BLOCKCHAIN I FINANSSEKTOREN

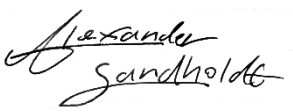
STUDIEOMRÅDEPROJEKT

Hvordan kan den finansielle sektor optimere deres værdikæde og forretnings-model vha. blockchain-teknologi, og på hvilke måder har blockchain-teknologi mulighed for at disrupte det finansielle marked?

ELEV & KLASSE
Haydara Alexander Issa Sandholdt
Hold 3.D

SKOLE & ÅRSTAL
Det Blå Gymnasium
Haderslev Handelsskole
2023

FAG & VEJLEDERE
Afsætning A - Majbrit L. Skou
Matematik A - Nicolai O. Hybschmann



Antal tegn: 49.503

Haydara Alexander Issa Sandholdt *(haydoo83)* 31. marts 2023
Det Blå Gymnasium, Haderslev Handelsskole, Hold 3.D
Studieområdeprojekt: *Blockchain-teknologi*

NAVN:	**Haydara Alexander Issa. Sandholdt.**
KLASSE:	**hh3d**
Område for studieområdeprojekt:	**Blockchain-teknologi**
Fag 1:	**afA**
Fag 2:	**mkA**
Vejleder fag 1:	**MS**
Vejleder fag 2:	**NOH**

Opgaveformulering:

Redegør for hvilke konkrete anvendelser af blockchain-teknologien der eksisterer inden for finanssektoren.

Foretag en matematisk redegørelse af kryptografi med fokus på blockchain-teknologi.

Analyser forretningsmodellen for en selvvalgt finansiel virksomhed, og diskuter hvilke muligheder og konsekvenser anvendelsen af blockchain-teknologi har for virksomhedens forretningsmodel.

Diskuter om blockchain-teknologi har mulighed for disrupte finansielle virksomheder.

Opgavens forventede omfang: 15-20 normal sider.

Haydara Alexander Issa Sandholdt *(haydoo83)* 31. marts 2023
Det Blå Gymnasium, Haderslev Handelsskole, Hold 3.D
Studieområdeprojekt: *Blockchain-teknologi*

RESUMÉ

Blockchain gør det muligt at håndtere data og transaktioner decentralt, og desuden med visse effektivisering- og omkostningsfordele. Derfor kigges der i denne opgave på, hvordan finanssektoren kan forbedre deres forretningsmodel ved anvendelsen af denne teknologi.

Opgaven indeholder indledningsvist en matematisk redegørelse af den kryptografi der er bag blockchain, som danner grundlaget for teknologiens eksistens, samt en redegørelse af blockchainanvendelser der allerede eksisterer i finanssektoren. Ydermere dykkes der også ned i Danske Banks forretningsmodel, som giver en forståelse for finanssektoren generelt, og det diskuteres, hvordan de 9 byggesten heri kan optimeres/forbedres vha. af blockchain. Desuden diskuteres det også på hvilke måder og i hvilken grad, blockchain-teknologi potentielt kan disrupte finansielle virksomheder.

Afslutningsvist konkluderes det, at blockchain kan anvendes til at decentralisere og automatisere visse processer og aktiviteter i finansielle virksomheder, og desuden at sikkerheden og pålideligheden heri opnås vha. af kryptografiske metoder og den decentrale struktur. Desuden også at teknologien potentielt helt kan disrupte finanssektoren, og i hvert fald vende rollerne blandt aktørerne i branchen.

Haydara Alexander Issa Sandholdt *(haydoo83)*
Det Blå Gymnasium, Haderslev Handelsskole, Hold 3.D
31. marts 2023
Studieområdeprojekt: *Blockchain-teknologi*

INDHOLD

1. INDLEDNING

Blockchain er stadig et nyere begreb, som oftest forbindes med fænomener som f.eks. kryptovaluta (Bitcoin, Ethereum, etc.) Disse bliver hyppigt forbundet med manglende gennemsigtighed, og som uden et reelt og sikkert grundlag. Dog kan den rette anvendelse af blockchain-teknologien være med til at sikre netop det - *gennemsigtighed* og *sikkerhed*.

Blockchain-begrebet dækker over en form fir decentral database, der er distribueret over et netværk af computere. Disse computere holder hver især en kopi af databasen, og i samarbejde med diverse konsensusmekanismer og kryptografiske elementer, sørger disse for, at alle handlinger på blockchain er autoriserede.

Man kan forestille sig en masse datablokke, der er kædet sammen således, at man ikke kan ændre i det foregående blokke og heller ikke den data og information de indeholder.

Blockchains har utallige og stadig ukendte anvendelsesmuligheder indenfor erhvervslivet, og man bør forvente at teknologien kommer til at spille en større rolle. I denne opgave ses der på anvendelsen af blockchain indenfor finanssektoren - vel at mærke i norden og primært Danmark.

Opgaven vil give en indsigt i hvordan blockchain allerede anvendes i finanssektoren, endvidere hvordan finansielle virksomheder kan optimere deres forretningsmodel vha. blockchain - og hvorfor, - og kigger desuden på hvilken rolle blockchain kan forventes at spille fremover i finanssektoren. Desuden vil opgaven forsøge at underbygge forståelsen af blockchain, ved også at berøre de bagvedliggende matematiske mekanismer der vedrører teknologien.

2. METODE

Opgaven er ud- og bearbejdet på baggrund af naturvidenskabelige og samfundsvidenskabelige tilgange og fagmetoder indenfor hhv. Matematik og Afsætning, som i sammenspil danner grundlag for besvarelsen.

2.1 AFSÆTNINGSFAGLIG METODEANVENDELSE

Empirien i opgaven består af både primære og sekundære kilder af både officiel og officiøs karakter. Det er en overvægt af kvalitative kilder i form af bløde artikler, udtalelser, etc., men også kvantitative data som f.eks. beskriver fænomener indenfor opgavens område.

Kilderne er valgt med kildekritiske overvejelser om faglighed og saglighed - og desuden med fokus på neutralitet.

Opgavens struktur følger Blooms taksonomiske niveauer for på bedst mulig vis at underbygge besvarelsen gradvist og korrekt.

Mere konkret metode bliver beskrevet under de relevante punkter.

2.2 MATEMATIKFAGLIG METODEANVENDELSE

I opgavens matematiske del arbejdes der primært *i matematik*[1], da der arbejdes med et abstrakt område - kryptografien bag blockchain, - og det derfor er nødvendigt vha. matematikken at konkretisere dette.

Derfor er der i det matematiske arbejde fokus definitioner, sætninger og beviser - og som led i det selvfølgelig også notation og begreber (og afklaring af disse), - til at præsentere teorien.

Det er selvfølgelig vigtigt også at anskueliggøre den teori der præsenteres. Derfor benyttes der også eksempler som fremmer forståelsen for både konceptet og anvendelsen.

Hovedkilderne (Stinson, 2002) og (Erlandsen, 2005) hvor den første er blevet brugt til undersøgelse af den bredeteori, og den sidste til at indsnævre fokus til det der er

[1] (Jensen, 2020)

mere relevante for emnet (i sammenspil med (Damsgaard, 2021)). Desuden (Riber, 2007) til at forstå kryptering overordnet, men bruges kun begrænset i opgaven.

Til forskel fra Afsætning bevæger matematikken i opgaven sig ikke over Blooms taksonomiske niveauer, men opererer i stedet på det rationale mod det udvidede abstrakte niveau.

I praksis arbejdes der meget deduktivt, i og med der arbejdes *i matematik*. Desuden er den matematiske del udformet til at give et overordnet kendskab til kryptografi, men hvor strukturen beholder hovedfokus på kryptering - og særligt den del der er brug for, for at kunne relatere det til blockchain.

