

21 Lektioner

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

Gigi

21 Lektioner

Hvad jeg har lært af at falde ned i Bitcoin-kaninhullet
Første udgave. Ophavsret ©2018–2024 Gigi / @dergigi /
dergigi.com



Denne bog og dens online version er distribueret under vilkårene for Creative Commons Attribution-ShareAlike 4.0 licensen. En referencekopi af denne licens kan findes på den officielle Creative Commons website.^a

^a<https://creativecommons.org/licenses/by-sa/4.0>

*Dedikeret til min kone, mit barn og alle
børn i denne verden. Må Bitcoin bringe jer
lykke og en vision for en fremtid, der er
værd at kæmpe for.*

Forord

Nogle kalder det en religiøs oplevelse, andre kalder det Bitcoin.

Jeg mødte Gigi første gang i et af mine åndelige hjem - Riga, Letland - hjemstedet for *The Baltic Honeybadger* konferencen, hvor de mest ivrige af de Bitcoin-troende valfarter til hvert år. Efter en dyb samtale over frokost var det bånd, Gigi og jeg knyttede, lige så mejslet i sten som en Bitcoin-transaktion, der blev gennemført, da vi gav hinanden hånden et par timer tidligere.

Mit andet åndelige hjem, Christ Church, Oxford, hvor jeg havde det privilegie at studere til min MBA, var stedet, hvor jeg oplevede mit „kaninhuls“-øjeblik. Ligesom Gigi transcenderede jeg de økonomiske, tekniske og sociale verdener og blev åndeligt opslugt af Bitcoin. Efter at have „købt på toppen“ i november 2013, var der flere ekstremt hårde lektioner i det ubarmhjertigt knusende og tilsyneladende uendelige 3-årige faldende marked. Disse 21 lektioner ville virkelig have tjent mig godt i den periode. Mange af disse lektioner er simpelthen naturlige sandheder, som for de uindviede er skjult af en uigennemsigtig, skrøbelig film. Ved slutningen af denne bog vil facaden dog krakelere.

På en stjerneklar aften i Oxford i slutningen af august 2016, blot et par uger efter at kniven igen var blevet stukket ind i mit hjerte, da Bitfinex-børsen blev hacket, sad jeg eftertænksomt i Christ Churchs „Masters Garden“. Tiderne var hårde, og jeg var ved at nå mit mentale og følelsesmæssige bristepunkt efter, hvad der syntes at være en livstid med tortur; ikke på grund af økonomisk tab, men på grund af det knusende åndelige tab, jeg følte ved at være isoleret i mit verdensbillede. Hvis bare der var en ressource som denne her på det tidspunkt, så jeg kunne se, at jeg ikke var alene. „Masters Garden“ er et meget specielt

sted for mig og mange, der gennem århunderne er kommet før mig. Det var her, Charles Dodgson, en matematiklærer fra Christ Church, observerede en af sine unge elever, Alice Liddell, datteren af dekanen for Christ Church. Dodgson, bedre kendt under sit pseudonym, Lewis Carroll, brugte Alice og haven som inspiration. Fra den magiske hellige have stirrede jeg dybt ind i kryptokløften, og den stirrede flammende tilbage. Min arrogance blev tilintetgjort og min stolthed fik et slag i ansigtet. Jeg havde endelig fundet fred.

21 Lektioner tager dig med på en ægte Bitcoin-rejse; ikke blot en rejse inden for filosofi, teknologi og økonomi, men også en rejse for sjælen.

Når man dykker dybere ned i den filosofi, der kortfattet er beskrevet i 7 af de 21 lektioner, kan man med tilstrækkelig tid og eftertanke komme så langt som til at forstå alle facetters oprindelse. Hans 7 lektioner om økonomi indfanger i enkle vendinger, hvordan vi er taget til fange af en lille gruppe *gale hattemagere*, og hvordan det er lykkedes dem at sætte skyklapper på vores sind, hjerter og sjæle. De 7 lektioner om teknologi beskriver Bitcoins skønhed og teknologisk-darwinistiske perfektion. Som ikke-teknisk bitcoiner giver lektionerne en god gennemgang af Bitcoins underliggende teknologiske natur, og endda teknologiens sande natur.

I denne flygtige oplevelse, som vi kalder livet, lever, elsker og lærer vi. Men hvad er livet andet end en tidsstemplet rækkefølge af begivenheder?

Det er ikke let at bestige Bitcoin-bjerget. Der er mange falske toppe, klipperne er hårde. Revner og sprækker findes overalt og venter på at opsluge dig. Når du har læst denne bog, vil du se, at Gigi er den ultimative Bitcoin-sherpa, og jeg vil altid være ham taknemmelig.

Hass McCook
29. november 2019

„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*

Indhold

I. Filosofi	9
1. Uforanderlighed og forandring	15
2. Knaphedens knaphed	19
3. Replikation og lokalitet	21
4. Problemet med identitet	23
5. En perfekt undfangelse	25
6. Ytringsfrihedens kraft	27
7. Grænserne for viden	29
II. Økonomi	31
8. Finansiel uvidenhed	35
9. Inflation	39
10. Værdi	45
11. Penge	47
12. Pengenes historie og undergang	51

13. Vanviddet i brøkreserve-bankvæsenet	59
14. Stabile penge	65
III. Teknologi	73
15. Styrke i tal	77
16. Refleksioner over „Stol ikke, bekræft“	85
17. At fortælle tid kræver arbejde	93
18. Bevæg dig langsomt, og undgå at ødelægge ting	97
19. Privatlivet er ikke dødt	101
20. Cypherpunks skriver kode	103
21. Metaforer for Bitcoins fremtid	107
Afsluttende tanker	115
IV. Den danske version	143

Om denne bog (... og om forfatteren)

Dette er en lidt usædvanlig bog. Men hey, Bitcoin er en usædvanlig teknologi, så en usædvanlig bog om Bitcoin passer måske ind. Jeg er ikke sikker på, om jeg er en usædvanlig fyr (jeg kan godt lide at tænke på mig selv som en *almindelig* fyr), men historien om, hvordan denne bog blev til, og hvordan jeg blev forfatter, er værd at fortælle.

Først og fremmest er jeg ikke forfatter, men ingeniør. Jeg har ikke studeret litteratur. Jeg har studeret kode og kodning, For det andet, jeg havde aldrig til hensigt at skrive en bog, og slet ikke en om Bitcoin. Jeg skriver endda ikke om Bitcoin på mit modersmål.¹ Jeg er bare en fyr, der blev bidt af Bitcoin-feberen. Hårdt.

Hvorfor er *jeg* berettiget til at skrive en bog om Bitcoin? Det er et godt spørgsmål. Det korte svar er nemt: Jeg hedder Gigi, og jeg er en bitcoiner.

Det lange svar er en smule mere nuanceret.

Min baggrund er inden for datalogi og softwareudvikling. I et tidligere liv var jeg en del af en forskningsgruppe, der blandt andet forsøgte at få computere til at tænke og ræsonnere. I et andet tidligere liv skrev jeg software til automatiseret pasbehandling og relaterede opgaver, hvilket er endnu mere skræmmende. Jeg ved en ting eller to om computere og vores netværksbaserede

¹Grunden til, at jeg skriver denne bog på engelsk, er, at min hjerne fungerer på mystiske måder. Hver gang noget teknisk dukker op, skifter den tilstand til engelsk.

verden, så jeg tror, jeg har et lille forspring i forhold til at forstå den tekniske side af Bitcoin. Men som jeg forsøger at skitsere i denne bog, er den tekniske side af sagen kun en lillebitte del af det bæst, som Bitcoin er. Og hver eneste af disse dele er vigtige.

Denne bog blev til på grund af et enkelt spørgsmål: „*Hvad har du lært af Bitcoin?*“ Jeg forsøgte at besvare dette spørgsmål i et enkelt tweet. Så blev tweetet til en tweetstorm. Tweetstormen blev til en artikel. Artiklen blev til tre artikler. Tre artikler blev til 21 Lektioner. Og 21 Lektioner blev til denne bog. Så jeg er nok bare virkelig dårlig til at sammenfatte mine tanker i et enkelt tweet.

„Hvorfor skrive denne bog?“, spørger du måske. Ingen er der et kort og et langt svar. Det korte svar er, at jeg simpelthen var nødt til det. Jeg var (og er stadig) besat af Bitcoin. Jeg finder det uendeligt fascinerende. Jeg kan tilsyneladende ikke stoppe med at tænke på det og de konsekvenser, det vil have for vores globale samfund. Det lange svar er, at jeg tror, at Bitcoin er den vigtigste opfindelse i vores tid, og flere mennesker skal forstå naturen af denne opfindelse. Bitcoin er stadig et af de mest misforståede fænomener i vores moderne verden, og det tog mig år at fuldt ud indse alvoren af denne fremmede teknologi. At indse, hvad Bitcoin er, og hvordan det fænomen vil ændre vores samfund, er en dybtgående oplevelse. Jeg håber at plante frøene, der måske fører til denne erkendelse, i dit sind.

Selvom dette afsnit har titlen „*Om denne bog (... og om forfatteren)*“, betyder denne bog, hvem jeg er, og hvad jeg har gjort, i det store hele ikke rigtig noget. Jeg er bare et knudepunkt i netværket, både bogstaveligt „og billedligt talt. Og du skal alligevel ikke stole på, hvad jeg siger. Som vi bitcoinere plejer at sige: Lav din egen undersøgelse, og vigtigst af alt: Stol ikke, bekræft.

Jeg gjorde mit bedste for at lave mit hjemmearbejde og give dig, kære læser, masser af kilder, du kan dykke ned i. Ud

over fodnoterne og citaterne i denne bog forsøger jeg at holde en opdateret liste over ressourcer på 21lessons.com/rabbithole og på bitcoin-resources.com, som også viser masser af andre håndplukkede ressourcer, bøger og podcasts, der vil hjælpe dig med at forstå, hvad Bitcoin er.

Kort sagt er dette blot en bog om Bitcoin, skrevet af en bitcoiner. Bitcoin har ikke brug for denne bog, og du har sandsynligvis ikke brug for denne bog for at forstå Bitcoin. Jeg tror, at Bitcoin vil blive forstået af dig, så snart *du* er klar, og jeg tror også, at de første brøkdele af en bitcoin vil finde dig, så snart du er klar til at modtage dem. I bund og grund vil alle få Bitcoin på det helt rigtige tidspunkt. I mellemtiden er Bitcoin, som den er, og det er nok.²

²Beautyon, *Bitcoin is. And that is enough.* [8]

Forord

At falde ned i Bitcoin-kaninhullet er en mærkelig oplevelse. Jeg føler, ligesom mange andre, at jeg har lært mere i de sidste par år ved at studere Bitcoin, end jeg har gjort i løbet af to årtier med formel uddannelse.

De følgende lektioner er en sammenfatning af, hvad jeg har lært. De blev først udgivet som en artikelserie med titlen „*What I've Learned From Bitcoin*“. Det følgende kan ses som den tredje udgave af den oprindelige serie.

Ligesom Bitcoin er disse lektioner ikke statiske. Jeg planlægger at arbejde på dem med jævne mellemrum og udgive opdaterede versioner og yderligere materiale i fremtiden.

I modsætning til Bitcoin behøver fremtidige versioner af dette projekt ikke at være bagudkompatible. Nogle lektioner kan blive udvidet, mens andre kan blive omarbejdet eller erstattet.

Bitcoin er en uudtømmelig lærermester, og derfor påstår jeg ikke, at disse lektioner er altomfattende eller komplette. De er en afspejling af min personlige rejse ned i kaninhullet. Der er mange flere lektioner at lære, og enhver person vil lære noget forskelligt af at træde ind i Bitcoins verden.

Jeg håber, at du vil finde disse lektioner nyttige, og at procesen med at lære dem ved at læse, ikke vil være lige så besværlig og smertefuld som det var at lære dem alene.

21 Lektioner

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

– Lewis Carroll, *Alice i Eventyrland*

Introduktion

„Men jeg bryder mig ikke om at være blandt gale mennesker,“ sagde Alice. „Åh, det kan du ikke undgå,“ sagde katten: „Her er vi tosede allesammen. Jeg er tosset. Du er tosset.“ „Hvordan 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*

I oktober 2018 stillede Arjun Balaji det uskyldige spørgsmål: *Hvad har du lært af Bitcoin?* Efter at have forsøgt at besvare spørgsmålet i et kort tweet, og uden held, indså jeg, at de ting, jeg har lært, er alt for mange til hurtigt at kunne besvare spørgsmålet, hvis det overhovedet kan besvares.

De ting, jeg har lært, handler naturligvis om Bitcoin - eller de er i det mindste relateret til det. Men selvom nogle af Bitcoins indre funktioner er forklaret, er de følgende lektioner ikke en forklaring på, hvordan Bitcoin fungerer, eller hvad den er, men de kan dog hjælpe med at udforske nogle af de temaer, Bitcoin berører: filosofiske spørgsmål, økonomiske realiteter og teknologiske innovationer.

Arjun Balaji
@arjunblj

Bitcoin is a game disguised to teach you about:

- Ethics of money production
- History of central banking & gold
- Adversarial system design
- Commodities markets
- Distributed systems engineering & the software lifecycle
- Securities law

What have you learned from Bitcoin?

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

511 people are talking about this

De 21 lektioner er struktureret i bundter af syv, hvilket resulterer i tre kapitler. Hvert kapitel betragter Bitcoin gennem en ny linse og uddrager, hvad man kan lære ved at inspicere dette mærkelige netværk fra en anden vinkel.

Kapitel 1 udforsker den filosofiske lære om Bitcoin. Samspillet mellem uforanderlighed og forandring, begrebet ægte knaphed, Bitcoins perfekte undfangelse, identitetsproblemet, modsigelsen mellem replikation og lokalitet, ytringsfrihedens kraft og grænserne for viden.

Kapitel 2 udforsker den økonomiske lære af Bitcoin. Disse lektioner omhandler finansiel uvidenhed, inflation, værdi, penge og pengenes historie, brøkreservebankvæsen og hvordan Bitcoin genindfører stabile penge på en snedig, indirekte måde.

Kapitel 3 udforsker nogle af de erfaringer, jeg har lært ved at undersøge teknologien i Bitcoin. Hvorfor der er styrke i tal, refleksioner over tillid, hvorfor det at fortælle tiden kræver arbejde, hvordan det at bevæge sig langsomt og ikke ødelægge ting er en egenskab og ikke en fejl, hvad Bitcoins skabelse kan fortælle os om privatliv, hvorfor cypherpunks skriver kode (og ikke love),

og hvilke metaforer der kan være nyttige til at udforske Bitcoins fremtid.

Hver lektion indeholder flere citater og links i teksten. Hvis en idé er værd at udforske nærmere, kan du følge linkene til relaterede værker i fodnoterne eller i bibliografiens.

Selvom en vis forhåndsviden om Bitcoin er gavnlig, håber jeg, at disse lektioner kan fordøjes af enhver nysgerrig læser. Selvom nogle relaterer til hinanden, bør hver lektion kunne stå for sig selv og de kan læses uafhængigt af hinanden. Jeg har gjort mit bedste for at undgå teknisk jargon, selvom nogle domænespecifikke ord er uundgåelige.

Jeg håber, at mine tekster kan inspirere andre til at grave under overfladen og undersøge nogle af de dybere spørgsmål, som Bitcoin rejser. Min egen inspiration kom fra en lang række forfattere og indholdsskabere, hvem jeg er evigt taknemmelig.

Sidst, men ikke mindst: Mit mål med at skrive dette er ikke at overbevise dig om noget som helst. Mit mål er at få dig til at tænke og at vise dig, at der er meget mere ved Bitcoin, end man umiddelbart skulle tro. Jeg kan ikke engang fortælle dig, hvad Bitcoin er, eller hvad Bitcoin vil lære dig. Det bliver du nødt til selv at finde ud af.

„Herfra er der ingen vej tilbage. Du tager den blå pille - historien slutter, du vågner op i din seng og tror på, hvad du vil tro på. Du tager den røde pille³ — du forbliver i Eventyrland, og jeg viser dig, hvor dybt kaninhullet når.“

— Morpheus

³den *orange* pille



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

Del I.

Filosofi

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 Eventyrland*

Hvis man ser overfladisk på Bitcoin, kan man konkludere, at den er langsom, spild af ressourcer, unødvendigt redundant og overdrevent paranoid. Hvis man ser nysgerrigt på Bitcoin, finder man måske ud af, at tingene ikke er, som de ser ud ved første øjekast.

Bitcoin har det med at tage dine antagelser og vende dem på hovedet. Efter et stykke tid, lige når du er ved at finde dig til rette igen, bryder Bitcoin igennem muren som en elefant i en porcelænsbutik og knuser dine antagelser endnu en gang.

Bitcoin er et barn af mange discipliner. Som blinde munke, der undersøger en elefant, vil alle se denne nye teknologi fra sin egen vinkel. Og alle vil nå frem til forskellige konklusioner om dyrets natur.

De følgende lektioner handler om nogle af mine antagelser, som Bitcoin knuste, og de konklusioner, jeg nåede frem til. Filosofiske spørgsmål om uforanderlighed, knaphed, lokalitet og identitet bliver udforsket i de første fire lektioner. Hver del består af syv lektioner.



Figur 0.1.: Blinde munke undersøger Bitcoin-elefanten

Del I – Filosofi:

1. Uforanderlighed og forandring
2. Knaphedens knaphed
3. Replikation og lokalitet
4. Problemet med identitet
5. En perfekt undfangelse
6. Ytringsfrihedens kraft
7. Grænserne for viden

Lektion 5 udforsker hvordan Bitcoins oprindelseshistorie ikke bare er fascinerende, men også helt afgørende for et lederløst system. De sidste to lektioner i dette kapitel udforsker ytringsfrihedens kraft og grænserne for vores individuelle viden, hvilket afspejles af Bitcoin-kaninhullets overraskende dybde.

Jeg håber, at du vil finde Bitcoins verden lige så lærerig, fascinerende og underholdende, som jeg gjorde og stadig gør. Jeg inviterer dig til at følge den hvide kanin og udforske dybderne i dette kaninhul. Hold nu fast i dit lommeur, hop ned og nyd faldet.

1. Uforanderlighed og forandring

*„Mon jeg er blevet en anden i nattens løb?
Vent nu lidt - var jeg den samme, da jeg stod
op i morges? Jeg synes næsten, jeg kan hu-
ske, 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

Bitcoin er i sagens natur svær at beskrive. Det er en *ny ting*, og ethvert forsøg på at drage en sammenligning med tidligere koncepter - om det så er ved at kalde det digitalt guld eller pengenes internet - vil utvivlsomt komme til kort. Uanset hvilken analogi du foretrækker, er der to aspekter af Bitcoin, som er helt essentielle: decentralisering og uforanderlighed.

En måde at tænke på Bitcoin er som en automatiseret social kontrakt¹. Softwaren er kun en brik i puslespillet, og at håbe på at ændre Bitcoin ved at ændre softwaren er en nytteløs øvelse. Man bliver nødt til at overbevise resten af netværket om at indføre ændringerne, hvilket mere er en psykologisk indsats end en softwareteknisk.

Det følgende vil måske lyde absurd i begyndelsen, som så mange andre ting på dette område, men ikke desto mindre tror jeg, at det er sandt: Du kan ikke ændre Bitcoin, men Bitcoin vil ændre dig.

¹Hasu, Unpacking Bitcoin's Social Contract [33]

„Bitcoin vil ændre os mere, end vi vil ændre den.“

– Marty Bent²

Det tog mig lang tid at indse dybden af dette. Eftersom Bitcoin bare er software, og det hele er open source, kan man bare ændre tingene efter forgodtbefindende, ikke? Forkert. *Meget* forkert. Det er ikke overraskende, at Bitcoins skaber fuldt ud var klar over dette.

„Bitcoins natur er sådan, at da version 0.1 blev frigivet, blev kerneldesignet mejslet i sten for resten af dens levetid.“

– Satoshi Nakamoto³

Mange mennesker har forsøgt at ændre Bitcoins natur. Indtil videre har de alle fejlet. Mens der er et endeløst hav af forgreninger og altcoins (alternativer til Bitcoins), gør Bitcoin-netværket stadig sin ting, ligesom det gjorde, da det første knudepunkt gik online. Altcoins vil ikke have betydning i det lange løb. Forgreningerne vil til sidst uddø. Bitcoin er det eneste, der virkelig betyder noget. Så længe vores grundlæggende forståelse af matematik og/eller fysik ikke ændrer sig, vil Bitcoin fortsætte uden bekymringer.

„Bitcoin er det første eksempel på en ny livsform. Den 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 stoppes. Hvis atomkrig ødelagde halvdelen af vores planet, ville den fortsætte med at leve ubeskadiget.“

– Ralph Merkle⁴

²Tales From the Crypt [10]

³BitcoinTalk forumindlæg: ‘Re: Transactions and Scripts...’ [57]

⁴DAOs, Democracy and Governance, [45]

Bitcoin-netværkets hjerteslag vil overleve alle vores.

At indse ovenstående ændrede mig langt mere, end de tidligere blokke i Bitcoins blokkæde nogensinde vil gøre. Det ændrede min tidspræference, min forståelse af økonomi, mine politiske synspunkter og så meget mere. Den ændrer endda folks kostvaner.⁵. Hvis du synes, at alt dette virker skørt, er du i godt selskab. Alt dette er skørt, men alligevel sker det.

Bitcoin har lært mig, at den ikke ændrer sig. Det gør jeg.

