BITCOIN SOM VALUTA: KRYPTOGRAFISK SIKKERHED OVERFOR MAKROØKONOMISK USIKKERHED

EN TVÆRFAGLIG ANALYSE AF BITCOINS KRYPTOGRAFISKE FUNDAMENT OG DENS MAKROØKONOMISKE IMPLIKATIONER SOM LOVLIGT BETALINGSMIDDEL

billede 1, USA TODAY, https://eu.usatoday.com/story/tech/2021/06/11/bitcoin-beach-el-salvador-glimpse-cryptocurrency-economy/7651287002/

Anslag m. mellemrum: 47.923

Levi van Boekel
Rysensteen Gymnasium

Abstract

Bitcoin (BTC) has since its original launch in 2009 gained worldwide attention. However, even though the trading price has increased dramatically, it remains unknown whether or not the so-call *currency* has meaningful socioeconomic implications. This paper, therefore, examines the macroeconomic consequences of adapting BTC as a legal tender, while simultaneously giving the reader a mathematical insight into Bitcoins signature algorithm, seck251k1. The project will in this context argue that there has arisen discrepancy between the narrative of Bitcoin as a *secure* mean of payment, and reality, where BTC is, cryptographically secure, but remains highly volatile and represents a neoliberal, heterodox, view on state interference in economy. A view, that currently remains ideological and requires further scientific examination.

The paper is structured so that it starts by giving a brief introduction to how currency markets influence the macroeconomic position of nations, such as their ability to compete in global markets. Thereafter the paper will examine Bitcoin's signature algorithm mathematically, as an understanding of Bitcoin's cryptographic security is fundamental for everybody wanting a thorough insight into the mechanism behind BTC. Finally, the paper will discuss the consequences of a state using a decentralized monetary unit, by taking a closer look at El Salvador's decision to accept Bitcoin as legal tender. The project will in this regard assess, whether or not BTC can be seen as macroeconomically *secure*. The theoretical framework for this discussion will be given by Austrian school and modern monetary theory.

1. Indholdsfortegnelse

2. Indledning

"Cryptocurrency is everything you don't understand about money combined with everything you don't understand about computers" (Oliver, 2018), sådan lød det fra den amerikanske tv-vært John Oliver, da han skulle beskrive kryptovaluta. For sandheden er, at selvom Bitcoin får stadig større indflydelse i den globale økonomi, er forståelse for kryptovaluta forbeholdt de få. Kryptovalutas rolle i den offentlige debat begrænser sig således til diskussioner blandt primært unge, mandlige individer, med interesse for finans. Men uanset, om man interesserer sig for økonomi eller ej, er en forståelse for kryptovaluta uundværlig, idet store banker, og pensionskasser allerede spekulerer deri. Der er med andre ord opstået en diskrepans mellem den brede offentligheds forståelse af kryptovaluta og dens stigende indflydelse. Dette blev eksemplificeret ved den lave danske mediedækning af det nylige krak af kryptobørsen FTX, der gik konkurs med over 5 milliarder USD i gæld (Reuters, 2023). Men også krakket af traditionelle banker, som Silicon Valley Bank, kan muligvis været forudsaget af kursudsving i kryptovaluta, da banken gav lån til adskillige krypto firmaer[1]. Kryptovalutas makroøkonomiske indflydelse blev dog allerede før disse krak for alvor manifesteret, da El Salvador den 5. juni 2021 indførte Bitcoin som statslig valuta. Det følgende projekt, har dermed til formål at belyse den tekniske del af Bitcoin, samt de makroøkonomiske konsekvenser, det kan have for et land at indføre Bitcoin som statslig valuta.

Projektet vil således starte med at redegøre for valutamarkedets og valutakursdannelsens overordnede betydning for det makroøkonomiske kredsløb, og løbende sætte dette i relation til kryptovaluta vha. bl.a. kvantitative data.

Herefter vil projektet blive meget teknisk, idet matematikken bag Bitcoin forklares. Denne matematik er alsidig, og dækker over en række områder, hvoraf mange ikke er i projektets omfang. Projektet vil dermed begrænse sin matematiske redegørelse til signaturalgoritmen, der bruges hvert sekund, når Bitcoin transaktioner valideres og vil således ikke dække matematikken bag Bitcoin mining, kursudsving eller Blockchain teknologien, om end disse dele er vigtige komponenter af Bitcoin. Valget om at fokusere på signaturalgoritmen er truffet, idet jeg anser en forståelse af algoritmen som et fundament for øvrigt arbejde indenfor feltet.

[1] Det er endnu for tidligt at sige, om disse krypto firmaet var skyld i bankens kollaps, men ifølge en række eksperter, kan forklaringen delvis findes blandt bankens høj-risiko kunder.

Projektet vil således motivere signaturalgoritmen ved at introducere asymmetrisk public-key kryptografi, og herefter vise, hvad signaturalgoritmens opgave er i den forbindelse. Dernæst tages et skridt tilbage fra kryptografiens verden, idet der introduceres to vigtige matematiske koncepter (modulo regning og endelige felter) for det videre arbejde med algoritmen. Afsluttende introduceres og redegøres for elliptisk kurvekryptografi, der er kernen i signaturalgoritmen. I den forbindelse vil jeg ved hjælp af Python kode illustrere, hvordan man kan signere vilkårlige transaktioner med algoritmen. Afsluttende argumenteres for, hvorfor man med rette kan hævde, at Bitcoin er kryptografisk sikret til det højest mulige.

Afsluttende vil jeg, med udgangspunkt i El Salvadors beslutning om at indføre Bitcoin som national valuta, diskutere, hvorvidt Bitcoin også kan anses som værende makroøkonomisk *sikkert*. Dette gøres, ved at tage udgangspunkt i hvilke fordele og ulemper det kan have for et lands økonomi at anvende kryptovaluta. Et sådant diskussionsspørgsmål, er meget stort, og det vil i projektet ikke være muligt at diskutere alle makroøkonomiske konsekvenser det vil medføre for et lands økonomi at anvende Bitcoin som statslig valuta. Diskussionen om kryptovalutas makroøkonomiske *sikkerhed*, vil derfor primært fokusere på de samfundsøkonomiske konsekvenser, der er forbundet med det faktum, at Bitcoin er decentralt og stater ikke på samme måde, som ved traditionel valuta, kan føre økonomisk politik, eller forøge mængden af penge i cirkulation. I diskussionen vil der blive anvendt viden om kryptering, samt makroøkonomisk teori.

2.1 Metode

I den samfundsfaglige del af projektet, vil der benyttes kvantitativ og komparativ metode, samt relevante teoretikere. Da projektets fokus er de makroøkonomiske konsekvenser af kryptovaluta, mener jeg, at disse metoder er mest hensigtsmæssige at tage i brug, idet projektet således kan sammenligne og analysere økonomiske konsekvenser på områder, hvor det er hensigtsmæssigt. Det er i den forbindelse klart, at konsekvenserne af El Salvadors indførsel af Bitcoin som statslig valuta, ikke kan overføres 1:1 til mere udviklede økonomier. I diskussionen vil de normative teoretikere danne ramme for, hvorvidt det er ønskværdigt, at stater har monopol over produktionen af penge, samt finans- og pengepolitik.

Diskussionens fundament er da givet ved den matematiske redegørelse, da en diskussion om Bitcoins makroøkonomiske konsekvenser ikke ville være aktuel, hvis man ikke kunne garantere sikkerheden! Det matematiske grundlag bag Bitcoins signaturalgoritme, er dog utrolig komplekst og projektet vil derfor skulle introducere en række nye matematiske emner, og give en redegørelse for de vigtigste regneoperationer indenfor disse emner. I denne del af

projektet, vil arbejdet være *i* matematik, og der vil således afklares centrale begreber og sætninger. For at fremme forståelse af emnerne, vil der således være både analytisk og grafisk problemløsning af udvalgte eksempler. Der vil ligeledes benyttes matematisk ræsonnement, når to sætninger bevises ved direkte bevis i afsnittet om modulo regning. Afslutningsvis vil der arbejdes *med* matematik, idet matematik anvendes til at beskrive forhold udenfor matematikken. Dette vil dog ikke ske i klassisk forstand, idet der ikke opstilles modeller eller lign., men den matematiske viden og teori anvendes sin rene form. I den forbindelse vil anvendelsens kryptografiske sikkerhed også vurderes.

3. Valutamarkedets og valutakursdannelsens overordnede makroøkonomiske betydning

Indenfor økonomi skelnes mellem flydende- og fastevalutakurser, hvor Danmark benytter sig af fastkurspolitik, og Bitcoins prisniveau er flydende. Det betyder i praksis, at den danske krone har en fast kurser overfor euroen og maksimalt må svinge $\pm 2{,}25$ (Trier, 2018, s. 89), mens Bitcoins kurs udelukkende er bestemt ud fra udbud og efterspørgsel. Det medfører enorme kurssvingninger, som illustreret i graferne nedenfor, og står i stærk kontrast til den danske krone, der har ligget nogenlunde stabilt siden 1982 (Trier, 2018, s.89).

graf 1, https://coinmarketcap.com/currencies/bitcoin/

Men selvom den danske krones kurs, har ligget nogenlunde stabilt siden 1982, betyder det ikke, at den danske krone ikke er blevet mindre værd over tid, tværtimod. I praksis falder købekraften nemlig hvert år, da den europæiske centralbank, forøger den samlede mængde af penge, der er i cirkulation. Omvendt er det, i hvert fald i teorien, med Bitcoin. Her er den samlede mængde af pengeenheder begrænset til 21 millioner, hvilket i teorien betyder, at BTC apprecierer over tid. Set i bredere tidsmæssigt perspektiv, holder påstanden kvantitativt stik, men man må indvende, at Bitcoins kursudvikling hidtil primært har været drevet af spekulation, hvorfor det er vanskeligt at sammenligne kursudviklingen med den danske krone. I bilag 1 og 2, ses ikke desto mindre grafer for købekraften af euro og kursen af Bitcoin.