2.3 FAGENES SAMSPIL

På overfladen kan det måske være udfordrende at anskue fagenes sammenhæng. I denne opgave beskrives en hård branche - finanssektoren - med et blødere fag som Afsætning. De værdikæder og forretningsmodeller der præger de finansielle virksomheder, er tit baseret på hårde kompetencer (hvem der kan gøre det bedst og billigst), og for at kunne behandle disse afsætningsfagligt, er det nødvendigt at have den matematiske forståelse for emnet i opgaven (blockchain-teknologi).

Altså er det nødvendigt at anvende matematikken til at forstå hvordan blockchain integrerer sig i finanssektoren afsætningsfagligt, og ligeledes hvordan det potentielt set kan påvirke branchen/markedet - også afsætningsfagligt.

3. BLOCKCHAIN I FINANSSEKTOREN

Som det indledningsvist blev introduceret, beskæftiger denne opgave sig med blockchain i finanssektoren. Derfor dannes der her et overblik over de mest gængse og lukrative anvendelser teknologien har indenfor området. Dog er det nødvendigt, først at uddybe og definere selve blockchain-begrebet nærmere.

3.1 BLOCKCHAIN-BEGREBET

En blockchain er en form for åben og transparent hovedbog. Den er distribueret ud til samtlige af blockchainens nodes (det vil sige medlemmer), der alle har en identisk kopi. Dataene herpå er gemt i datablokke, og disse blokke er kædet sammen - dermed navnet *blok-kæde* - på en særlig måde, således at man ikke kan manipulere med tidligere blokke i kæden, men kun tilføje.

Handlinger der foretages på blockchainen, er synlige for alle medlemmer - det vil sige at forsøg uautoriseret manipulation med kæden er usædvanligt vanskeligt, i det vil blive opdaget af netværket (i spil med konsensusmekanismer[2] som sikrer ensartethed). På trods af at handlinger på blockchainen er åbne og synlige, kan selve indholdet ikke tolkes, da - det takket været underliggende krypteringsmekanismer, - kræver en særlig nøgle for at kunne forstå indholdet. [3]

Dette er ikke en udtømmende uddybelse af blockchain-begrebet, men da opgavens emne vedrører selve anvendelsen af teknologien og ikke selve opbyggelsen af den - med undtagelse af de mest basale matematiske, kryptografiske elementer (og dermed ikke de tekniske, programmatiske aspekter som muliggør teknologien i praksis), - er ovenstående udformet med den fortsatte forståelse af opgaven i øjemed.

3.2 ANVENDELSER

Blockchain er som sagt stadig en ny teknologi med mange oversete anvendelsesmuligheder. Dog findes der allerede en række kendte anvendelser af teknologien. Her kigges der specifikt på nogle af anvendelserne indenfor finanssektoren.

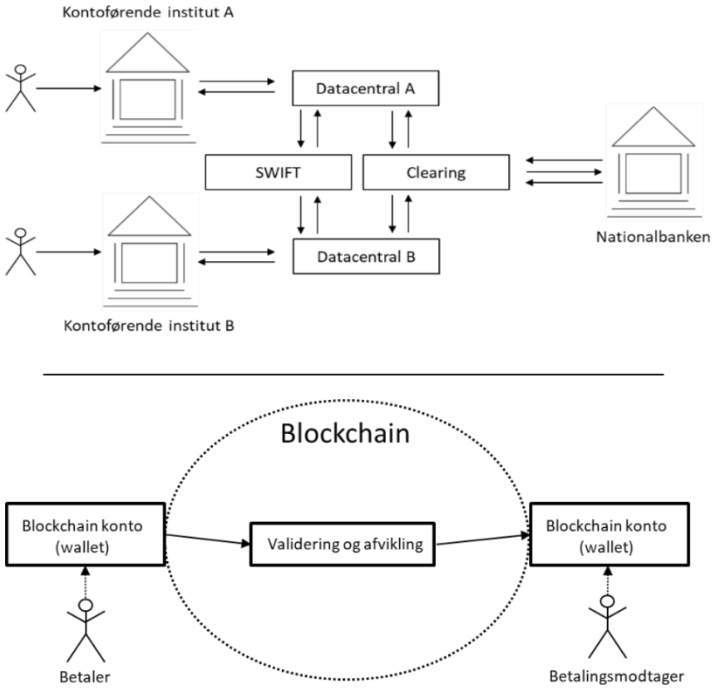
[2] Konsensusmekanismer i blockchain refererer til de regler og protokoller der på netværket sørger for enighed og sikkerhed blandt medlemmerne. Eksempler på disse er PoW (Proof of Work) eller PoS (Proof of Stake).
[3] (Damsgaard, 2021)

3.2.1 Betalingstransaktioner & -infrastruktur

I dag afhænger betalingstransaktioner af en lang række mellemled, herunder både clearing- og afviklingssystemer[4] og generelt en lang række centrale myndigheder. Og disse er nødvendige for at bevare sikkerheden og troværdigheden til systemet. Imidlertid er det dog muligt vha. blockchain af forenkle og effektivisere disse processer.

Den danske fintech[5] virksomhed, ZTLment, har i samarbejde med finanstilsynet gennemført et testforløb. Formålet med forløbet var primært regulatorisk afklaring, men ikke desto mindre har det vist, at blockchain er et reelt og muligvis bedre alternativ til den traditionelle betalingsinfrastruktur. ZTLment kerneaktivitet beskrives som:

> "ZTLment benytter blockchain-teknologi til at tilbyde virksomheder at afvikle business-to-business (B2B) betalinger i realtid ved brug af e-penge udstedt på blockchain."[6]



Figur 3.1: Traditionel betalingsinfrastruktur kontra vha. blockchain. Kilde: (Finanstilsynet, 2022)

[4] Clearing- og afviklingssystemer bruges ifm. finansielle transaktioner til at sikre, at betalinger og overførsler gennemføres korrekt og sikkert. Clearing involverer godkendelse og afstemning af transaktioner, mens afvikling er den faktiske overførsel mellem parterne.
[5] Fintech er forkortelse for "Financial Technology".
[6] (Finanstilsynet, 2022)

På figuren ovenover illustreres hvordan transaktionsprocessen kan simplificeres og effektiviseret vha. betalingsinfrastruktur der udnytter blockchain. Nærmere ses det hvordan de tidligere nævnte centraliserede aktører. kan erstattes af nogle underliggende blockchain-processer. Derved kan transaktioner både gennemføres hurtigere (i realtid), lige så - eller mere, - sikkert, med færre omkostninger og mulige fejlled sammenlignet med traditionelle transaktioner.[7]

På sådan vis har ZTLment mulighed for på en konkurrencedygtig måde at formidle transaktioner mellem virksomheder.

3.2.2 Intelligente kontrakter

Intelligente kontrakter, *Smart Contracts*, er et digitalt, programmeret alternativ til traditionelle juridiske kontrakter - et mere beskrivende ord kunne være *automatiske kontrakter*[8].

Intelligente kontrakter er i al sin simpelhed et lille computerprogram, bestående af række hvis-betingelser, der følger et format lign: "*Hvis betingelse er opfyldt, udfør da konsekvens.*". Intelligente kontrakter adskiller sig her fra juridiske kontrakter, i det følger princippet om *code is law*[9]. Traditionelle kontrakter fortolkes af mennesker og i sidste ende af domstolene - dermed kan fortolkning ofte diskuteres. En intelligent kontrakt fortolkes af en computer, og dermed er formuleringen ikke til fortolkning. Det kan både været en ulempe og en fordel. Traditionelle kontrakter gør for det meste hvad de tiltænkt, da diverse sædvaner og præcedens ofte tillader diverse uspecifikke formuleringer. En intelligent kontrakt gør som den er programmeret til, og intet andet.