⁵Inside the World of the Bitcoin Carnivores, [59]

2. Knaphedens knaphed

„Det er mere end nok - jeg håber, jeg ikke vokser mere...“

– Alice

Generelt synes den teknologiske udvikling at gøre ting mere tilgængelige. Flere og flere mennesker er i stand til at nyde, det, der tidligere har været luksusvarer. Snart vil vi alle leve som konger, hvilket de fleste af os allerede gør. Som Peter Diamandis skrev i *Abundance* [24]: „Teknologi er en ressourcefrigørende mekanisme. Den kan forvandle det, som engang var knapt, til det, der nu er rigeligt.“

Bitcoin, som i sig selv er en avanceret teknologi, bryder med denne tendens og skaber en ny vare, som er virkelig knap. Der er endda nogle, der hævder, at det er en af de mest knappe ting i universet. Udbuddet af Bitcoins kan ikke øges, uanset hvor mange kræfter der anvendes på at skabe mere.

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

– Saifedean Ammous¹

Paradoksalt nok gør den det ved hjælp af en kopieringsmekanisme. Transaktionerne sendes, blokkene distribueres, den distribuerede hovedbog (som er en logbog med alle transaktionerne) er - ja, du gættede det - distribueret. Alle disse ord betyder i virkeligheden bare kopiering. For pokker, Bitcoin kopierer endda sig selv til så mange computere som muligt ved at tilskynde individuelle mennesker til at køre fulde knudepunkter og udvinde nye blokke.

¹Præsentation af Bitcoinstandarden [2]

Alt det arbejde, der er med duplikering, er en vidunderlig, koordineret indsats for at skabe ægte knaphed.

I en tid med overflod har Bitcoin lært mig, hvad reel knaphed er.

3. Replikation og lokalitet

*Så kom der en vred stemme - kaninens - „Pat,
Pat! Hvor er du?“*

– Lewis Carroll, *Alice i Eventyrland*

Bortset fra kvantemekanik er lokalitet ikke et problem i den fysiske verden. Spørgsmålet „*Hvor er X?*“ kan let besvares, uanset om X er en person eller et objekt. I den digitale verden er spørgsmålet om *hvor* allerede et vanskeligt spørgsmål, men ikke umuligt at besvare. Hvor er dine e-mails egentlig? Et dårligt svar ville være „*skyen*“, som bare er en andens computer. Men hvis du ønskede finde alle de harddiske, som dine e-mails er gemt på, kunne du i teorien finde dem.

Med bitcoin er spørgsmålet om „*hvor*“ *virkeligt* vanskeligt. Hvor er dine bitcoins helt præcist?

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

– Daniel Dennett¹

Problemet er todelt: For det første er den distribuerede hovedbog distribueret gennem fuld replikation, hvilket betyder, at hovedbogen er overalt. For det andet er der ingen bitcoins. Hverken fysisk eller *teknisk*.

Bitcoin holder styr på et sæt ubrugte transaktionsoutputs uden nogensinde at skulle henvise til en enhed, der repræsenterer

¹Daniel Dennett, *Where Am I?* [22]

en bitcoin. Eksistensen af én bitcoin udledes ved at se på mængden af ubrugte transaktionsoutputs og gennemgå alle tidligere overførsler, hvor summen af alle overførelser giver 100 millioner satoshis, som er basisenheden for en bitcoin.

„Hvor er de på nuværende tidspunkt i transit? For det første er der ingen bitcoins. De eksisterer simpelt hen ikke. De eksisterer ikke. Der er hovedbogsposter i en hovedbog, der er delt. De findes ikke på noget fysisk 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 Valkenburgh²

Så hvad ejer du egentlig, når du siger „*Jeg har en bitcoin*“, hvis der ikke findes nogen bitcoins? Kan du huske alle de mærkelige ord, som du blev tvunget til at skrive ned af din bitcoin-tegnebog? Det viser sig, at disse magiske ord er, hvad du ejer: en trylleformular³ som kan bruges til at tilføje poster til den offentlige hovedbog - nøglerne til at „flytte“ nogle bitcoins. Det er derfor, at dine private nøgler i praksis *er* dine bitcoins. Hvis du tror, at jeg finder på alt det her, er du velkommen til at sende mig dine private nøgler.

Bitcoin har lært mig, at lokalitet er en vanskelig størrelse.

²Peter Van Valkenburgh i podcasten *What Bitcoin Did*, episode 49 [73]

³The Magic Dust of Cryptography: How digital information is changing our society [31]

4. Problemet med identitet

„Hvem er du?“ spurgte larven.

– Lewis Carroll, *Alice i Eventyrland*

Nic Carter har i en hyldest til Thomas Nagels behandling af det samme spørgsmål, i forbindelse med en flagermus, skrevet en fremragende artikel, der diskuterer følgende spørgsmål: Hvordan er det at være en bitcoin? Han viser på glimrende vis, at åbne, offentlige blokkæder i almindelighed og Bitcoin i særdeleshed lider under den samme gåde som Theseus' skib¹: Hvilken Bitcoin er den rigtige Bitcoin?

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

– Nic Carter²

Det ser ud til, at teknologiens fremskridt fortsætter med at tvinge os til at tage disse filosofiske spørgsmål alvorligt. Før

¹I identitetens metafysik er Theseus' skib et tankeeksperiment, der rejser spørgsmålet om, hvorvidt et objekt, der har fået udskiftet alle sine komponenter, grundlæggende forbliver det samme objekt. [98]

²Nic Carter, *What is it like to be a bitcoin?* [19]

eller senere vil selvkørende biler blive konfronteret med virkelige versioner af „sporvognsproblemet“, hvor de bliver tvunget til at træffe etiske beslutninger om, hvilke liv der betyder noget, og hvilke der ikke gør.

Kryptovalutaer, især siden den første omstridte hårde-forgrening, tvinger os til at tænke over og blive enige om identitetens metafysik. Det er interessant, at de to største eksempler, vi hidtil har set, har ført til to forskellige svar. Den 1. august 2017 delte Bitcoin sig i to lejre. Markedet besluttede, at den uændrede kæde er den originale Bitcoin. Et år tidligere, den 25. oktober 2016, delte Ethereum sig i to lejre. Markedet besluttede, at den ændrede kæde er den oprindelige Ethereum.

Hvis fuldt decentraliseret, vil spørgsmålene stillet af *Theseus'* skib skulle besvares igen og igen, så længe disse netværk af værdioverførsel eksisterer.

Bitcoin har lært mig, at decentralisering er i modstrid med identitet.

5. En perfekt undfangelse

„Deres hoveder er væk,“ råbte soldaterne som svar....

– Lewis Carroll, *Alice i Eventyrland*

Alle elsker en god oprindelseshistorie. Bitcoins oprindelseshistorie er fascinerende, og detaljerne i den er vigtigere, end man umiddelbart skulle tro. Hvem er Satoshi Nakamoto? Var han én person eller en gruppe mennesker? Var han en kvinde? Et tidsrejsende rumvæsen eller en avanceret kunstig intelligens? Hvis vi ser bort fra de besynderlige teorier, vil vi nok aldrig finde ud af det. Og det er vigtigt.

Satoshi valgte at være anonym. Han plantede frøet til Bitcoin. Han blev hængende længe nok til at sikre, at netværket ikke døde i sin barndom. Og så forsvandt han.

Det som kan se ud som et underligt anonymitetsstunt, er faktisk afgørende for et ægte decentraliseret system. Der er ingen centraliseret kontrol, ingen centraliseret autoritet og ingen opfinder. Ingen at retsforfølge, torturere, afpresse eller udnytte. Det er en perfekt undfangelse af teknologi.

„En af de største ting, Satoshi gjorde, var at forsvinde.“

– Jimmy Song¹

¹Jimmy Song, *Why Bitcoin is Different.* [67]

Siden Bitcoins fødsel er der blevet skabt tusindvis af andre kryptovalutaer. Ingen af disse kloner deler dens oprindelseshistorie. Hvis du vil erstatte Bitcoin, bliver du nødt til at overgå dens oprindelseshistorie. Ideernes overlevelse dikteres af de fortællinger, som spredes.

„Guld blev først formet til smykker og brugt til byttehandel for mere end 7.000 år siden. Guldets fængslende glans førte til, at det blev betragtet som en gave fra guderne.“

Münze Österreich²

Ligesom guld i oldtiden, kan Bitcoin betragtes som en gave fra guderne. I modsætning til guld er Bitcoins oprindelse udelukkende menneskelig. Og denne gang ved vi, hvem guderne bag udvikling og vedligeholdelse er: mennesker over hele verden, anonyme eller ej.

Bitcoin har lært mig, at fortællinger er vigtige.

²Münze Österreich, *Gold: The Extraordinary Metal* [47]

6. Ytringsfrihedens kraft

*„Undskyld?“ sagde musen og rynkede panden,
men meget høfligt, „talte du?“*

– Lewis Carroll, *Alice i Eventyrland*

Bitcoin er en idé. En idé, som i sin nuværende form er manifestationen af et maskineri, der udelukkende drives af tekst. Alle aspekter af Bitcoin er tekst: Hvidbogen (whitepaper) er tekst. Softwaren, som køres af knudepunkterne, er tekst. Hovedbogen er tekst. Transaktioner er tekst. Offentlige og private nøgler er tekst. Alle aspekter af Bitcoin er tekst og svarer dermed til ytring.

„Kongressen må ikke vedtage nogen lov, der vedrører oprettelsen af en religion, eller forbud mod dens frie udøvelse; eller indskrænker ytringsfriheden, eller presensis frihed, eller folks ret til fredeligt at samles og at anmode staten om at få klagemål behandlet.“

– Første tilføjelse til USA's forfatning

Selvom det sidste slag i kryptokrigen¹ ikke er blevet udkæmpet endnu, vil det være meget svært at kriminalisere en idé, især en der er baseret på udveksling af tekstbeskeder. Hver gang en stat forsøger at forbyde tekst eller tale, glider vi ned ad en absurd sti, som uundgåeligt fører til vederstyggeligheder såsom

¹Kryptokrigen er et uofficielt navn for USA's og dets allieredes forsøg på at underminere kryptering. [27] [78]

ulovlige tal² og ulovlige primtal³.

Så længe der er en del af verden, hvor tale er fri som i *frihed*, er Bitcoin ustoppelig.

„Der er ikke noget tidspunkt i en Bitcoin-transaktion, hvor Bitcoin ophører med at være *tekst*. Det er *altid tekst*, hele tiden. Bitcoin er *tekst*. Bitcoin er *tale*. Det kan ikke reguleres i et frit land som USA med umistelige garanterede rettigheder og en *første forfatningstilføjelse*, der udtrykkeligt udelukker udgivelseshandlinger fra statsligt tilsyn.“

– Beautyon⁴

Bitcoin har lært mig, at ytringsfrihed og fri software er ustoppelige i et frit samfund.

²Et ulovligt tal er et tal, der repræsenterer information, som er ulovlig at besidde, fremsige, formidle eller på anden måde overføre i visse jurisdiktioner.[84]

³Et ulovligt primtal er et tal, der repræsenterer information, hvis besiddelse eller distribution er forbudt i visse jurisdiktioner. Et af de første ulovlige primtal blev fundet i 2001. Når det fortolkes på en bestemt måde, beskriver det et computerprogram, der omgår det digitale rettighedsstyringssystem, der bruges på DVD'er. Distribution af et sådant program i USA er ulovligt i henhold til Digital Millennium Copyright Act. Et ulovligt primtal er en form for ulovligt tal.[85]

⁴Beautyon, *Why America can't regulate Bitcoin* [7]

7. Grænserne for viden

„Ned, ned, ned. Ville faldet aldrig få en ende?“

– Lewis Carroll, *Alice i Eventyrland*

At begynde at arbejde med Bitcoin er en ydmygende oplevelse. Jeg troede, at jeg vidste ting. Jeg troede, at jeg var veludannet. Jeg troede, at jeg i det mindste kunne min datalogi. Jeg har studeret det i årevis, så jeg burde da vide alt om digitale signaturer, hashfunktioner, kryptering, driftssikkerhed og netværk, ikke sandt?

Forkert.

Det er svært at lære alle de grundlæggende elementer, der får Bitcoin til at virke. At forstå dem alle i dybden er på grænsen til det umulige.

„Ingen har fundet bunden af Bitcoin-kaninhullet.“

– Jameson Lopp¹

Min liste over bøger, jeg skal læse, bliver ved med at vokse hurtigere, end jeg kan nå at læse dem. Listen over aviser og artikler, der skal læses, er næsten uendelig. Der er flere podcasts om alle disse emner, end jeg nogensinde ville kunne nå at lytte til. Det er virkelig overvældende. Desuden udvikler Bitcoin sig, og det er næsten umuligt at holde sig ajour med den accelererende innovationshastighed. Støvet fra det første lag har ikke

¹Jameson Lopp, tweet fra 11. november 2018 [42]



Figur 7.1.: Bitcoin-kaninhullet er bundløst.

engang lagt sig endnu, og folk har allerede bygget det andet lag og arbejder på det tredje.

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

Del II.

Økonomi

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 Eventyrland*

Penge vokser ikke på træerne. Det er tåbeligt at tro, at de gør det, og vores forældre sørger for, at vi ved det, ved at gentage dette ordsprog som et mantra. Vi bliver opfordret til at bruge penge fornuftigt, til ikke at bruge dem letsindigt, og til at spare dem op i gode tider, så de kan hjælpe os gennem de dårlige. Penge vokser trods alt ikke på træerne.

Bitcoin har lært mig mere om penge, end jeg nogensinde troede, jeg ville få brug for at vide. Gennem den blev jeg tvunget til at udforske pengenes historie, bankvæsenet, forskellige økonometriske skoler og mange andre emner. Min søgen efter at forstå Bitcoin førte mig ned ad et væld af stier, hvoraf jeg forsøger at udforske nogle i dette kapitel.

I de første syv lektioner blev nogle af de filosofiske spørgsmål, som Bitcoin berører, diskuteret. De næste syv lektioner vil undersøge penge og økonomi nærmere.

Del II – Økonomi:

8. Økonomisk uvidenhed
9. Inflation
10. Værdi
11. Penge
12. Pengenes historie og undergang
13. Vanværdet i brøkreserve-bankvæsenet
14. Stabile penge

Igen vil jeg kun være i stand til at kradse i overfladen. Bitcoin er ikke bare ambitiøst, men også bredt og dybt, hvilket gør det umuligt at dække alle relevante emner i en enkelt lektion, essay, artikel eller bog. Jeg tvivler på, at det overhovedet er muligt.

Bitcoin er en ny form for penge, hvilket gør det afgørende at lære om økonomi for at forstå den. Økonomi handler om menneskelige handlinger og sammenspillet mellem økonomiske aktører, og det er sandsynligvis en af de største og mest uklare brikker i Bitcoin-puslespillet.

Igen er disse lektioner en udforskning af de forskellige ting, jeg har lært af Bitcoin. De er en personlig afspejling af min rejse ned i kaninhullet. Da jeg ikke har nogen økonomisk baggrund, er jeg helt sikkert uden for min komfortzone og klar over, at enhver forståelse, jeg måtte have, er ufuldstændig. Jeg vil gøre mit bedste for at skitsere, hvad jeg har lært, selv med risiko for at gøre mig selv til grin. Når alt kommer til alt, forsøger jeg stadig at besvare spørgsmålet: „*Hvad har du lært af Bitcoin?*“

Efter syv lektioner set gennem filosofiens briller, lad os bruge økonomiens briller til at se på syv mere. En tur på økonomiklasse er alt, hvad jeg kan tilbyde denne gang. Slutdestination: *stabile penge*.

8. Finansiel uvidenhed

„'Og hun vil sikkert synes, jeg er en dum lille pige! Nej, jeg vil ikke spørge om det. Jeg kan måske læse navnet et eller andet sted.'“

– Lewis Carroll, *Alice i Eventyrland*

En af de mest overraskende ting for mig var den mængde af finans, økonomi og psykologi, der kræves for at få en forståelse af, hvad der ved første øjekast ser ud til at være et rent *teknisk* system - et computernetværk. Som en lille fyr med behårede fødder sagde: „Det er en farlig forretning, Frodo, at træde ind i Bitcoin-verdenen. Du læser hvidbogen, og hvis du ikke holder dig på mætten, er det ikke til at vide, hvor du bliver ført hen.“

For at forstå et nyt monetært system, er man nødt til at kende det gamle. Jeg begyndte meget hurtigt at indse, at den mængde finansiel uddannelse, jeg havde fået i uddannelsessystemet, stort set var *nul*.

Som femårig begyndte jeg at stille mig selv en masse spørgsmål: Hvordan fungerer banksystemet? Hvordan fungerer aktiemarkedet? Hvad er fiat-penge? Hvad er *almindelige* penge? Hvorfor er der så megen gæld?¹ Hvor mange penge bliver der egentlig trykt, og hvem bestemmer det?

¹<https://www.usdebtclock.org/>

Efter en mild panik over omfanget af min uvidenhed, fandt jeg tryghed i at indse, at jeg var i godt selskab.

„Er det ikke ironisk, at Bitcoin har lært mig mere om penge end alle de år, jeg har brugt på at arbejde for finansielle institutioner? … herunder, da jeg startede min karriere i en centralbank“

– Aaron²

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

– Dunny³

Dette er blot to af de mange bekendelser, der florerer på Twitter.⁴ Bitcoin, som blev udforsket i Lektion 1, er en levende ting. Mises hævdede, at økonomi også er en levende ting. Og som vi alle ved fra personlig erfaring, er levende ting i sagens natur svære at forstå.

„Et videnskabeligt system er blot en station i en endeløs søgen efter viden. Det er nødvendigvis påvirket af den 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.“

– Ludwig von Mises⁵

²Aaron (@aarontaycc, @fiatminimalist), tweet fra 12. december 2018 [46]

³Dunny (@BitcoinDunny), tweet fra 28. november 2017 [25]

⁴Se <http://bit.ly/btc-learned> for flere bekendelser på Twitter.

⁵Ludwig von Mises, *Human Action* [74]

Vi læser alle om forskellige finanskriser i nyhederne, og underer os over, hvordan disse store redningspakker fungerer. Vi er forundrede over, at ingen nogensinde synes at blive stillet til ansvar for skader, der løber op i billioner. Jeg er stadig forundret, men i det mindste er jeg begyndt at få et indblik i, hvad der foregår i finansverdenen.

Nogle mennesker går endda så langt, at de tilskriver den generelle uvidenhed om disse emner til systemisk, bevidst uvidenhed. Mens historie, fysik, biologi, matematik og sprog alle er en del af vores uddannelse, bliver verdenen inden for penge og økonomi overraskende nok kun udforsket overfladisk, hvis overhovedet. Jeg spekulerer på, om folk stadig ville være villige til at optage så meget gæld, som de gør i øjeblikket, hvis alle blev uddannet i privatøkonomi og i, hvordan penge og gæld fungerer. Og så spekulerer jeg på, hvor mange lag aluminium der skal til for at lave en effektiv solvpapirhat. Sandsynligvis tre.

„Disse nedbrud og redningspakker er ikke tilfældigheder. Og det er heller ikke et uheld, at der ikke er nogen finansiell uddannelse i skolen. Det er overlagt. Ligesom det før borgerkrigen var ulovligt at udanne en slave, har vi ikke lov til at lære om penge i skolen.“

– Robert Kiyosaki⁶

Ligesom i Troldmanden fra Oz bliver vi bedt om ikke at være opmærksomme på manden bag kulisserne. I modsætning til i Troldmanden fra Oz, har vi nu ægte trolddom⁷: et ucensurerbart, åbent, grænseløst netværk af værdioverførsel. Der er ingen kulisser, og magien er synlig for alle.⁸

⁶Robert Kiyosaki, *Why the Rich are Getting Richer*[40]

⁷<http://bit.ly/btc-wizardry>

⁸<https://github.com/bitcoin/bitcoin>

Bitcoin har lært mig at kigge bag kulisserne og at se min økonomiske uvidenhed i øjnene.

9. Inflation

*„Min kære, her må vi løbe så hurtigt, vi kan,
bare for at blive samme sted. Og hvis du vil
nogen steder hen, må du løbe dobbelt så hur-
tigt.“*

– Hjerter Dame

At forsøge at forstå den monetære inflation, og hvordan et ikke-inflationært system som Bitcoin kan ændre den måde, hvorpå vi gør tingene, var udgangspunktet for min rejse ind i økonomiens verden. Jeg vidste, at inflation var den hastighed, hvormed nye penge blev skabt, men jeg vidste ikke meget mere end det.

Mens nogle økonomer mener, at inflation er en god ting, mener andre, at „hårde“ penge, som ikke let kan skabes - som vi havde det i guldstandardens dage - er afgørende for en sund økonomi. Bitcoin, der har et fastsat udbud på 21 millioner, læner sig opad den sidstnævnte lejr.

Normalt er effekten af inflation ikke umiddelbart indlysende. Afhængigt af inflationsraten (og andre faktorer) kan der gå flere år mellem årsag og effekt. Ikke nok med det, men inflationen påvirker også forskellige grupper af mennesker mere end andre. Som Henry Hazlitt påpeger i *Økonomi i én lektion*: „Økonomiens kunst består i at se ikke blot på de umiddelbare, men også på de længere effekter af enhver handling eller politik; den består i at spore konsekvenserne af denne politik ikke blot for én gruppe, men for alle grupper.“

En af mine personlige aha-oplevelser var erkendelsen af, at udstedelse af ny valuta - trykning af flere penge - er en helt anderledes økonomisk aktivitet end alle de andre økonomiske

aktiviteter. Mens rigtige varer og rigtige tjenester producerer rigtig værdi for rigtige mennesker, gør det at trykke penge det modsatte: Det fjerner værdi fra alle, der har den valuta, som er inflationær.