Kursen af valutaer som euro, eller den danske krone, vil desuden være præget af en række pengepolitiske tiltag som eksempelvis ændringer i renteniveauet. En stigning fra ECB vil her medføre, at euroen apprecierer, da efterspørgslen efter euro forøges, mens et faldt i renteniveauet vil have den modsatte effekt. I skrivende stund, er renteniveauet eks. steget med

0,5% point, som et forsøg på at mindske inflationen[2]. Men selvom pengepolitiske tiltag også har en indflydelse på BTC pris, er kursen her langt mere usikker og volatil, og afhænger i større grad, af såkaldte *black swan* begivenheder (Taleb, 2021). Disse begivenheder er uforudsete, meget usandsynlige, men har enorme konsekvenser for det pågældende marked (Scott, 2022). Et eksempel på en sådan begivenhed, er krakket af FTX, der fik kursen på BTC til at falde med 22% på blot en dag. Hertil vil man kunne indvende, at den høje eksponering overfor disse begivenheder hænger sammen med Bitcoin forholdsvis lave samlede markedsværdi (marketcap), der per 18.3.23, er 550 milliarder USD mindre end Amazon, 1.9 billion USD mindre end Apple og 12.5 billion USD mindre end guld (8marketcap, 2023). Argumentet vil derfor være, at Bitcoin bliver langt mindre volatilt, når dens markedsværdi forøges (Nicolaisen et al, 2022). Ikke desto mindre, gør den høje volativitet i dag, at indførslen af Bitcoin som statslig valuta vil have en stor effekt på det pågældende lands internationale konkurrenceevne og det samfundsøkonomiske kredsløb. Nærmere bestemt, vil Bitcoin som national valuta medføre enorm usikkerhed, da konkurrenceevnen ville ændres markant dagligt. Konkurrenceevnen vil da falde, når Bitcoin stiger i pris (varerne i det pågældende land, vil blive dyrere for udenlandske kunder), og stige, når Bitcoin falder i pris (varerne i det pågældende land, vil blive billigere for udenlandske kunder). Indfører man således Bitcoin i et land som Danmark, hvor både eksport og import udgør store dele af det samfundsøkonomiske kredsløb, vil det være en stor udfordring at have en så varierende konkurrenceevne. Lavere eksport vil nemlig betyde, at den danske BNP vil falde, hvilket medfører et fald i beskæftigelse og dermed en forringelse af betalingsbalancen (Trier, 2018, s.93). Tager man derimod udgangspunkt i et land med en svagere økonomi, er det ikke entydigt, hvorvidt Bitcoins volativitet er et problem, idet eksempelvis Argentinas inflation er over 100%, og konkurrenceevnen dermed allerede er i et lavpunkt (Reuters, 2023).

Hvorvidt Bitcoin er en fordel for et lands makroøkonomiske forhold, vil diskuteres nærmere i slutningen af projektet, men det er inden da værd at opsummere, at Bitcoins valutakurs er flydende, hvilket betyder, at kursen bestemmes af udbud og efterspørgsel og dermed er langt mere volatil end traditionelle valuta. Det kan medføre makroøkonomiske usikkerheder, ved bl.a. at påvirke et lands konkurrenceevne, og dermed det samfundsøkonomiske kredsløb, negativt. Dertil kommer, at BTC ikke kan reguleres i samme grad som nationale valuta.

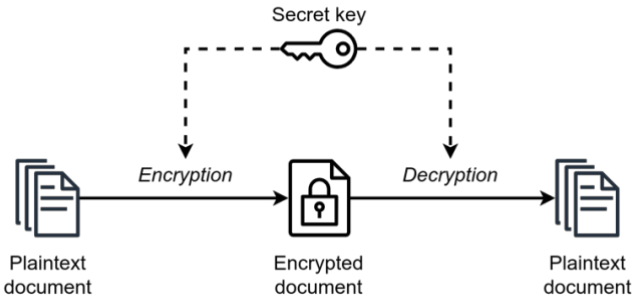
[2] Det skal nævnes, at den ECB varslede stigningen kort efter den amerikanske nationalbank hævede deres renter, hvilket tyder på, at det ikke nødvendigvis var deres egen beslutning at hæve renterne, men at dette skulle ske, da valutamarkederne er meget tæt knyttet sammen. Hvis den ECB dermed ikke havde hævet renten, ville der være en sandsynlighed for, at en stor mængde kapital ville bevæge sig mod USA.

De næste par sider, vil dog tage et skridt tilbage fra økonomiens verden og redegøre for den matematik, der ligger til grund for, at man ved hjælp af Bitcoin netværket, kan sende anonyme og decentrale transaktioner.

4. Matematikken bag Bitcoins signaturalgoritme

4.1 Public-key kryptografi: En introduktion

Et afgørende aspekt af Bitcoins signaturalgoritme bygger på såkaldt asymmetrisk public-key kryptering, der blev introducerede af professorer fra Stanford University i 1976 og sidenhen er blevet en uundværlig del af moderne kryptografi. Redegørelsen af public key kryptering i projektet bygger på videomateriale udgivet af professor i datalogi ved University of Nottingham, Sean Riley (Riley 2014). Ideen bag asymmetrisk public key kryptering udspringer fra et dilemma, som professorerne ved Stanford University stod overfor. De forestillede sig to individer, Alice og Bob, som ønsker at kommunikere krypteret med hinanden. Den hidtil anvendte metode var i den forbindelse, at Alice og Bob skulle enes om en symmetrisk algoritme. Det vil sige en algoritme, hvor der bruges samme system til at kryptere og dekryptere beskeden. I figur 1 nedenfor er en sådan situation illustreret.



Figur 1, MarcT0K (icons by JGraph), https://en.wikipedia.org/wiki/Symmetric-key_algorithm

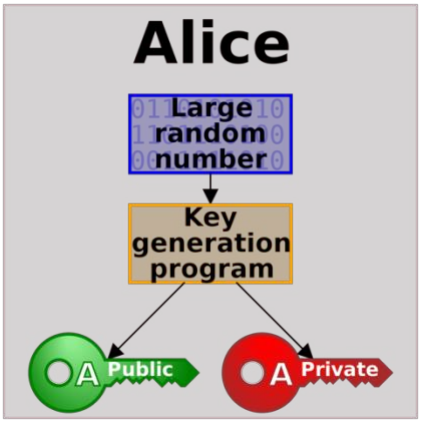
Det mest kendte eksempel på en symmetrisk algoritme er Cæsar koden[3], men udover at netop denne symmetrisk algoritme er forholdsvis simpel at gætte, påpegede professorerne, at var en grundlægge udfordring ved at benytte sig af symmetrisk kryptering. Nærmere bestemt vil det være nødvendigt for begge parter at kende til krypteringsalgoritmen, og hvis de to parter ikke kan kommunikere dette analogt via en sikker kanal, vil de ikke kunne kryptere deres besked. Det vil med andre ord være nødvendigt for Bob og Alice at mødes fysisk for at etablere enighed om, hvilken krypteringsalgoritme de vil skulle benytte sig af. Det er dermed tydeligt, at denne

[3] En krypteringsform, hvor man erstatter hvert bogstav i den besked man ønsker at kryptere, erstattes af et andet bogstav et fast antal pladser længere nede af alfabetet.

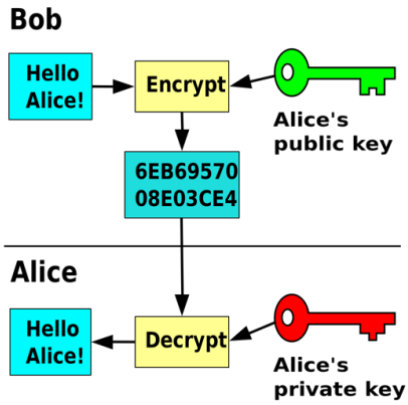
krypteringsform ikke egner sig til eksempelvis Bitcoin, der skal håndtere store mængder af internationale transaktioner dagligt.

4.2 De grundlæggende egenskaber ved asymmetrisk public key kryptering

Det var ud fra det dilemma, at professorerne ved Stanford udviklede det, de kaldte asymmetrisk public key kryptering. I stedet for at enes om en krypteringsalgoritme, generes i dette tilfælde et sæt virtuelle nøgler til hver bruger man ønsker at kommunikere med (i dette tilfælde Alice og Bob) vha. en matematisk algoritme, der omtales som systemets signaturalgoritme. Denne asymmetriske signaturalgoritme har, som vist i figur 2, til opgave at generere en privat og en offentlig nøgle til hver bruger i systemet. Disse to nøgler er bundet sammen vha. matematiske beregninger, og kaldes asymmetriske, idet disse matematiske beregninger er tilpas komplekse og sørger for, at man ikke kan gætte sig til brugerens private nøgle, ved at kende den offentlige. Bitcoin benytter secpk256k1 til at generere disse nøgler, da den vurderes til at være mest effektiv, men det er også muligt at bruge andre algoritmer som eks. *Diffie–Hellman key exchange*.



Figur 3, KohanX (talk), https://en.wikipedia.org/wiki/Public-key_cryptography



Figur 2, Davidgothberg, , https://en.wikipedia.org/wiki/Public-key_cryptography,

Efter Alice har generet en privat og en offentlig nøgle, vil hun skulle gøre en potentiel afsender opmærksom på hendes offentlige nøgle — den fungerer som en slags digital postkasse. I Bitcoin regi, fungerer ens offentlige nøgle som en digitale pung, som alle kan sende penge til (deraf navnet Bitcoin-Wallet). Det er altså ligesom i Alices' tilfælde nødvendigt for potentielle afsendere at have adgang til den offentlige nøgle, hvorfor mange Bitcoin brugere offentliggører deres wallet-adresse og knytter den til deres navn på en række registrere.

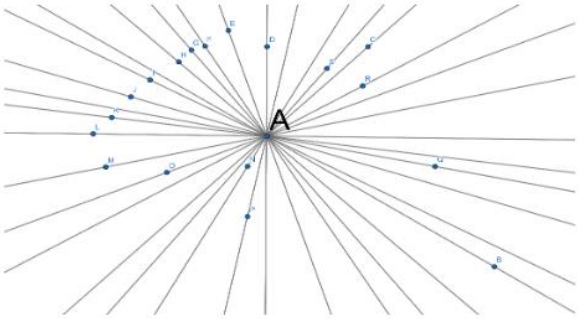
Når Bob har modtaget Alices offentlige nøgle, vil han, som vist i figur 3, kryptere sin besked med denne nøgle. Det matematiske forhold mellem Alices' offentlige og private nøgle gør nu, at hun som den eneste (antaget, at hun ikke har delt sin private nøgle med nogle) kan dekryptere

beskeden. I Bitcoins tilfælde betyder det, at ens private nøgle fungerer som den eneste adgang til ens pung, der indeholder alle ens Bitcoin. En transaktion mellem Alice og Bob, hvor Bob ønsker at sende penge til Alice, fungerer dermed ved, at Bob finder Alices' offentlige nøgle og sender Bitcoins til denne adresse, hvorefter Alice som den eneste har mulighed for at åbne sin digitale pung, og validere, at hun har modtaget de aftale Bitcoins[4]. Præcis, hvordan forholdet mellem de to nøgler er, og hvordan de generes, bygger på tre matematiske koncepter, der vil introduceres i de kommende afsnit.

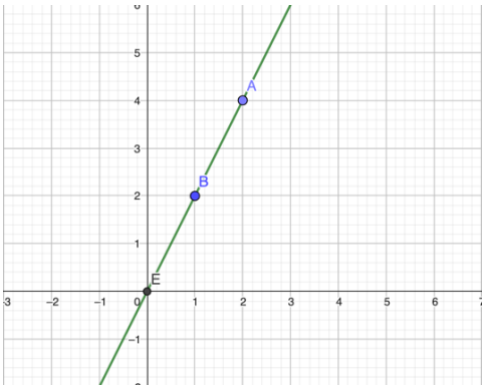
4.3 Motivation af endelige felter og deres anvendelse i kryptografi

Motivationen og redegørelsen af endelige felter og dele af modulo regning tager udgangspunkt i forelæsninger fra professor i datalogi Christof Paar (Paar, 2014) og videomateriale udgivet af kryptografen, Cryptoclear (Cryptoclear, 2021).

Lad os antage, at Alice og Bob nu ønsker at bruge deres viden om funktioner fra gymnasiet til at kreere en asymmetrisk kryptering. Bob husker i den forbindelse tilbage til, at et punkt i et todimensionelt plan kan skæres af uendelig mange linjer (figur 4), der skærer y-aksen uendelig mange steder, mens to punkter kun kan skæres af netop en linje (figur 5), der skærer y-aksen i netop et punkt.