Netop fordi intelligente kontrakter er baseret på en række logiske udsagn, og eksekveres på baggrund af data, er det alt afgørende at disse ikke manipuleres med uautoriseret. Denne sikkerhed kan opnås ved at have kontrakten på en blockchain, der vha. dens opbygning og struktur sikrer troværdighed og gennemsigtighed som beskrevet tidligere.[10]

---

[7] (Finanstilsynet, 2022)
[8] (Nordgaard, 2017)
[9] *Code is law* er udtryk for, at en computer udelukkende følger den kode der instruerer den, og ikke tager hensyn til udefrakommende faktorer.
[10] (Damsgaard, 2021) & (Kryptos Redaktionen, 2021)

Anvendelsen af intelligente kontrakter indenfor finanssektoren kan strømline processer ifm. lån, bankgarantier, automatiske betalinger, etc.

3.2.3 Andre anvendelsesområder

Blockchain kan udnyttes på lang række andre områder, bl.a.:

- Identitetsgodkendelse[11]
- E-penge & internationale transaktioner[12]
- Pantsætning[13]

3.3 OPSUMMERING

En fællesnævner for ovenstående er at man kan fjerne/minimere antallet af mellemled og centrale myndigheder. Dette kan lad sig gøre som følge af en central pointe man kan udlede af ovenstående - nemlig hvori sikkerheden og træværdigheden består. Disse omtalte mellemled og centrale myndigheder har hidtil ageret som trygheds- og sikkerhedsinstanser og -institutioner; Nationalbanken og clearing- og afviklingssystemer ved betalingsinfrastruktur, og advokater og domstole ved kontrakter. Ved blockchain er det den distribuerede model sammen med konsensusmekanismerne der i sammenspil med krypteringen (som uddybes i næste afsnit) repræsenterer sikkerheden og troværdigheden.

Dette løser også en kendt problemstilling ved centrale myndigheder - *hvem skal vogte vogteren?* Traditionelle centrale myndigheder består af mennesker, og dermed er der i sidste ende risiko for korruption - dette problem løses ved blockchain.

Implementeringen og anvendelsen af blockchain har altså mulighed for at øge effektivitet, sikkerhed og pålidelighed og desuden minimere omkostninger.

[11] (chirag, 2023)
[12] (Danmarks Nationalbank, 2022)
[13] (Portilla, et al., 2022)

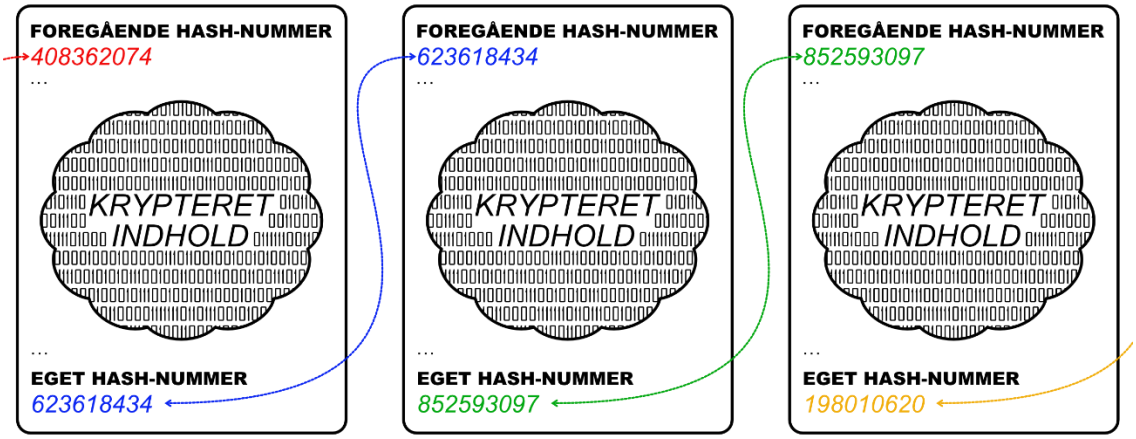
4. BLOCKCHAINS KRYPTOGRAFI

I forrige afsnit blev fordelene ved blockchain nævnt som bl.a. øget effektivitet, sikkerhed og pålidelighed - denne påstand bygges tildeles på sikkerheden ved den distribuerede model, og tildeles på sikkerheden ved de underliggende *kryptografiske* algoritmer og koncepter som teknologien bygger på.

4.1 KRYPTOGRAFIENS ROLLE I BLOCKCHAIN

Kryptografi hører under Kryptologi, altså læren om hemmeligholdelse af information. Kryptografi er hovedemnet indenfor Kryptologi, og omhandler i sin essens om at danne protokoller, der forhindrer en trejdepart indsigt i hemmelige data.[14]

Kryptografi er den matematik og logik der primært vedrører blockchain-teknologi. Denne redegørelse afgrænses til de kryptografiske områder, der er relevante for forståelsen og opbygningen af blockchain-teknologien.[15]



Figur 4.1: Hashing & kryptering i en blockchain. Kilde: (Damsgaard, 2021), bearbejdet

På figuren ovenover indgår "hash-numre". Disse fremkommer ved kryptografiske funktioner, men vil ikke blive behandlet i det følgende - se evt. *bilag 1, s. 42* for en kort introduktion.

Som tidligere nævnt er selve blockchainen og dens indhold synlig for alle nodes. Det betyder dog ikke at de kan forstå indholdet, da det - som illustreret på Figur

[14] (Stinson, 2002)
[15] (Damsgaard, 2021)

4.1, - er krypteret. Det vil sige, at det kræver den rette nøgle, altså den rette autorisation, for at dekryptere og dermed forstå indholdet.[64]

Netop hvordan kryptering fungerer matematiks set, er hvad det kommende vil behandle.

4.2 INTRODUKTION TIL KRYPTOGRAFI

Inden der begyndes, er det vigtigt først at have styr på vores mængdebetegnelser[16]:

- De *naturlige tal* $\mathbb{N}$ (0 er ikke et naturligt tal), altså:
$$\mathbb{N} = \{1,2,3,4,5, \dots\}$$
- De *hele tal* $\mathbb{Z}$ (både negative og positive), altså:
$$\mathbb{Z} = \{-2, -1,0,1,2,3,4, \dots\}$$
- De *rationale tal* $\mathbb{Q}$ (dvs. alle brøker af hele tal), altså:
$$\mathbb{Q} = \{\frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0\}$$

4.2.1 Det grundlæggende krypteringskoncept

Processen at tage en besked og slører den, således at den bliver ulæselig for en trejdepart, kaldes *kryptering.* Processen at tage den slørede besked og gøre den læsbar, kaldes *dekryptering*. Heri findes bl.a. begreberne[17]:

- **Klartekst:** *Den originale besked i uændret form*
- **Kryptotekst:** *Den krypterede - altså den slørede - besked*
- **Nøgle:** *En tekst eller et tal der anvendes til kryptere klarteksten (om denne nøgle også anvendes til at dekryptere kryptoteksten, kommer an på hvorvidt der er tale om et symmetrisk eller et asymmetrisk kryptosystem).*

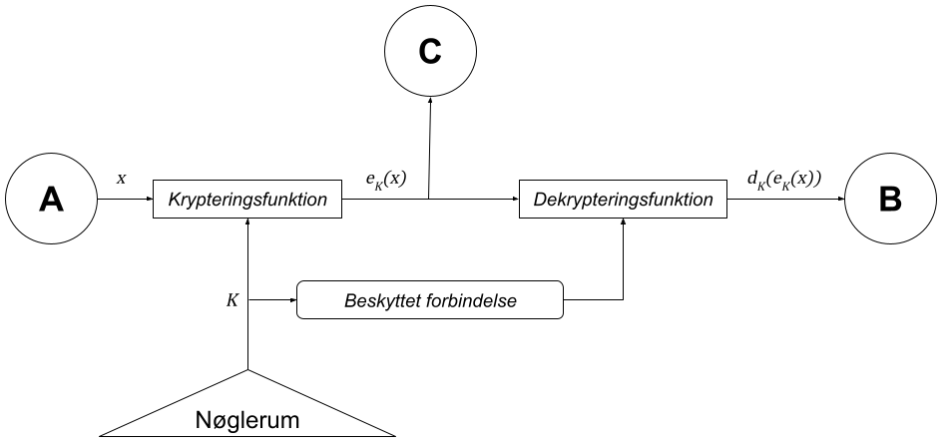
[16] (Erlandsen, 2005)
[17] (Erlandsen, 2005)