„Ren inflation - det vil sige, den blotte udstedelse af flere penge, hvilket resulterer i højere lønninger og priser - kan give det indtryk, at der skabes mere efter-spørgsel. Men den faktiske produktion og udveksling af virkelige varer øges ikke.“

– Henry Hazlitt¹

Inflationens destruktive kraft bliver tydelig, så snart en smule inflation bliver til *meget* inflation. Hvis der opstår hyperinflation, bliver tingene hurtigt slemme.² Når den inflationære valuta falder fra hinanden, kan den ikke lagre værdi over tid, og folk vil skynde sig at få fat i de varer, der kan.

En anden konsekvens af hyperinflation er, at alle de penge, som folk har sparet op i løbet af deres liv, reelt set forsvinder. Papirpengene i din tegnebog vil selvfølgelig stadig være der, men de vil være værdiløst papir.

Penge falder også i værdi med såkaldt „mild“ inflation. Det sker bare langsomt nok til, at de fleste mennesker ikke lægger mærke til, at deres købekraft mindskes. Og når først seddelpreserne kører, kan hvad der før var mild inflation, med et tryk på en knap, blive til højere inflation. Som Friedrich Hayek påpegede i et af sine essays, fører mild inflation som regel til decideret inflation.

¹Henry Hazlitt, *Økonomi i én lektion* [36]

²<https://da.wikipedia.org/wiki/Hyperinflation> [83]



Figur 9.1.: Hyperinflation in the Weimar Republic (1921-1923)

„En mild, stabil inflation hjælper ikke - den kan kun føre til decideret inflation.“

– Friedrich Hayek³

Inflation er især lusket, fordi den favoriserer dem, der er tættere på seddelpresserne. Det tager tid for de nyskabte penge at cirkulere og priserne at tilpasse sig, så hvis du er i stand til at få fat i flere penge, før alle penge devalueres, er du foran inflationskurven. Det er også derfor, at inflation kan ses som en skjult skat, fordi staten i sidste ende tjener på det, mens alle andre ender med at betale prisen.

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

– Friedrich Hayek⁴

³Friedrich Hayek, *1980s Unemployment and the Unions* [34]

⁴Friedrich Hayek, *Good Money* [35]

Indtil videre er alle statskontrollerede valutaer med tiden blevet erstattet eller kollapset fuldstændig. Uanset hvor lille inflationsraten er, er „stabil“ vækst bare en anden måde at sige eksponentiel vækst. I naturen, som i økonomien, vil alle systemer, der vokser eksponentielt, til sidst flade ud eller lide af et katastrofalt sammenbrud.

„Det kan ikke ske i mit land“ tænker du sikkert. Det tænker du ikke, hvis du er fra Venezuela, som i øjeblikket lider af hyperinflation. Med en inflationsrate på over 1 million procent er penge stort set værdiløse. [75]

Det sker måske ikke inden for de næste par år, eller med den valuta, der bruges i dit land. Men et blik på listen over historiske valutaer⁵ viser, at det uundgåeligt vil ske over en tilstrækkelig lang periode. Jeg husker og brugte mange af de nævnte: den østrigske schilling, den tyske mark, den italienske lire, den franske franc, det irske pund, den kroatiske dinar osv. Min bedstemor brugte endda den østrig-ungarske krone. Som tiden går, bliver de valutaer, der i øjeblikket bruges⁶ vil langsomt, men sikkert bevæge sig mod deres respektive kirkegårde. De vil opleve hyperinflation eller blive erstattet. De vil snart være historiske valutaer. Vi vil gøre dem forældede.

„Historien har vist, at staterne uundgåeligt vil falde for fristelsen til at øge pengemængden.“

– Saifedean Ammous⁷

⁵Se *List of historical currencies* på den engelske udgave af Wikipedia. [91]

⁶Se *List of currencies* på den engelske udgave af Wikipedia [90]

⁷Saifedean Ammous, *Bitcoinstandarden* [1]

Hvorfor er Bitcoin anderledes? I modsætning til statslige valutaer, er monetære varer ikke reguleret af stater, men af fysikagens love⁸, have en tendens til at overleve og endda bevare deres respektive værdi over tid. Det bedste eksempel på dette indtil videre er guld, som med det passende navn *Guld-til-anstændigt-jakkesæt-forhold*⁹ bevarer den sin værdi over hundreder og endda tusinde år. Den er muligvis ikke perfekt „stabilt“ - et tvivlsomt koncept i første omgang - men den værdi, det har, vil i det mindste være i samme størrelsesorden.

Hvis en monetær vare eller valuta er god til at fastholde sin værdi over tid og rum, anses den for at være *hård*. Hvis den ikke formår at opretholde sin værdi, på grund af nem forringelse eller inflation, betragtes den som en *blød* valuta. Begrebet hårdhed er essentielt for at forstå Bitcoin og fortjener en grundigere undersøgelse. Vi vil tage emnet op igen i den sidste økonomilektion: stabile penge.

Efterhånden som flere og flere lande rammes af hyperinflation, vil flere og flere mennesker blive nødt til at forholde sig til virkeligheden med hårde og bløde penge. Hvis vi er heldige, vil nogle centralbankchefer måske endda blive tvunget til at revurdere deres pengepolitiske strategier. Uanset hvad der måtte ske, vil den indsigt, jeg har fået takket være Bitcoin, sandsynligvis være uvurderlig, uanset udfaldet.

Bitcoin har lært mig om den skjulte skat ved inflation samt katastrofen forbundet med hyperinflation.

⁸Gigi, *Bitcoin's Energy Consumption - A shift in perspective* [30]

⁹Historien viser, at prisen på en ounce (31,1 gram) guld svarer til prisen på et anstændigt jakkesæt, ifølge Sionnas investeringsforvaltere [43]

10. Værdi

„Det var den hvide kanin, der traskede lang-som tilbage igen og så sig ængsteligt omkring, som om den havde mistet noget...“

– Lewis Carroll, *Alice i Eventyrland*

Værdi er på en måde paradoksal, og der er flere teorier¹ som forsøger at forklare, hvorfor vi værdsætter visse ting frem for andre ting. Dette paradoks har mennesker været opmærksomme på i tusinder af år. Som Platon skrev i sin dialog med Euthydemus, værdsætter vi nogle ting, fordi de er sjældne, og ikke blot på grund af deres nødvendighed for vores overlevelse.

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

– Platon²

Dette paradoks af værdi³ viser noget interessant om os mennesker: Det virker, som om vi værdsætter ting på et subjektivt⁴ grundlag, men gør det med visse ikke-tilfældige kriterier. Noget kan være *dyrebart* for os af forskellige årsager, men ting vi

¹Se *Theory of value (economics)* på den engelske udgave af Wikipedia [102]

²Platon, *Euthydemus* [61]

³Se *Paradox of value* på den engelske udgave af Wikipedia [96]

⁴Se *Subjective theory of value* på den engelske udgave af Wikipedia [100]

værdsætter, deler visse karakteristika. Hvis vi let kan kopiere noget, eller hvis det er i naturligt overflod, værdsætter vi det ikke.

Det ser ud til, at vi værdsætter noget, fordi det er knapt (guld, diamanter, tid), svært eller arbejdskrævende at producere, uerstatteligt (et gammelt fotografi af en, vi elsker), er nyttigt på en måde, hvor det gør os i stand til at gøre ting, vi ellers ikke kunne, eller en kombination af disse, såsom store kunstværker.

Bitcoin er alt det ovenstående: Den er ekstrem knap (21 millioner), stadig sværere at producere (blokbelønning halveres), kan ikke erstattes (en tabt privat nøgle er tabt for evigt) og gør det muligt for os at udføre nogle ret nyttige ting. Det er uden tvivl det bedste værktøj til værdioverførsel på tværs af grænser, modstandsdygtigt over for censur og konfiskation i processen. Den er også et selvstændig værdilager, der giver enkeltpersoner mulighed for at opbevare deres formue uafhængigt af banker og stater. Bare for at nævne et par ting.

Bitcoin har lært mig, at værdi er subjektiv, men ikke vilkårlig.

11. Penge

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

– Den vise

Hvad er penge? Vi bruger dem hver dag, men alligevel er dette spørgsmål overraskende svært at besvare. Vi er afhængige af dem i stort og småt, og hvis vi har for få, bliver vores liv meget vanskeligt. Alligevel tænker vi sjældent over den ting, der angiveligt får verden til at dreje rundt. Bitcoin har tvunget mig til at besvare det samme spørgsmål igen og igen: Hvad pokker er penge overhovedet?

I vores „moderne“ verden vil de fleste nok tænke på papirstykker, når de taler om penge, selvom de fleste af vores penge bare er et tal på en bankkonto. Vi bruger allerede nuller og ettal-ler som vores penge, så hvordan er Bitcoin anderledes? Bitcoin er anderledes, fordi det i sin kerne er en meget anderledes *type* penge end de penge, vi bruger i øjeblikket. For at forstå dette bliver vi nødt til at se nærmere på, hvad penge er, hvordan de blev til, og hvorfor guld og sølv blev brugt i det meste af handelshistorien.

Muslingeskaller, guld, sølv, papir, bitcoin. I sidste ende **er penge det, som folk accepterer som betalingsmiddel**, uanset dets form eller mangel på samme.

Penge er en genial opfindelse. En verden uden penge er vanvittigt kompliceret: Hvor mange fisk koster et par nye sko? Hvor mange køer koster et nyt hus? Hvad nu, hvis jeg ikke har brug for noget lige nu, men er nødt til at skille mig af med mine snart rådne æbler? Man behøver ikke meget fantasi for at indse, at en byttehandel er vanvittigt ineffektiv.

Det fantastiske ved penge er, at de kan veksles til *alt muligt andet* - det er noget af en opfindelse! Som Nick Szabo¹ sammenfatter på glimrende vis i *Shelling Out: The Origins of Money* [69], har vi mennesker brugt alle mulige ting som penge: perler lavet af sjældne materialer som elfenben, skaller eller særlige knogler, forskellige slags smykker og senere sjældne metaller som sølv og guld.

„I den forstand minder den (Bitcoin) mere om et ædelmetal. I stedet for at udbuddet ændrer sig for at holde værdien den samme, er udbuddet forudbestemt, og værdien ændrer sig.“

– Satoshi Nakamoto²

Som de dovne væsener vi er, tænker vi ikke så meget over ting, der bare fungerer. For de fleste af os fungerer penge helt fint. Ligesom med vores biler eller computere er de fleste af os kun tvunget til at tænke over disse tings indre funktion, hvis de bryder sammen. Folk, der har set deres livsopsparing forsvinde på grund af hyperinflation, kender værdien af stærke penge, ligesom folk, der har set deres venner og familie forsvinde på grund af grusomhederne i Nazityskland eller Sovjetunionen forstår værdien af privatliv.

Det særlige ved penge er, at de er altomfattende. Penge er halvdelen af enhver transaktion, hvilket giver dem, der har ansvaret for at skabe penge, en enorm magt.

¹<http://unenumerated.blogspot.com/>

²Satoshi Nakamoto, i et svar til Sepp Hasslberger [51]

„I betragtning af at penge udgør halvdelen af alle kommercielle transaktioner, og at hele civilisationer bogstaveligt talt opstår og falder på baggrund af kvaliteten af deres penge, taler vi om en fantastisk magt, som foregår i det skjulte. Det er magten til at skabe illusioner, der fremstår virkelige, så længe de varer. Det er selve kernen af centralbankernes magt.“

– Ron Paul³

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

Pengene gennemgik flere iterationer. De fleste iterationer var gode. De forbedrede vores penge på den ene eller anden måde. Men for ganske nylig blev vores penges indre funktioner korrumpe. I dag er næsten alle vores penge simpelthen skabt *ud af den blå luft* af magthaverne. For at forstå, hvordan det kunne ske, var jeg nødt til at lære om pengenes historie og efterfølgende undergang.

Om det vil kræve en række katastrofer, eller blot en enorm uddannelsesindsats for at rette op på denne korruption, er endnu uvist. Jeg beder til guderne for stabile penge om, at det bliver det sidste.

Bitcoin har lært mig, hvad penge er.

³Ron Paul, *End the Fed* (Afskaf den amerikanske centralbank) [58]

12. Pengenes historie og undergang

„De ville ikke huske de enkle regler, som deres venner havde givet dem, såsom 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, hvor der står 'gift', er det næsten sikkert, at det giver problemer før eller siden.“

– Lewis Carroll, *Alice i Eventyrland*

Mange mennesker tror, at penge er understøttet af guld, som er låst væk i store bankbokse, beskyttet af tykke mure. Det stoppede med at være sandt for mange årtier siden. Jeg er ikke sikker på, hvad jeg tænkte dengang, for jeg var i meget større problemer og havde stort set ingen forståelse af guld, papirpenge, eller hvorfor de overhovedet skulle være understøttet af noget.

En del af processen med at lære om Bitcoin er at forstå fiat-penge: hvad de betyder, hvordan de opstod, og hvorfor de måske ikke er den bedste idé, vi nogensinde har haft. Så hvad er fiat-penge egentlig? Og hvordan endte vi med at bruge dem?

Hvis noget er pålagt ved *fiat*, betyder det blot, at det er pålagt gennem en formel godkendelse eller et forslag. Således er fiat-penge penge, blot fordi *nogen* siger, at de er penge. Da alle stater bruger fiat-penge i dag, gælder det også *din* stat. Desværre er du ikke *frei* til at være uenig i dette værdiforslag. Du vil hurtigt føle, at dette forslag er alt andet end ikke-voldeligt. Hvis du nægter at bruge denne papirvaluta til at drive forretninger og betale skat, vil de eneste mennesker, du vil kunne diskutere økonomi



*late Middle English: from Latin, 'let it be done,' from *fieri* 'be done or made.'*

Figur 12.1.: fiat — ‘Lad det ske’

med, være dine cellekammerater.

Værdien af fiat-penge stammer ikke fra deres indbyggede egen-skaber. Hvor gode en bestemt type fiat-penge er, hænger kun sammen med den politiske og skattemæssige ustabilitet hos dem, der drømmer dem frem. Deres værdi pålægges ved dekret, vilkårligt.

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

Vi har allerede været inde på varepenge ovenfor. Folk brugte særlige knogler, muslingeskaller og ædelmetaller som penge. Senere blev det især mønter lavet af ædelmetaller som guld og sølv, der blev brugt som penge. Den ældste mønt, der indtil videre er blevet fundet, er fremstillet af en naturlig blanding af guld og sølv, og blev produceret for mere end 2700 år siden.¹ Hvis noget er nyt ved Bitcoin, er det ikke konceptet *coin* (mønt).

¹Ifølge den græske historiker Herodot, der skrev i det femte århundrede f.Kr., var lydierne det første folk, der brugte guld- og sølv-mønter. [48]



Figur 12.2.: Lydisk mønt. Billedet er licenseret under Creative Commons Attribution Share-Alike 4.0 af Classical Numismatic Group, Inc.

Det viser sig, at hamstring af mønter, eller *hodling*, for at bruge nutidens sprog, er næsten lige så gammelt som mønter. Den tidligste mønthamstrer var en person, der lagde næsten hundrede af disse mønter i en krukke og begravede den i fundamentet til et tempel, som først blev fundet 2.500 år senere. Det er en ret god offline opbevaring, hvis du spørger mig.

Én af ulempene ved at bruge ædelmetalmønter er, at de kan blive klippet, hvilket effektivt forringør møntens værdi. Nye mønter kan blive præget af de afklippede mønter, hvilket øger pengemængden over tid og devaluerer hver enkelt mønt i procesen. Folk barberede bogstaveligt talt så meget af deres sølvdollars, som de kunne slippe afsted med.

Da stater kun er glade for inflation, hvis det er dem, der skaber den, blev der gjort en indsats for at stoppe denne guerilla-devaluering. På klassisk politi-og-røver-manér blev møntklipperne stadig mere kreative med deres teknikker, hvilket tvang „møntmestrene“ til at blive endnu mere kreative med deres modforanstaltninger. Isaac Newton, den verdensberømte fysiker, der er kendt for *Principia Mathematica*, var en af disse mestre. Han tilskrives æren for at have tilføjet de små striber på siden af



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

mønterne, som stadig kan ses den dag i dag. Tiden med nem møntbarbering var forbi.

Selv med disse metoder til devaluering af mønter² holdt i skak, har de stadig andre problemer. De er klodsede og ikke særlig praktiske at transportere, især når der skal ske store værdioverførsler. Det er ikke særlig praktisk at dukke op med en stor pose sølv dollars, hver gang du vil købe en Mercedes.

Nu vi taler om tyske ting: Hvordan den amerikanske *dollar* fik sit navn, er en anden interessant historie. Ordet „dollar“ er afledt af det tyske ord *Thaler*, en forkortelse for *Joachimsthaler* [101]. En Joachimsthaler var en mønt, der blev præget i byen *Sankt Joachimsthal*. Thaler er simpelthen en forkortelse for nogen (eller noget), der kommer fra dalen, og fordi Joachimsthal var *dalen* for sølv møntproduktion, omtalte folk simpelthen disse sølv mønter som *Thaler*. Thaler (tysk) blev til daalders (hollandsk) og til sidst dollars (engelsk).

²Udover at klippe mønterne, var svedning (at ryste mønterne i en pose og opsamle det støv, der blev slidt af) og tilstopning (at lå et hul i midten og hamre mønten flad for at lukke hullet) de mest fremtrædende metoder til devaluering af mønter. [92]



Figur 12.4.: Den oprindelige „dollar“. Sankt Joachim er afbilledet med sin kappe og troldmandshat. Billedet er cc-by-sa af Wikipedia-bruger Berlin-George

Indførelsen af repræsentative penge indvarslede de stærke penge undergang. Guldcertifikater blev introduceret i 1863, og omkring femten år senere blev sølvdollaren også langsomt, men sikkert erstattet af gældsbeviser: sølvcertifikatet. [99]

Det tog omkring 50 år fra introduktionen af de første sølvcertifikater, til disse stykker papir blev forvandlet til noget, som vi i dag ville genkende som en amerikansk dollar.

Bemærk, at den amerikanske sølv-dollar fra 1928 i figur 12.5 stadig går under navnet *sølvcertifikat*, hvilket indikerer, at dette faktisk blot er et dokument, der angiver, at indehaveren af dette stykke papir har krav på et stykke sølv. Det er interessant at se, hvordan teksten, der indikerer dette, er blevet mindre fremtrædende over tid. Sporet af „certifikat“ forsvandt helt efter et stykke tid og blev erstattet af den beroligende erklæring om, at dette er Federal Reserves sedler.

Som nævnt ovenfor, skete det samme med guld. Det meste af verden havde en bimetallisk standard [77], hvilket betyder, at mønster primært var lavet af guld og sølv. At have certifikater



Figur 12.5.: En amerikansk sølv доллар fra 1928. „Betales til ihændehaveren på forespørgsel.“ Billede cc-by-sa af National Numismatic Collection ved the Smithsonian Institution

for guld, som kunne indløses til guldmønter, var sandsynligvis en teknologisk forbedring. Papir er mere praktisk, lettere, og da det kan opdeles vilkårligt blot ved at printe et mindre tal, er det lettere at opdele i mindre enheder.

For at minde indehaverne (brugerne) om, at disse certifikater var repræsentative for ægte guld og sølv, blev de farvet i overensstemmelse hermed, og det fremgik tydeligt af selve certifikatet. Du kan læse skriften flydende fra top til bund.

„Dette bekræfter, at der er deponeret et hundrede dollars i guldmønt i USA's skatkammer, som kan udbetales til ihændehaveren på forespørgsel.“

I 1963 blev ordene „PAYABLE TO THE BEARER ON DEMAND“ (betales til ihændehaveren på forespørgsel) fjernet fra alle nyudstede sedler. Fem år senere ophørte indløsningen af papirsedler til guld og sølv.

De ord, som hentyder til oprindelsen og idéen bag papirpenge, blev fjernet. Den gyldne farve forsvandt. Det eneste, der blev



Figur 12.6.: Dette er et amerikansk 100 dollars guldcertifikat fra 1928. Billedet er cc-by-sa fra National Numismatic Collection, National Museum of American History.

tilbage, var papiret og dermed statens mulighed for at trykke så mange sedler, som den ønsker.

Afskaffelsen af guldstandarden i 1971 fuldendte dette århundrede-lange trick. Penge blev forvandlet til den illusion, vi alle deler den dag i dag: fiat-penge. De har værdi, fordi dem, der har kommandoen over en hær og driver fængsler, siger, at de har værdi. Som man tydeligt kan læse på enhver dollarseddel, der er i omløb i dag: „DENNE SEDDEL ER LOVLIGT BETALINGS-MIDDEL“. Med andre ord: Den har værdi, fordi sedlen siger det.

I øvrigt er der en anden interessant lektion i nutidens penge-sedler, skjult i det åbne. På den anden linje står der, at dette er et lovligt betalingsmiddel „FOR AL GÆLD, OFFENTLIG OG PRIVAT“. Hvad der måske er indlysende for økonomer, var overraskende for mig: Alle penge er gæld. Jeg har stadig ondt i hovedet på grund af det, og jeg vil overlade udforskningen af forholdet mellem penge og gæld som en øvelse til læseren.



Figur 12.7.: En 20-dollarseddel fra 2004-serien, der bruges i dag.
'DENNE SEDDEL ER LOVLIGT BETALINGS-MIDDEL'

Som vi har set, blev guld og sølv brugt som penge i årtusinder. Med tiden blev mønter lavet af guld og sølv erstattet af papir. Papir blev langsomt accepteret som betaling. Denne accept skabte en illusion - illusionen om, at papiret i sig selv har værdi. Det sidste skridt var helt at afbryde forbindelsen mellem repræsentationen og det faktiske: at afskaffe guldstandarden og overbevise alle om, at papiret i sig selv er værdifuldt.