Figur 5, Vedantu, https://www.vedantu.com/question-answer/lines-can-pass-through-one-given-point-class-8-maths-cbse-5ee496126e2ad60d527131f7



Figur 4, egen graf

Bob forestiller sig nu, at skæringen med y-aksen skal ved den y-værdi, der er lig det tal han ønsker at kryptere. Da han ønsker at kryptere tallet 1, kommer han frem til nedenstående ligning, og to punkter, der ligger på grafen for *f*.

$$f(x) = 1 + \frac{1}{3}x, \qquad f(1) = 1 + \frac{1}{3}, \qquad f(3) = 2$$

Ligning 1

[4] Skulle Alice på et tidspunkt miste sin private nøgle, gør det matematiske forhold mellem hendes public- og private key, at det ikke vil være muligt for hende at få adgang til sine midler igen.

Bob kommunikerer nu punktet $f(3)$ til Alice, der jf. figur 4 uden yderligere information, har ingen mulighed for at finde frem til $f(x)$. Denne egenskab benævnes perfect secrecy, og er en nødvendighed for et hvert felt, der skal bruges til kryptografi. Bob fortæller dog også Alice sit punkt, $f(1)$, da han netop ønsker, at Alice kan finde frem til det tal, han krypterede. I princippet burde Alice nu ved hjælp af to-punktsformlen kunne beregne sig frem til skæringen med y-aksen, men det er her problemet opstår! Hvis man, som vist i bilag 3, forsøger at programmere en computer til at udføre regneoperationen, vil man ikke kunne komme tilbage til Bobs oprindelige tal, idet computeren efter et bestemt antal decimaler bliver upræcis, hvis den skal regne med rationelle tal. Mens den nemmeste, og mest intuitive løsning ville være at udarbejde en ny ligning, hvor både værdi- og definitionsmængden består af heltal, som vist nedenfor, er der en stor udfordring forbundet med dette.

$$g(x) = 1 + x, \qquad f(3) = 4\,, \qquad f(1) = 2$$

Ligning 2

Nærmere bestemt, er *perfect secrecy* egenskaben nu gået tabt, fordi Alice med hendes viden udelukkende om $f(3)$ kan udelukkende, at det hemmelige nummer er 2, da dette skulle betyde, at funktionen skulle være givet ved $g(x) = 2 + \frac{3}{2}x$, hvilket ikke kan lade sig gøre, da rationelle tal som bekendt ikke måtte benyttes. Bob står altså overfor en problemstilling, hvor han ved, at han skal begrænse talmængden i systemet til heltal i eksempelvis intervallet $[0, 2^{20000}]$, men hvor *perfect secrecy* skal bevares, således, at alle tal i intervallet er lige sandsynlige som løsning, når man kun kender til sit eget tal. Det viser sig, at den simpleste løsning til Bobs problemstilling er at benytte sig af endelige felter.

4.4 En introduktion til endelige felter

Den grundlæggende tanke bag et endeligt felt, er, at man ønsker at skabe en mængde, der udelukkende består af de elementer og regneoperationer, der er nødvendige for ens formål. I Bobs tilfælde svarer det til feltet over alle heltal tal, $\mathbb{Z}$, der indeholder følgende elementer, da det var disse, Bob skulle bruge til at skabe en simpel algoritme til kryptering af hans besked :

$$f(x) = ax + b, \qquad f(x_1) = y_1, \qquad f(x_2) = y_2$$

$$a = \frac{y_2 - y_1}{x_2 - x_1}$$

$$b = y_1 - a \cdot x_1$$

ligning 3

Af praktiske årsager vælger Bob nu at forenkle det endelige felt til kun at indeholde multiplikation og addition, ved at definere følgende inverse, hvor $-b$ og b^{-1} er notationer til at beskrive et element og ikke en operation.

$$\text{Lad } -b \text{ være den additive invers, hvorom følgende gælder: } a - b = a + -b$$

$$Lad\ b^{-1}\ være\ den\ multiplikative\ invers, hvorom\ følgende\ gælder: \frac{a}{b} = a \cdot b^{-1}$$

definition 1

Ligning 1 bliver da:

$$f(x) = ax + b, \qquad f(x_1) = y_1, \qquad f(x_2) = y_2$$

$$a = (y_2 + -y_1) \cdot (x_2 + -x_1)^{-1}$$

$$b = y_1 + -(b \cdot x_1)$$

ligning 4

Og Bob kan nu ved at tilføje en række aksiomer, kreere et felt. Alle feltets egenskaber er defineret nedenfor.

1. Lad elementerne i feltet være givet ved: $a + b, a \cdot b, -b \vee b^{-1}$
2. Lad feltet være kommunativt: $a + b = b + a \vee a \cdot b = b \cdot a$
3. Lad feltet være associativt: $(a + b) + c = a + b + c \vee (a \cdot b) \cdot c = a \cdot b \cdot c$
4. Lad der eksistere to tal, $0 \wedge 1$, hvorom følgende gælder: $0 \neq 1 \vee a + 0 = a \vee a \cdot 1 = a$
5. Lad feltet være distributivt: $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$

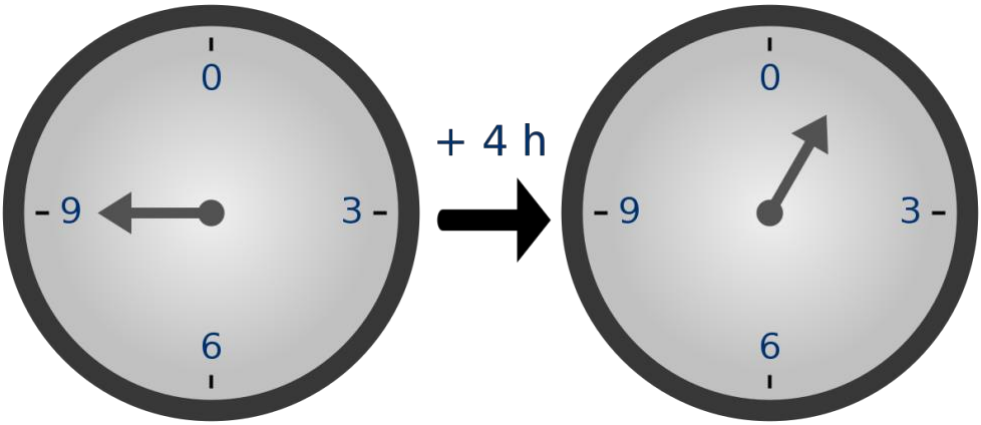
sætning 1

Lader Bob dette felt være defineret for alle heltal, vil han have skabt et matematisk korrekt uendeligt felt, der opfylder kravet om *perfect secrecy*. Beviset for den matematiske korrekthed af *perfect secrecy* er vedhæftet som bilag 4 og 5, da det ikke er i projektets omfang at gengive dem. Det er i forbindelse værd at nævne, at feltet jf. sin definition ikke skal bestå af tal.

Bob vælger dog at blive ved tal, og vil definere sit felt i intervallet $[0\ , 2^{20000}]$. Han skaber dermed et endeligt felt. Men han opdager hurtigt, at dette interval er meget stort, og at beregningerne indenfor feltet vil tage lang tid. Han ved dog samtidig, at tallet skal være tilpas stort, således, at en udefrakommende ikke vil kunne angribe systemet ved *brute-force*. Han står altså overfor en udfordring, hvor han skal vælge en intervalstørrelse, der skal sikre feltet uden at kræve for meget regnekraft. Heldigvis, for Bob, kan denne udfordring løses ved benytte sig af modulo regning, og lade det endelige felt være defineret i et interval modulo p. Hvad det betyder for det endelige felt og hvordan det gøres, vil forklares nærmere i de følgende afsnit.

4.5 En kort introduktion til modulo regning

Modulo regning kan mest intuitivt forklares med udgangspunkt i et analogt ur, som vist nedenfor.



Figur 6, Spindled, https://en.wikipedia.org/wiki/Modular_arithmetic

Betragter man uret til venstre, når klokken er 21:00, og ser på det igen 4 timer senere, vil man ikke sige, at klokken er 25:00, men 1:00 om morgenen. Denne sammenhæng udtrykkes ved modulo regning, og ure i vores del af verden er defineret i et interval modulo 24[5]. Det betyder, at klokken aldrig kan være mere end eller lig 24:00, og man *starter forfra* ved 0, når den øvre grænse af intervallet nås. Mere generelt siger man, at definitionsmængden for et felt, modulo p, er givet ved $[0, p[$. Modulo p kan da defineres således:

Modulo P: Adder eller subtraher P fra n, indtil n tiltager en værdi i intervallet mellem 0(inklusiv) og P (eksklusiv). Ofte skrevet $n \; mod \; P$, eller $n \; \% \; P$

definition 2

Indenfor modulo regning gælder en række regneregler, og det ligger ikke i projektets omfang, at gennemgå dem alle. Projektet vil dermed, udover at have givet ovenstående introduktion til modulo regning, begrænse sig til multiplikative inverse, modulo regnings muligheder for at gøre beregninger med store tal utrolig regneeffektive og bevis af kongruens for multiplikation og addition. Beviserne tager udgangspunkt videomateriale udgivet af en matematiker, der går under alias ”The Math Sorcerer” (Sorcerer 2019).

Vis at $a \equiv b \bmod n \; \wedge c \equiv d \bmod n$, medfører sandheden af; $ac \equiv bd \bmod n$

Bevis: Antag, at $a \equiv b \bmod n \; \wedge \; c \equiv d \bmod n$, så gælder:

$a \equiv b \bmod n \implies \exists \, k \in \mathbb{Z}$, der opfylder $a - b = k \cdot n$

[5] Tager man udgangspunkt i det amerikanske klokkesystem, vil intervallet være modulo 12, idet klokken i USA eks. ikke kan være 13, men 1PM

$c \equiv d \bmod n \implies \exists\, r \in \mathbb{Z}$, der opfylder $c - d = r \cdot n$

Deraf følger:

$ac - bd = ac - cb + cb - bd$

$= c(a - b) + b(c - d)$

$= c(k \cdot n) + b(r \cdot n)$

$= (ck + br) \cdot n, \qquad$ hvor $ck \wedge br \in \mathbb{Z}$

Det er hermed vist, at $a \equiv b \bmod n \wedge c \equiv d$, medfører $ac \equiv bd \bmod n$, da $ac - bd = (ck + br) \cdot n \in \mathbb{Z}$. Højresiden af lighedstegnet er dermed lig en konstant, $i \in \mathbb{Z} \cdot n$ som var netop det, der skulle bevises. ■

bevis 1

Tilsvarende er kongruens for addition bevist nedenfor.