Definition 2.1: Et (symmetrisk) kryptosystem består af 5 mængder $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ hvori følgende er opfyldt[18]:

1. $\mathcal{P}$ er et sæt af mulige *klartekster* (P fra det engelske *plaintexts*)
2. $\mathcal{C}$ er et sæt af mulige *kryptotekster* (C fra det engelske *ciphertects*)
3. $\mathcal{K}$, *nøglerummet*, er et sæt af mulige *nøgler* (K fra det engelske *keys*)
4. For hver nøgle $K \in \mathcal{K}$, er der en *krypteringsfunktion* $e_K \in \mathcal{E}$ og en tilsvarende *dekrypteringsfunktion* $d_K \in \mathcal{D}$, for hvori det gælder at hver $e_K : \mathcal{P} \to \mathcal{C}$ og $d_K : \mathcal{C} \to \mathcal{P}$ er funktioner således at $d_K(e_K(x)) = x$ for hvert klartekstelement $x \in \mathcal{P}$

Med afsæt i Definition 2.1 kan vi tage et kig på et simpelt kryptosystem

Eksempel 2.2



Figur 4.2: Kommunikationsforløbet ved symmetrisk kryptering. Kilde: (Stinson, 2002), bearbejdet.

Lad os formulere et tænkt eksempel med udgangspunkt i Figur 4.2. Person A ønsker at sende klarteksten x, *"studieområdeprojekt"*, til Person B, altså:

$$x = "studieområdeprojekt"$$

Under overleveringen ønsker Person A ikke at Person C opsnapper beskeden undervejs. Derfor omdanner Person A *klarteksten* til en *kryptotekst* ved at flytte samtlige bogstaver K gange frem i alfabetet (Efter *å* kommer *a*, og før *a* kommer *å*) - Person A og B har på forhånd aftalt *nøglen* $K = 3$. Lad dette være en funktion af e, altså:

[18] (Stinson, 2002)

$$e(x) = \text{"VWXGLHRPUCGHSURMHNW"}$$

***BEMÆRK** der benyttes små bogstaver til klarteksten og blok bogstaver til kryptoteksten for at fremme læseligheden.*

Person A kender x, mens Person C og B kun kender $e(x)$. Person A ønskede oprindeligt at kommunikere klarteksten til Person B. For at dekryptere beskeden skal Person B flytte samtlige bogstaver K gange tilbage i alfabetet. Lad dette være en funktion af d, altså:

$$d\big(e(x)\big) = \text{"studieområdeprojekt"}$$

[19]

Dette kryptosystem, hvor man rykker samtlige bogstaver K gange frem, hedder *Caesar-substitution* efter den romerske kejser *Julius Caesar.* Dette er desuden et symmetrisk kryptosystem, idet den samme nøgle anvendes til både kryptering og dekryptering.[20]

4.2.2 Bogstaver som tal

Når vi ønsker at kryptere tekstbeskeder, er det nødvendigt at kunne håndtere bogstaver og andre tegn som tal. Dette kan gøres forholdsvist simpelt, f.eks. kan vi tildele alle bogstaver i alfabetet en numerisk værdi fra $0 - 28$:

DEN SIMPLE TEGNTABEL[21]

TEGN	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
NUM.	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14

TEGN	p	q	r	s	t	u	v	w	x	y	z	æ	ø	å
NUM.	15	16	17	18	19	20	21	22	23	24	25	26	27	28

[19] Bearbejdet eksempel fra (Erlandsen, 2005)
[20] (Stinson, 2002)
[21] (Stinson, 2002)

I praksis er det ofte brug for flere tegn. I så fald udvider man blot tabellen. De fleste computere i dag benytter sig bl.a. af tegntabellerne ASCII (som indeholder 256 forskellige tegn) og UTF-8 (som er stort nok til at indeholde stort set alle skriftsprog).[22]

Eksempel 2.3:
Lad os forsøge at omdanne en tekstbesked med en numerisk repræsentation, f.eks. ordet ”æble”:

$$\text{"æble"} \rightarrow (26,1,11,4)$$

Dog er det nødvendigt at håndtere ordet som ét tal i stedet for en samling tal. Derfor vil man hurtigt se, at eksemplet kan give problemer; Tallet 261114 kan både tolkes som *ælbe*, *æbbo*, *ælo* og *æbbbe* udover *æble.* For at imødekomme dette kunne man f.eks. beslutte at alle bogstaver skulle repræsenteres med to cifre, således at:

$$\text{"æble"} \rightarrow (26,01,11,04)$$

Når man så modtager tallet 26011104 vil man så tolke det:

$$\underbrace{26}_{æ}\,\underbrace{01}_{b}\,\underbrace{11}_{l}\,\underbrace{04}_{e}$$

[23]

Metoderne der anvendes i praksis, adskiller sig fra ovenstående. Pointen er blot at man kan behandle/betragte bogstaver som tal.[24]

4.2.3 Blokkryptering

[22] (Erlandsen, 2005)
[23] Bearbejdet eksempel fra (Erlandsen, 2005)
[24] (Erlandsen, 2005)

I det foregående eksempel krypteres et bogstav ad gangen. Dette er i praksis ikke så anvendeligt. Samtidig kan vi ved lange nok tal (bogstaver som tal) også møde begrænsninger. Derfor er det en god ide at kryptere lidt ad gangen; Det kan forstås som blok-kryptering - hertil høre begrebet:

- ***Blokstørrelse:*** *Antallet af elementer (læs: bogstaver) i beskeden* x.

Definition 2.4: For et *blok-kryptosystem* gælder det at samtlige klartekstelementer $x \in \mathcal{P}$ har samme blokstørrelse. Det samme gælder for alle kryptotekstelementer $y \in \mathcal{C}$. Blokstørrelsen af hhv. x og y behøver ikke være ens.

4.2.4 Kodebrydning & Kerckhoffs princip

Som bruger/designer af et kryptosystem, må man aldrig vurdere systemet sikkert udelukkende på baggrund af hemmeligholdelsen af selve krypteringsmetoden. I stedet bør man antage, at *en angriber kender kryptosystemet*[25]:

Kerckhoffs princip: *En angriber kender det anvendte kryptosystem.*

I udarbejdelsen af et kryptosystem, er det ligeledes nødvendigt at kende til de forskellige kodebrydningsmetoder, for at kunne forebygge mod dem.

Her vil man hurtigt opdage at Caesar-substitution beskrevet i Eksempel 1.1 ikke er tilstrækkeligt sikkert, idet der effektivt kun er 29 forskellige nøgler - en angriber vil altså hurtigt kunne finde den rette nøgle ved blot at prøve sig frem.[26]

4.3 TALTEORI

Det blev i forrige afsnit nævnt, at det er nødvendigt for et kryptosystem. at nøglen ikke kan gættes - eller at den i hvert fald er meget svær og ressourcekrævende at gætte.

[25] (Stinson, 2002)
[26] (Erlandsen, 2005)

For senere at kunne opfylde det kriterie, er det nødvendigt at introducere relevant talteori. Beviserne heri holdes på et minimum af hensyn til både opgavens omfang og for at bevare fokus på selve krypteringen.

