængelige for alle, undtagen den mest dovtne iagttager. Den første knudepunkt kom online i 2009, efter at Satoshi havde vundet skabelses-blokken<sup>8</sup> og frigav softwaren

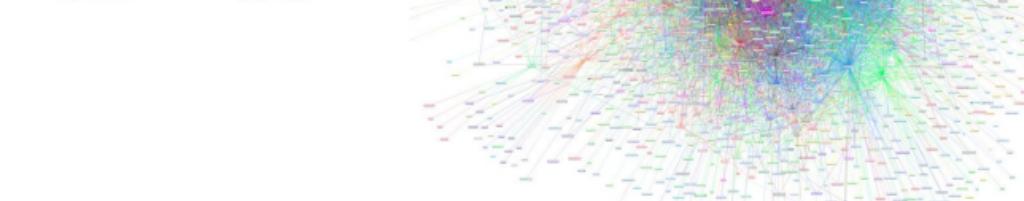
1.4.: Hal Finney skrev det første tweet, der nævner  
i januar 2009.

Hans knudepunkt var ikke alene længe. Hal Finney var den første, der forstod ideen og han sluttede sig til netværket. I dag, da dette skrives, kører mere end 75.000<sup>9</sup> knudepunkter.

Det faktum at Lightning-netværket er et voksende  
okollens basislag er ikke det eneste, der vokser i  
Lightning-netværket, en teknologi der bygger over  
sig selv. Det vokser endnu hurtigere.

I januar 2018 havde Lightning-netværket 40 knudepunkter og 10 kanaler [103]. I april 2019 var netværket vokset til 100 knudepunkter og omkring 40.000 kanaler. Husk på, at Lightning er en eksperimentel teknologi, hvor tab af medlemmer er almindeligt. Men tendensen er klar: Tusindvis af mensker er nu engageret i at oprette kanaler og ivrige efter at bruge det.

Det er et godt stort udviklingspotentiale, der har oplevet internettets meteoriske fremgang. Det er også et godt stort udviklingspotentiale mellem internettet og Bitcoin åbenlyse. Begge teknologier, begge markeder, begge muligheder, nye industrier og nye måder at leve på. Denne teknologi var den bedste metafor til at forstå, hvor interntetet og Bitcoin vil mødes.



5.: Lightning-netværket, januar 2018 vs. dec 2018. Kilde: Jameson Lopp

in er på vej hen. Eller, som Andreas Antonopoulos siger: *pengenes internet*. Disse metaforer er en god måde at forstå teknologien på, selvom historien ikke gentager sig selv, så rimeligt.

Det er dog vigtigt at bemærke, at de potentielle teknologier er svære at forstå og bliver ofte overset. Selvom jeg har en stor interesse i sådanne teknologier, bliver jeg konstant overrasket over tempoet i fremmede lande. At se Bitcoin-økosystemet vokse er som at følge med i et let optagelse af internettets opståen. Det er fascinerende.

Men den genugivelse efter at forstå Bitcoin har ført mig ned ad historien i mere end én måde. At forstå gamle samfundsstrukturen af penge, og hvordan kommunikationsnetværk udvikler sig sammen en del af rejsen. Fra håndøksen til smarte





# Afsluttende tanker



Vorligt, „og fortsæt, indtil du kommer til slutningen. Og hold så op.“

– Lewis Carroll, *Alice i Eventyrlandalen*

nævnt i begyndelsen tror jeg, at ethvert svar på „Hvad har du lært af Bitcoin?“ altid vil være ufuldstændig, da det er en sammenhæng mellem teknologi, teknosfæren og økonomi - er for indviklet, empatisk og tingene bevæger sig for hurtigt til nogensind at være forstået af en enkelt person.

uden at forstå det fuldt ud, og til trods for alle de tilsyneladende mangler, fungerer Bitcoin utvivlsomt med at producere blokke cirka hvert tiende minut på en smuk måde. Jo længere Bitcoin fortsætter, des flere mennesker vil vælge at bruge den.