Bitcoin har lært mig om pengenes historie og det største trick i økonomiens historie: fiat-valuta.

13. Vanviddet i brøkreserve-bankvæsenet

Men ak, - det var for sent at ønske! Hun blev ved med at vokse og vokse, og snart måtte 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 døren 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. Hvad skal der dog blive af mig?“

– Lewis Carroll, *Alice i Eventyrland*

Værdi og penge er ikke trivielle emner, især ikke i vor tid. Processen med at skabe penge i vores banksystem er heller ikke triviel, og jeg kan ikke slippe følelsen af, at det er bevidst. Det, jeg tidligere kun er stødt på i akademiske og juridiske tekster, ser også ud til at være almindelig praksis i finansverdenen: Intet forklares i enkle vendinger, ikke fordi det virkelig er komplekst, men fordi sandheden er skjult bag lag på lag af fagsprog og *tilsyneladende* kompleksitet. „Ekspansiv pengepolitik, kvantitativ lempelse, finanspolitiske stimuleringer af økonomien.“ Publikum nikker samtykkende, hypnotiseret af de fancy ord.

Brøkreservebankvæsen og kvantitativ lempelse er fancy ord, der tilslører virkeligheden ved at maskere den med kompleksitet og gøre den svær at forstå. Hvis du forklarer dem for en femårig,

vil det vanvittige i dem begge hurtigt fremstå klart.

Godfrey Bloom, der talte til Europa-Parlamentet under en fælles debat, sagde det meget bedre, end jeg nogensinde kunne:

„[...] Du forstår ikke rigtig, hvad en bank er. Alle banker er fallit. Bank Santander, Deutsche Bank, Royal Bank of Scotland - de er alle fallit! Og hvorfor er de fallit? Det er ikke Guds værk. Det er ikke en slags tsunami. De er fallit, fordi vi har et system, der hedder brøkreservebankvæsen, hvilket betyder, at bankerne kan låne penge ud, som de faktisk ikke har! Det er en kriminel skandale, og den har stået på alt for længe. Vi har falskmøntneri - nogle gange kaldet kvantitativ lempelse - et andet navn for falskmøntneri. Den kunstige trykning af penge, som, hvis den var foretaget af en almindelig person, ville sende dem i fængsel i meget lang tid og indtil vi begynder at sende bankfolk - og jeg inkluderer centralbankfolk og politikere - i fængsel for denne skændsel, vil den fortsætte.“

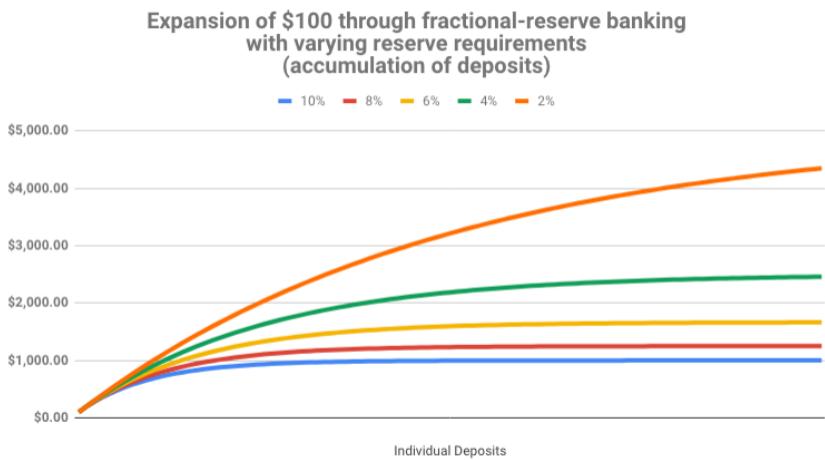
– Godfrey Bloom¹

Lad mig gentage den vigtigste del: Banker kan udlåne penge, som de faktisk ikke har.

Takket være brøkreservebankvæsen, behøver en bank kun at beholde en lille *brøkdel* af hver krone, der bliver sat ind. Det er et sted mellem 0 og 10%, som regel i den lave ende, hvilket gør tingene endnu værre.

Lad os bruge et konkret eksempel til bedre at forstå denne skøre idé: En brøkdel af 10% er tilstrækkeligt, og vi bør være i stand til at foretage alle beregningerne i vores hoved. Så hvis du indsætter 100 dollars i banken - fordi du ikke vil gemme dem

¹Fælles debat om Europas bankunion [17]



Figur 13.1.: Pengenes multiplikatoreffekt

under din madras - så skal de kun beholde den aftalte *brøkdel* af dem. I vores eksempel ville det være \$10, fordi 10% af \$100 er \$10. Nemt, ikke?

Så hvad gør bankerne med resten af pengene? Hvad sker der med dine 90 dollars? De gør, hvad banker gør, de låner dem ud til andre mennesker. Resultatet er en pengemultiplikatoreffekt, som øger pengemængden i økonomien enormt (figur 13.1). Dit oprindelige indskud på \$100 vil snart blive til \$190. Ved at udlåne 90% af de nyoprettede \$90, vil der snart være \$271 i økonomien. Og \$343,90 derefter. Pengemængden øges rekursivt, fordi banker bogstaveligt talt låner penge, som de ikke har. [93]. Uden et eneste abracadabra forvandler bankerne på magisk vis 100 dollars til 1.000 dollars eller mere. Det viser sig, at en ti-folds multiplikation er nemt. Det tager kun nogle få lånerunder.

Misforstå mig ikke: Der er ikke noget galt med at låne penge ud. Der er ikke noget galt med renter. Der er end ikke noget galt



Figur 13.2.: Yellen (direktør for den amerikanske centralbank) er en stærk modstander af en revision af den amerikanske centralbank (Federal Reserve), mens *Bitcoin Sign Guy* i baggrunden stærkt argumenterer for køb af bitcoin.

med at benytte gode, gamle, almindelige banker til at opbevare din formue et sikrere sted end i din sokkeskuffe.

Centralbanker er imidlertid en helt anden sag. De er deformiteter af finansiell regulering, delvist offentlige, delvist private. De leger Gud med noget, der påvirker os alle og som er en del af vores globale civilisation, og gør det skamløst. De er kun interesseret i den nærmeste fremtid, og tilsyneladende uden nogen form for ansvarlighed eller mulighed for revision (se figur 13.2).

Selvom Bitcoin stadig er inflationær, vil den snart ikke være det længere. Det strengt begrænsede udbud på 21 millioner bitcoins vil i sidste ende helt fjerne inflationen. Vi har nu to monetære verdener: en inflationær verden, hvor penge trykkes vilkårligt, og Bitcoins verden, hvor mængden er endelig og let at kontrollere for alle. Den ene er tvunget på os med vold, den

anden er åben for alle, der ønsker at deltage. Ingen adgangsbarrierer, ingen at spørge om lov. Frivillig deltagelse. Det er det smukke ved Bitcoin.

Jeg vil argumentere for, at debatten mellem keynesianske² og østrigske³ økonomer ikke længere er rent akademisk. Satoshi formåede at bygge et system til værdioverførsel på steroider og skabte i processen de hårdeste penge, der nogensinde har eksisteret. På den ene eller anden måde vil flere og flere mennesker lære om det svindelnummer, som brøkreservebankvæsenet er. Hvis de kommer til samme konklusion som de fleste østrigere (økonomer der følger den østrigske skole) og bitcoinere, vil de måske slutte sig til det stadig voksende internet af penge. Ingen kan stoppe dem, hvis de vælger at gøre det.

Bitcoin har lært mig, at brøkreservebankvæsen er det rene vanvid.

²Teorier ifølge John Maynard Keynes og hans efterfølgere [86]

³Skolen for økonomisk tænkning baseret på metodisk individualisme er kendt som den Østrigske Økonomiske Skole [76]

14. Stabile penge

„Det første, jeg skal gøre,“ sagde Alice til sig 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 Eventyrland*

Den vigtigste lektion, jeg har lært fra Bitcoin, er, at stærke penge på den lange bane er overlegne i forhold til svage penge. Stærke penge, også omtalt som *stabile penge*, er enhver globalt handlet valuta, der fungerer som et pålideligt værdilager.

Selvfølgelig er Bitcoin stadig ung og volatil. Kritikere vil hævde, at den ikke lagrer værdi pålideligt. Volatilitetsargumentet misser pointen. Volatilitet er forventeligt. Det vil tage markedet et stykke tid at finde ud af, hvad den rette pris er for disse nye penge. Og som det ofte påpeges i spøg, er det baseret på en målefejl. Hvis du tænker i dollars, vil du ikke være i stand til at se, at én bitcoin altid vil være én bitcoin værd.

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

– Pater Bernard W. Dempsey, S.J.¹

¹Bernard W. Dempsey, S.J., *Interest and Usury* [21, p. 210]

$$\sum_{i=0}^{32} \frac{210000 \lfloor \frac{50*10^8}{2^i} \rfloor}{10^8} \quad (14.1)$$

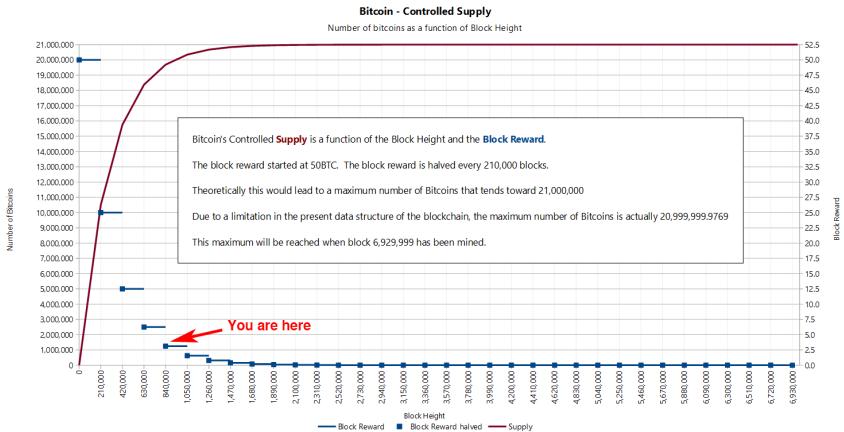
Figur 14.1.: Bitcoins forsyningsformel

Som en hurtig tur gennem de glemte valutaers kirkegård har vist, vil penge, der kan trykkes, blive trykt. Indtil nu har ingen i historien været i stand til at modstå denne fristelse.

Bitcoin håndterer fristelsen til at trykke penge på en genial måde. Satoshi var bevidst om vores grådighed og fejlbarlighed - derfor valgte han noget mere pålideligt end menneskelig tilbageholdenhed: matematik.

Selvom denne formel er nyttig til at beskrive Bitcoins udbud, kan den faktisk ikke findes nogen steder i koden. Udstedelsen af nye bitcoin sker på en algoritmisk kontrolleret måde ved at reducere den belønning, der udbetales til minedriverne hvert fjerde år [13]. Formlen ovenfor bruges til hurtigt at opsummere, hvad der sker under overfladen. Hvad der virkelig sker, kan bedst ses ved at se på ændringerne i blokbelønningen, belønningen der udbetales til den, der finder en gyldig blok, hvilket sker cirka hvert 10. minut.

Formler, logaritmfunktioner og eksponentiale er ikke lige frem intutive at forstå. Begrebet *soliditet* er måske lettere at forstå, hvis man ser på det fra en anden vinkel. Når vi ved, hvor meget der er af noget, og når vi ved, hvor svært det er at producere eller få fat i det, forstår vi straks dets værdi. Det, der gælder for Picassos malerier, Elvis Presleys guitarer og Stradivarius-violiner, gælder også for fiat-valutaer, guld og bitcoins.



Figur 14.2.: Bitcoins kontrollerede udbud

Hårdheden af en fiat-valuta afhænger af, hvem der har ansvaret for de respektive trykpresser. Nogle stater kan være mere villige til at trykke større mængder valuta end andre, hvilket resulterer i en svagere valuta. Andre stater kan være mere restriktive i deres 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 måtte have brug for til sig selv, stort set uden omkostninger.“

– Jörg Guido Hülsmann²

Før vi havde fiat-valutaer, blev pengenes soliditet bestemt af de naturlige egenskaber ved de ting, vi brugte som penge. Guldetts mængde på jorden er begrænset af fysikkens love, da den er begrænset både af sjældne begivenheder som supernovaer og

²Jörg Guido Hülsmann, *The Ethics of Money Production* [39]

neutronstjernekollisioner, og af det store arbejde forbundet med at udvinde det. Det er især på grund af guldets natur som et tungt grundstof, at det hovedsageligt findes begravet dybt under jordens overflade.

Afskaffelsen af guldstandarden gav plads til en ny virkelighed: At tilføre nye penge kræver kun en dråbe blæk. I vores moderne verden kræver det en endnu mindre indsats at tilføje et par nuller til saldoen på en bankkonto: Det er nok bare at ændre et par bits i en bankcomputer.

Princippet, der er skitseret ovenfor, kan udtrykkes mere generelt som forholdet mellem „lager“ og „produktion“. Kort sagt er *beholdningen*, hvor meget der er af noget i øjeblikket. Til vores formål er beholdningen et mål for den aktuelle pengemængde. *Produktionen* er, hvor meget der produceres over en periode (f.eks. pr. år). Nøglen til at forstå stabile penge ligger i at forstå forholdet mellem lager og produktion.

Det er svært at beregne forholdet mellem lager og produktion for fiat-penge, da mængden af penge afhænger af, hvordan man betragter det. [94] Man kan nøjes med at tælle pengesedler og mønter (M_0), tilføje rejsechecks og indlån (M_1), inkludere opsparingskonti og investeringsforeninger samt nogle andre ting (M_2) og endda tilføje indskudsbeviser til det hele (M_3). Desuden varierer det fra land til land, hvordan alt dette defineres og måles. Siden den amerikanske centralbank stoppede med at offentliggøre [62] tal for M_3 , må vi nøjes med den monetære forsyning M_2 . Jeg ville elske at få bekræftet disse tal, men jeg tror, vi indtil videre er nødt til at stole på den amerikanske centralbank.

Guld, som er et af de sjældneste metaller på jorden, har det højeste forhold mellem lager og produktion. Ifølge US Geological Survey er der blevet udvundet lidt mere end 190.000 tons. I de sidste par år er der blevet udvundet omkring 3.100 tons guld om året. [68]

$$\frac{190,000t}{3,100t} = 61 \quad (14.2)$$

Figur 14.3.: Forholdet mellem lager og produktion for guld

Ved hjælp af disse tal kan vi nemt beregne forholdet mellem lager og produktion for guld (se figur 14.3).

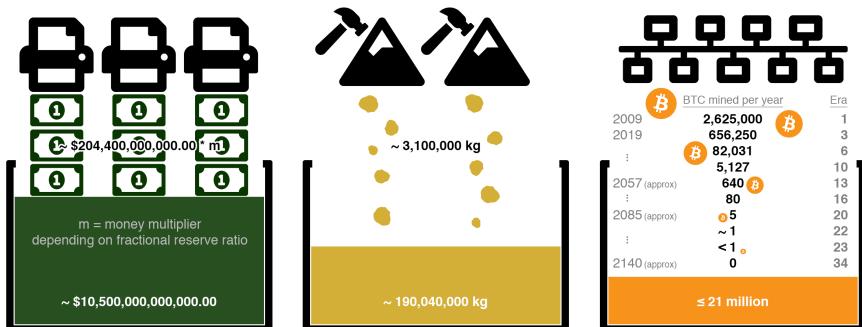
Intet har et højere forhold mellem lager og produktion end guld. Det er grunden til, at guld indtil nu har været de hårdeste penge, der findes. Det siges ofte, at alt det guld, der er udvunget indtil nu, ville kunne være i to svømmebassiner af olympisk størrelse. Ifølge mine beregninger³, ville vi have brug for fire. Så måske skal ordsproget opdateres, eller også er svømmebassiner i olympisk størrelse blevet mindre.

Tilbage til Bitcoin. Som du nok ved, har bitcoin-minedrift været meget populært i de seneste år. Dette skyldes, at vi stadig er i de tidlige faser af det, der kaldes *belønnings-æraen*, hvor minedrivere belønnes med *en masse* bitcoin for deres beregningsmæssige indsats. Vi er i øjeblikket i belønnings-æra nummer 3, der begyndte i 2016 og vil slutte i begyndelsen af 2020, sandsynligvis i maj. Selvom bitcoin-forsyningen er forudbestemt, tillader Bitcoins interne funktioner kun omtrentlige datoer. Ikke desto mindre kan vi forudsige med sikkerhed, hvor høj Bitcoins forhold mellem lager og produktion vil være. Spoiler alert: det vil være højt.

Hvor højt? Det viser sig, at Bitcoin vil blive uendeligt svært (se Figur 14.4).

På grund af en eksponentiel nedgang i minedriftbelønningen, vil mængden af nye bitcoin aftage, hvilket resulterer i en himmel-

³<https://bit.ly/gold-pools>



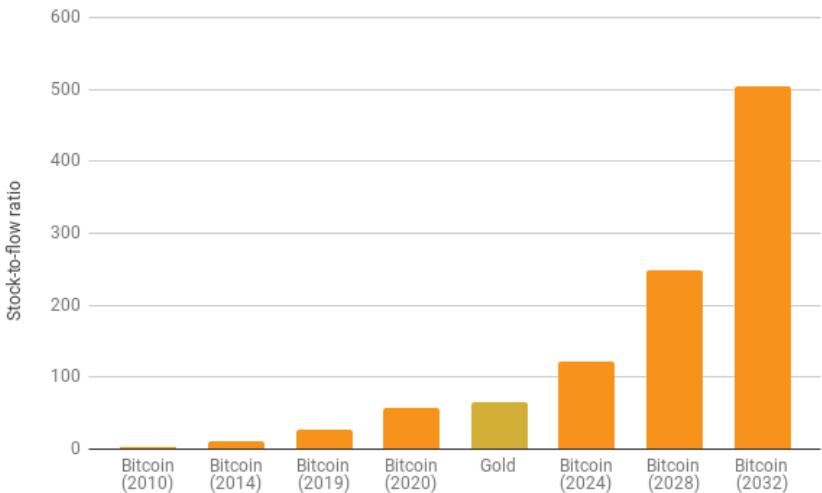
Figur 14.4.: Visualisering af forholdet mellem lager og produktion for USD, guld og Bitcoin

flugt af forholdet mellem lager og produktion. Den vil indhente guld i 2020, kun for at overgå det fire år senere ved at fordoble sin soliditet igen. Sådan en fordobling vil ske 32 gange i alt. Takket være eksponentialfunktionens kraft vil antallet af bitcoin, der bliver udvundet per år, falde til under 100 bitcoin om 50 år og under 1 bitcoin om 75 år. Den globale vandhane, som er blokbelønningen, vil tørre ud omkring året 2140 og effektivt stoppe produktionen af bitcoin. Dette er et langt spil. Hvis du læser dette, er du stadig tidligt på den.

Når bitcoin nærmer sig et uendeligt forhold mellem lager og produktion, vil den være de mest stabile penge, der findes. Uendelig stabilitet er svær at slå.

Set med økonomiske briller er Bitcoins *vanskelighedsjustering* nok dens vigtigste komponent. Hvor svært det er at udvinde bitcoin, afhænger af, hvor hurtigt nye bitcoins bliver udvundet.⁴ Det er den dynamiske justering af netværkets minedriftssværhedsgrad, der gør det muligt for os at forudsige dens fremtidige udbud.

⁴Det afhænger faktisk af, hvor hurtigt gyldige blokke bliver fundet, men til vores formål er dette det samme som „at udvinde bitcoins“ og vil være det i de næste 120 år.



Figur 14.5.: Stigende forhold mellem lager og produktion for bitcoin sammenlignet med guld

Enkeltheden i justeringsalgoritmen for sværhedsgrad kan aفلde opmærksomheden fra dens dybde, men justeringen af sværhedsgraden er virkelig en revolution af einsteiniske proportioner. Den sikrer, at uanset hvor meget eller hvor lidt indsats der bruges på minedrift, vil Bitcoins kontrollerede udbud ikke blive forstyrret. I modsætning til enhver anden ressource, uanset hvor meget energi nogen vil lægge i at mine bitcoin, vil den samlede belønning ikke stige.

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

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

overlevet i sin barndom. Det er det, der sikrer netværket i dets belønningsåera. Det er det, der sikrer en stabil og retfærdig fordeling⁵ af nye bitcoin. Det er termostaten, der regulerer Bitcoins pengepolitik.

Einstein viste os noget nyt: Uanset hvor hårdt du skubber en genstand, vil det på et tidspunkt ikke være muligt at bevæge den hurtigere. Satoshi viste os også noget nyt: Uanset hvor hårdt du graver efter dette digitale guld, vil du på et tidspunkt ikke kunne få flere bitcoins ud af det. For første gang i menneskets historie har vi en monetær vare, som du ikke kan producere mere af, uanset hvor meget du prøver.

Bitcoin har lært mig, at stabile penge er essentielle.

⁵Dan Held, *Bitcoin's Distribution was Fair* [37]

Del III.

Teknologi

Teknologi

„Denne gang vil jeg bære mig klogere ad “ sagde hun til sig selv. Så tog hun den lille guldnøgle og åbnede døren ud til haven

– Lewis Carroll, *Alice i Eventyrland*

Gyldne nøgler, ure, der kun virker ved et tilfælde, kapløb for at løse mærkelige gåder og bygherrer uden ansigter eller navne. Det, der lyder som eventyr fra Eventyrland, er dagligdag i Bitcoin-verdenen.