4.3.1 Primtal

Primtalsteorien udelades her af hensyn til opgavens omfang og fokus. Det er nødvendigt at være bekendt med primtal - herunder især primfaktorisering, for den videre forståelse - se evt. *bilag 2, s. 43.*

Bid mærke i, at menneskeheden hidtil har erfaret, at primfaktorisering for store nok tal er ressource- og tidskrævende - meget tidskrævende. Dette faktum bliver vigtigt senere.[27]

4.3.2 Division med rest

I avanceret kryptering er division med rester, altså *moduloregning*, helt centralt. Det antages, at læser er bekendt med det basale her indenfor - se evt. *bilag 3, s. 46.*

Definition 3.9: For $n, p \in \mathbb{Z}$ hvor der findes et $q \in \mathbb{Z}$ så $pq = n$, således at $r = 0$ (fra Sætning 3.7), skrives $p|n$ betydende "p går op i n".[28]

Definition 3.10: For $n, m \in \mathbb{Z}$ og $p \in \mathbb{N}$ hvor $r_n = r_m$ (fra Sætning 3.7), altså hvor division med p efterlader samme rest for både n og m, så siges det at n er kongruent med m modulo p, og skrives:

$$n \equiv m \ \$ \ p$$

[29]

Eksempel 3.11:

- $11 \equiv 6 \ \$ \ 5$ da $11 = (5)(2) + 1$ og $6 = (5)(1) + 1$ og dermed at $r = 1$ (fra Sætning 3.7) er ens i begge tilfælde. Desuden gælder $11 \equiv 6 \equiv 1$ også.
- $14 \not\equiv 11 \ \$ \ 5$ da resten er hh. 4 og 1

[30]

[27] (Riber, 2007)
[28] (Erlandsen, 2005)
[29] (Erlandsen, 2005)

Af eksemplet kan følgende udledes

Sætning 3.12: For $m \equiv n \$ p$ hvor $m, n \in \mathbb{Z}$ og $p \in \mathbb{N}$ gælder det at $p|m-n$.[31]

BEVIS

Lad $m \equiv n \$ p$ således at disse har samme rest r ved division med p (Definition 3.10). I sammenhæng med Sætning 3.7 må der altså findes to tal $q, z \in \mathbb{Z}$ så at:

$$m = pq + r$$
$$n = pz + r$$

Trækkes disse fra hinanden fås:

$$m - n = pq + r - (pz + r)$$
$$m - n = pq + r - pz - r = pq - pz$$
$$m - n = p(q - z)$$

Hvilket betyder at $m - n$ kan skrives som p gange et tal da $(q - z)$ jo kan beregnes til et tal. Med andre ord går p $(q - z)$ gange op i $m - n$, og altså $p|m - n$. [32]

4.3.3 Restklasser

Kongruens er netop blevet introduceret - dette hører sammen med restklasser.

For et $p \in \mathbb{N}$ kan der for ethvert $n \in \mathbb{R}$ findes en uendelig liste af tal der er kongruente med $m \$ p$ og betegnes $[n]_p$.[33]

Eksempel 3.13:
Vi ønsker at finde mængden af alle tal der er kongruente med $n \$ 5$, altså restklassen $[n]_5$, når $n = \{0,1,2,3,4,5,6\}$:

q	$[\mathbf{0}]_5$	$[\mathbf{1}]_5$	$[\mathbf{2}]_5$	$[\mathbf{3}]_5$	$[\mathbf{4}]_5$	$[\mathbf{5}]_5 = [\mathbf{0}]_5$	$[\mathbf{6}]_5 = [\mathbf{1}]_5$

[30] Bearbejdet eksempel fra (Erlandsen, 2005)
[31] (Erlandsen, 2005)
[32] (Erlandsen, 2005)
[33] (Erlandsen, 2005)

-1	-5	-4	-3	-2	-1	0	1
0	0	1	2	3	4	5	6
1	5	6	7	8	9	10	11
2	10	11	12	13	14	15	17
∞	$5q+0$	$5q+1$	$5q+2$	$5q+3$	$5q+4$	$5q+0$	$5q+1$

[34]

Af tabellen kan følgende definition udledes

Definition 3.14: For $p \in \mathbb{N}$ og $n \in \mathbb{R}$ defineres restklassen for $n \$ p$ som:

$$[n]_p = \{m \in \mathbb{Z} \mid m \equiv n \$ p\}$$

Altså at restklassen for n $\$ p$ består af samtlige tal i $\mathbb{Z}$ der er kongruente med $n \$ p$.[35]

Definition 3.15: Givet $p \in \mathbb{N}$ betegner $\mathbb{Z}_p$ mængden af restklasser for modulo p.[36]

Eksempel 3.16
Øverst i dette afsnit sås en tabel bestående af restklasser - disse indgår i $\mathbb{Z}_5$, altså består denne af følgende elementer:

$$\mathbb{Z}_5 = \{[0]_5, [1]_5, [2]_5, [3]_5, [4]_5\}$$

[37]

4.3.4 Modulær aritmetik

I tidligere afsnit blev restklasser introduceret - disse kan man regne med.

Sætning 3.17: i $\mathbb{Z}_n$ gælder samme regneregler som i $\mathbb{Z}$. Dvs. at $\mathbb{Z}_n$ er lukket overfor addition, subtraktion og multiplikation. [38]

[34] Bearbejdet eksempel fra (Erlandsen, 2005)
[35] (Erlandsen, 2005)
[36] (Erlandsen, 2005)
[37] (Erlandsen, 2005)

Dette er meget kompliceret emne, som blot er beskrevet meget overordnet her af hensyn til opgavens omfang. Vid at Sætning 3.17 gælder, se evt. (Erlandsen, 2005).

4.3.5 Eulers Sætning & ϕ-funktion

Definition 3.18: Lad ϕ være en funktion af $n \in \mathbb{N}$ der definere *antallet af tal* $\leq n$ der er indbyrdes primiske med n.[39]

Definition 3.19: Lad ϕ være en funktion af $n \in \mathbb{N}$ der definerer *antallet af tal* $\leq n$ der er indbyrdes primiske med n

BEMÆRK Hvis $p \in \mathbb{N}$ er et primtal kan $\phi(p)$ beregnes som:

$$\phi(p) = p - 1$$

da primtal jf. Definition 3.1 kun har to divisorer må samtlige tal i $\mathbb{N}$ være indbyrdes primisk med p.

[40]

Sætning 3.20: Hvis $p, q \in \mathbb{N}$ begge er primtal gælder:

$$\phi(pq) = (p - 1)(q - 1)$$

[41]

[38] Sætning fra (Erlandsen, 2005), regneoperationer i $\mathbb{Z}$ fra (Lorenzen, Jørgensen, Carstensen, & Frandsen, 2017)
[39] (Erlandsen, 2005)
[40] (Erlandsen, 2005)
[41] (Erlandsen, 2005)

Sætning 3.21: Endelig siger *Eulers sætning;* Givet at a er indbyrdes primisk med n gælder det at:

$$[a]_n{}^{\phi(n)} = [1]_n \in \mathbb{Z}_n$$
$$\leftrightarrow$$
$$a^{\phi(n)} \equiv 1 \ \$ \ n$$

[42]

4.4 ASYMMETRISK KRYPTERING

Alle foregående afsnit har arbejdet hen mod nu at kunne forstå og præsentere asymmetrisk kryptering. Stort set alt kryptering på internettet - og i blockchain, - fungerer vha. asymmetriske kryptosystemer.

Asymmetriske kryptosystemer har nogle særlige fordele over symmetriske kryptosystemer - især det, at de gør brug af både en offentligt nøgle og en privat nøgle (som introduceres i næste afsnit).[43]

4.4.1 Offentlig nøgle-kryptering

I Figur 4.2 sås det hvordan man krypterede en besked vha. af samme nøgle. Dette viser sig i praktisk - ja, at være upraktisk. Tænk hvis man havde en nøgle man frit kunne offentliggøre, som folk kunne bruge til at kryptere beskeder til en, hvorefter man selv havde en hemmelig nøgle, som vil kunne dekryptere dem? Så vil alle kunne sende krypterede beskeder til hinanden, uden at alle skulle gemme en liste over samtlige forhåndsaftale nøgler, man måtte have med folk.[44]

Idéen bag offentlig nøgle-kryptering er, at der findes et kryptosystem, hvor der er beregningsmæssigt umuligt at bestemme dekrypteringsfunktionen d_{K_d} på baggrund af krypteringsfunktionen e_{K_e}.