„Det er sandt, at ting er smukke, når de fungerer. Kunst er funktion.“

– Giannina Brascia

Bitcoin er født af internettet. Den vokser eksponentielt og spredes gennem værtenes netværk mellem discipliner. Det er for eksempel

enkeltstående opfindelse er ansvarlig for dens s  
ombinationen af flere tidlige uafhængige brikk  
af spilteoretiske incitamenter, der udgør den rev  
in er. Den smukke blanding af mange discipliner  
atoshi til et geni.

enhver komplet system skal Bitcoin foretage at  
m effektivitet, omkostninger, sikkerhed og mange  
per. Ligesom der ikke er nogen perfekt løsning på  
rkant fra en cirkel, vil enhver løsning på de pro  
in forsøger at løse, også altid være ufuldkomme

Jeg tror ikke, at vi nogensinde vil få gode peng  
n, før vi tager dem ud af statens hænder. Det v  
e, vi kan ikke tage dem ud af statens hænder me  
d; det eneste vi kan gøre er at indføre noget vi  
dige, indirekte bagveje, som de ikke kan stoppe.

– Friedrich Hayek<sup>1</sup>

er den snedige, indirekte bagvej som de ikke ka  
dermed måden, hvorpå man kan genintroducere  
nge. Den skaber et suverænt individ bag hvort

Ligesom det at fjerne en del fra et komplekst system  
helheden, synes det at ødelægge forståelsen af den.  
Prøv at forsøge dele af den i isolation. Hvis bare én person  
„er bort“ fra sit ordforråd og erstatter det med „en“, vil jeg  
dø som en lykkelig mand.

Men alle omstændigheder fortsætter min rejse. Jeg  
vove mig længere ned i kaninhullets dybder, og jeg  
kan ikke tage med på turen.<sup>12</sup>



I tanketegang om Bitcoin og de emner, den berørte til at nævne dem alle, men jeg vil gøre mit bane nogle få.

Tak til Arjun Balaji for tweeten, der motiverede mig til dette.

Tak til Marty Bent for at give endeløs stof til efterunderholdning. Hvis du ikke abonnerer på *Marty's Tales From The Crypt*, er du gået glip af noget. Skal Marty der guider os gennem kaninhullet.

Tak til Michael Goldstein og Pierre Rochard for udlen af materiale og levering af den bedste Bitcoin via Nakamoto Institute. Og tak for skabelsen af Nakamotocast, som i høj grad har påvirket mit filosofiske syn på Bitcoin.

Tak til Saifedean Ammous for hans overbevisninger, disse tweets og for at have skrevet Bitcoinstandard.

Tak til Francis Pouliot for at dele sin begejstring over denne tidskæden.

Tak til Andreas M. Antonopoulos for alt det uddannende

til Guy Swann for at producere en lydversion af s.com.

til Friar Hass for hans åndelige støtte og vejledning at tage sig tid til at skrive et forord til denne bog.

til min kone for at holde mig og min besættelse i

til min familie for at støtte mig i både gode og

st, men ikke mindst, tak til alle bitcoin-maksimer, coin-minimalister, shills, bots og shitposters, som den smukke have, som Bitcoin Twitter er.

idst, tak fordi du læste dette. Jeg håber, du nød også, som jeg nød at skrive det.

- Blinde munke undersøger Bitcoin-elefanten . . .
- Bitcoin-kaninhullet er bundløst. . . . .
- Hyperinflation in the Weimar Republic (1921-1923) . . . . .
1. fiat — ‘Lad det ske’ . . . . .
2. Lydisk mønt. Billedet er licenseret under Creative Commons Attribution Share-Alike 4.0 af Classical Numismatic Group, Inc. . . . . .
3. Sølvmønter med varierende grad af afklipning. . . . .
4. Den oprindelige „dollar“. Sankt Joachim er afbildet med sin kappe og troldmandshat. Billede cc-by-sa af Wikipedia-bruger Berlin-George . . . . .
5. En amerikansk søldollar fra 1928. „Betales ihændehaveren på forespørgsel.“ Billede cc-by-sa af National Numismatic Collection ved the Smithsonian Institution . . . . .
6. Dette er et amerikansk 100 dollars guldcertifikat fra 1928. Billedet er cc-by-sa fra National Numismatic Collection, National Museum of American History . . . . .