Vis at $a \equiv b \bmod n \wedge c \equiv d \bmod n$, medfører sandheden af; $(a + c) \equiv (b + d) \bmod n$

Bevis: Antag, at $a \equiv b \bmod n \wedge c \equiv d \bmod n$, så gælder:

$a \equiv b \bmod n \implies \exists\, k \in \mathbb{Z}$, der opfylder $a - b = k \cdot n$

$c \equiv d \bmod n \implies \exists\, r \in \mathbb{Z}$, der opfylder $c - d = r \cdot n$

Deraf følger:

$(a + c) - b - d = k \cdot n + r \cdot n$

$(a + c) - (b + d) = k \cdot n + r \cdot n$

$(a + c) - (b + d) = (k + r) \cdot n, \qquad$ hvor $(k + r) \cdot n \in \mathbb{Z}$

Det er hermed vist, at $a \equiv b \bmod n \wedge c \equiv d$, medfører $(a + c) \equiv (b + d) \bmod n$, da $(a + c) - (b + d) = (k + r) \cdot n \in \mathbb{Z}$. Højresiden af lighedstegnet er dermed, ligesom i beviset ovenfor en konsant, $i \in \mathbb{Z} \cdot n$, som netop var det, der skulle bevises. ■

bevis 2

4.6 Sammenhængen mellem modulo regning, endelige felter og kryptografi

Det kan bevises, at tal indenfor modulo regning har en egenskab, der på engelsk benævnes exponentiation og er defineret herunder.

Hvis $a \equiv b \pmod P$, så gælder $a^k \equiv b^k \pmod P$ for alle hele $k > 0$

sætning 2

Det betyder, at to tal, a og b, med samme rest (eksempelvis 15 og $-9 \bmod 12$), fortsat vil have samme rest, hvis de opløftes i k, hvor k er et helt tal, større end 0. I praksis medfører det, at restværdien af meget store tal, kan beregnes utrolig effektivt. I eksemplet illustreres dette ved tallet $2^{80} \bmod 1000$, der er så stort, at computere almindeligvis ikke vil kunne regne effektivt med det.

$$2^{80} = (2^{10})^8 = 1024^8 = (1024^4)^2 = 1.099.511.627.776^2 = 776^2 =$$
$$(700 + 76) \cdot (700 + 76) = 490.000 + 2 \cdot 700 \cdot 76 + 76 \cdot 76 =$$
$$640000 + 106.400 + 5.776 = 0 + 400 + 776 = 1176 = 176 \text{ [mod 1000]}$$

eksempel 1

Men selvom modulo regning, gør nogle regneoperationer markant nemmere, er det endnu ikke klart, hvorvidt et felt modulo p opfylder aksiomerne i definition 2 og dermed kan skabe et endeligt felt. I den forbindelse, er det forholdsvis simpelt at påvise kommutativitet, associativitet, identitetselementerne og distributivitet, mens invers- addition, og specielt multiplikation[6], er langt mindre intuitivt at vise, og for nogle "felter" modulo p ikke er defineret[7]. For mens additive invers altid kan defineres, findes der kun en multiplikativ invers i feltet p, hvis $p \in \mathbb{Z}_{\mathbb{P}}$. Vi kan dermed opskrive følgende definition for de nødvendige regneoperationer i det endelige felt modulo p, der er defineret for alle værdier i feltet.

Lad et felts orden være givet ved modulo p, hvor $p \in \mathbb{Z}_{\mathbb{P}}$.
Lad addition $a + b$ være givet ved: $a + b \bmod \mathbb{P}$
Lad multiplikation $a \cdot b$ være givet ved: $a \cdot b \bmod \mathbb{P}$
Lad den additive invers $-b$ være givet ved: $\mathbb{P} - b$
Lad den multiplikative invers b^{-1} være givet ved Euklids udviede algoritme.

definition 5

Det er dermed under antagelse af, at de øvrige aksiomer i definition 2 er opfyldt, vist, at der kan skabes et felt modulo p, hvor $p \in \mathbb{Z}_{\mathbb{P}}$. Det betyder, at Bob kan lade sin algoritme virke i feltet, og dermed udnytte egenskaber som bl.a. *exponentiation* sammen med de øvrige fordele et felt medfører. Herunder det faktum, at talmængden er uendelige gange mindre i et endeligt felt, end hvis det var uendeligt. I Bitcoin regi benyttes ikke den samme algoritme, som Bob og Alice bruger, men årsagen til, at Bitcoins krypteringsalgoritme er defineret i det endelige felt *modulo p,* hvor $p \in \mathbb{Z}_{\mathbb{P}}$, er den samme. Modulære felter gør det simpelthen muligt at regne utrolig effektivt under samme sikkerhedsniveau. Præcis hvordan endelige felter *modulo p*, hvor $p \in \mathbb{Z}_{\mathbb{P}}$, anvendes i Bitcoins signaturalgoritme, og hvordan algoritmen er opbygget, vil gennemgås i de næste afsnit.

[6] Et bevis for, at den multiplikative invers altid eksisterer i et felt mod p, hvor $p \in \mathbb{Z}_{\mathbb{P}}$ kræver kendskab til Euklids udvidede algoritme og ligger udenfor projektets omfang.
[7] Og dermed gør, at de ikke kan betegnes som felter idet de ikke opfylder kravet om en multiplikativ invers vist i definition 2.

4.7 Punkt addition og dublering indenfor elliptisk kurvekryptografi

Den følgende redegørelse tager udgangspunkt i Prof. Dr. Fabian Schär forelæsningsserie, " Bitcoin, Blockchain and Cryptoassets" (Schär, 2014), samt en artikel fra backend udvikler Mikhail Karavaev (Karavaev, 2022).

En elliptisk kurve er i virkeligheden ikke meget andet, end en funktion med kryptografisk favorable egenskaber, der er defineret i et endeligt felt modulo p, hvor $p \in \mathbb{Z}_{\mathbb{P}}$. I det følgende, vil den elliptiske kurve dog først beskrives i et kontinuert spektrum, da regneoperationerne kun kan forstås grafisk, når funktionen tegnes kontinuert. Formelt blev elliptisk kurve for første gang defineret af Karl Weierstrass, som vist nedenfor:

$$y^2 = x^3 + ax + b, \qquad \text{hvor } 4a^3 + 27b^2 \neq 0$$

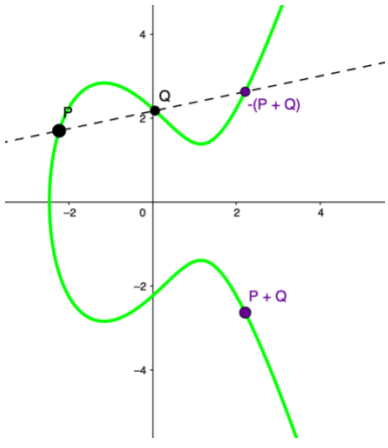
definition 5

Funktionen har den egenskab, at den er symmetrisk omkring x-aksen og ikke har nogle singularitetspunkter[8]. Det betyder, løst sagt, at der ikke må findes nogle punkter på grafen, hvor tangenten er udefineret. Dette er en vigtig egenskab, når man dublerer punkter på grafen.

Både addition og dublering, er to koncepter, der virker forholdsvis u-intuitive, men ikke desto mindre har enorm kryptografisk relevans. Ønsker man at addere to punkter P og Q, der ligger på grafen, gøres det ved at tegne en sekant, der skærer punkterne P og Q. Denne sekant vil herefter skære grafen i et, og netop et punkt. Dette punkt noteres $-(P+Q)$, og er den inverse til $P+Q$. Spejler man nu $-(P+Q)$ over x-aksen, vil man ende i punktet $P+Q$. Grafisk er dette illustreret nedenfor, hvor den elliptiske kurve er på formen: $y^2 = x^3 - 4x + 5$

Algebraisk beregnes $P+Q$, hvor $P\ (-2.2, 1{,}9)$ og $Q(0, 2.1)$ således:

$$s = \frac{y_{p_1} - y_{p_2}}{x_{p_1} - x_{p_2}} = \frac{1.9 - 2.1}{-2.2 - 0} = 0.091$$
$$x_{p_3} = s^2 - \left(x_{p_1} - x_{p_2}\right) = 0.091^2 - (-2.2 - 0)$$
$$x_{p_3} = 2.21$$
$$y_{p_3} = s \cdot \left(x_{p_1} - x_{p_3}\right) - y_{p_1}$$
$$y_{p_3} = 0.091 \cdot (-2.2 - 2.21) - 1.9 = -2.30$$
$$\underline{P + Q(2.21, -2{,}30)}$$



Figur 7, egen graf

eksempel 2

Tilsvarende kan man dublere punkter, ved at finde tangenten til det punkt man ønsker at dublere og indtegne denne. I det andet punkt, som denne tangent skærer grafen i, vil man nu have $-2P$, der betegnes som den inverse til den første dublering af P. Spejles dette punkt over x-aksen, vil

[8] Dette er sikret ved: $4a^3 + 27b^2 \neq 0$

man have punktet $2P$. Herunder ses den algebraiske udregning af $P+P$, hvor $P\left(-0.5, \sqrt{2.875}\right), a=-2$, og $b=2$, samt den grafiske repræsentation af det. Da man her skal udregne tangenten til punktet P, er det tydeligt, at der ikke må findes nogle singularitetspunkter på grafen.

$$s = (y^2 = x^3 - ax + b)' = \frac{3{x_p}^2 + a}{2y_p}$$

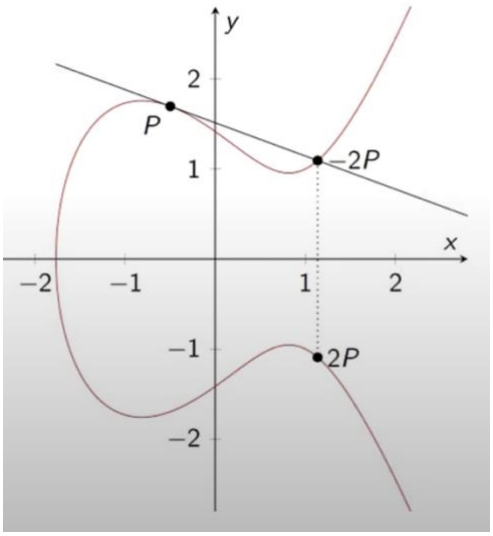
$$s = \frac{3 \cdot (0.5)^2 - 2}{2 \cdot \sqrt{2.875}} = -0.3686$$

$$x_{2P} = s^2 - 2x_P = (-0.3686)^2 - 2 \cdot (-0.5) = 1.14$$

$$y_{2P} = s \cdot (x_P - x_{2P}) - y_P$$

$$y_{2P} = -0.3686 \cdot (-0.5 - 1.14) - \sqrt{2.875} = -1.1$$

eksempel 3



Figur 8, Prof. Dr. Fabian Schär, https://www.youtube.com/watch?v=6FlK3AZTz5k

Med kendskab til disse to regneoperationer, er det værd at gentage, at Bitcoin og andre systemer, ikke benytter elliptisk kurvekryptografi over et kontinuert spektrum. Dette hænger sammen med de sikkerheds- og effektivitetsudfordringer, der er forbundet med et uendeligt felt, som blev nævnt i afsnittene om felter. Bitcoin benytter sig dermed af følgende elliptiske kurve, der benævnes *secp256k1*:

$$y^2 = x^3 + 7 \mod p \text{ i feltet } \mathbb{F}_p, \text{hvor } p = 2^{256} - 2^{23} - 2^9 - 2^6 - 2^4 - 1 \ \wedge \in \ \mathbb{Z}_{\mathbb{P}}$$

definition 5

Af praktiske årsager, giver det dog ikke mening at behandle netop denne elliptiske kurve yderligere, idet feltets orden er så stor, at funktionen ikke kan tegnes i sin fulde mængde[9]. Det er også værd at holde sig for øje, at division som vist i eksempel 3 og 4, ikke er muligt, når man lader den elliptiske kurve være defineret i et endeligt felt, da der her ikke er defineret en regneoperation for division. Man vil i stedet benytte sig af den multiplikative invers. I det kommende afsnit, vil det vises, hvordan regneoperationerne fra elliptisk kurvekryptografi benyttes til at genere offentlige og private nøgler. Dette vil først gøres simpelt i en *lille* cyklisk subgruppe, hvorefter der vil blive benyttet Python Kode til at genere et sæt offentlige og private nøgler, til at signere en simpel besked.