Som vi undersøgte i kapitel II, Store dele af det nuværende finansielle system er systematisk ødelagt. Ligesom Alice, kan vi kun håbe på at klare os bedre denne gang. Men takket være en pseudonym opfinder har vi en utrolig sofistikeret teknologi til at hjælpe os denne gang: Bitcoin.

At løse problemer i et radikalt decentraliseret og fjendtligt miljø kræver unikke løsninger. Hvad der ellers ville være triviele problemer at løse, er alt andet end det i denne mærkelige verden af knudepunkter. Bitcoin er afhængig af stærk kryptografi til de fleste løsninger, i hvert fald hvis man ser på det med teknologiens briller. Hvor stærk denne kryptografi er, vil blive udforsket i en af de følgende lektioner.

Kryptografi er det, Bitcoin anvender for at eliminere tilliden til myndighederne. I stedet for at stole på centraliserede institutioner, stoler systemet på den endelige autoritet i vores univers: fysikken. Der er dog stadig nogle få korn af tillid tilbage. Vi vil undersøge disse gran i den anden lektion i dette kapitel.

Del III – Teknologi:

15. Styrke i tal
16. Refleksioner over „Stol ikke, bekræft“
17. At fortælle tiden kræver arbejde
18. Bevæg dig langsomt, og undgå at ødelægge ting
19. Privatlivet er ikke dødt
20. Cypherpunks skriver kode
21. Metaforer for Bitcoins fremtid

De sidste lektioner udforsker den teknologiske udviklings etos i Bitcoin, som uden tvivl er lige så vigtig som selve teknologien. Bitcoin er ikke den næste skinnende app på din telefon. Det er grundlaget for en ny økonomisk virkelighed, og derfor bør Bitcoin behandles som finansiel software af atomreaktor-kvalitet.

Hvor befinder vi os i denne økonomiske, samfundsmæssige og teknologiske revolution? Fortidens netværk og teknologier kan tjene som metaforer for Bitcoins fremtid, der udforskes i den sidste lektion i dette kapitel.

Endnu en gang skal du spænde dig fast og nyde turen. Som med alle eksponentielle teknologier, er vi på vej mod himlen.

15. Styrke i tal

„Lad mig se: fire gange fem er tolv, og fire gange seks er tretten, og fire gange syv er fjorten - åh nej! Jeg når aldrig op på tyve med den hastighed!“

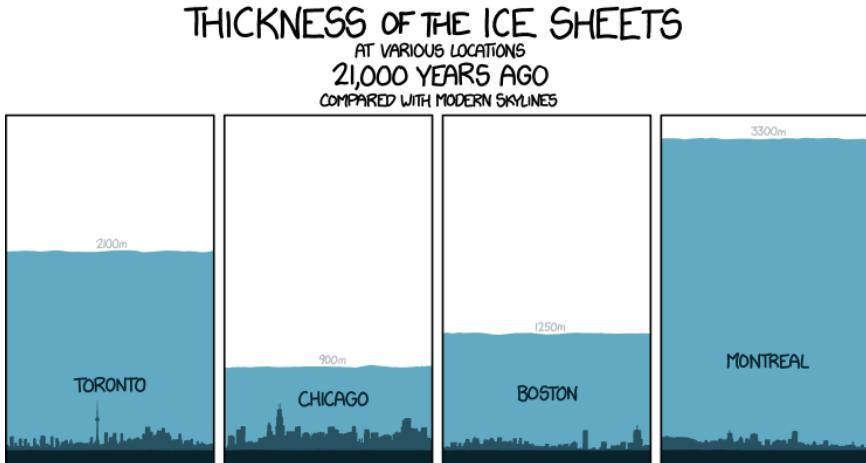
– Lewis Carroll, *Alice i Eventyrland*

Tal er en vigtig del af vores hverdag. Store tal er dog ikke noget, som de fleste af os er fortrolige med. De største tal, vi kan støde på i hverdagen, er i størrelsesordenen millioner, milliarder eller billioner. Vi kan læse om millioner af mennesker i fattigdom, milliarder af dollars brugt på redningspakker til banker og billioner af dollars i statsgæld. Selvom det er svært at finde hoved og hale i disse overskrifter, er vi nogenlunde fortrolige med størrelsen af disse tal.

Selvom vi måske er fortrolige med milliarder og billioner, begynder vores intuition allerede at svigte når vi arbejder med tal i denne størrelsesorden. Har du en fornemmelse af, hvor længe du skal vente på, at der går en million/milliard/trillion sekunder? Hvis du er ligesom mig, er du fortapt uden faktisk at regne på tallene.

Lad os se nærmere på dette eksempel: Forskellen mellem hver er en stigning på tre størrelsesordener: 10^6 , 10^9 , 10^{12} . Det er ikke særlig nyttigt at tænke i sekunder, så lad os omsætte det til noget, vi kan forstå:

- 10^6 : En million sekunder var $1\frac{1}{2}$ uge siden.
- 10^9 : En milliard sekunder er næsten 32 år siden.



Figur 15.1.: For omkring 1 billion sekunder siden. Kilde: xkcd 1225

- 10^{12} : For en billion sekunder siden var Manhattan dækket af et tykt lag is.¹

Så snart vi bevæger os ind i den moderne kryptografis astronomiske sfære, svigter vores intuition katastrofalt. Bitcoin er bygget op omkring store tal og den næsten umulige opgave, det er at gætte dem. Disse tal er langt, langt større end noget, vi kan støde på i dagligdagen. Mange størrelsesordener større. At forstå, hvor store disse tal i virkeligheden er, er afgørende for at forstå Bitcoin som helhed.

Lad os kigge nærmere på SHA-256², en af hash-funktionerne³ der bruges i Bitcoin, som et konkret eksempel. Det er kun naturligt at tænke på 256 bits som „to hundrede og seksoghalv-

¹En billion sekunder (10^{12}) var 31.710 år siden. Den sidste istid nåede sit højeste niveau for 33.000 år siden. [88]

²SHA-256 er en del af SHA-2-familien af kryptografiske hashfunktioner, der er udviklet af den amerikanske sikkerhedstjeneste NSA. [97]

³Bitcoin bruger SHA-256 til hashing af blokke. [12]

tres“, hvilket slet ikke er et stort tal. Men tallet i SHA-256 taler om størrelsesordener - noget vores hjerne ikke er gearet til at håndtere.

Bitlængden er et praktisk mål, men den sande betydning af 256-bit sikkerhed går tabt i oversættelsen. Ligesom millionerne (10^6) og milliarderne (10^9) ovenfor, omhandler tallet i SHA-256 en størrelsesordenen (2^{256}).

Så hvor stærk er SHA-256 egentlig?

„SHA-256 er meget stærk. Det er ikke som det trinvise skridt fra MD5 til SHA1. Den kan holde i flere årtier, medmindre der opstår et massivt gen-nembrudsangreb.“

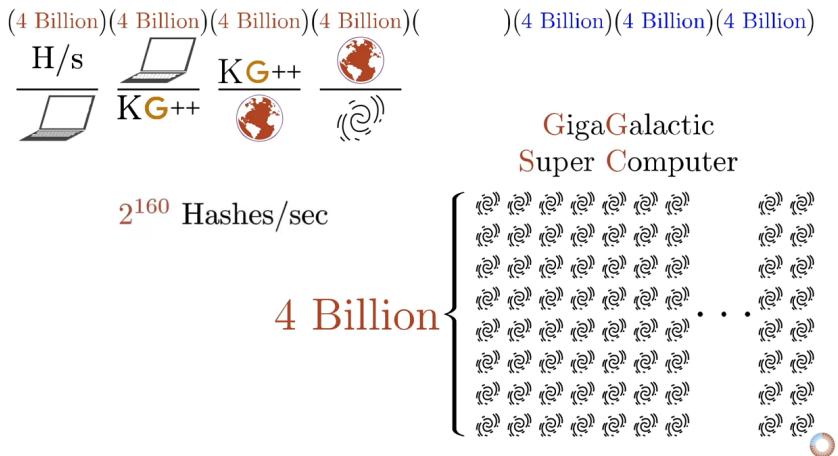
– Satoshi Nakamoto⁴

Lad os skære det ud i pap. 2^{256} er lig med følgende tal:

115 kvattuordecillioner 792 tredecillioner 89 duo-decillioner 237 undecillioner 316 decillioner 195 novem-decillioner 423 oktodecillioner 570 septendecillioner 985 sexdecillioner 8 quindecillioner 687 quattuor-decillioner 907 tredecillioner 853 duodecillioner 269 un-decillioner 984 kvintilliard 665 kvintillion 640 kva-drilliard 564 kvadrillion 39 trilliard 457 trillion 584 billiard 7 billioner 913 milliarder 129 millioner 639 tusind 936.

Det er mange kvintillioner! Det er stort set umuligt at forstå dette tal. Der er intet i det fysiske univers at sammenligne det med. Det er langt større end antallet af atomer i det observerbare univers. Den menneskelige hjerne er simpelthen ikke skabt til at forstå det.

⁴Satoshi Nakamoto, i et svar på et spørgsmål om SHA-256-kollisioner. [55]



Figur 15.2.: Illustration af SHA-256-sikkerhed. Original grafik af Grant Sanderson også kendt som 3Blue1Brown.

En af de bedste visualiseringer af den sande styrke i SHA-256 er en video af Grant Sanderson. Den hedder meget passende „*How secure is 256 bit security?*“⁵ Den viser på smukkeste vis, hvor stort et 256-bit rum er. Gør dig selv en tjeneste og brug fem minutter på at se den. Som alle andre *3Blue1Brown*-videoer er den ikke bare fascinerende, men også usædvanligt godt lavet. Advarsel: Du falder måske ned i et matematisk kaninhul.

Bruce Schneier [65] brugte de fysiske grænser for beregning til at sætte dette tal i perspektiv: Selv hvis vi kunne bygge en optimal computer, som ville bruge al energi til rådighed, til at flippe bits perfekt [87], bygge en Dyson-sfære⁶ rundt om vores sol og lade den køre i 100 milliarder milliarder år, ville vi stadig kun have en chance på 25% for at finde en nål i en høstak på 256 bit.

⁵Se videoen på https://youtu.be/S9JGmA5nY_u

⁶En Dyson-sfære er en hypotetisk megastruktur, som fuldstændigt omslutter en stjerne og opsamler en stor procentdel af dens energiudbytte. [81]

„Disse tal har intet at gøre med apparaternes teknologi; de er de maksimale værdier, som termodynamikken tillader. Desuden antyder de kraftigt, at brute-force-angreb mod 256-bit nøgler vil være umulige, indtil computere bliver bygget af noget andet end fysiske materialer og optager noget andet end plads.“

– Bruce Schneier⁷

Det er svært at overdrive betydningen af dette. Stærk kryptografi vender op og ned på magtbalancen i den fysiske verden, som vi er så vant til. Ubrydelige ting findes ikke i den virkelige verden. Hvis du bruger tilstrækkelig kraft, vil du kunne åbne enhver dør, kasse eller skattekiste.

Bitcoins skattekiste er meget anderledes. Den er sikret af stærk kryptografi, som ikke giver plads til brute force. Og så længe de underliggende matematiske antagelser holder, er brute force det eneste, vi har. Bevares, der er også risikoen for et globalt angreb med \$5 skruenøgler (figur 15.3) Men tortur vil ikke virke på alle bitcoin-adresser, og bitcoins kryptografiske vægge vil afværge alle brute force-angreb. Selv hvis du angriber med en kraft som tusind sole, bogstaveligt talt.

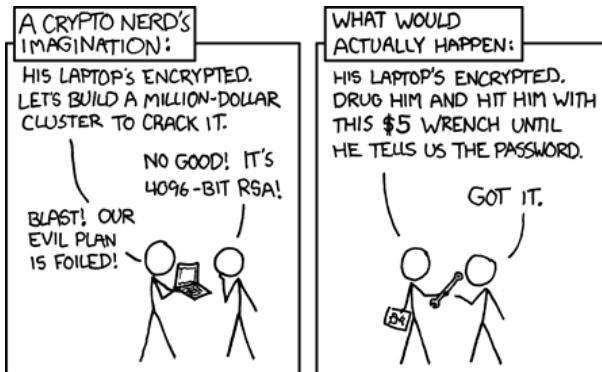
Denne kendsgerning og dens implikationer blev gribende opsummeret i opfordringen til at benytte kryptografiske våben: „*Ingen form for tvang vil nogensinde kunne løse et matematisk problem.*“

„Det er ikke indlysende, at verden skulle fungere på denne måde, men på én eller anden måde smiler universet til kryptering.“

– Julian Assange⁸

⁷Bruce Schneier, *Applied Cryptography* [64]

⁸Julian Assange, *A Call to Cryptographic Arms* [5]



Figur 15.3.: \$Angreb med 5\$ skruenøgle. Kilde: xkcd 538

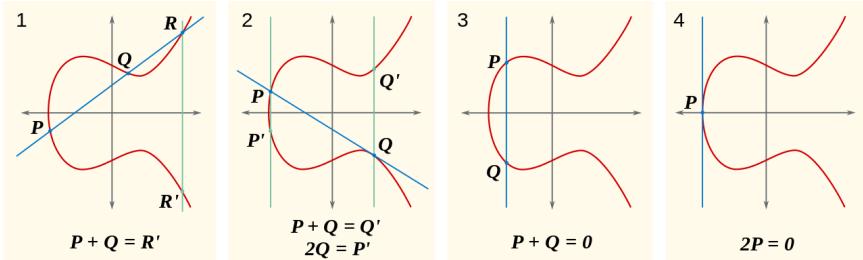
Ingen ved endnu med sikkerhed, om universets smil er ægte eller ej. Det er muligt, at vores antagelse om matematiske asymmetrier er forkert og at vi finder ud af, at P faktisk er lig med NP [95], eller at vi overraskende finder hurtige løsninger på specifikke problemer [79] som vi i øjeblikket antager, er svære at løse. Hvis det skulle være tilfældet, vil kryptografi, som vi kender den, ophøre med at eksistere, og konsekvenserne vil højst sandsynligt ændre verden til ukendelighed.

„Vires in Numeris“ = „Styrke i tal“⁹

Vires in numeris er ikke kun et fængende motto, der bruges af bitcoinere. Erkendelsen af, at der er en ufattelig styrke at finde i tal, er dybtgående. Forståelsen af den omvending af den eksisterende magtbalance, som det muliggør, ændrede mit syn på verden og den fremtid, der ligger foran os.

Et direkte resultat af dette er det faktum, at du ikke behøver at spørge nogen om lov til at deltage i Bitcoin. Der er ingen side, man skal tilmelde sig, ingen virksomhed, der har ansvaret, ingen

⁹ *Vires in Numeris* blev først foreslået som et Bitcoin-motto af bitcointalk-brugeren *epii* [26]



Figur 15.4.: Eksempler på elliptiske kurver. Grafik cc-by-sa Emmanuel Boutet.

myndighed, man skal sende ansøgningsskemaer til. Du skal blot generere et stort tal, og så er du stort set klar. Den centrale myndighed for kontooprettelse er matematik. Og kun Gud ved, hvem der er ansvarlig for det.

Bitcoin er bygget på vores bedste forståelse af virkeligheden. Selvom der stadig er mange åbne problemer inden for fysik, datalogi og matematik, er vi dog ret sikre på visse ting. At der er en asymmetri mellem at finde løsninger og validere korrektheden af disse løsninger er en af disse ting. At beregning kræver energi er en anden. Med andre ord: Det er sværere at finde en nål i en høstak end at tjekke, om den spidse ting i din hånd faktisk er en nål eller ej. Og det kræver arbejde at finde nålen.

Det enorme omfang af mulige bitcoin-adresser er virkelig overvældende. Antallet af private nøgler er endnu højere. Det er fascinerende, hvor meget af vores moderne verden, der kan koges ned til usandsynligheden af at finde en nål i en ubegribelig stor høstak. Jeg er nu mere bevidst om dette faktum end nogensinde før.

Bitcoin har lært mig, at der er styrke i tal.

16. Refleksioner over „Stol ikke, bekræft“

„Nu til beviserne,“ sagde kongen, „og derefter dommen.“

– Lewis Carroll, *Alice i Eventyrland*

Bitcoin sigter mod at erstatte eller i det mindste give et alternativ til konventionel valuta. Konventionel valuta er bundet til en centraliseret myndighed, uanset om vi taler om lovligt betalingsmiddel som den amerikanske dollar eller moderne monopolpenge som Fortnites V-Bucks. I begge eksempler er du tvunget til at stole på, at den centrale myndighed udsteder, administrerer og cirkulerer dine penge. Bitcoin løser denne binding, og det vigtigste problem, 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 betalingssystem baseret på kryptografiske beviser i stedet for tillid“

– Satoshi Nakamoto¹

Bitcoin løser tillidsproblemet ved at være fuldstændig decentraliseret, uden en central server eller betroede parter. Ikke engang betroede *tredjeparter*, men betroede parter, punktum. Uden central autoritet, er der simpelthen *ingen* at stole på. Innovationen ligger i den fuldstændige decentralisering. Det er roden til Bitcoins modstandskraft, og grunden til at den stadig er

¹Satoshi Nakamoto, officiel Bitcoin-meddelelse [52] og hvidbog [49]

i live. Decentralisering er også grunden til, at vi har minedrift, knudepunkter, hardware-tegnebøger, og ja, blokkæden. Det eneste, du skal „stole på“, er at vores forståelse af matematik og fysik ikke er helt forkert, og at flertallet af minedrivere handler ærligt (hvilket de er motiverede til at gøre).

Mens den almindelige verden opererer under antagelsen „*stol, men bekræft*“, opererer Bitcoin under antagelsen „*stol ikke, bekræft.*“ Satoshi understregede vigtigheden af at fjerne tillid tydeligt i både introduktionen og konklusionen af Bitcoins hvidbog.

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

– Satoshi Nakamoto²

Bemærk, at *uden at være afhængig af tillid* bruges i en meget specifik sammenhæng her. Vi taler om betroede tredjeparter, dvs. andre enheder, som du stoler på til at producere, opbevare og behandle dine penge. Det antages for eksempel, at du kan stole på din computer.

Som Ken Thompson demonstrerede i sin Turing Award-forelæsning, er tillid et ekstremt vanskeligt koncept i beregningsverdenen. Når man kører et program, er man nødt til at stole på alle mulige former for software (og hardware), som i teorien kan ændre det program, man forsøger at køre, på en ondsindet måde. Som Thompson opsummerede i sin *Reflections on Trusting Trust*: „Moralen er indlysende. Du kan ikke stole på kode, som du ikke helt selv har skabt.“ [70]

Thompson demonstrerede, at selv hvis du har adgang til kildekoden, kan din kompiler - eller ethvert andet program, der håndterer programmet eller hardwaren - blive kompromitteret,

²Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* (hvidbogen om Bitcoin) [49]

```

char s[ ] = {
    '\V',
    '0',
    '\n',
    '}' ,
    '}',
    '\V',
    '\V',
    '/',
    '/',
    '\n',
    (213 lines deleted)
    0
};

/*
 * The string s is a
 * representation of the body
 * of this program from '0'
 * to the end.
 */
main( )
{
    int i;

    printf("char s[%d] = %s;\n",
        for(i=0; s[i]; i++)
            printf("%4d, %c", i, s[i]);
    printf("%s;\n", s);
}

```

Here are some simple transliterations to allow a non-C programmer to read this code.

- = assignment
- == equal to EQ.
- != not equal to NE.
- ++ increment
- 'x' single character constant
- "" multiple character string
- %d format to convert to decimal
- %s format to convert to string
- \ tab character
- \n newline character

FIGURE 1.

Excerpts copied with permission of the Association for Computing Machinery

To what extent should one trust a statement that a program is free of Trojan horses? Perhaps it is more important to trust the people who wrote the software.

KEN THOMPSON

```

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

```

FIGURE 2.2

```

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

```

FIGURE 2.1

```

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

```

FIGURE 2.3.

The moral is obvious. You can't trust code that you did not totally create yourself. (Especially code from companies that employ people like me.) No amount of source-level verification or scrutiny will protect you from using untrusted code.

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

FIGURE 3.1

```

compile(s)
char *s;
{
    if(match(s, "pattern"))
        compile("bug");
    return;
}
...

```

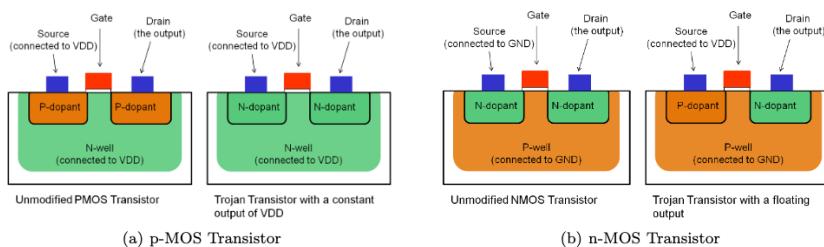
FIGURE 3.2

```

compile(s)
char *s;
{
    if(match(s, "pattern1"))
        compile("bug1");
    return;
}
if(match(s, "pattern 2"))
    compile("bug 2");
return;
}
...

```

FIGURE 3.3



Figur 16.2.: Fra *Stealthy Dopant-Level Hardware Trojans* af Becker, Regazzoni, Paar, Burleson

og det vil være meget svært at opdage denne bagdør. I praksis findes der således ikke et virkelig *tillidsløst* system. Du ville være nødt til at skabe al din software *og* al din hardware (assemblerere, kompilere, linkere osv.) fra bunden uden hjælp fra ekstern software eller software-understøttet maskineri.