Bitcoins kontrollerede udbud . . . . .
Forholdet mellem lager og produktion for guld . . . . .
/visualisering af forholdet mellem lager og produktion for USD, guld og Bitcoin . . . . .
Stigende forhold mellem lager og produktion for bitcoin sammenlignet med guld . . . . .
 For omkring 1 billion sekunder siden. Kilde: xkc 225 . . . . .
Illustration af SHA-256-sikkerhed. Original grafik af Grant Sanderson også kendt som 3Blue1Brown. . . . .
Angreb med 5\$ skruenøgle. Kilde: xkcd 538 . . . . .
Eksempler på elliptiske kurver. Grafik cc-by-sa Emmanuel Boutet. . . . .
 Uddrag fra Ken Thompsons artikel ‘Reflections on Trusting Trust’ . . . . .
Fra <i>Stealthy Dopant-Level Hardware Trojans</i> af Becker, Regazzoni, Paar, Burleson . . . . .
Hvad kom først, hønen eller ægget? . . . . .
 Uddrag fra hvidbogen. Var der nogen, der sagde idskæde? . . . . .





talen - og dermed de næste af de interessante ressourcer online.

Min bibliografi inkluderer en række bøger, artikler og ressourcer. Hvis ressourcen har en tilknyttet URL, var den opdateret i oktober 2019, hvor jeg havde adgang til den på den relevante kilde. Hvis en af de følgende URL'er fører til en fejl, så er jeg ikke sikker på hvilken. Lad mig venligst vide det<sup>13</sup> så jeg kan opdatere min bibliografi.

Bitcoin og IPFS løser det.



Saifedean Ammous. Presentation on the standard. [https://www.bayernlb.de/immedia/de/ir/downloads\\_1/bayernlb\\_researchsonderpublikationen\\_1/bitcoin\\_munich\\_may2018.pdf](https://www.bayernlb.de/immedia/de/ir/downloads_1/bayernlb_researchsonderpublikationen_1/bitcoin_munich_may2018.pdf), May 2018.

Jay Pantone Anonymous 4chan Poster, Robin and Vince Vatter. A lower bound on the length of the shortest superpattern. <https://oeis.org/A180632.pdf>, October 2018.

Andreas M Antonopoulos. *Mastering Bitcoin: Programming the Open Blockchain*. "O'Reilly Media, Inc.", 2014.

Julian Assange. Cypherpunks: Freedom and the future of the internet - introduction: A call to cryptographic arms. <https://cryptome.org/assange-crypto-arms.htm>, December 2012.

United Nations General Assembly. The universal declaration of human rights, December 1948.

arty Bent. Tales from the crypt – a podcast about <https://tftc.io/tales-from-the-crypt/>, 2017.

f Bezos. To our shareholders. [http://corporate-ir.net/media\\_files/irol/97/976640ports/Shareholderletter97.pdf](http://corporate-ir.net/media_files/irol/97/976640ports/Shareholderletter97.pdf), 1997.

coin Wiki contributors. Block hashing algorithm —  
Wiki. [https://en.bitcoin.it/w/index.php?title=Block\\_hashing\\_algorithm&oldid=66452](https://en.bitcoin.it/w/index.php?title=Block_hashing_algorithm&oldid=66452), 2019.

coin Wiki contributors. Controlled supply —  
Wiki. [https://en.bitcoin.it/w/index.php?title=Controlled\\_supply&oldid=66483](https://en.bitcoin.it/w/index.php?title=Controlled_supply&oldid=66483), 2019.

coin Wiki contributors. Genesis block —  
Wiki. [https://en.bitcoin.it/w/index.php?title=Segregated\\_Witness&oldid=66902](https://en.bitcoin.it/w/index.php?title=Segregated_Witness&oldid=66902), 2019.

coin Wiki contributors. Pay to script hash —  
Wiki. [https://en.bitcoin.it/w/index.php?title=Pay\\_to\\_script\\_hash&oldid=66902](https://en.bitcoin.it/w/index.php?title=Pay_to_script_hash&oldid=66902), 2019.

what-is-it-like-to-be-a-bitcoin-56109f3e  
November 2018.

Guix Contributors. Guix — bootstrapping. [https://gnu.org/manual/en/html\\_node/Bootstrapping](https://gnu.org/manual/en/html_node/Bootstrapping) 2019.