[9] 256^2 alene er et så stort tal (det er mindre end den feltorden Bitcoin bruger), at adskillige videoer er lavet med det formål at illustrere tallets størrelse. Min personlig favorit er fra matematikeren 3Blue1Brown (3Blue1Brown 2018), og er værd at se, hvis du ligesom jeg har svært ved at forholde dig til et tal af den størrelse.

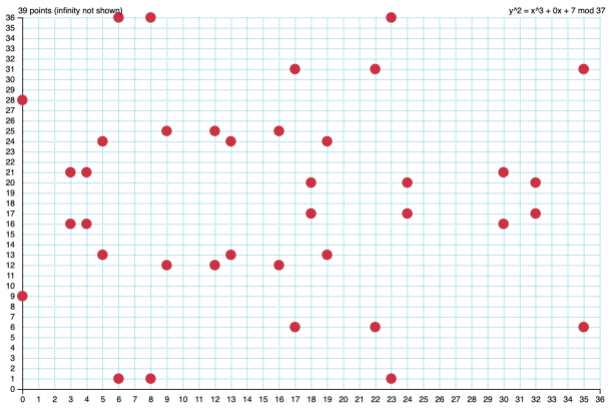
4.8 Sådan genereres offentlige- og private nøgler, samt signaturer ved hjælp af elliptisk kurvekryptografi

For at undersøge, hvordan offentlige- og private nøgler genereres ved hjælp af elliptisk kurvekryptografi, betragtes nedenstående ligning og tilhørende graf for en elliptisk kurve:

$$y^2 = x^3 + 7 \bmod p \text{ i feltet } \mathbb{F}_p, \text{hvor } p = 37 \ \wedge \in \ \mathbb{Z}_{\mathbb{P}}$$

definition 6

For at gøre arbejdet med denne kurve mere forståeligt, skabes en sub-gruppe af orden 13. Det gøres ved at udvælge et *generator* punkt, der ligger på linjen. Dette noteres som G. Herefter defineres den cykliske subgruppe bestående af $[0, G, 2G, \dots, (n-1) \cdot G[$ elementer. Gruppen kaldes cyklisk, idet man ved at addere G til $12G$, ender i 0, og herefter igen kommer til G, ved at ligge G til 0. Indenfor denne endelige subgruppe kan man udføre de samme operationer, som defineret førhen, man skal dog benytte sig af den multiplikative invers, da division ikke er defineret i feltet.



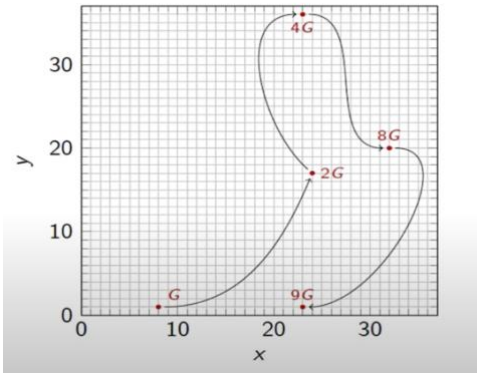
Figur 9, egen graf

Ønsker man nu at signere en vilkårlig transaktion, gøres dette ved en privat nøgle, og et generatorpunkt. Man kan i den forbindelse forestille sig Bob, der ønsker at sende Bitcoin til Alice, og vælger sin private nøgle, k_{prv}, til at være lig 9[10] og generatorpunktet $G(8,1)$. Den private nøgle beskriver her, hvor mange gange, Bob skal addere generatorpunktet til sig selv, for at ende i et bestemt punkt, der er hans offentlige nøgle. Bobs private nøgle er således et tal, mens hans offentlige nøgle er et punkt på grafen, der er matematisk forbundet med den private nøgle. Det er i den forbindelse, grundet modulo regnings *exponentiation* egenskab enkelt at beregne ens offentlige nøgle ud fra den private. Her kan man anvende den såkaldte *double and add* algoritme, der går ud på at dublere ens generatorpunkt indtil man lander ved $k_{prv} - 1$ og herefter lægger en til. Operationen er både illustreret grafisk og algebraisk nedenfor.

[10] Det er i Bitcoin netværket ikke muligt at vælge sin private nøgle eller sit generatorpunkt selv. I praksis vil en algoritme genere disse værdier til ham.

1. Dubler: $2 \circ G = 2G$
2. Dubler: $2 \circ 2G = 4G$
3. Dubler: $2 \circ 4G = 8G$
4. Adder: $8G + G = 9G = (23,1)$

eksempel 4



Figur 10, Prof. Dr. Fabian Schär, https://www.youtube.com/watch?v=6FlK3AZTz5k

I den forbindelse er det værd at notere, at den hidtil bedste måde, at gætte sig til ens private nøgle ud fra ens offentlige er, ved at benytte *brute-force*. Det vil altså sige at man vil skulle evaluere hvert G, for herefter at se, om netop denvariation af G passer med det punkt, den offentlige nøgle giver en. I tilfældet af den cykliske subgruppe med orden 13, vil man forholdsvis nemt kunne regne alle muligheder igennem, men da Bitcoin som benævnt benytter en absurd høj orden, er det på nuværende tidspunkt umuligt at bryde algoritmen. Ifølge datamagasinet Datarecovery (Datarecovery 2022), vil et *brute force* angreb på en privat nøgle i Bitcoin systemet kunne tage flere millioner år med den teknologi, der er til rådighed i dag. Udfordringen som potentielle *brute force* angribere står overfor, kaldes ofte et diskret logaritmisk problem. I Bilag 6 kan der i forbindelse ses to grafer, hvoraf den ene beskriver den tid et *brute force* angreb ville tage, versus den tid det tager at generere ens offentlige nøgle, med kendskab til den private.

Bob mangler nu blot at bestemme sig for, hvor mange penge han ønsker at sende og vælger, derfor at overføre Alice 50 Bitcoin[11]. Nedenfor er en oversigt over alle elementer af krypteringen, som Bob kender til.

- $y^2 = x^3 + 7$
- $G = (8,1)$
- $k_{prv} = 9$
- $k_{pub} = (23,1)$
- $t = 50$

eksempel 5

Det næste bob nu skal gøre, er at signere transaktionen. Dette gør han som vist nedenfor, hvor i^{-1} henviser til et element, I praksis vil det også være nødvendigt at vælge en ny værdi af i hver gang man signerer en transaktion.

1. Vælg et tilfældigt tal, i, f. eks. $i = 7$
2. Udregn
   a. $P = i \cdot G = 7G = (18,20)$
   b. $r = x_P \bmod n = 18 \bmod 13 = 5$
   $s = \{i^{-1}(t + r \cdot k_{prv})\} \bmod n = \{2 \cdot (4 + 5 \cdot 9)\} \bmod 13 = 7$

[11] Mængden af Bitcoins, der sendes er offentlig information og kan enhver tid ses på eks. Blockchain.com.

3. Send
   a. $(r, s) = (5,7)$
   b. $t = 50$
   c. $k_{pub} = (23,1)$

eksempel 6

Når Bob har sendt informationerne under punkt 3 ud i netværket, vil enhver bruger kunne verificere, at transaktionen stammer fra Bobs offentlige nøgle, og dermed er signeret af hans private, uden at kende sidstnævnte. Hvordan denne verificering fungerer matematisk, vil det næste, og dermed sidste afsnit, om matematikken bag Bitcoin, omhandle.

4.9 Verificering af transaktioner ved hjælp af elliptisk kurvekryptografi

Når en bruger i Bitcoin netværker ønsker at validere transaktionen, har vedkommende følgende information til rådighed:

- $y^2 = x^3 + 7$
- $G = (8,1)$
- $k_{pub} = (23,1)$
- $t = 50$
- $(r, s) = (5,7)$

eksempel 7

Det næste en bruger i netværket nu vil skulle gøre, er at gennemføre nedenstående udregninger, hvor s^{-1} henviser til et element.

1. Udregn
   a. $\{u_1 = (s^{-1} \cdot \mathrm{t}\} \bmod n = 2 \cdot 4 \bmod 13 = 8$
   b. $\{u_1 = (s^{-1} \cdot \mathrm{r}\} \bmod n = 2 \cdot 5 \bmod 13 = 10$
   c. $P = u_1 \circ G + u_2 \circ K_{pub}$
      $= 8G + 10 \circ (23,1)$
      $= (32,20) + (8,36)$
      $= (18,20)$
2. Valider signatur: $x_P \bmod n = r$
   $18 \bmod 13 = 5$

eksempel 8

Da *r* værdien i valideringen er den samme, som den Bob sendte ud i systemet, da han signerede transaktionen, kan enhver bruger i systemet være sikker på, at det var ham, der sendte transaktionen.

Når Bitcoin transaktionen signeres, sker det med nøjagtig samme system som beskrevet ovenfor, dog med den forskel, at tallene er markant større. I Karavaevs artikel (Karavaev 2022), er der et Python script, der dog gør det muligt, at generere private, og offentlige nøgler, der har samme længde, og sikkerhed som Bitcoins. Et sæt offentlige og private nøgler, samt de tilhørende *r* og *s* værdier, og teksten *t*, er gengivet nedenfor. En validering af transaktionen overlades til den interesserede læser.

$k_{priv} = 351542111765844629223328709809998173523852882241119129719938042 3$

$k_{pub} = (344807344836230720827784825287873678372135073024661265145612315350866024036 54,$
$105941393891844704893760173495074081152689852835867478910291072870636461280 83)$

$t = 2944$

$r = 834518934753058296096824526776377711367360609630152378054164538586324134705 88$

$s = 878454905452018515686874904062982898715563375425326367523732191390120426318 86$

eksempel 9

4.10 Afsluttende ord om Bitcoins signaturalgoritme

Matematikken bag Bitcoins signaturalgoritme bygger således på tre matematiske fundamenter: endelige felter, modulo regning og elliptisk kurvekryptografi. Mens endelige felter, garanterer *perfect secrecy* og modulo regning, gør regneoperationerne mere effektive, har elliptiske kurver en række egenskaber, der gør krypteringen asymmetrisk og utrolig stærk. Bitcoins signaturalgoritme, secp256k1, har således ikke været udsat for nogle nævneværdige angreb siden dens første implementering i 2009, på trods af, at et angreb vil kunne give hackerne adgang til over 504 milliarder USD per 18. marts 2023. På baggrund af denne sandhed, etableres ofte det narrativ, at Bitcoin er en *sikker* valuta, og selvom det kryptografisk holder stik, er det ikke entydigt, hvorvidt *valutaen* også er makroøkonomisk *sikker*. Det næste afsnit vil da diskutere de makroøkonomiske konsekvenser ved indførslen af Bitcoin som statslig valuta, og i den forbindelse vurdere det herskende narrativ ud fra et makroøkonomisk perspektiv.