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

– Carl Sagan³

Et *Ken Thompson hack* er en særlig genial bagdør der er svær at opdage, så lad os tage et hurtigt kig på en bagdør, der svær at opdage, som fungerer uden ændringer i softwaren. Forskere har fundet en metode til at kompromittere sikkerhedskritisk hardware på ved at ændre polariteten af urenheder i silicium. [9] Bare ved at ændre de fysiske egenskaber af det materiale, som computerchips er lavet af, var de i stand til at kompromittere en kryptografisk sikker tilfældig talgenerator. Da denne ændring ikke er synlig, kan en sådan bagdør ikke opdages ved optisk inspektion, som er en af de vigtigste mekanismer til afsløring af manipulation med chips.

³Carl Sagan, *Cosmos* [63]

Lyder det skræmmende? Tja, selv hvis du kunne bygge alt fra bunden, ville du stadig være nødt til at stole på den underliggende matematik. Du ville være nødt til at stole på, at *secp256k1* er en elliptisk kurve uden bagdøre. Ja, ondsindede bagdøre kan indsættes i kryptografiske funktioners matematiske fundament, og det er uden tvivl allerede sket mindst én gang. [80] Der er gode grunde til at være paranoid, og faktum er, at alt lige fra din hardware til din software, herunder de elliptiske kurver, der bruges, kan have bagdøre [82] er nogle af dem.

„Stol ikke. Bekræft.“

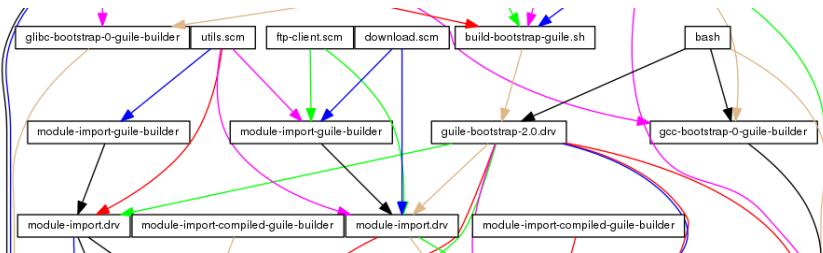
– Bitcoinere overalt

Ovenstående eksempler burde illustrere, at *tillidsløs* databehandling er utopisk. Bitcoin er nok det system, der kommer tættest på denne utopi, men det er stadig *tillidsminimeret* - med det formål at fjerne tillid, hvor det er muligt. Man kan sige, at tillidskæden er uendelig, da du også bliver nødt til at stole på, at beregning kræver energi, at P ikke er lig med NP, og at du faktisk befinner dig i virkeligheden og ikke er fanget i en simulation af ondsindede aktører.

Udviklere arbejder på værktøjer og procedurer for at minimere den resterende tillid yderligere. For eksempel har Bitcoin-udviklere skabt Gitian⁴, som er en softwaredistributionsmetode til at skabe deterministiske builds. Ideen er, at hvis flere udviklere er i stand til at reproducere identiske binære filer, reduceres risikoen for ondsindet manipulation. Fancy bagdøre er ikke den eneste angrebsvektor. Simpel afpresning eller pengeafpresning er også reelle trusler. Som i hovedprotokollen, bruges decentralisering til at minimere tilliden.

Der gøres forskellige forsøg på at forbedre det kendte „hønen-eller-ægget“ opstartsproblem, som Ken Thompsons hack så glim-

⁴<https://gitian.org/>



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

rende påpegede [20]. En sådan indsats er Guix⁵ (udtalt *geeks*), som bruger funktionelt erklæret pakkehåndtering, hvilket fører til builds der er reproducerbare bit-for-bit. Resultatet er, at du ikke længere behøver at stole på nogen softwareleverende servere, da du kan bekræfte, at den serverede binære fil ikke er blevet manipuleret ved at genopbygge den fra bunden. For nylig blev en anmodning godkendt til at integrere Guix i Bitcoins byggeproces.⁶

Heldigvis er Bitcoin ikke afhængig af en enkelt algoritme eller et enkelt stykke hardware. En effekt af Bitcoins radikale decentralisering er en distribueret sikkerhedsmodel. Selvom man ikke skal tage let på de bagdøre, der er beskrevet ovenfor, er det usandsynligt, at alle software-tegnebøger, alle hardware-tegnebøger, alle kryptografiske biblioteker, alle knudepunkts-implementeringer og alle kompilere i alle sprog er kompromitterede. Det er muligt, men meget usandsynligt.

Bemærk, at du kan generere en privat nøgle, uden at være afhængig af computerhardware eller -software. Du kan slå plat eller krone [4] et par gange, men afhængigt af din mønt og kastestil, er denne kilde til tilfældighed måske ikke tilstrækkeligt tilfældig. Der er en grund til, at lagringsprotokoller som Glaci-

⁵<https://guix.gnu.org>

⁶Se Pull Request 15277 af bitcoin-core:

<https://github.com/bitcoin/bitcoin/pull/15277>

er⁷råder dig til at bruge terninger af kasinokvalitet som en af to kilder til entropi.

Bitcoin tvang mig til at reflektere over, hvad det egentlig indebærer at stole på nogen. Det øgede min bevidsthed om opstartsproblemet og den implicitte tillidskæde i udvikling og drift af software. Det gjorde mig også opmærksom på de mange måder, hvorpå software og hardware kan blive kompromitteret.

Bitcoin har lært mig, at jeg ikke skal stole, men bekræfte.

⁷<https://glacierprotocol.org/>

17. At fortælle tid kræver arbejde

„Kære, kære! Jeg kommer for sent!“

– Lewis Carroll, *Alice i Eventyrland*

Det siges ofte, at bitcoins udvindes, fordi tusindvis af computere arbejder på at løse *meget komplekse* matematiske problemer. Visse problemer skal løses, og hvis du beregner det rigtige svar, „producerer“ du bitcoins. Selvom denne forenklede opfattelse af bitcoin-minedrift måske er lettere at formidle, misser den en del af pointen. Bitcoins produceres eller skabes ikke, og hele prøvelsen handler egentlig ikke om at løse bestemte matematiske problemer. Matematikken er heller ikke særlig kompleks. Det, der er komplettest, er *at fortælle tiden* i et decentraliseret system.

Som beskrevet i hvidbogen er bevis-for-arbejde-systemet (også kaldet minedrift eller mining) en måde at implementere en distribueret tidsstempelserver på.

Da jeg først lærte, hvordan Bitcoin fungerer, tænkte jeg også, at bevis-for-arbejde er ineffektivt og spild af tid. Efter et styk-

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

3. Timestamp Server

The solution we propose begins with a timestamp server. A timestamp server works by taking a hash of a block of items to be timestamped and widely publishing the hash, such as in a newspaper or Usenet post [2-5]. The timestamp proves that the data must have existed at the time, obviously, in order to get into the hash. Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it.



4. Proof-of-Work

To implement a distributed timestamp server on a peer-to-peer basis, we will need to use a proof-of-work system similar to Adam Back's Hashcash [6], rather than newspaper or Usenet posts. The proof-of-work involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits. The average work required is exponential in the number of zero bits required and can be verified by executing a single hash.

Figur 17.1.: Uddrag fra hvidbogen. Var der nogen, der sagde tidskæde?

ke tid begyndte jeg at ændre perspektiv på Bitcoins energiforbrug [30]. Det ser ud til, at bevis-for-arbejde stadig er bredt misforstået i dag, i år 10 EB (efter Bitcoin).

Eftersom de problemer, der skal løses i bevis-for-arbejde, er opdigtede, synes mange mennesker at mene, at det er *nytteløst* arbejde. Hvis fokus udelukkende er på beregningerne, er det en forståelig konklusion. Men Bitcoin handler ikke kun om beregning. Det handler om *uafhængigt at blive enige om begivenhedernes rækkefølge*

Bevis-for-arbejde er et system, hvor alle kan validere, hvad der skete, og i hvilken rækkefølge det skete. Denne uafhængige validering er det, der fører til konsensus, en enighed mellem flere parter om, hvem der ejer hvad.

I et radikalt decentraliseret miljø har vi ikke den luksus at have absolut tid. Ethvert ur ville introducere en betroet tredjepart, et centralt punkt i systemet, som man skulle stole på, og som kunne angribes. „Timing er det grundlæggende problem,“ som Grisha Trubetskoy påpeger [72]. Dette problem løste Satoshi genialt ved at implementere et decentraliseret ur via en blokkæde, der benytter sig af bevis-for-arbejde. Alle er på forhånd enige om, at kæden med det mest akkumulerede arbejde er kilden til sandheden. Det er per definition det, der faktisk skete. Denne aftale er det, der nu er kendt som Nakamoto-konsensus.

„Netværket tidsstempler transaktioner ved at have dem ind i en løbende kæde, der fungerer som bevis for hændelsesforløbet“

– Satoshi Nakamoto¹

Uden en konsekvent måde at fortælle tiden, er der ingen konsekvent måde at skelne mellem før og efter. Pålidelig organisering er umulig. Som tidligere nævnt er Nakamoto-konsensus

¹Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* (hvidbogen om Bitcoin) [49]

Bitcoins måde at fortælle tiden på. Systemets incitamentsstruktur producerer et sandsynligt korrekt, decentraliseret ur ved at udnytte både grådighed og egeninteresse hos konkurrerende deltagere. Det faktum, at dette ur er upræcist, er irrelevant, fordi rækkefølgen af begivenheder i sidste ende er entydig og kan bekræftes af alle.

Takket være bevis-for-arbejde er både arbejdet *og* valideringen af arbejdet radikalt decentraliseret. Alle kan tilslutte sig og forlade Bitcoin efter forgodtbefindende, og alle kan validere alt på alle tidspunkter. Ikke nok med det, men alle kan validere systemets tilstand *individuelt* uden at skulle stole på nogen andre for validering.

Det tager tid at forstå bevis-for-arbejde. Det er ofte kontraintuitivt, og selvom reglerne er simple, fører de til ret komplekse fænomener. For mig hjalp det at ændre mit perspektiv på mine-drift. Nyttigt, ikke ubrugeligt. Validering, ikke beregning. Tid, ikke blokke.

Bitcoin har lært mig, at det er svært at fortælle hvad klokken er, især hvis man er decentraliseret.

18. Bevæg dig langsomt, og undgå at ødelægge ting

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*

Det er måske et forældet mantra, men „bevæg dig hurtigt og ødelæg ting“ er stadig måden hvorpå en stor del af tech-verdenen opererer. Ideen om, at det er ligegyldigt, hvis du ikke gør det rigtigt første gang, er en grundlæggende søjle i *fejl tidligt, fejl ofte* mentaliteten. Succes måles i vækst, og så længe du vokser, er alt i orden. Hvis noget ikke virker i første omgang, skifter du simpelthen fokus og prøver igen. Med andre ord: kast lort mod væggen og se, hvad der bliver hængende.

Bitcoin er meget anderledes. Den er anderledes på grund af sit design. Den er anderledes af nødvendighed. Som Satoshi påpegede, er e-valuta blevet forsøgt mange gange før, og alle tidligere forsøg er mislykkedes, fordi der var et hoved, der kunne skærdes af. Det nye ved Bitcoin er, at det er et dyr uden hoveder.

„Mange mennesker afviser automatisk e-valuta som en tabt sag på grund af alle de virksomheder, der har fejlet siden 1990’erne. Jeg håber, det er indlysende, at det var den centralt kontrollerede natur af deres systemer, der dømte dem til døden.“

– Satoshi Nakamoto¹

¹Satoshi Nakamoto, i et svar til Sepp Hasslberger [53]

En konsekvens af denne radikale decentralisering er en indbygget modstand mod forandring. „Bevæg dig hurtigt og ødelæggning“ fungerer ikke og kommer aldrig til at fungere på Bitcoins basislag. Selv hvis det var ønskeligt, ville det ikke være muligt uden at overbevise *alle* om at ændre deres vaner. Det er en distribueret konsensus. Det er Bitcoins natur.

„Bitcoins natur er sådan, at når version 0.1 er frigivet, er kerneldesignet mejslet i sten resten af dens levetid.“

– Satoshi Nakamoto²

Det er en af de mange paradoxale egenskaber ved Bitcoin. Vi har alle en tendens til at tro, at alt, der er software, nemt kan ændres. Men dyrets natur gør det forbandet svært at ændre det.

Som Hasu smukt viser i *Unpacking Bitcoin's Social Contract* [33], Det er kun muligt at ændre reglerne for Bitcoin ved at *foreslå* en ændring og derefter *overbevise* alle brugerne af Bitcoin om at benytte denne ændring. Dette gør Bitcoin meget modstandsdygtig over for ændringer, selvom det er software.

Modstandsdygtighed er en af Bitcoins vigtigste egenskaber. Kritiske softwaresystemer skal være anti-skrøbelige, hvilket er det, som samspillet mellem Bitcoins sociale lag og dets tekniske lag garanterer. Monetære systemer er i deres natur fjendtlige, og som vi har vidst i tusindvis af år, er et solidt fundament afgørende i et fjendtligt miljø.

„Og skybruddet kom, og floderne steg, og stormene suste og ramte det hus. Men det faldt ikke, for dets fundament var lagt på klippen.“

– Matthæus 7:24-27

²Satoshi Nakamoto, i et svar til Gavin Andresen [53]

I denne lignelse om de kluge og de tåbelige bygmestre er Bitcoin ikke huset. Det er klippen. Uforanderlig, ubevægelig og fundamentet for et nyt finansielt system.

Ligesom geologer ved, at klippeformationer altid er i bevægelse og udvikling, kan man se, at Bitcoin også altid er i bevægelse og udvikling. Det handler simpelthen om at vide, hvor man skal kigge, og hvordan man skal betragte det.

Indførelsen af *pay to script-hash*³ og *adskilt vidne*⁴ er et bevis på, at Bitcoins regler kan ændres, hvis nok brugere er overbevist om, at ændringen er til fordel for netværket. Sidstnævnte har muliggjort udviklingen af Lightning-netværket⁵, som er et af de huse, der bliver bygget på Bitcoins solide fundament. Fremtidige opgraderinger som Schnorr-signaturer [60] vil forbedre effektiviteten og privatlivet samt scripts (intelligente kontrakter), som ikke kan skelnes fra almindelige transaktioner takket være Taproot [32]. Kluge bygherrer bygger på solide fundamenter.

Satoshi var ikke kun en klog bygherre rent teknologisk. Han forstod også, at det ville være nødvendigt at træffe kluge beslutninger ideologisk.

³*Pay to script hash*-transaktioner (P2SH) blev standardiseret i BIP 16.

De gør det muligt at sende transaktioner til en script-hash (en adresse, der starter med 3) i stedet for en hash af en offentlig nøgle (en adresse, der starter med 1). [15]

⁴*adskilt vidne* (Segregated Witness (forkortet SegWit)) er en implementeret protokolopgradering, der har til formål at beskytte mod transaktionsfejl og øge kapaciteten i hver blok. SegWit adskiller *vidnet* fra listen af input. [16]

⁵<https://lightning.network/>

„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 Nakamoto⁶

Åbenhed er altafgørende for sikkerheden og en naturlig del af open source og den frie softwarebevægelse. Som Satoshi påpegede, skal sikre protokoller og den kode, der implementerer dem, være tilgængelig - der opnås ingen sikkerhed gennem uklarhed. En anden fordel er, at dette genrelaterer til decentralisering: en kodebase, der kan køres, studeres, ændres, kopieres og distribueres frit, sikrer, at den spredes vidt og bredt.

Det er Bitcoins radikalt decentraliserede natur, der gør, at den bevæger sig langsomt og velovervejet. Et netværk af knudepunkter, der hver især drives af et suverænt individ, er i sagens natur modstandsdygtigt over for ændringer - ondsindede eller ej. Uden mulighed for at tvinge opdateringer ned over brugerne er den eneste måde at indføre ændringer på langsomt at overbevise hver eneste af disse individer om at benytte en ændring. Denne ikke-centrale proces med at introducere og implementere ændringer er det, der gør netværket utroligt modstandsdygtigt over for ondsindede ændringer. Det er også det, der gør det sværere at reparere ødelagte ting end i et centraliseret miljø, hvilket er grunden til, at alle forsøger ikke at ødelægge ting til at starte med.

Bitcoin har lært mig, at det at bevæge sig langsomt er en af dens funktioner, ikke en fejl.

⁶Satoshi Nakamoto, i et svar til SmokeTooMuch [54]

19. Privatlivet er ikke dødt

Alle deltagerne spilledede på én gang uden at 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 i jorden og råbte: „af med hans hoved!“ eller: „af med hendes hoved!“

– Lewis Carroll, *Alice i Eventyrland*

Hvis man skal tro på eksperterne, har privatlivets fred været dødt siden 80’erne¹. Den pseudonyme opfindelse af Bitcoin og andre begivenheder i vores nyere historie viser, at det ikke er tilfældet. Privatlivet lever, på trods af, at det på ingen måde er let at undslippe overvågningsstaten.

Satoshi gjorde sig store anstrengelser for at skjule sine spor og skjule sin identitet. Ti år senere er det stadig uvist, om Satoshi Nakamoto var en enkelt person, en gruppe mennesker, en mand, en kvinde eller en tidsrejsende kunstig intelligens, som skabte sig selv for at overtage verdensherredømmet. Lægger vi konspirationsteorierne til side, ser vi, at Satoshi valgte at identificere sig som en japansk mand, og derfor antager jeg ikke, men respekterer hans valgte køn og omtaler ham som *han*.

Uanset hvad hans virkelige identitet måtte være, havde Satoshi succes med at skjule den. Han satte et opmuntrende eksempel for alle, der ønsker at forblive anonyme: Det er muligt at have privatliv på internettet.

¹<https://bit.ly/privacy-is-dead>



Figur 19.1.: Jeg er ikke Dorian Nakamoto.

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

– Edward Snowden²

Satoshi var ikke den første pseudonyme eller anonyme opfinder, og han bliver heller ikke den sidste. Nogle har direkte efterlignet denne pseudonyme publikationsstil, blandt andre Tom Elvis Yedusor fra MimbleWimble [71], mens andre har offentliggjort avancerede matematiske beviser, mens de har forblevet helt anonyme [3].

Det er en mærkelig ny verden, vi lever i. En verden, hvor identitet er valgfri, og bidrag accepteres på baggrund af fortjeneste, samt hvor folk kan samarbejde og handle frit. Det vil kræve noget tilvænning at blive fortrolig med disse nye paradigmer, men jeg er overbevist om, at alt dette har potentialet til at ændre verden til det bedre.

Vi bør alle huske, at privatliv er en grundlæggende menneskerettighed³. Så længe folk udøver og forsvarer disse rettigheder, er kampen for privatlivets fred langt fra slut.

Bitcoin har lært mig, at privatlivets fred ikke er død.

²Edward Snowden, svarer på læsernes spørgsmål [66]

³Verdenserklæringen om Menneskerettigheder, *artikel 12*. [6]

20. Cypherpunks skriver kode

„Jeg kan se, at du prøver at opfinde noget.“

– Lewis Carroll, *Alice i Eventyrland*

Ligesom mange andre gode idéer, opstod Bitcoin ikke ud af ingenting. Det blev gjort muligt ved at benytte og kombinere mange innovationer og opdagelser inden for matematik, fysik, computervidenskab og andre områder. Satoshi var utvivlsomt et geni, men han ville ikke have været i stand til at opfinde Bitcoin uden de giganter, hvis skuldre han stod på.

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

– Ludwig von Mises¹

En af disse giganter er Eric Hughes, en af grundlæggerne af cypherpunk-bevægelsen og forfatter til *A Cypherpunk's Manifesto*. Det er svært at forestille sig, at Satoshi ikke var påvirket af dette manifest. Det indbefatter mange ting, som Bitcoin muliggør og udnytter, såsom direkte og private transaktioner, elektroniske penge og kontanter, anonyme systemer og forsvar af privatlivets fred ved hjælp af kryptografi og digitale signaturen.

¹Ludwig von Mises, *Human Action* [74]

„Privatliv er en nødvendighed for et åbent samfund i den elektroniske tidsalder. Da vi ønsker privatlivets fred, må vi sikre, at hver part i en transaktion kun har kendskab til det, der er direkte nødvendigt for den pågældende transaktion. Derfor kræver privatlivets fred i et åbent samfund anonyme transaktionssystemer. Indtil nu har kontanter været det primære system. Et anonymt transaktionssystem er ikke et hemmeligt transaktionssystem. Vi Cypherpunks er dedikerede til at bygge anonyme systemer. Vi forsvarer vores privatliv med kryptografi, med anonyme systemer til videresendelse af e-mail, med digitale signaturer og med elektroniske penge. Cypherpunks skriver kode.“

– Eric Hughes²

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

På ægte cypherpunk-manér satte Satoshi sig derfor ned og begyndte at skrive kode. Denne kode tog en abstrakt idé og biviste overfor verden, at den faktisk virkede. Denne kode plantede frøet til en ny økonomisk virkelighed. Takket være denne kode kan alle bekræfte, at dette nye system rent faktisk fungerer, og hvert cirka 10. minut beviser Bitcoin over for verden, at den stadig er i live.