Bernard W. Dempsey. *Interest and Usury*. American Council on Public Affairs, <https://babel.hathitrust.org/cgi/pt?id=mdp.39015011903997&seq=230>, 1940.

Daniel C Dennett and Douglas R Hofstadter. *The Mind's I : Fantasies and reflections on self and soul*. HarperCollins, 1981.

Jeff Desjardins. The rising speed of technological adoption. <https://www.visualcapitalist.com/rising-speed-technological-adoption/>, 2017.

Peter Diamandis. *Abundance : the future is better than you think*. Free Press, New York, 2012.

Dunny. I've learned more about finance, econo

sannah Fox and Lee Rainie. How the internet has  
elf into american life. <https://pewrsr.ch/32M7Q>  
ary 2014.

liam Gibson. The science in science  
<https://www.npr.org/2018/10/22/1067220/>  
e-science-in-science-fiction, October 2018

i. Bitcoin's energy consumption – a s  
pective. <https://dergigi.com/2018/0>  
tcoin-s-energy-consumption/, June 2018.

i. The magic dust of cryptography –  
tal information is changing our society  
gravity. <https://dergigi.com/2018/0>  
e-magic-dust-of-cryptography/, Aug 2018.

egory Maxwell. Taproot: Privacy preserving sw  
scripting. <https://lists.linuxfoundatio>  
bermail/bitcoin-dev/2018-January/015614.  
18.

Henry Hazlitt. *Economics in One Lesson*.  
Ludwig von Mises Institute, <https://mises.org/library/economics-one-lesson>, 1946.

Dan Held. Bitcoin's distribution was fair. <https://blog.petervis.com/bitcoins-distribution-was-fair-e2ef7bbbc> 2018.

Eric Hughes. A cypherpunk's manifesto. <http://www.activism.net/cypherpunk/manifesto.html>. March 1993.

Guido Jörg Hülsmann. *Ethics of Money Production*. Ludwig von Mises Institute, <https://mises.org/library/ethics-money-production>. 2008.

Robert Kiyosaki. Why the rich are getting richer. <https://youtu.be/abMQhaMdQu0>, July 2016.

Kaspersky Lab. From festive fun to password Managing money online this christmas. <https://www.kaspersky.com/resource-center/white-papers/managing-money-online-this-christmas>

ce Mayer. The 7 network effects of bitcoin.  
<https://www.thrivenotes.com/7-network-effects-of-bitcoin/>, January 2016.

raph C. Merkle. Daos, democracy and governance.  
<https://alcor.org/cryonics/Cryonics2030.pdf>, page 28, July-August 2016.

Minimalist. Isn't it ironic that bitcoin has more about money than all these years i've been working for financial institutions? <https://twitter.com/fiatminimalist/status/107288081566143632>, December 2018.

The Austrian Mint. Gold: The extraordinary metal.  
<https://www.muenzeoesterreich.at/eng/discover/investors/gold-the-extraordinary-metal>, November 2017.

British Museum. The origins of coinage.  
[https://www.britishmuseum.org/explore/themes/money/the\\_origins\\_of\\_coinage.aspx](https://www.britishmuseum.org/explore/themes/money/the_origins_of_coinage.aspx), 2007.

Satoshi Nakamoto. Bitcoin open source implementation of p2p currency. <http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source>, February 2009.

Satoshi Nakamoto. Re: Bitcoin open source implementation of p2p currency. <http://p2pfoundation.net/forum/topics/bitcoin-open-source>, February 2009.

Satoshi Nakamoto. Re: Questions about bitcoin. <https://bitcointalk.org/index.php?topic=13.msg46>, December 2009.

Satoshi Nakamoto. Dealing with sha-256 collisions. <https://bitcointalk.org/index.php?topic=13.msg1585#msg1585>, June 2010.

Satoshi Nakamoto. Re: 0.3 almost ready. <https://bitcointalk.org/index.php?topic=199.msg1670#msg1670>, June 2010.