5. De makroøkonomiske konsekvenser ved at indføre Bitcoin som statslig valuta

Da El Salvador i september 2021 ved lov vedtog Bitcoin som lovligt betalingsmiddel, var det internationale samfund kritisk overfor beslutningen. IMF anbefalede eksempelvis. blot kort tid efter indførslen, at El Salvador skulle genoverveje beslutningen og fjerne BTC som statslig valuta (Reuters, 2022). I dag, halvandet år senere, er El Salvadors økonomi ikke imploderet, og landet har netop afbetalt 800 millioner USD i udenlandsk gæld (Bukele, 2023), som mange troede, de ikke havde (Avelar & Kurmanaev, 2023). Det er dermed ved første blik, ikke tydeligt, hvorvidt El Salvadors valg om at indføre Bitcoin som statslig valuta, har haft positive eller negative konsekvenser for landet. Den følgende diskussion, vil derfor forsøge at komme de makroøkonomiske konsekvenser af BTC nærmere ved, med udgangspunkt i El Salvador, at diskutere fordele og ulemper ved at anvende BTC på statsligt niveau. Diskussionens konklusioner, perspektiveres herefter til det herskende narrativ om BTC som en *sikker* valuta. I diskussionen vil der anvendes matematisk viden om kryptering, samt makroøkonomisk teori.

5.1 Konsekvenserne af Bitcoin som statslig valuta i El Salvador

Et af præsident Bukeles hovedargumenter for at indføre BTC var, at omkring 70% af den El Salvadoranske befolkning, i 2021 ikke havde adgang til en bankkonto, selvom omkring 99% af befolkning havde adgang til en smartphone (Eglau & Pfister, 2021). Det betød, at mange borgere skulle ty til vekselbureauer som Western Union og betale høje transaktionsgebyrer — en tendens, der går mod FN's første verdensmål om finansiel inklusivitet (FN, 2015). I dag ved vi, at BTC ikke løste problemet borgerne stod overfor, da blot 20%[12] af voksne El Salvadoranere benyttede sig af den statslige Bitcoin wallet 7,5 måned efter lanceringen (Morris, 2022), og omkring 80% af brugerne ikke indsatte penge, men blot brugte de 30 USD bonus, man fik (Alvarez et. al, 2023). Denne lave tilslutning gør også, at det for mange økonomer, herunder IMF, er svært at vurdere, hvilke makroøkonomiske konsekvenser indførslen helt konkret har haft i praksis (O'Boyle, 2023). Der har dog, unægteligt, været en række udfordringer forbundet med valget om BTC som statslig valuta. Først og fremmest, har det gjort landets valuta, langt mere volatil, hvilket som benævnt i første afsnit, har en stor betydning for et lands konkurrenceevne. I praksis har det betydet, at El Salvadors nationalbank eks. købte Bitcoins for 106,4 millioner USD i november, som i slutningen af februar 2023, var 52,2 millioner USD værd (O'Boyle, 2023). Indførslen har desuden betydet, at El Salvador har oplevet vanskeligheder med at handle med Kina, der er en af deres største handelspartnere (Eglau & Pfister, 2021). Dertil kommer, at El Salvador efter beslutningen ikke længere modtager støtte fra IMF (Eglau & Pfister, 2021).

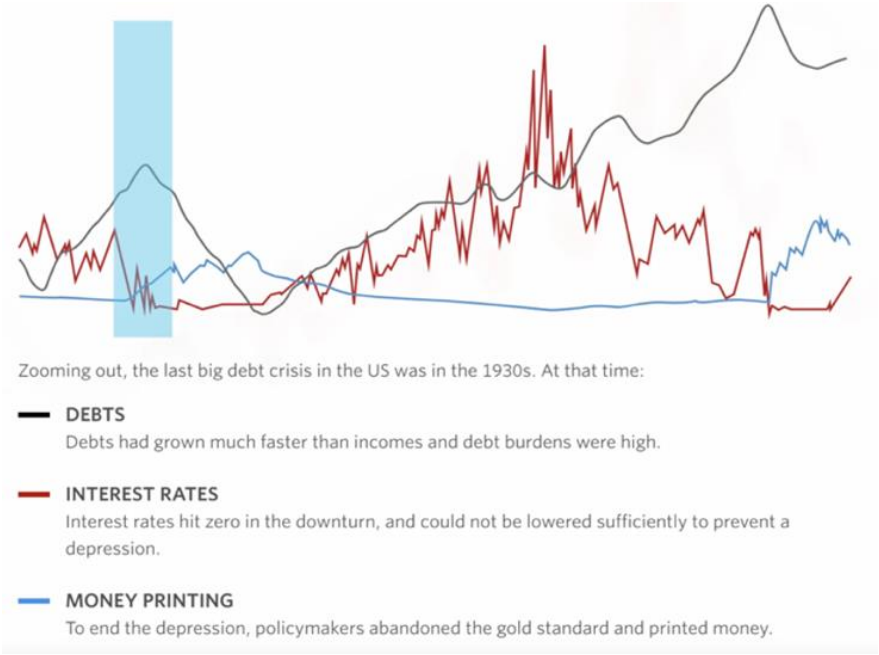
Men i og med landet, parallelt med Bitcoin stadigvæk accepter USD, er det ikke muligt at drage konklusion om, hvad det kan betyde for en nations økonomi udelukkende at benytte sig af en valuta, hvor man hverken har kontrol over pengepolitikken, eller produktionen[13]. Ikke desto mindre, er spørgsmålet efter min opfattelse en af de vigtigste aspekter af diskussionen om BTC og valutaens makroøkonomiske sikkerhed, og vil derfor i det næste afsnit, diskuteres teoretisk ud fra moderne monetær teori (MMT) og østrigsk skole.

5.2 MMT vs. østrigsk skole — hvordan bør stater håndtere penge?

Ifølge forskere fra den heterodokse, neo liberale, østrigske skole, bør penge skabes af markedskræfterne, og ikke staterne. Dette fastslog F.A. Hayek i sit værk, *The Denationalization of Money* i 1976, hvor han beskrev, at stater aldrig vil kunne skabe *gode* penge (Hayek, 2011).

[12] Det er uvist, hvorvidt de 20%, der benytter sig af den statslige Wallet, havde en bankkonto i forvejen.
[13] Man vil i den forbindelse kunne indvende, at El Salvador heller ikke har nogen indflydelse på USD, men Dollaren bliver trods alt styret af verdens største økonomi, der fører aktiv pengepolitik og produktion.

Argumentet er her bl.a., at politikere, og regeringer handler pengepolitisk populistisk, idet de ikke vedtager det, der er bedst for samfundet på lang sigt, men handler sådan, at de bliver genvalgt på kort sigt (Hayek, 2011). Hayek argumenterer dermed for, at penge- og finanspolitiske tiltag per definition er problematiske, og skaber et samfund, hvor den brede befolkning er underlagt et statsligt monopol, der styrer den samlede pengeproduktion (Caporale, 2015). Den østrigske skole anser dermed statsgæld som grundlæggende problematisk, og vil med udgangspunkt i nedenstående graf argumentere for, at vi, grundet forkert økonomisk politik, nærmer os et krak, i størrelse af 1930.



graf 2, Mike Co, https://burningw0rds.medium.com/modern-monetary-theory-versus-bitcoin-76e1e47f96c

Fortaler for den østrigske skole vil da argumentere for, at Bitcoin er netop den valuta, verden har brug for. Nærmere bestemt, er ideen, at der indføres en såkaldt global *Bitcoin standard*[14] (Ammous, 2018), der de facto skaber denationaliseret global økonomi. Staten trækker sig dermed tilbage, og nærmer sig den klassiske liberale *natvægterstat*. Det er imidlertid svært at argumentere faktuelt for et så fjernt og utopisk stadie, og forklaringer for denationaliseringen af penge, bliver da meget ideologisk betonet. Selv samme tendens gør sig gældende blandt Bitcoin fanatikere, der ud fra et liberalt markedssyn argumenterer for, at alle de største finanskriser, har været skabt af staters pengepolitiske inkompetence (Nicolaisen et al., 2022). Den makroøkonomiske konsekvens af at indføre Bitcoin som statslig valuta bliver dermed jf. østrigsk skole, at verden bliver et bedre sted, fordi stater får mindre magt (Ammous, 2018), og markedet kan skabe den bedste valuta for folket (Hayek, 2011).

[14] Det vil sige en ækvivalent til den engang herskende guld standard i USA.

I stærk kontrast til dette syn på staters rolle i penge- og finanspolitik, samt Bitcoin, placerer moderne monetær teori sig. Denne økonomiske teori påpeger nemlig, at staters monopol til at producere penge, er en afgørende faktor for at den globale økonomi kan fungere i sin nuværende form (Lockert, 2022). I forlængelse af dette, argumenterer MMT for, at et statsligt underskud ikke per definition er dårligt for en stats økonomiske situation, da veludviklede stater kan forøge mængden af penge i cirkulation uden et økonomisk kollaps (Lockert, 2022). Dermed lægger MMT sig tæt op af Keynes syn på økonomisk politik, der netop påpegede, at stater bør benytte sig af finans- og pengepolitiske tiltag, alt efter den økonomiske konjunktur. MMT argumenterer f.eks. for, at stater bør, og kan, garantere statslige arbejdspladser i perioder med høj arbejdsløshed (Lockert, 2022). Mange økonomer er i dag enige om, at de fleste udviklede stater fører en mere eller mindre MMT orienteret økonomisk politik (Tymoigne, 2021). MMT argumenterer desuden for, at det er nødvendigt for kapitalismen, at den samlede pengemængde forøges konstant på et sundt niveau, idet det driver inflation, og dermed skaber incitament til at bruge penge, og dermed konsumere varer (Tymoigne, 2021). Men denne politik vil ikke, kunne fortsætte, hvis et land benytter sig af en decentral valuta som BTC. Konsekvenserne ved at indføre BTC som statslig valuta, vil da ifølge MMT være fatale, og ende i ekstrem økonomisk usikkerhed med høj arbejdsløshed og store konjunkturudsving, hvor staten ikke kan interferere og rette op på udviklingen. Desuden skaber man med Bitcoin en valuta, der per definitionen apprecierer (der er en begrænset mængde), hvilket betyder, at der ikke er noget incitament til at bruge penge, hvilket resulterer i deflation, der igen resulterer i økonomisk usikkerhed. Desuden vil tilhængere af MMT argumentere for, at den østrigske skoles påstand om fordelene ved denationalisering af valuta, mangler kvantitativt og videnskabeligt grundlag.

5.3 En kort kommentar om matematisk sikkerhed

En anden vinkel, som mange Bitcoin fanatikere lægger vægt på, er den matematiske sikkerhed, der er forbundet med systemet. Men, selvom det er rigtigt, og vist tidligere i projektet, at Bitcoin er et sikkert betalingsmiddel, er det ikke ens betydning med, at det er bedre sikret, end banker eller nationale institutioner. I praksis benyttes der nemlig også her en sikkerhedsalgoritme, der tager udgangspunkt 2^{256} bit sikkerhed, som eks. DES, IDEA og RC4. For at bryde disse algoritmer, vil man, ligesom i Bitcoins tilfælde, skulle benytte sig af kvantecomputere, som endnu ikke eksisterer (Javed, 2023). Argumentet om Bitcoins sikkerhed, handler dermed i virkeligheden om, at man anser Bitcoin som værende mere sikkert, fordi det er er decentralt og ikke kan kontrolleres af nogen stat. Her vil man kunne indvende, at et kollaps af netværket vil

resultere i økonomiske ruiner for alle brugere, mens ens indestående i banker, i vores del af verden, er forsikret op til 100.000€ (Hendriksen, 2020).