[42] (Erlandsen, 2005)
[43] (Riber, 2007)
[44] (Riber, 2007)

Det viser sig, at det netop kan lade sig gøre - og det takket været den talteori vi netop har gennemgået.[45]

Næst præsenteres *RSA-kryptosystemet*[46]. Der findes andre offentlig nøgle-kryptosystemer - bl.a. Elliptisk kurve-kryptering, - som både har sine fordele og ulemper, men RSA-kryptering er nok det mest udbredte og populære (og det der formentligt introduktionsvist giver den bedste forståelse og det bedste overblik).[47]

4.4.2 RSA-kryptering

Med afsæt i Definition 2.1, vil *RSA-kryptosystemet* blive defineret i det følgende.

Kryptosystem 4.1: *Forklaring og definition af RSA-kryptosystemet*

NØGLE-PARRET

Først skal nøgle-parret bestående af den offentlige og hemmelige nøgle dannes. Først vælges to store[48] primtal p og q - disse danner tilsammen:

$$m = pq$$

Her skal man sørge for m består af flere cifre end klartekst-længden. Ofte vælges man p og q så ciffer-længden af m er større én større end klarteksten.

Næst vælges et k indbyrdes primisk med $\phi(m) = (p-1)(q-1)$ (fra Sætning 3.20)

Nu haves:

$$\text{Offentlig nøgle } K_e = (k, m) \mid Hemmelig\ nøgle\ K_d = \phi(m)$$

[45] (Stinson, 2002)
[46] RSA er et akronym for Ron Rivest, Adi Shamir og Leonard Adleman som beskrevet systemet i 1977.
[47] (Stinson, 2002)
[48] Når det her siges *store*, menes der op mod flere hundrede cifre, da det er her, at det bliver beregningsmæssigt umuligt at finde dekrypteringsfunktionen ud fra krypteringsfunktionen - som nævnt i indledningen til dette afsnit. Den vigtige faktor der blev nævnt tilbage i Eksempel 3.4 om primfaktorisering, er netop det her.

KRYPTERING

Både klar- og kryptotekst skal være elementer i $\mathbb{Z}_m$. For en klartekst $[n]_m \in \mathbb{Z}_m$ defineres:

$$e_{K_e}([n]_m) = [n]_m^{K_e} = y$$

DEKRYPTERING

Til en kryptotekst $[n]_m^{K_e}$ skal to hjælpestørrelse u og v beregnes som løser ligningen:

$$ku + \big(-\phi(m)\big)v = 1$$

Hvordan disse størrelser beregnes, uddybes i næste afsnit. Givet u og v haves nemlig:

$$\begin{aligned}([n]_m^k)^u &= [n]_m^{ku} \\ &= [n]^{1+\phi(m)v} \\ &= [n]\big([n]^{\phi(m)}\big)^v \\ &= [n][1]^v \\ &= [n]\end{aligned}$$

Og tilbage er klarteksten $[n]$.

***BEMÆRK** at $[n]\big([n]^{\phi(m)}\big)^v = [n][1]^v$ lader sig gøre pga. af Eulers sætning (Sætning 3.21). Denne antager også at n og m er indbyrdes primisk. Det kan dog vises at dette ikke er nødvendigt for at $[n]^{\phi(m)} = [1]$ så længe m er et produkt af to primtal - hvorfor udelades her, da det ligger ude for rammerne af den talteori der er introduceret her.*

***BEMÆRK** at ifølge regneregler i restklasser jf. Sætning 3.17 må $[1]^v = [1]$ og derfor også $[n][1] = [n]$*

For en kryptotekst $[n]_m^{K_e}$ defineres altså:

$$d_{K_d}(y) = y^u = \left([n]_m^{K_e}\right)^u$$

BEREGNING AF u & v

Her vil den generelle metode til at beregne $u, v \in \mathbb{Z}$ som løser ligningen:

$$1 = au + bv$$

vises (Denne ligning er tilsvarende den i afsnittet om dekryptering).

Vi skal benytte *Euklids algoritme:*

Givet to tal $r_0, r_1 \in \mathbb{Z}$, kan vi lave division med rest (Sætning 3.7) -denne rest kaldes r_2:

$$r_0 = r_1 q_1 + r_2$$

Således kan vi fortsætte:

$$r_1 = r_2 q_2 + r_3$$
$$r_2 = r_3 q_3 + r_4$$
$$r_3 = r_4 q_4 + r_5$$

Indtil:

$$r_{n-2} = r_{n-1} q_{n-1} + r_n$$
$$r_{n-1} = r_n q_n + 0$$

BEMÆRK *r_n betegner den rest man får, inden man får rest* 0 *(som er r_{n+1})*

Næst opstilles to hjælpefølger:

$u_0, u_1, u_2, \dots, u_n$ hvor $u = u_n$

$v_0, v_1, v_2, \dots, v_n$ hvor v $= v_n$

Sæt desuden:

$$u_0 = 1, u_1 = 0$$
$$v_0 = 0, v_1 = 1$$

De næste led i følgerne beregnes:

$$u_k = u_{k-2} - q_{k-1}u_{k-1}$$
$$v_k = v_{k-2} - q_{k-1}v_{k-1}$$

Ovenstående forstås bedst på tabel-form:

$\boldsymbol{k}$	$\boldsymbol{q_k}$	$\boldsymbol{r_k}$	$\boldsymbol{v_k}$	$\boldsymbol{u_k}$
0	−	r_0	1	0
1	q_1	r_1	0	1
2	q_2	r_2	$v_2 = 1 - q_1 \cdot 0 = 1$	$u = 0 - q_1 \cdot 1 = -q_1$
3	q_3	r_3	$v_3 = 0 - q_2 \cdot 1 = -q_2$	$u_3 = 1 - q_2(-q_1)$
…	…	…	…	…
n	q_n	r_n	$v_n = v$	$u_n = u$
$n+1$		0		

BEMÆRK *n kan f.eks. sagtens være 4, og vil derfor ikke passe i ovenstående. Tabellen bruges blot til at demonstrere processen.*

Påstand 4.2: $r_k = r_0u_k + r_1v_k$

BEVIS

Bemærk først at:

$$\begin{aligned} r_0 &= r_0u_0 + r_1v_0 \\ &= r_0(1) + r_1(0) \\ &= r_0 \end{aligned}$$

$$\begin{aligned} r_1 &= r_0u_1 + r_1v_1 \\ &= r_0(0) + r_1(1) \\ &= r_1 \end{aligned}$$

Kan vi vise påstanden gælder for $k-1$ og $k-2$ og dermed også k, må den nødvendigvis også passe for 0, 1 og 2. Dermed også $1, 2$ og 3. (*induktionsbevis*)

Hvis vi siger at påstanden gælder for $k-1$ og $k-2$, altså:

$$\begin{aligned} r_{k-1} &= r_0u_{k-1} + r_1v_{k-2} \\ r_{k-2} &= r_0u_{k-2} + r_1v_{k-2} \end{aligned}$$

Så kan vi indsætte dette i det oprindelig udtryk for r_k efter en rokering:

$$\begin{aligned} r_k &= r_{k+1}1_{k+1} + r_{k+2} \\ -r_{k+2}(-1) &= r_{k+1}(-1) - r_k(-1) \\ r_{k+2} &= r_k - r_{K+1} \end{aligned}$$

Ved indsættelse:

$$\begin{aligned} r_k &= r_{k-2} - q_{k-1}r_{k-1} \\ &= (r_0u_{k-2} + r_1v_{k-2}) - q_{k-1}(r_0u_{k-1} + r_1v_{k-1}) \\ &= r_0u_{k-2} + r_1v_{k-2} - q_{k-1}r_0u_{k-1} - q_{k-1}r_1v_{k-1} \\ &= r_0(u_{k-2} - q_{k-1}u_{k-1}) + r_1(v_{k-2} - q_{k-1}v_{k-1}) \\ &= r_0u_k + r_1v_k \end{aligned}$$

Og hermed er Påstand 4.2 bevist.