For at sikre, at hans innovation overgik fantasien og blev til virkelighed, skrev Satoshi koden til at implementere sin idé, før han skrev hvidbogen. Han sørgede også for ikke at forsinke³ udgivelsen for evigt. Når alt kommer til alt, „er der altid en ting mere at gøre.“

²Eric Hughes, *A Cypherpunk's Manifesto* [38]

³„Vi bør ikke udsætte for evigt, indtil hver eneste mulige funktionalitet er færdig.“ - Satoshi Nakamoto [56]

```

23 map<uint256, CBlockIndex*> mapBlockIndex;
24 const uint256 hashGenesisBlock("0x000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f");
25 CBlockIndex* pindexGenesisBlock = NULL;
26 int nBestHeight = -1;
27 uint256 hashBestChain = 0;
28 CBlockIndex* pindexBest = NULL;
29 ...
675 int64 CBlock::GetBlockValue(int64 nFees) const
676 {
677     int64 nSubsidy = 50 * COIN;
678
679     // Subsidy is cut in half every 4 years
680     nSubsidy >= (nBestHeight / 210000);
681
682     return nSubsidy + nFees;
683 }
684
685 unsigned int GetNextWorkRequired(const CBlockIndex* pindexLast)
686 {
687     const unsigned int nTargetTimespan = 14 * 24 * 60 * 60; // two weeks
688     const unsigned int nTargetSpacing = 10 * 60;
689     const unsigned int nInterval = nTargetTimespan / nTargetSpacing;
690
691     // Genesis block
692     if (pindexLast == NULL)
693         return bnProofOfWorkLimit.GetCompact();

```

Figur 20.1.: Kodeuddrag fra Bitcoin version 0.1

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

– Satoshi Nakamoto⁴

I nutidens verden af endeløse løfter og tvivlsom udførelse var der desperat brug for en udøvelse af dedikeret opbygning. Vær bevidst, overbevis dig selv om, at du faktisk kan løse problemerne, og implementér løsningerne. Vi bør alle stræbe efter at være lidt mere cypherpunk.

Bitcoin har lært mig, at cypherpunks skriver kode.

⁴Satoshi Nakamoto, Re: Bitcoin P2P e-cash papir [50]

21. Metaforer for Bitcoins fremtid

„Jeg ved, at der helt sikkert vil ske noget interessant...“

– Lewis Carroll, *Alice i Eventyrland*

I de sidste par årtier er det tydeligt, at teknologisk innovation ikke følger en lineær trend. Uanset om man tror på den teknologiske singularitet eller ej, er det ubestrideligt, at fremskridtene på mange områder er eksponentielle. Ikke alene det, men hastigheden, hvormed teknologier bliver taget i brug, accelererer også. Før du ved af det, er busken i den lokale skolegård væk, og dine børn bruger Snapchat i stedet. Eksponentielle kurver har en tendens til at give dig en forskrækkelse, længe før du ser dem komme.

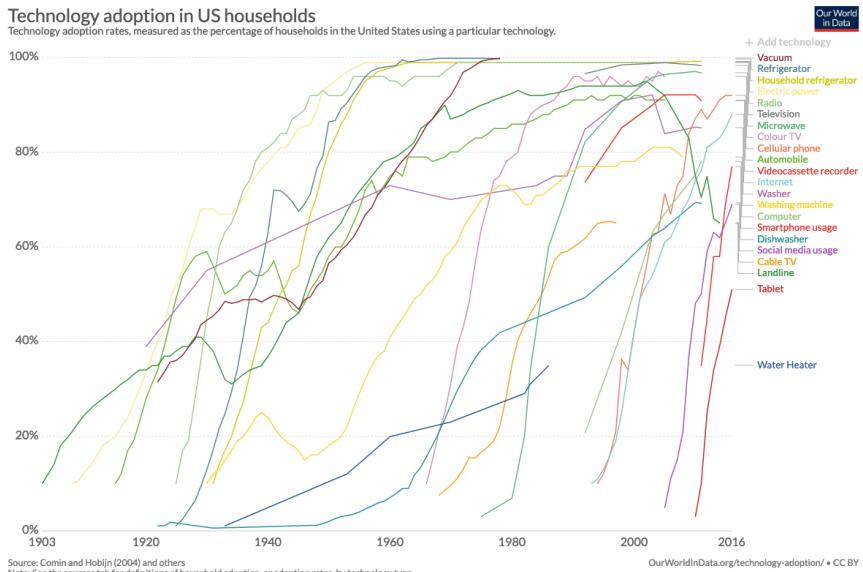
Bitcoin er en eksponentiel teknologi, der bygger på eksponentielle teknologier. *Our World in Data*¹ viser smukt den stigende hastighed af teknologisk adoption, startende i 1903 med introduktionen af fastnettelefoner (se Figur 21.1). Fastnettelefoner, elektricitet, computere, internettet og smartphones følger alle eksponentielle tendenser i pris, ydeevne og udbredelse. Bitcoin gør også dette [23].

Bitcoin har ikke én, men flere netværkseffekter², som alle resulterer i eksponentielle vækstmønstre inden for deres respektive områder: pris, brugere, sikkerhed, udviklere, markedsandel og anvendelse som globale penge.

Efter at have overlevet sin spæde begyndelse fortsætter Bitcoin med at vokse hver dag i mere end ét aspekt. Indrømmet, tek-

¹<https://ourworldindata.org/>

²Trace Mayer, *The Seven Network Effects of Bitcoin* [44]



Figur 21.1.: Bitcoin er bogstaveligt talt helt uden for skalaen.

nologien har ikke nået sin modenhed endnu. Den befinner sig måske i ungdomsårene. Men hvis teknologien er eksponentiel, er vejen fra ubemærkethed til allestedsnærværende kort.

I sin TED Talk fra 2003 valgte Jeff Bezos at bruge elektricitet som en metafor for nettets fremtid.³ Alle tre fænomener - elektricitet, internettet og Bitcoin - er *aktivierende* netværksteknologier, der muliggør andre ting. De er infrastrukturer, der skal bygges ovenpå, og deres natur er at være grundlaget for andre teknologier.

Elektricitet har eksisteret i lang tid nu. Vi tager den for givet. Internettet er betydeligt yngre, men de fleste tager det også for givet. Bitcoin er ti år gammel og er trængt ind i den offentlige bevidsthed under den sidste hype-cyklus. Kun de tidligste brugere tager den for givet. Som tiden går, vil flere og flere mennesker

³<http://bit.ly/bezos-web>



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

anerkende Bitcoin som noget, der bare er.⁴

I 1994 var internettet stadig forvirrende og det var ikke intuitivt. Når man ser denne gamle optagelse af *Today Show*⁵ bliver det tydeligt, at det, der føles naturligt og intuitivt nu, faktisk ikke var det dengang. Bitcoin er stadig forvirrende og fremmed for de fleste, men ligesom internettet er naturligt for den digitalt indfødte, vil det at bruge og stable sats⁶ være en selvfølge for fremtidens bitcoin-indfødte.

„Fremitiden er allerede her - den er bare ikke jævnt fordelt.“

– William Gibson⁷

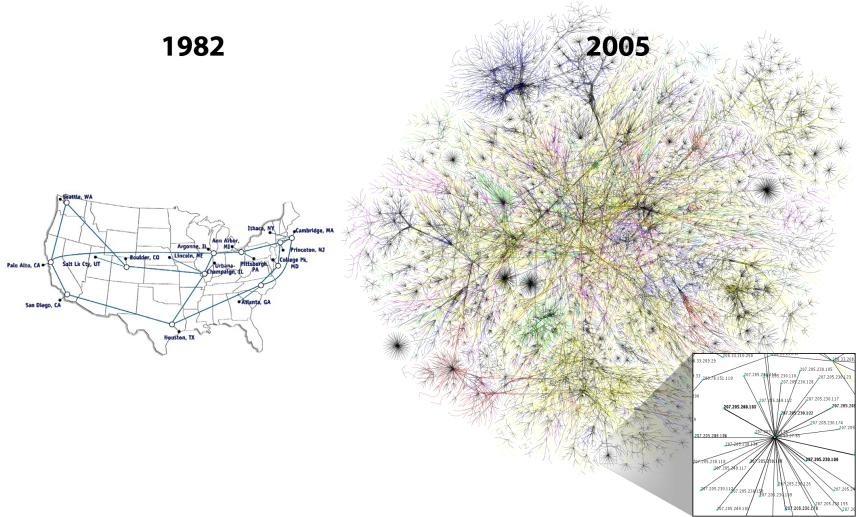
I 1995 brugte omkring 15% af voksne amerikanere internettet. Historiske data fra Pew Research Center [28] viser, hvordan internettet har vævet sig ind i alle vores liv. Ifølge en forbrugerundersøgelse foretaget af Kaspersky Lab [41], har 13% af de

⁴Dette er kendt som *Lindy-effekten*. Lindy-effekten er en teori om, at den fremtidige forventede levetid for ikke-forgængelige fænomener som en teknologi eller en idé er proportional med deres nuværende alder, således at hver ekstra periode med overlevelse indikerer en længere forventet restlevetid. [89]

⁵https://youtu.be/U1JkuSyNg_C

⁶<https://twitter.com/hashtag/stackingsats>

⁷William Gibson, *The Science in Science Fiction* [29]



Figur 21.3.: Internettet, 1982 vs 2005. Kilde: cc-by Merit Network, Inc. og Barrett Lyon, Opte Project

adspurgte brugt Bitcoin og dens kloner til at betale for varer i 2018. Selvom betalinger ikke er det eneste anvendelsesområde for bitcoin, er det en indikation af, hvor vi befinner os i internettid: Vi er i begyndelsen til midten af 90’erne.

I 1997 udtalte Jeff Bezos i et brev til aktionærerne [11] at „Dette er dag 1 for internettet“, og han erkendte det store uudnyttede potentiale for både internettet og sin virksomhed. Uanset hvilken dag det er for Bitcoin, er de enorme mængder uudnyttet potentiale tydelige for alle, undtagen den mest dovtne iagttager.

Bitcoins første knudepunkt kom online i 2009, efter at Satoshi havde udvundet *skabelses-blokken*⁸ og frigav softwaren ud i

⁸Skabelses-blokken er den første blok i Bitcoins blokkæde. Moderne versioner af Bitcoin tæller den som blok 0, selvom tidlige versioner talte den som blok 1. Skabelses-blokken er normalt inkluderet i softwaren til de applikationer, der bruger Bitcoin-blokkæden. Den er speciel, fordi den ikke refererer til en tidligere blok og producerede en blokbelønning, der



Figur 21.4.: Hal Finney skrev det første tweet, der nævnte bitcoin, i januar 2009.

naturen. Hans knudepunkt var ikke alene længe. Hal Finney var en af de første, der forstod ideen og han sluttede sig til netværket. Ti år senere, da dette skrives, kører mere end 75.000^9 knudepunkter Bitcoin.

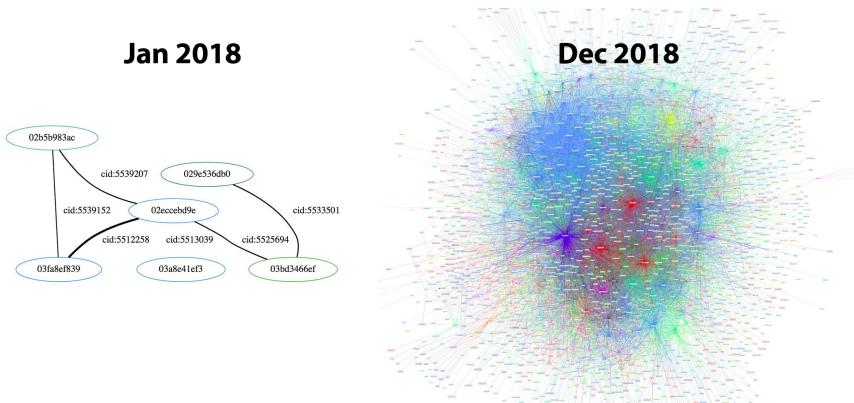
Protokollens basislag er ikke det eneste, der vokser eksponentielt. Lightning-netværket, en teknologi der bygger ovenpå Bitcoin, vokser endnu hurtigere.

I januar 2018 havde Lightning-netværket 40 knudepunkter og 60 kanaler [103]. I april 2019 var netværket vokset til mere end 4.000 knudepunkter og omkring 40.000 kanaler. Husk på, at dette stadig er en eksperimentel teknologi, hvor tab af midler kan ske og sker. Men tendensen er klar: Tusindvis af mennesker er hensynsløse og ivrige efter at bruge det.

For mig, der har oplevet internettets meteoriske fremgang, er parallelerne mellem internettet og Bitcoin åbenlyse. Begge er netværk, begge er eksponentielle teknologier, og begge skaber nye muligheder, nye industrier og nye måder at leve på. Ligesom elektricitet var den bedste metafor til at forstå, hvor internettet er på vej hen, kan internettet være den bedste metafor til

ikke kan bruges. Parameteren *coinbase* indeholder, sammen med de normale data, følgende tekst: „*The Times 03/Jan/2009 Kansler på randen af anden redningspakke til bankerne*“ [14]

⁹<https://bit.ly/luke-nodecount>



Figur 21.5.: Lightning-netværket, januar 2018 vs. december 2018. Kilde: Jameson Lopp

at forstå, hvor bitcoin er på vej hen. Eller, som Andreas Antonopoulos siger, Bitcoin er *pengenes internet*. Disse metaforer er en god påmindelse om, at selvom historien ikke gentager sig selv, så rimer den ofte.

Eksponentielle teknologier er svære at forstå og bliver ofte undervurderede. Selvom jeg har en stor interesse i sådanne teknologier, bliver jeg konstant overrasket over tempoet i fremskridt og innovation. At se Bitcoin-økosystemet vokse er som at se en hurtigspolet optagelse af internettets opståen. Det er fantastisk opløftende.

Min søgen efter at forstå Bitcoin har ført mig ned ad historiens stier på mere end én måde. At forstå gamle samfundsstrukturer, fortidens penge, og hvordan kommunikationsnetværk udviklede sig, var alt sammen en del af rejsen. Fra håndøksen til smartphonen har teknologien utvivlsomtændret vores verden mange gange. Netværksteknologier er særligt transformerende: skrift, veje, elektricitet og internettet. De har alle ændret verden. Bitcoin har ændret min verden og vil fortsætte med at ændre tankerne og hjerterne hos dem, der tør bruge den.

Bitcoin har lært mig, at det er vigtigt at forstå fortiden for at forstå dens fremtid. En fremtid, som kun lige er begyndt...

Afsluttende tanker

Konklusion

„Begynd ved begyndelsen,“ sagde kongen alvorligt, „og fortsæt, indtil du kommer til slutningen. Og hold så op.“

– Lewis Carroll, *Alice i Eventyrland*

Som nævnt i begyndelsen tror jeg, at ethvert svar på spørgsmålet „*Hvad har du lært af Bitcoin?*“ altid vil være ufuldstændigt. Symbiosen af hvad der kan ses som flere levende systemer - Bitcoin, teknosfæren og økonomi - er for indviklet, emnerne for mange, og tingene bevæger sig for hurtigt til nogensinde at blive fuldt ud forstået af en enkelt person.

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

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

– Giannina Braschi¹⁰

Bitcoin er født af internettet. Den vokser eksponentielt og udvisker grænserne mellem discipliner. Det er for eksempel ikke klart, hvor teknologiens verden ender, og hvor en anden verden begynder. Selvom Bitcoin kræver computere for at fungere effektivt, er datalogi ikke tilstrækkeligt for at forstå den. Bitcoin

¹⁰Giannina Braschi, *Empire of Dreams* [18]

er ikke kun grænseløs med hensyn til sin indre funktion, men også grænseløs i forhold til akademiske discipliner.

Økonomi, politik, spilteori, monetær historie, netværksteori, finansiering, kryptografi, informationsteori, censur, lovgivning og regulering, menneskelig organisation og psykologi - alle disse og mange flere er ekspertiseområder, der kan bidrage til forståelsen af, hvordan Bitcoin fungerer, og hvad Bitcoin er.

Ingen enkeltstående opfindelse er ansvarlig for dens succes. Det er kombinationen af flere tidlige uafhængige brikker, sat sammen af spilteoretiske incitamenter, der udgør den revolution, som Bitcoin er. Den smukke blanding af mange discipliner er det, der gør Satoshi til et geni.

Som ethvert komplekst system skal Bitcoin foretage afvejninger mellem effektivitet, omkostninger, sikkerhed og mange andre egenskaber. Ligesom der ikke er nogen perfekt løsning på at udlede en firkant fra en cirkel, vil enhver løsning på de problemer, som Bitcoin forsøger at løse, også altid være ufuldkommen.

„Jeg tror ikke, at vi nogensinde vil få gode penge igen, før vi tager dem ud af statens hænder. Det vil sige, vi kan ikke tage dem ud af statens hænder med vold; det eneste vi kan gøre er at indføre noget via snedige, indirekte bagveje, som de ikke kan stoppe.“

– Friedrich Hayek¹¹

Bitcoin er den snedige, indirekte bagvej som de ikke kan stoppe, og er dermed måden, hvorpå man kan genintroducere verden til gode penge. Den skaber et suverænt individ bag hvert knudepunkt, ligesom Da Vinci forsøgte at løse det uløselige problem med at kvadrere en cirkel ved at placere den vitruvianske mand

¹¹Friedrich Hayek on Monetary Policy, the Gold Standard, Deficits, Inflation, and John Maynard Keynes <https://youtu.be/EYhEDxFwFRU>

i cirklens centrum. Knudepunkter fjerner effektivt ethvert koncept om et centrum og skaber et system, som er forbløffende anti-skrøbeligt og ekstremt svært at lukke ned. Bitcoin lever, og dens hjerteslag vil sandsynligvis overleve os alle.

Jeg håber, du har nydt disse 21 lektioner. Måske er den vigtigste lektion, at man bør undersøge Bitcoin holistisk og fra flere vinkler, hvis man gerne vil have noget, der minder om et komplet billede. Ligesom det at fjerne en del fra et komplekst system ødelægger helheden, synes det at ødelægge forståelsen af Bitcoin at undersøge dele af den i isolation. Hvis bare én person fjerner „blokkæden“ fra sit ordforråd og erstatter det med „en kæde af blokke“, vil jeg dø som en lykkelig mand.

Under alle omstændigheder fortsætter min rejse. Jeg planlægger at vove mig længere ned i kaninhullets dybder, og jeg inviterer dig til at tage med på turen.¹²

¹²<https://twitter.com/dergigi>

Takkeord

Tak til de utallige forfattere og indholdsproducenter, der har påvirket min tankegang om Bitcoin og de emner, den berører. Der er for mange til at nævne dem alle, men jeg vil gøre mit bedste for at nævne nogle få.

- Tak til Arjun Balaji for tweeten, der motiverede mig til at skrive dette.
- Tak til Marty Bent for at give endeløs stof til eftertanke og underholdning. Hvis du ikke abonnerer på *Marty's Bent* og *Tales From The Crypt*, er du gået glip af noget. Skål for Matt og Marty der guider os gennem kaninhullet.
- Tak til Michael Goldstein og Pierre Rochard for udvælgelsen af materiale og levering af den bedste Bitcoin-litteratur via Nakamoto Institute. Og tak for skabelsen af Noded Podcast, som i høj grad har påvirket mit filosofiske syn på Bitcoin.
- Tak til Saifedean Ammous for hans overbevisninger, nådesløse tweets og for at have skrevet Bitcoinstandarden
- Tak til Francis Pouliot for at dele sin begejstring over at opdage tidskæden.
- Tak til Andreas M. Antonopoulos for alt det uddannelsesmateriale, han har udgivet i årenes løb.
- Tak til Peter McCormack for hans ærlige tweets og podcasten *What Bitcoin Did*, som fortsat leverer fantastiske indsigt fra mange områder inden for feltet.

- Tak til Jannik, Brandon, Matt, Camilo, Daniel, Michael, og Raphael for at give feedback på de tidlige udkast til nogle lektioner. En særlig tak til Jannik, der korrekturlæste flere udkast flere gange.
- Tak til Dhruv Bansal og Matt Odell for at tage sig tid til at diskutere nogle af disse ideer med mig.
- Tak til Guy Swann for at producere en lydversion af 21lesson.com.
- Tak til Friar Hass for hans åndelige støtte og vejledning, og for at tage sig tid til at skrive et forord til denne bog.
- Tak til min kone for at holde mig og min besættelse ud.
- Tak til min familie for at støtte mig i både gode og dårlige tider.
- Sidst, men ikke mindst, tak til alle bitcoin-maksimalister, shitcoin-minimalister, shills, bots og shitposters, som holder til i den smukke have, som Bitcoin Twitter er.

Og til sidst, tak fordi du læste dette. Jeg håber, du nød det lige så meget, som jeg nød at skrive det.