5.4 Delkonklusion: De makroøkonomiske konsekvenser ved at indføre Bitcoin som statslig valuta

Det er således ved El Salvador som eksempel vist, at der endnu ikke er stor opbakning blandt lokalbefolkningen til at indføre et så komplekst finansielt produkt som Bitcoin. Det betyder, at det er vanskeligt drage konklusioner om væsentlige makroøkonomiske konsekvenser af eksperimentet i El Salvador, idet landet parallelt med BTC fortsat har accepteret USD. Spørgsmålet om, hvilke konsekvenser en decentral valuta har for en nation, forbliver således delvist teoretisk, hvor østrigsk skole på den side argumenterer for, at en denationalisering af penge, er nødvendig, og MMT på den anden side påpeger, hvordan den kapitalistiske økonomi ikke kan fungere med en apprecierende valuta i en nation, der har ingen kontrol over egen finans- og pengepolitik. Men, uanset hvilken af de normative teorier man hælder til, er der ingen tvivl om, at der på nuværende tidspunkt er en række *usikkerheder* forbundet med at indføre Bitcoin som statslig valuta. Herunder eks. dens høje volativitet og det manglende kvantitative fundament for den østrigske skoles påstand om, at en denational valuta vil forberede staters makroøkonomiske forhold. Dertil kommer, at argumentet om øget matematisk sikkerhed ved BTC, ikke holder stik i sin bogstavelige forstand, idet bankforbindelser og nationale institutioner er krypteret i samme grad. Kernen af både sikkerhedsspørgsmålet, men også dele af de makroøkonomiske overvejelser, forbliver da ideologiske, da de i bunder i en mistro til stater og deres monopolistiske evne til at justere pengecirkulationen.

6. Konklusion

Projektet har således forsøgt at give læseren en bedre forståelse af Bitcoin ved at forklare matematikken bag signaturalgoritmen, samt belyse de makroøkonomiske konsekvenser det vil have for et land at indføre Bitcoin som statslig valuta. Det kan i den forbindelse fastholdes, at valutakurser og valutamarkedet har en række konsekvenser for det samfundsøkonomiske kredsløb, og at indførslen af en valuta med en så høj volativitet som Bitcoin, alt andet lige, vil øge den økonomiske usikkerhed, ved påvirke et lands konkurrenceevne, BNP og betalingsbalance i negativ grad. Matematisk kan det derimod konkluderes, at Bitcoins signaturalgoritme, er af ekstrem høj sikkerhed og fungerer ved at lade en elliptisk kurve være defineret over et endeligt felt modulo p og her udføre en række asymmetriske regneoperationer. Med udgangspunkt i El Salvadors indførsel af Bitcoin som statslig valuta, kan det desuden fastholdes, at opbakningen til en kompleks, decentral valuta endnu ikke er synderlig høj. Det betyder, at Bitcoins makroøkonomiske konsekvenser i El Salvador var forholdsvis begrænsede, ikke mindst fordi landet fortsat accepterer USD som statslig valuta. Spørgsmålet om, hvilke makroøkonomiske konsekvenser en decentral valuta vil have for en nation, forbliver dermed, til en vis grad, teoretisk, hvor den østrigske skole med Hayek i spidsen advokerer for en denationalisering af valuta, og moderne monetarister argumenterer for vigtigheden af en stærk stat, der har monopol på pengeproduktionen, samt finans- og pengepolitik. Men, uanset teoretisk synsvinkel, kan det fastholdes, at indførslen af Bitcoin som statslig valuta, unægteligt, vil være forbundet med en række usikkerheder, grundet dens høje volativitet. Dertil kommer, at den østrigske skoles argument for denationalisering af valuta, i høj grad bygger på neoliberale præmisser, og ikke substantiel økonomisk forskning. Der er således opstået en diskrepans mellem Bitcoins narrativ, der i høj grad påpeger valutaens sikkerhed, og virkeligheden, hvor BTC er kryptografisk sikret, men vil medføre en række makroøkonomiske usikkerheder som lovligt betalingsmiddel.

7. Litteraturliste

3Blue1Brown, B.B (2018) How secure is 256-bit security? [Video]. Youtube. https://www.youtube.com/watch?v=S9JGmA5_unY

Alvarez, F., Argente, D. & Patten, D. (2022, april). Are Cryptocurrencies Currencies? Bitcoin as Legal Tender in El Salvador. Becker Friedman Institute. https://bfi.uchicago.edu/wp-content/uploads/2022/04/BFI_WP_2022-54.pdf

Ammous, S. (2018). The Bitcoin Standard: The Decentralized Alternative to Central Banking. Cato Journal. https://www.cato.org/sites/cato.org/files/serials/files/cato-journal/2018/9/cj-v38n3-14.pdf

Avelar, B. & Kurmanaev, A. (2022, 5. juli). A Poor Country Made Bitcoin a National Currency. The Bet Isn't Paying Off.. The New York Times. https://www.nytimes.com/2022/07/05/world/americas/el-salvador-bitcoin-national-currency.html?

Blackpenredpen, B.B (2019) What does a ≡ b (mod n) mean? Basic Modular Arithmetic, Congruence [Video]. Youtube. https://www.youtube.com/watch?v=6dZLq77gSGU

Bukele, N.. (2023, 24. januar). Well, we just paid in full, 800 million dollars plus interest.. Twitter. https://twitter.com/nayibbukele/status/1617700039534731264

Can Brute Force Attacks Crack Bitcoin Private Keys?. (2022). https://datarecovery.com/rd/can-brute-force-attacks-crack-bitcoin-private-keys/. Lokaliseret på Datarecovery.com

Caporale, M. . (2015). Dissolving 'the unholy marriage': Hayek's recommendation on monetary and fiscal policy. Econstor. https://www.econstor.eu/bitstream/10419/147472/1/868008559.pdf

Cryptoclear, C. 2021) Finite Fields in Cryptography: Why and How [Video]. Youtube. https://www.youtube.com/watch?v=ColSUxhpn6A

Eglau, V. . & Pfister, S. . (2021, 6. december). El Salvadors gewagte Pläne mit dem Kryptogeld. Deutschlandfunk. https://www.deutschlandfunk.de/bitcoin-als-staatswaehrung-in-el-salvador-100.html

Falktoft, P.. (Vært), Bjerre, E. . (Vært) & Nicolaisen, N. (Vært). (s.d.). Her Går Det Godt, kryptospecial [Audiopodcast]. Podimo. podimo.dk

FN, F. (2015). IGNITING SDG PROGRESS THROUGH DIGITAL FINANCIAL INCLUSION. https://sustainabledevelopment.un.org/content/documents/2655SDG_Compendium_Digital_Financial_Inclusion_September_2018.pdf

Hayek, F. A. (2011). Denationalization of Money: The Argument Refined. Ludwig von Mises Institute

Hendriksen, R. (2020). Sådan er du sikret, hvis din bank går konkurs. I: Forbrugerrådet Tænk. https://taenk.dk/privatoekonomi/banker-og-kreditforeninger/bank-gaar-konkurs

Javed, K. (2023). Is Online Banking Safe? How Do Banks Protect Your Information?. Make Use Of. https://www.makeuseof.com/is-online-banking-safe-how-banks-protect-information/

Karavaev, M.. (2022). Elliptic curves and ECDSA: everything to know to sign a transaction in Bitcoin from scratch. Level Up Coding.

Lockert, M. (2022, 22. juli). What is Modern Monetary Theory? Understanding the alternative economic theory that's becoming more mainstream. Business Insider. https://www.businessinsider.com/personal-finance/modern-monetary-theory?r=US&IR=T

Morris, C.. (2022, 27. april). El Salvador's Bitcoin strategy continues to lose steam after 7.5 months. Fortune. https://fortune.com/2022/04/27/el-salvador-bitcoin-strategy-chivo-losses/

O'Boyle, B.. (2023, 11. februar). IMF says El Salvador's bitcoin risks have not materialized but 'should be addressed'. Reuters. https://www.reuters.com/business/finance/imf-says-el-salvadors-bitcoin-risks-have-not-materialized-should-be-addressed-2023-02-11/

Oliver, J. O. (2018). Cryptocurrencies: Last Week Tonight with John Oliver (HBO) [Video]. Youtube. https://www.youtube.com/watch?v=g6iDZspbRMg

Over 16,000 Assets ranked by Market Cap. (s.d.). I: 8 Marketcap. Lokaliseret den 18. marts 2023 på https://8marketcap.com/

Paar, C. P. (2014) Lecture 7: Introduction to Galois Fields for the AES by Christof Paar [Video]. Youtube. https://www.youtube.com/watch?v=x1v2tX4_dkQ

Prof. Dr. Schar , F. S. & Prof. Dr. Aleksander Berentsen , A. B. (2020). Bitcoin, Blockchain and Cryptoassets. The MIT Press.

Prof. Dr. Schär, F. S. (2021, 14. april). Bitcoin, Blockchain and Cryptoassets [Video]. Youtube. https://www.youtube.com/watch?v=6FlK3AZTz5k

Reuters, R. (2022, 26. januar). IMF urges El Salvador to remove Bitcoin as legal tender. BBC. https://www.bbc.com/news/world-latin-america-60135552

Reuters, R. (2023, 12. januar). FTX recovers $5bn but scale of losses to customers still unknown. The Guardian.

Reuters, R. (2023, 15. marts). Argentina's inflation rate soars past 100%, its worst in over 30 years. *The Guardian*. https://www.theguardian.com/world/2023/mar/15/argentina-inflation-rate-100-perce

Scott, Gordon. (2022). Black Swan in the Stock Market: What Is It, With Examples and History. Investopedia. https://www.investopedia.com/terms/b/blackswan.asp

Riley, S. R. (2014, 22. april). Public Key Cryptography - Computerphile [Video]. Youtube. https://youtu.be/GSIDS_lvRv4

Taleb, N. (2021). Bitcoin, Currencies, and Fragility. Tandon School of Engineering, New York University. https://www.fooledbyrandomness.com/BTC-QF.pd

The Math Sorcerer, M.S (2019) Congruence Modulo n Addition Proof [Video]. Youtube. https://www.youtube.com/watch?v=j20XBwHwt3Y

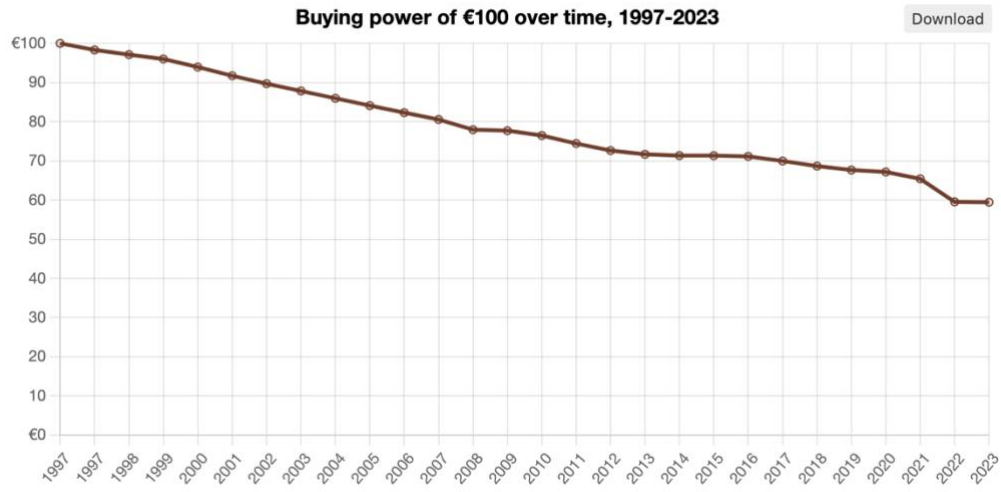
The Math Sorcerer, M.S (2019) Congruence Modulo n Multiplication Proof - Clever Proof [Video]. Youtube. https://www.youtube.com/watch?v=1AJ5sGyfkqU

The Math Sorcerer, M.S (2019) Congruence Modulo n Multiplication Proof - Clever Proof [Video]. Youtube. https://www.youtube.com/watch?v=1AJ5sGyfkqU

Trier, P. T. (2018). Økonomi. Gyldendal.