Nu mangles kun følgende påstand for at kunne beregne hjælpestørrelserne

Påstand 4.3: Såfremt r_0 og $r_1$er indbyrdes primiske er $r_n = 1$.
(Bevis udelades da det rækker udenfor teorien redegjort for heri)

Med disse påstande på plads kan vi sige

Sætning 4.4: Hvis r_0 og r_1 er indbyrdes primiske, samt at rest ved gentagen division indtil $r_{n+1} = 0$, må:

$$r_n = 1 = r_0 u_n + r_1 v_n$$

[49]

4.4.3 Et eksempel

Med Sætning 4.4 på plads, er det på tide at komme med et eksempel.

Person B vil gerne gøre det muligt for andre at sende ham beskeder krypteret. Han vælger RSA-kryptosystemet, således at det blot er nødvendigt at offentliggøre en offentlig-nøgle. Et nøgle-par skal dannes:

Person B vælger en blokstørrelse på 2 og bruger desuden *den simple tegntabel* (begge disse informationer offentliggøres også). Derfor vil et klartekstelement bestå af 4 cifre.

Person B skal nu vælge to tal primtal p, q, hvis produkt overstiger længen af klartekstelementer - der vælges:

$$p = 137$$
$$q = 367$$

Således at deres produkt:

$$m = 137 \cdot 367 = 50279$$

Desuden:

[49] Uddybet bevis fra (Erlandsen, 2005)

$$\phi(50279) = (137 - 1)(367 - 1) = 49776$$

Nu findes et k som er indbyrdes primisk med 49776:

$$k = 7$$

Nu haves nøgle-parret:

$$\text{Offentlig nøgle } K_e = (k = 7, m = 50279) \mid Hemmelig\ nøgle\ K_d = \phi(m) = 49776$$

Den offentlige nøgle offentliggøres frit tilgængeligt, og en Person B ønsker at sende en besked til Person A, nemlig:

blockchain

Desuden blev blokstørrelsen på 2 og at *den simple tegntabel benyttes også offentliggjort, beskeden bliver derfor:*

$$\underbrace{0111}_{\text{bl}}\ \underbrace{1402}_{\text{oc}}\ \underbrace{1002}_{\text{kc}}\ \underbrace{0700}_{\text{ha}}\ \underbrace{0813}_{\text{in}}$$

Disse blokke kan betragtes som restklasser i $\mathbb{Z}_m = \mathbb{Z}_{50279}$, altså:

$$[0111], [1402], [1002], [0700], [0813]$$

Nu skal disse modulo $m = 50279$ regnes ud, og opløftes i $k = 7$, således:

$$[18680], [31371], [24706], [40925], [36965]$$

Person A kan nu sendte dette til Person B.

Nu skal Person B til at dekryptere, og skal derfor beregne hjælpestørrelserne u og v, og udfylder tabellen til Euklids algoritme:

$$r_k = r_0 u_k + r_1 v_k$$

$$r_0 = 7q_1 + r_2$$

$\boldsymbol{k}$	$\boldsymbol{q_k}$	$\boldsymbol{r_k}$	$\boldsymbol{v_k}$	$\boldsymbol{u_k}$
0	$-$	-49776	1	0
1	-7110	7	0	1
2	-1	-6	1	7110
3	-6	1	$v = 1$	$u = 7111$
		0		

Vi kan tjekke disse:

$$7(7111) + 1(-49776) = 46777 - 46776 = 1$$

Nu kendes hjælpestørrelserne. For dekryptere kryptoteksten opløftes i u'te.

Nu kan Person B dekryptere:

$$[18680]^{7111} = [1012] = \text{bl}$$
$$[31371]^{7111} = [1402] = \text{oc}$$
$$[24706]^{7111} = [1002] = \text{kc}$$
$$[40925]^{7111} = [0700] = \text{ha}$$
$$[36965]^{7111} = [0813] = \text{in}$$

blockchain

Person B forstod en besked, modtaget fra Person A, uden at evt. Person C der måtte have opsnappet kryptoteksten under overleveringen, har kunne forstå den. *Success.*[50]

[50] Tilpasset eksempel fra (Erlandsen, 2005)

5. DANSKE BANK SOM BLOCKCHAIN-BANK

I de foregående afsnit er det blevet opbygget en grundlæggende viden for selve blockchain-begrebet og dets anvendelser, samt en mere underbyggende forståelse af hvordan blockchain virker.

Det er nu på tide nærmere at analysere forretningsmodellerne i den finansielle sektor, samt yderligere se nærmere på hvordan denne kan drage fordel af blockchain-teknologien. Her tages der udgangspunkt i Danske Bank A/S.

5.1 METODE

Analysen vil overordnet set kredse Om *Busi*ness Model *Canvas* og *de 9 byggesten*[51] heri - men vil også kort inddrage andre interne analyser. Der vil desuden blive brugt elementer af eksterne analyser

Først analyseres Danske Banks interne situation. Derefter kigges der kort på hvilke eksterne forhold der ligger op til ændring af virksomheden internt. Med afsæt i disse forhold, kigges der på hvordan forretningsmodellen kan optimeres/forbedres vha. af blockchain.

Før at kunne gøre dette, er det vigtigt at kende til Danske Bank - derfor inddrages der indledningsvist elementer af en virksomhedskarakterstik.

5.2 OM DANSKE BANK

Danske Bank er en nordisk bank (og en servicevirksomhed), og har hovedsæde i København. Virksomheden tilbyder en bred vifte af finansielle produkter og tjenester, og befinder sig på både det danske, svenske, norske og finske marked - desuden har de filialer og tilstedeværelse i Irland, UK, USA, Indien, Polen og Litauen, men deres kernemarkeder befinder sig i Skandinavien.

Danske Bank servicerer over 3,3 millioner kunder - både private og erhvervs - indenfor deres primære forretningsområder: *Personal Banking, Private Banking. Business Banking samt LC&I (Large Corporations & Institutions).*

[51] BMC (*Business Model Canvas*) og dens 9 byggesten beskrives i (Osterwalder & Pigeneur, 2012) - ligesom store dele af den teori der bruges heri om forretningsmodeller og deres sammensætning også beskrives i denne.

Danske Bank står bl.a. bag den populære mobilbetalings-app, *MobilePay*, men er ikke længere hovedaktionær. De står også bag apps som *Lommepenge* og *Billy*.

Resten af analysen tager afsæt i forretningsområdet *Personal Banking,* og de produkter og tjenester der udbydes her indenfor.

5.3 DEN INTERNE SITUATION

5.3.1 Danske Banks BMC

Bankens målgruppe må siges at være at ret bred. Demografisk og kønsmæssigt bevæger den sig på hele spektret, og tager ikke hensyn til hverken alder eller køn i den forstand. Man kan muligvis snakke om, at banken primært henvender sig til et segment med et samlet forretningsomfang på under eller omkring mio.kr. 2 - dette fordi deres kundeprogram ikke udvides over mio.kr. 2[52], og andre banker derfor henvender sig til de segmenter, der har meget store formuer - man kan også tale om at dette nærmere hører til Private Banking. Danske Bank henvender sig altså til et massemarked, hvor der kun adskilles/segmenteres efter forretningsomfanget.

Dog kan det nævnes, at banken har et specifikt program til unge kunder mellem 18-27 år[53], hvor en lang række kerneprodukter tilbydes gratis - her kan der tales om freemium-modellen. Banken har interessere i at erhverve unge kunder, der på sigt bliver til loyale, gamle, betalende kunder - ungdomsårene er godt fundament til at danne det; Som ung danner man præference og loyalitet, og i start 20'erne begynder man at tage større finansielle beslutninger - som banken er interesseret i deltage i.