Satoshi Nakamoto. Re: Transactions and scripthash160 ... equalverify checksig. <https://bitcointalk.org/index.php?topic=199.msg1670#msg1670>

ter Wuille. Schnorr signatures for secp  
<https://github.com/sipa/bips/blob/bip-schnor...> mediawiki, 2019.

to. *Plato in Twelve Volumes*, Vol. 3.  
mus section 304a/304b). Harvard University  
<http://www.perseus.tufts.edu/hopper/text?d=perseus%3Atext%3A1999.01.0178%3Atext%3DEuthy...>  
a section%3D304a, 2017.

ederal Reserve. Money stock measures – discontin  
m3. <https://www.federalreserve.gov/Releas.../discm3.htm>, 2005.

arl Sagan. *Cosmos*. Random House, 1980.

nce Schneier. *Applied Cryptography: Protocols, P  
s and Source Code in C*. John Wiley and Sons, 1996.

nce Schneier. Schneier on security. <https://www.schneier.com>, 2019.

Nick Szabo. Shelling out: The origins of money  
[/nakamotoinstitute.org/shelling-out/](https://nakamotoinstitute.org/shelling-out/), 20

K. Thompson. Reflections on trusting trust. In AC  
award lectures, page 1983, 2007.

Tom Elvis Jedusor. Mimblewimble  
<https://github.com/mimblewimble/docs/wiki/MimbleWimble-Origin>, 2016.

Grisha Trubetskoy. Blockchain proof-of-work is  
ralized clock. <https://grisha.org/blog/2018/explaining-proof-of-work/>, 2018.

Peter Van Valkenburgh. Coin center's peter van va  
on preserving the freedom to innovate with pub  
chains. <http://bit.ly/valkenburgh>, November

Ludwig von Mises. *Human Action*. Ludwig von  
stitute, <https://mises.org/library/human-action/html/p/607>, 1949.

ikipedia contributors. Crypto wars — Wikipedia, the free encyclopedia. [https://en.wikipedia.org/w/index.php?title=Crypto\\_Wars&oldid=916147143](https://en.wikipedia.org/w/index.php?title=Crypto_Wars&oldid=916147143), 2019.

ikipedia contributors. Discrete logarithm — Wikipedia, the free encyclopedia. [https://en.wikipedia.org/w/index.php?title=Discrete\\_logarithm&oldid=9625575](https://en.wikipedia.org/w/index.php?title=Discrete_logarithm&oldid=9625575), 2019.

ikipedia contributors. Dual ec drbg — Wikipedia, the free encyclopedia. [https://en.wikipedia.org/w/index.php?title=Dual\\_EC\\_DRBG&oldid=918490393](https://en.wikipedia.org/w/index.php?title=Dual_EC_DRBG&oldid=918490393), 2019.

ikipedia contributors. Dyson sphere — Wikipedia, the free encyclopedia. [https://en.wikipedia.org/w/index.php?title=Dyson\\_sphere&oldid=9166219](https://en.wikipedia.org/w/index.php?title=Dyson_sphere&oldid=9166219), 2019.

ikipedia contributors. Elliptic-curve cryptography — Wikipedia, the free encyclopedia. <https://en.wikipedia.org/w/index.php?title=Elliptic-cryptography&oldid=916608234#Backdoors>, 2019.

php?title=Illegal\_prime&oldid=913087454, Wikipedia contributors. Keynesian economics — Wikipedia, the free encyclopedia. [https://en.wikipedia.org/w/index.php?title=Keynesian\\_economics&oldid=919881690](https://en.wikipedia.org/w/index.php?title=Keynesian_economics&oldid=919881690), 2019.

Wikipedia contributors. Landauer's principle — Wikipedia, the free encyclopedia. [https://en.wikipedia.org/w/index.php?title=Landauer%27s\\_principle&oldid=907333330](https://en.wikipedia.org/w/index.php?title=Landauer%27s_principle&oldid=907333330), 2019.

Wikipedia contributors. Last glacial maximum — Wikipedia, the free encyclopedia. [https://en.wikipedia.org/w/index.php?title=Last\\_Glacial\\_Maximum&oldid=919510280](https://en.wikipedia.org/w/index.php?title=Last_Glacial_Maximum&oldid=919510280), 2019.

Wikipedia contributors. Lindy effect — Wikipedia, the free encyclopedia. [https://en.wikipedia.org/w/index.php?title=Lindy\\_effect&oldid=921214819](https://en.wikipedia.org/w/index.php?title=Lindy_effect&oldid=921214819), 2019.