Tymoigne, E. (2021, december). Seven Replies to the Critiques of Modern Money Theory . Levy Economics Institute . https://www.levyinstitute.org/pubs/wp_996.pdf

8. Bilag

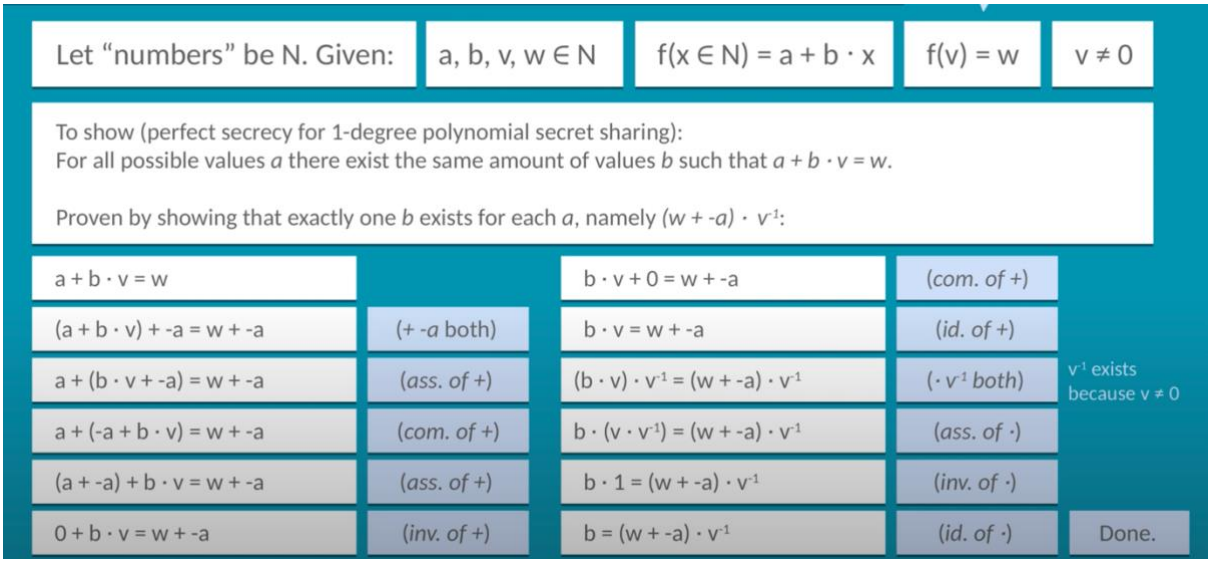


Bilag 1, https://www.in2013dollars.com/Euro-inflation, data fra ECB

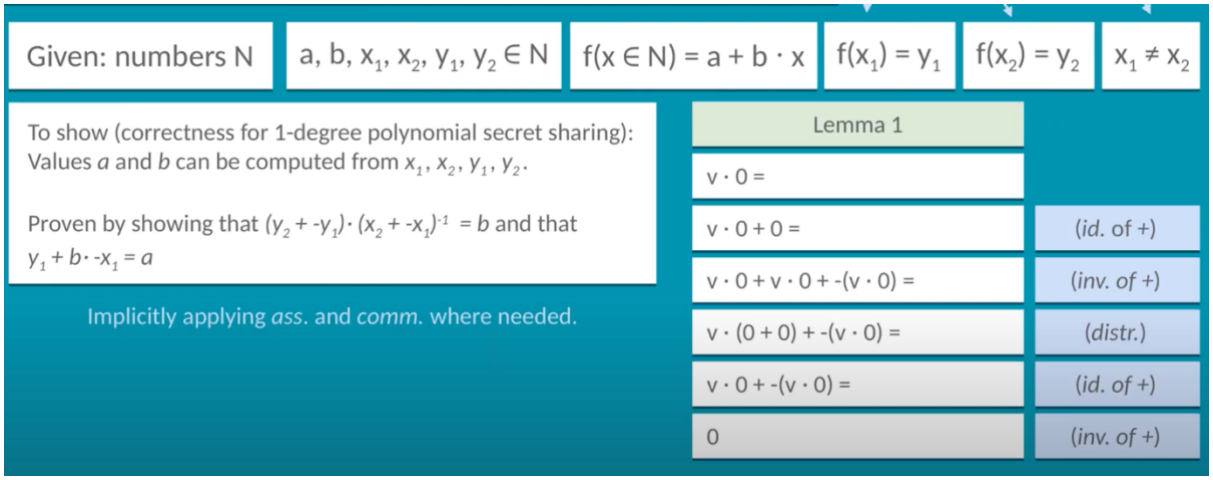
Bilag 2, https://coinmarketcap.com/currencies/bitcoin/

```
Python 3.7.4
>>> def f(x):
...     return 1 + 1/3 * x
...
>>> alice = f(3)
>>> bob = f(1)
>>> alice
2.0
>>> bob
1.3333333333333333
>>> '{0:.60f}'.format(bob)
'1.333333333333333259318465024989563971757888793945312500000000'
```

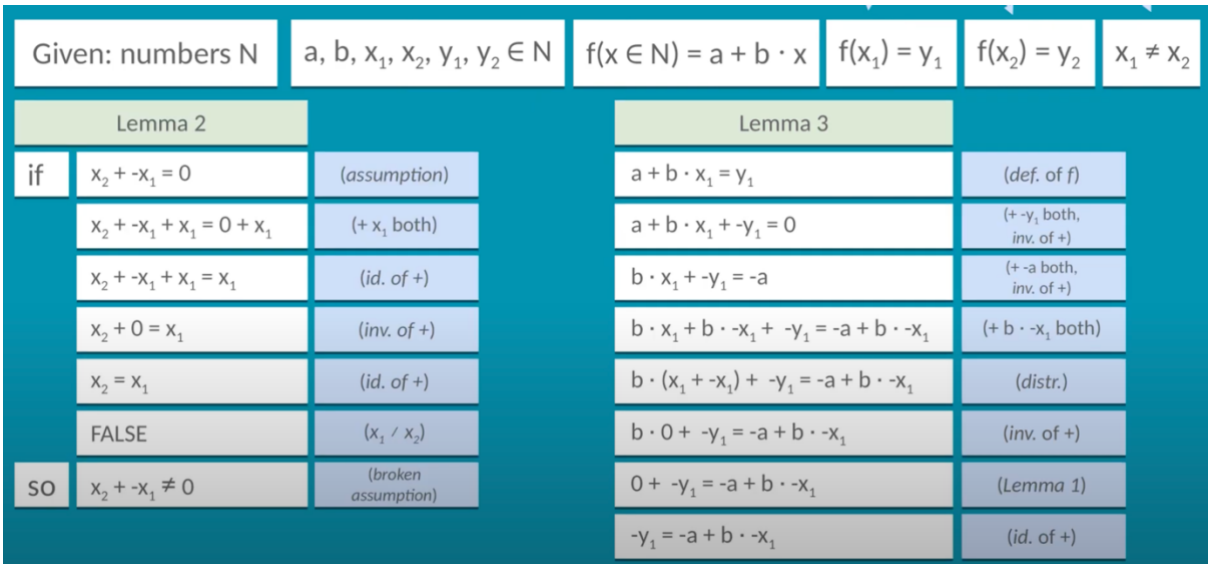
Bilag 3, Cryptoclear, https://www.youtube.com/watch?v=ColSUxhpn6A



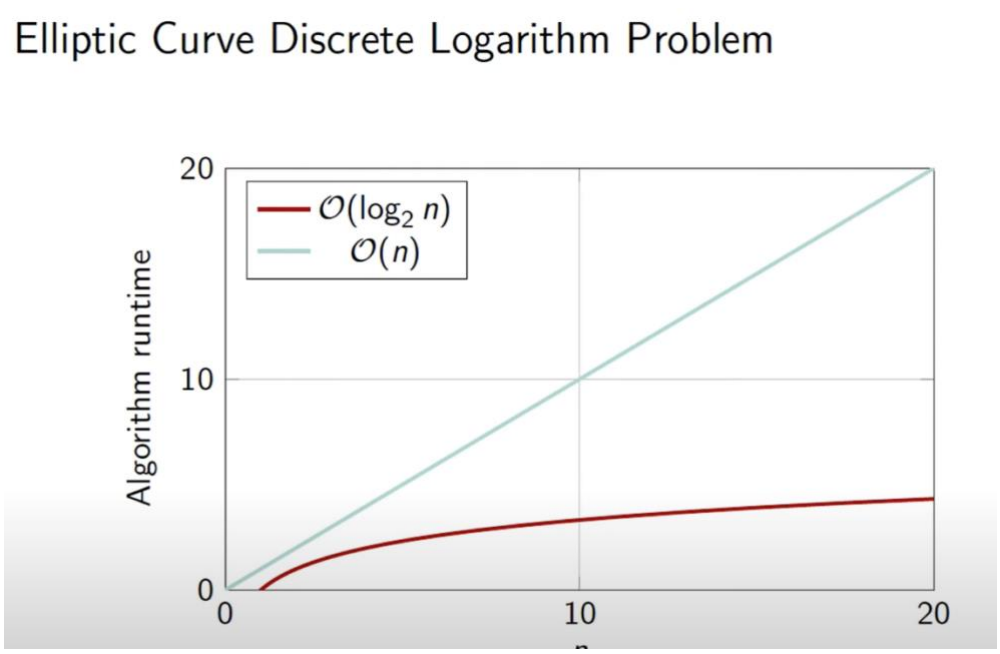
Bilag 4, Cryptoclear, https://www.youtube.com/watch?v=ColSUxhpn6A



Bilag 4, Cryptoclear, https://www.youtube.com/watch?v=ColSUxhpn6A



Bilag 5 fortsat, Cryptoclear, https://www.youtube.com/watch?v=ColSUxhpn6A



Bilag 6, Prof. Dr. Fabian Schär, https://www.youtube.com/watch?v=6FlK3AZTz5k