Figurer

0.1. Blinde munke undersøger Bitcoin-elefanten	12
7.1. Bitcoin-kaninhullet er bundløst.	30
9.1. Hyperinflation in the Weimar Republic (1921-1923)	41
12.1. fiat — ‘Lad det ske’	52
12.2. Lydisk mønt. Billedet er licenseret under Creative Commons Attribution Share-Alike 4.0 af Classical Numismatic Group, Inc.	53
12.3. Sølvmønter med varierende grad af afklipning. . .	54
12.4. Den oprindelige „dollar“. Sankt Joachim er afbilledet med sin kappe og troldmandshat. Billedet er cc-by-sa af Wikipedia-bruger Berlin-George . .	55
12.5. En amerikansk sølv доллар fra 1928. „Betales til ihændehaveren på forespørgsel.“ Billede cc-by-sa af National Numismatic Collection ved the Smithsonian Institution	56
12.6. Dette er et amerikansk 100 dollars guldcertifikat fra 1928. Billedet er cc-by-sa fra National Numismatic Collection, National Museum of American History.	57
12.7. En 20-dollarseddel fra 2004-serien, der bruges i dag. ‘DENNE SEDDEL ER LOVLIGT BETALINGSMIDDEL’	58
13.1. Pengenes multiplikatoreffekt	61

13.2. Yellen (direktør for den amerikanske centralbank) er en stærk modstander af en revision af den amerikanske centralbank (Federal Reserve), mens <i>Bitcoin Sign Guy</i> i baggrunden stærkt argumenterer for køb af bitcoin.	62
14.1. Bitcoins forsyningsformel	66
14.2. Bitcoins kontrollerede udbud	67
14.3. Forholdet mellem lager og produktion for guld	69
14.4. Visualisering af forholdet mellem lager og produktion for USD, guld og Bitcoin	70
14.5. Stigende forhold mellem lager og produktion for bitcoin sammenlignet med guld	71
15.1. For omkring 1 billion sekunder siden. Kilde: xkcd 1225	78
15.2. Illustration af SHA-256-sikkerhed. Original grafik af Grant Sanderson også kendt som 3Blue1Brown.	80
15.3. \$Angreb med 5\$ skruenøgle. Kilde: xkcd 538	82
15.4. Eksempler på elliptiske kurver. Grafik cc-by-sa Emmanuel Boutet.	83
16.1. Uddrag fra Ken Thompsons artikel ‘Reflections on Trusting Trust’	87
16.2. Fra <i>Stealthy Dopant-Level Hardware Trojans</i> af Becker, Regazzoni, Paar, Burleson	88
16.3. Hvad kom først, hønen eller ægget?	90
17.1. Uddrag fra hvidbogen. Var der nogen, der sagde tidskæde?	93
19.1. Jeg er ikke Dorian Nakamoto.	102
20.1. Kodeuddrag fra Bitcoin version 0.1	105
21.1. Bitcoin er bogstaveligt talt helt uden for skalaen. .	108

21.2. Mobiltelefon, ca. 1965 vs. 2019.	109
21.3. Internettet, 1982 vs 2005. Kilde: cc-by Merit Network, Inc. og Barrett Lyon, Opte Project	110
21.4. Hal Finney skrev det første tweet, der nævnte bitcoin, i januar 2009.	111
21.5. Lightning-netværket, januar 2018 vs. december 2018. Kilde: Jameson Lopp	112

Om bibliografiens

I dag er der udgivet mange af bøger om Bitcoin. Men det meste af samtalens - og dermed de fleste af de interessante ressourcer - findes online.

Denne bibliografi inkluderer en række bøger, artikler og online-ressourcer. Hvis ressourcen har en tilknyttet URL, var denne aktiv i oktober 2019, hvor jeg havde adgang til den pågældende ressource. Hvis en af de følgende URL'er fører til en død side, beklager jeg. Lad mig venligst vide det¹³ så jeg kan opdatere linket/linkene.

P.S.: Bitcoin og IPFS løser det.

¹³<https://dergigi.com/contact>

Litteratur

- [1] Saifedean Ammous. *The Bitcoin Standard: The Decentralized Alternative to Central Banking*. Wiley, 2017.
- [2] Saifedean Ammous. Presentation on the bitcoin standard. https://www.bayernlb.de/internet/media/de/ir/downloads_1/bayernlb_research_sonderpublikationen_1/bitcoin_munich_may_28.pdf, May 2018.
- [3] Jay Pantone Anonymous 4chan Poster, Robin Houston and Vince Vatter. A lower bound on the length of the shortest superpattern. <https://oeis.org/A180632/a180632.pdf>, October 2018.
- [4] Andreas M Antonopoulos. *Mastering Bitcoin: Programming the Open Blockchain*. ”O'Reilly Media, Inc.”, 2014.
- [5] Julian Assange. Cypherpunks: Freedom and the future of the internet - introduction: A call to cryptographic arms. <https://cryptome.org/2012/12/assange-crypto-arms.htm>, December 2012.
- [6] United Nations General Assembly. The universal declaration of human rights, December 1948.
- [7] Beautyon. Why america can't regulate bitcoin. <https://hackernoon.com/why-america-cant-regulate-bitcoin-8c77cee8d794>, March 2018.

- [8] Beautyon. Bitcoin is. and that is enough. <https://hackernoon.com/bitcoin-is-and-that-is-enough-e3116870eed1>, October 2019.
- [9] Georg T Becker, Francesco Regazzoni, Christof Paar, and Wayne P Burleson. Stealthy dopant-level hardware trojans. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 197–214. Springer, 2013.
- [10] Marty Bent. Tales from the crypt – a podcast about bitcoin. <https://tftc.io/tales-from-the-crypt/>, 2017.
- [11] Jeff Bezos. To our shareholders. http://media.corporate-ir.net/media_files/irol/97/97664/reports/Shareholderletter97.pdf, 1997.
- [12] Bitcoin Wiki contributors. Block hashing algorithm — Bitcoin Wiki. https://en.bitcoin.it/w/index.php?title=Block_hashing_algorithm&oldid=66452, 2019.
- [13] Bitcoin Wiki contributors. Controlled supply — Bitcoin Wiki. https://en.bitcoin.it/w/index.php?title=Controlled_supply&oldid=66483, 2019.
- [14] Bitcoin Wiki contributors. Genesis block — Bitcoin Wiki. https://en.bitcoin.it/w/index.php?title=Segregated_Witness&oldid=66902, 2019.
- [15] Bitcoin Wiki contributors. Pay to script hash — Bitcoin Wiki. https://en.bitcoin.it/w/index.php?title=Pay_to_script_hash&oldid=64705, 2019.
- [16] Bitcoin Wiki contributors. Segregated witness — Bitcoin Wiki. https://en.bitcoin.it/w/index.php?title=Segregated_Witness&oldid=66902, 2019.

- [17] Godfrey Bloom. Why the whole banking system is a scam. <https://youtu.be/hYzX3YZoMrs>, May 2013.
- [18] Giannina Braschi. *Empire of Dreams*. AmazonCrossing, 2011.
- [19] Nic Carter. Bitcoin's existential crisis / what is it like to be a bitcoin? <https://medium.com/s/story/what-is-it-like-to-be-a-bitcoin-56109f3e6753>, November 2018.
- [20] Guix Contributors. Guix — bootstrapping. https://guix.gnu.org/manual/en/html_node/Bootstrapping.html, 2019.
- [21] Bernard W. Dempsey. *Interest and Usury*. American Council on Public Affairs, <https://babel.hathitrust.org/cgi/pt?id=mdp.39015011903997&seq=230>, 1943.
- [22] Daniel C Dennett and Douglas R Hofstadter. *The mind's I: fantasies and reflections on self and soul*. Harvester Press, 1981.
- [23] Jeff Desjardins. The rising speed of technological adoption. <https://www.visualcapitalist.com/rising-speed-technological-adoption/>, February 2017.
- [24] Peter Diamandis. *Abundance : the future is better than you think*. Free Press, New York, 2012.
- [25] Dunny. I've learned more about finance, economics, technology, cryptography, human psychology, politics, game theory, legislation, and myself in the last three months of crypto than the last three and a half years of college. <https://twitter.com/BitcoinDunny/status/935330541263519745>, November 2017.

- [26] epii. New bitcoin logo. <https://bitcointalk.org/index.php?topic=4994.msg140770#msg140770>, May 2011.
- [27] Electronic Frontier Foundation. The crypto wars:governments working to undermine encryption. https://www.eff.org/files/2014/01/03/cryptowarsonepagers-1_cac.pdf, 2018.
- [28] Susannah Fox and Lee Rainie. How the internet has woven itself into american life. <https://pewrsr.ch/32M7Qmg>, February 2014.
- [29] William Gibson. The science in science fiction. <https://www.npr.org/2018/10/22/1067220/the-science-in-science-fiction>, October 2018.
- [30] Gigi. Bitcoin's energy consumption – a shift in perspective. <https://dergigi.com/2018/06/10/bitcoin-s-energy-consumption/>, June 2018.
- [31] Gigi. The magic dust of cryptography – how digital information is changing our societybitcoin's gravity. <https://dergigi.com/2018/08/17/the-magic-dust-of-cryptography/>, Aug 2018.
- [32] Gregory Maxwell. Taproot: Privacy preserving switchable scripting. <https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2018-January/015614.html>, 2018.
- [33] Hasu. Unpacking bitcoin's social contract. <https://uncommoncore.co/unpacking-bitcoins-social-contract>, December 2018.

- [34] Friedrich August Hayek. *1980s Unemployment and the Unions: Essays on the Impotent Price Structure of Britain and Monopoly in the Labour Market*. Institute of Economic Affairs, 1984.
- [35] Friedrich August Hayek. *The Collected Works of F.A. Hayek, Volume 6, Good Money, Part II*. Routledge, 1999.
- [36] Henry Hazlitt. *Economics in One Lesson*. Ludwig von Mises Institute, <https://mises.org/library/economics-one-lesson>, 1946.
- [37] Dan Held. Bitcoin's distribution was fair. <https://blog.picks.co/bitcoins-distribution-was-fair-e2ef7bbbc892>, 2018.
- [38] Eric Hughes. A cypherpunk's manifesto. <https://www.activism.net/cypherpunk/manifesto.html>, March 1993.
- [39] Guido Jörg Hülsmann. *Ethics of Money Production*. Ludwig von Mises Institute, <https://mises.org/library/ethics-money-production>, 2008.
- [40] Robert Kiyosaki. Why the rich are getting richer. <https://youtu.be/abMQhaMdQu0>, July 2016.
- [41] Kaspersky Lab. From festive fun to password panic: Managing money online this christmas. <https://www.kaspersky.com/blog/money-report-2018/>, 2018.
- [42] Jameson Lopp. No one has found the bottom of the bitcoin rabbit hole. <https://twitter.com/lopp/status/1061415918616698881>, November 2018.

- [43] Margo Rapport. History shows price of an ounce of gold equals price of a decent men's suit, says sionna investment managers. <https://www.businesswire.com/news/home/20110819005774/en/History-Shows-Price-Ounce-Gold-Equals-Price>, 2011.
- [44] Trace Mayer. The 7 network effects of bitcoin. <https://www.thrivenotes.com/the-7-network-effects-of-bitcoin/>, January 2016.
- [45] Ralph C. Merkle. Daos, democracy and governance. <https://alcor.org/cryonics/Cryonics2016-4.pdf#page=28>, July-August 2016.
- [46] Fiat Minimalist. Isn't it ironic that bitcoin has taught me more about money than all these years i've spent working for financial institutions? <https://twitter.com/fiatminimalist/status/1072880815661436928>, December 2018.
- [47] The Austrian Mint. Gold: The extraordinary metal. <https://www.muenzeoesterreich.at/eng/discover/for-investors/gold-the-extraordinary-metal>, November 2017.
- [48] British Museum. The origins of coinage. https://www.britishmuseum.org/explore/themes/money/the_origins_of_coinage.aspx, 2007.
- [49] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. October 2008.
- [50] Satoshi Nakamoto. Re: Bitcoin p2p e-cash paper. <https://www.metzdowd.com/pipermail/>

cryptography/2008-November/014832.html, November 2008.

- [51] Satoshi Nakamoto. Bitcoin open source implementation of p2p currency. <http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source?commentId=2003008%3AComment%3A9562>, February 2009.
- [52] Satoshi Nakamoto. Bitcoin open source implementation of p2p currency. <http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source>, February 2009.
- [53] Satoshi Nakamoto. Re: Bitcoin open source implementation of p2p currency. <http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source>, February 2009.
- [54] Satoshi Nakamoto. Re: Questions about bitcoin. <https://bitcointalk.org/index.php?topic=13.msg46#msg46>, December 2009.
- [55] Satoshi Nakamoto. Dealing with sha-256 collisions. <https://bitcointalk.org/index.php?topic=191.msg1585#msg1585>, June 2010.
- [56] Satoshi Nakamoto. Re: 0.3 almost ready. <https://bitcointalk.org/index.php?topic=199.msg1670#msg1670>, June 2010.
- [57] Satoshi Nakamoto. Re: Transactions and scripts: Dup hash160 ... equalverify checksig. <https://bitcointalk.org/index.php?topic=195.msg1611#msg1611>, June 2010.
- [58] Ron Paul. *End the Fed*. Grand Central Publishing, <http://endthefed.org/books/>, 2009.

- [59] Jordan Pearson. Inside the world of the bitco-in carnivores: Why a small community of bitco-in users is eating meat exclusively. https://motherboard.vice.com/en_us/article/ne74nw/inside-the-world-of-the-bitcoin-carnivores, September 2017.
- [60] Pieter Wuille. Schnorr signatures for secp256k1. <https://github.com/sipa/bips/blob/bip-schnorr/bip-schnorr.mediawiki>, 2019.
- [61] Plato. *Plato in Twelve Volumes, Vol. 3. (Euthydemus section 304a/304b)*. Harvard University Press, <http://www.perseus.tufts.edu/hopper/text?doc=Perseus%3Atext%3A1999.01.0178%3Atext%3DEuthyd.%3Asection%3D304a>, 2017.
- [62] Federal Reserve. Money stock measures – discontinuance of m3. <https://www.federalreserve.gov/Releases/h6/discm3.htm>, 2005.
- [63] Carl Sagan. *Cosmos*. Random House, 1980.
- [64] Bruce Schneier. *Applied Cryptography: Protocols, Algorithms and Source Code in C*. John Wiley and Sons, 2017.
- [65] Bruce Schneier. Schneier on security. <https://www.schneier.com>, 2019.
- [66] Edward Snowden. Edward Snowden: Nsa whistleblower answers reader questions. <https://www.theguardian.com/world/2013/jun/17/edward-snowden-nsa-files-whistleblower>, June 2013.

- [67] Jimmy Song. Why bitcoin is different. <https://medium.com/@jimmysong/why-bitcoin-is-different-e17b813fd947>, April 2018.
- [68] U.S. Geological Survey. National minerals information center — mineral commodity summaries. <https://www.usgs.gov/centers/nmic/mineral-commodity-summaries>, 2019.
- [69] Nick Szabo. Shelling out: The origins of money. <https://nakamotoinstitute.org/shelling-out/>, 2002.
- [70] K. Thompson. Reflections on trusting trust. In *ACM Turing award lectures*, page 1983, 2007.
- [71] Tom Elvis Jedusor. Mimblewimble origin. <https://github.com/mimblewimble/docs/wiki/MimbleWimble-Origin>, 2016.
- [72] Grisha Trubetskoy. Blockchain proof-of-work is a decentralized clock. <https://grisha.org/blog/2018/01/23/explaining-proof-of-work/>, 2018.
- [73] Peter Van Valkenburgh. Coin center’s peter van valkenburg on preserving the freedom to innovate with public blockchains. <http://bit.ly/valkenburgh>, November 2018.
- [74] Ludwig von Mises. *Human Action*. Ludwig von Mises Institute, <https://mises.org/library/human-action-0/html/p/607>, 1949.
- [75] Wikipedia contributors. 2013–present economic crisis in venezuela — Wikipedia, the free encyclopedia. <https://en.wikipedia.org/w/index.php?>

[title=2013%E2%80%93present_economic_crisis_in_Venezuela&oldid=918242758](https://en.wikipedia.org/w/index.php?title=2013%E2%80%93present_economic_crisis_in_Venezuela&oldid=918242758), 2019.

- [76] Wikipedia contributors. Austrian school — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Austrian_School&oldid=920008469, 2019.
- [77] Wikipedia contributors. Bimetallism — Wikipedia, the free encyclopedia. <https://en.wikipedia.org/w/index.php?title=Bimetallism&oldid=920537299>, 2019.
- [78] Wikipedia contributors. Crypto wars — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Crypto_Wars&oldid=916147143, 2019.
- [79] Wikipedia contributors. Discrete logarithm — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Discrete_logarithm&oldid=909625575, 2019.
- [80] Wikipedia contributors. Dual ec drbg — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Dual_EC_DRBG&oldid=918490393, 2019.
- [81] Wikipedia contributors. Dyson sphere — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Dyson_sphere&oldid=916621053, 2019.
- [82] Wikipedia contributors. Elliptic-curve cryptography — Wikipedia, the free encyclopedia. <https://en.>

wikipedia.org/w/index.php?title=Elliptic-curve_cryptography&oldid=916608234#Backdoors, 2019.

- [83] Wikipedia contributors. Hyperinflation — Wikipedia, the free encyclopedia. <https://en.wikipedia.org/w/index.php?title=Hyperinflation&oldid=919343724>, 2019.
- [84] Wikipedia contributors. Illegal number — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Illegal_number&oldid=918772989, 2019.
- [85] Wikipedia contributors. Illegal prime — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Illegal_prime&oldid=913087454, 2019.
- [86] Wikipedia contributors. Keynesian economics — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Keynesian_economics&oldid=919881690, 2019.
- [87] Wikipedia contributors. Landauer's principle — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Landauer%27s_principle&oldid=907333330, 2019.
- [88] Wikipedia contributors. Last glacial maximum — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Last_Glacial_Maximum&oldid=919510280, 2019.
- [89] Wikipedia contributors. Lindy effect — Wikipedia, the free encyclopedia. <https://en.wikipedia.org/>

w/index.php?title=Lindy_effect&oldid=921214819, 2019.

- [90] Wikipedia contributors. List of currencies — Wikipedia, the free encyclopedia. [https://en.wikipedia.org/w/index.php?title=List_of_currencies&oldid=897955050](https://en.wikipedia.org/w/index.php?title>List_of_currencies&oldid=897955050), 2019.
- [91] Wikipedia contributors. List of historical currencies — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=List_of_historical_currencies&oldid=919919705, 2019.
- [92] Wikipedia contributors. Methods of coin debasement — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Methods_of_coin_debasement&oldid=917940627, 2019.
- [93] Wikipedia contributors. Money multiplier — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Money_multiplier&oldid=918027413, 2019.
- [94] Wikipedia contributors. Money supply — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Money_supply&oldid=921152289, 2019.
- [95] Wikipedia contributors. P versus np problem — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=P_versus_NP_problem&oldid=919882161, 2019.
- [96] Wikipedia contributors. Paradox of value — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Paradox_of_value&oldid=919882161.

[org/w/index.php?title=Paradox_of_value&oldid=906068208](https://en.wikipedia.org/w/index.php?title=Paradox_of_value&oldid=906068208), 2019.

- [97] Wikipedia contributors. Sha-2 — Wikipedia, the free encyclopedia. <https://en.wikipedia.org/w/index.php?title=SHA-2&oldid=917408454>, 2019.
- [98] Wikipedia contributors. Ship of theseus — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Ship_of_Theseus&oldid=923020256, 2019.
- [99] Wikipedia contributors. Silver certificate (united states) — Wikipedia, the free encyclopedia. [https://en.wikipedia.org/w/index.php?title=Silver_certificate_\(United_States\)&oldid=917688197](https://en.wikipedia.org/w/index.php?title=Silver_certificate_(United_States)&oldid=917688197), 2019.
- [100] Wikipedia contributors. Subjective theory of value — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Subjective_theory_of_value&oldid=893004286, 2019.
- [101] Wikipedia contributors. Thaler — Wikipedia, the free encyclopedia. <https://en.wikipedia.org/w/index.php?title=Thaler&oldid=914457345>, 2019.
- [102] Wikipedia contributors. Theory of value (economics) — Wikipedia, the free encyclopedia. [https://en.wikipedia.org/w/index.php?title=Theory_of_value_\(economics\)&oldid=919603374](https://en.wikipedia.org/w/index.php?title=Theory_of_value_(economics)&oldid=919603374), 2019.
- [103] Wilma Woo. 'unfairly cheap' lightning network mainnet hits 40 nodes, 60 channels. <https://bitcoinist.com/bitcoin-lightning-network-mainnet-nodes/>, January 2018.

Del IV.

Den danske udgave

Om den danske udgave

Denne danske version af 21 Lektioner er blevet oversat af et team af danske Bitcoin-entusiaster, der er passionerede om at spredde budskabet om Bitcoin og dens potentielle til at forbedre verden.

Vi håber, at du har nydt at læse 21 Lessons og at du vil være med til at sprede budskabet.

Motivation

Vi har oversat 21 Lektioner til dansk, da vi tror på, at den tilbyder en lettilgængelig introduktion til Bitcoin og dens principper. I modsætning til mange andre bøger om Bitcoin dækker 21 Lektioner et bredt spektrum af de elementer, der gør Bitcoin til Bitcoin. Den er kortfattet, skrevet på et letforståeligt dansk og med et begrænset brug af teknisk jargon. Vi har alle startet samme sted, hvor vi kigger på den hvide kanin, der hopper af sted, og som i Alice i Eventyrland så starter rejsen hvor Alice hopper ned i kaninhullet uden at tænke på hvorfor en kanin har et lommeur og vest. Eventyret ville dog have været anderledes, hvis Alice havde haft en rejseberetning med skrevet af Bob eller Gigi.

Handling

Vi opfordrer dig til at lære mere om Bitcoin og blive involveret i Bitcoin-fællesskabet. Du kan finde mere information på følgende ressourcer:

- **Telegram-kanalen ”EnOgTyve”:** Chat for danske Bitcoin-entusiaster hvor alle der vil lære mere om Bitcoin er velkomne. Link: t.me/enogtyvedk.
- **EnOgTyve’s portal:** Dansksproget portal med masser af information om Bitcoin. Link: www.enogtyve.org.
- **Bogen *Bitcoinstandarden*:** En detaljeret økonomisk analyse af Bitcoin, gode penges egenskaber og af de samfundsproblemer fiat-valutaer har skabt.
Link: www.bitcoinstandarden.dk.
- **Bitcoinskolens.net:** Bitcoinskolens mission er at informere om og undervise dig i bitcoin, så du selv kan træffe dine egne valg på et oplyst grundlag. www.bitcoinskolens.net.

Taknemmelighed

Teamet vil gerne takke følgende personer for deres bidrag til oversættelsen og korrekturlæsning:

- Peter Isaksen (plus hans hustru), redaktør
- Rasmus Hansen
- Pierre Vendelboe
- Btcblot
- Rune Kristensen

Følg den hvide kanin!