Wikipedia contributors. List of currencies — Wikipedia, the free encyclopedia. [https://en.wikipedia.org/w/index.php?title=List\\_of\\_currencies&oldid=919881690](https://en.wikipedia.org/w/index.php?title=List_of_currencies&oldid=919881690), 2019.

kipedia contributors. Money multiplier — Wikipedia, the free encyclopedia. [https://en.wikipedia.org/w/index.php?title=Money\\_multiplier&oldid=9027413](https://en.wikipedia.org/w/index.php?title=Money_multiplier&oldid=9027413), 2019.

kipedia contributors. Money supply — Wikipedia, the free encyclopedia. [https://en.wikipedia.org/w/index.php?title=Money\\_supply&oldid=9211519](https://en.wikipedia.org/w/index.php?title=Money_supply&oldid=9211519).

kipedia contributors. P versus np problem — Wikipedia, the free encyclopedia. [https://en.wikipedia.org/w/index.php?title=P\\_vs\\_NP\\_problem&oldid=9882161](https://en.wikipedia.org/w/index.php?title=P_vs_NP_problem&oldid=9882161), 2019.

kipedia contributors. Paradox of value — Wikipedia, the free encyclopedia. [https://en.wikipedia.org/w/index.php?title=Paradox\\_of\\_value&oldid=9068208](https://en.wikipedia.org/w/index.php?title=Paradox_of_value&oldid=9068208), 2019.

kipedia contributors. Sha-2 — Wikipedia, the free encyclopedia. <https://en.wikipedia.org/w/index.php?title=SHA-2&oldid=917408454>, 2019.

— Wikipedia, the free encyclopedia. [https://en.wikipedia.org/w/index.php?title=Subjective\\_theory\\_of\\_value&oldid=893004286](https://en.wikipedia.org/w/index.php?title=Subjective_theory_of_value&oldid=893004286), 2019.

Wikipedia contributors. Thaler — Wikipedia, the free encyclopedia. <https://en.wikipedia.org/w/index.php?title=Thaler&oldid=914457345>, 2019.

Wikipedia contributors. Theory of value (economics) — Wikipedia, the free encyclopedia. [https://en.wikipedia.org/w/index.php?title=Theory\\_of\\_value\\_\(economics\)&oldid=9196032019](https://en.wikipedia.org/w/index.php?title=Theory_of_value_(economics)&oldid=9196032019).

Wilma Woo. 'unfairly cheap' lightning network has 40 nodes, 60 channels. <https://bitcointalk.org/index.php?topic=1011110.0>. January 2018.

otes



## **Del IV.**

# **Den danske udgave**



# ation

oversat 21 Lektioner til dansk, da vi tror på, at den gængelig introduktion til Bitcoin og dens principper til mange andre bøger om Bitcoin dækker 21 af spektrum af de elementer, der gør Bitcoin til Bitcoin. Skrevet på et letforståeligt dansk og med et minimum af teknisk jargon. Vi har alle startet samme sted, på den hvide kanin, der hopper af sted, og som i Alice i Eventyrland så starter rejsen hvor Alice hopper ned i kanten. Det er ikke tænke på hvorfor en kanin har et lommeur og ved ikke dog have været anderledes, hvis Alice havde været i et møde med skrevet af Bob eller Gigi.

ne. Link: t.me/enogtyvedk.

**DgTyve's portal:** Dansksproget portal med information om Bitcoin. Link: [www.enogtyve.org](http://www.enogtyve.org).

**gen Bitcoinstandarden:** En detaljeret økonomisk analyse af Bitcoin, gode penges egenskaber og af de samme problemer fiat-valutaer har skabt.

Link: [www.bitcoinstandarden.dk](http://www.bitcoinstandarden.dk).

**coinskolen.net:** Bitcoinskolens mission er at informere og undervise dig i bitcoin, så du selv kan træffe en valg på et oplyst grundlag. [www.bitcoinskolen.net](http://www.bitcoinskolen.net)

## Sammenhæld

I gerne takke følgende personer for deres bidrag til artiklen og korrekturlæsning:

Ter Isaksen (plus hans hustru), redaktør

Erasmus Hansen

Jørgen Vendelboe