Bankers værditilbud er generelt ret homogent og standardiseret. Naturligvis består værditilbuddet af både indlån, udlån, rådgivning og tilbyder ofte en række formuehåndteringsredskaber i form af investeringsplatforme. Dette er også tilfældet for Danske Bank. Banken gør dog alligevel visse ting for at bringe præferencebaserede elementer med ind i et forholdsvist homogent værditilbud.

[52] https://danskebank.dk/privat/kundeprogram/fordele
[53] https://danskebank.dk/privat/kundeprogram

Danske Bank har haft stor fokus på at øge deres digitale bekvemmelighed/anvendelse af deres produkter og tjenester. Alle banker tilbyder efterhånden en NetBank, men Danske Banks er en af de bedste mht. til hastighed og brugervenlighed[54]. Desuden vinder deres Mobilbank-app priser[55]. I en verden hvor det foretrækkes at kunne styre sit liv fra mobilen, er dette en væsentlig faktor ift. værditilbuddet.

Desuden tilbyder Danske Bank deres kernefunktioner billigt ift. andre banker; Ved de fleste banker er der begrænsninger på antal konti. Ved Danske Bank koster det ikke noget at oprette ekstra konti[56]. Desuden er overførselsgebyrerne meget lave, og i mange tilfælde helt gebyrfri[57]. Banken tilbyder altså kerneydelserne billigt sammenlignet med andre banker.

Altså fremhæves bankens værditilbud i form af en billig pris samt bekvemmelighed/anvendelighed

De mest centrale kanaler, er naturligvis deres lokale filialer og diverse andre kontaktmuligheder (hjemmeside, telefon, mail, etc.)

Man kan også tale om, at det have en bank opfylder et tryghedsbehov i behovspyramiden, og at kunderne - i sammenspil med fordelene i værditilbuddet, - derfor selv opsøger banken.

Naturligvis har banken også andre salgskanaler i form af samarbejder, m.v., men disser ikke lige så tydelige som ved andre virksomheder.

Bankens relation til kunderne er i høj grad kendetegnet ved selvbetjening i form af deres digitale platforme (Net- og Mobilbank). Dog er der selvfølgelig en personlig betjening/relation ifm. med f.eks. lån; herunder rådgivning, vurdering af kreditværdighed, etc.

Det er værd at nævne at banken har været genstand for diverse shitstorms i medierne. Banken har derfor på det seneste forsagt at fremhæve et filantropisk

[54] (Christensen, 2017)
[55] (Danske Bank, 2021).
[56] (Danske Bank, 2023)
[57] (Danske Bank, 2022)

ansvar ved bl.a. at engagere sig i FN's verdensmål, have fokus på Corporate Governance, og udvikler desuden aktivt læringsmateriale til børn.[58]

Danske Banks indtægtsstrømme adskiller sig ikke væsentligt fra andre banker. Indtægterne kommer primært fra 3 områder: forskellen mellem ind- og udlånsrenten, indtægter fra gebyrer, og indtægter fra egen investeret kapital.

Virksomhedens nøgleressourcer består naturligvis af deres finansielle ressourcer, altså deres indlån, som er et absolut hovedelement i at drive deres forretning.

Derudover selvfølgelig deres digitale ressourcer i from af Net- og Mobilbank, og deres egen interne infrastruktur.

Selvfølgelig medarbejdere; Både i form af dygtige rådgivere som front-end personale. Og dygtige kreative stillinger til konceptudvikling, samt dygtig administration som back-end personale.

Deres bygninger (og design generelt) er også en vigtig nøgle ressource, da det er disse der udgør deres Physical Evidence, som udviser tryghed, stabilitet og soliditet overfor forbrugeren

Nøgleaktiviteterne udgør de processer banken foretager sig ifm. med deres tjenesteydelser: formidling af transaktioner, kreditvurdering, rådgivning, etc.

Desuden selvfølgelig også vedligeholdelsen og konceptudviklingen af deres resterende produkter.

Især nøglepartnere har et tæt sammenspil med nøgleaktiviteterne; Der skal afviklings- og clearingsystemer til at håndtere transaktionsformidlingen (disse leveres af partnere), it-leverandører ifm. med deres digitale platforme, og desuden samarbejdspartnere de benytter i deres rådgivning (Pensionsselskaber og andre bankrelaterede ydelser).

[58] (Danske Bank, 2023)

Til sidst kigges på deres omkostningsstruktur. Her afholdes der selvfølgelig omkostninger til bl.a. betalingsformidling, drift af deres digitale ydelser, aflønninger, etc.

5.3.2 Andre interne forhold

Givet bankens størrelse og deres markedsleder position, - og naturen af deres forretningsmodel, - er det klart at banken nyder godt at visse omkostningsfordele ifm. deres stordrift, og desuden deres selvbetjente alternativer til personlig service.

Af det kan man udlede en omkostningslederstrategi, da de henvender sig til en bred målgruppe med fokus på lave omkostninger.

Da værditilbuddet i virkeligheden er relativt homogent, men alligevel kommunikeres og sælges på en præferencebestemt måde, kan det give mening at placere virksomheden i Bowmans strategiske ur[59].

Der kan argumenteres for at banken heri benytter en hybridstrategi, i det de som sagt tilbyder lave priser, men alligevel oplever en højere kundeværdi - i det man får adgang til deres innovative digitale løsninger.

Det kan svært at udpege en decideret kernekompetence der adskiller sig fra andre banker. Man kan argumentere for, at deres evne til at innovere digitalt adskiller sig fra andre banker (Her tænkes der på de diverse apps de står bag), men det er nok i virkeligheden mere en fokuskompetence.

Deres konkurrencemæssige fordele består primært i deres stordrift.

5.4 DEN EKSTERNE SITUATION

Bankers forretningsmodeller kom til pga. af nogle omverdensforhold - og de vil ligeledes forandres pga. af nogle omverdensforhold.

Bankforretning blev etableret tilbage i 1600-tallet hvor man så en stærk udvikling i de økonomiske forhold i den uafhængige omverden, og der opstod et behov for kredit-, betaling- og risikoformidling. Nu ses der er ny udvikling i de teknolo-

[59] (Østergaard, Mortensen, Marquart, Bregendahl, & Haase, 2017)

giske forhold - blockchain. Dette vedrører mange slags virksomheder - og er banker er ikke undtaget.

Blockchain-teknologien har mulighed for at optimere banker indefra (som det uddybes i næste afsnit), men præsentere også helt nye muligheder for forretningsmodeller som helt kan gå uden om bankerne - som dermed påvirker konkurrenterne i den afhængige omverden.

Hvis der ses på konkurrenterne og dermed branchen, ses en ny type virksomhed bevæge sig mod den nære konkurrence - blockchains introduktion har nemlig gjort såkaldte DeFi-virksomheder mulige. DeFi står for *Decentralized Finance,* og som navnet antyder tilbyder de decentrale finansielle løsninger vha. blockchain[60].

Vha. af kryptovaluta kan de helt uden en central myndighed formidle transaktioner (også på tværs af lande), formidle lån, og generelt kan en masse traditionelle centralt styrede ydelser omdannes til en DeFi-løsning

5.5 BLOCKCHAINIFISERING

Der er altså nogle omverdensforhold, der lægger op til forandring for bankerne.

For at forstå hvordan forretningsmodellen kan optimeres, må vi først kigge lidt nærmere på kunderne - hvilke kriterier er egentlig relevante ved bank valg[61]:

- 66% vægter *konkurrencedygtige produkter*
- 62% vægter *god og overskuelig netbank*
- 53% vægter *produkter der er gennemskuelige*
- 51% vægter *image og omdømme*
- 44% vægter *kemi med rådgiver*

De to mest afgørende faktorer præsterer Danske Bank allerede godt på - men de omtalte DeFi-ydelser har potentiale til at præstere endnu bedre. Et glimrende eksempel er virksomheden ZTLment, som tidligere blev præsenteret. ZTLment kan tilbyde betalinger mellem virksomheder uden om bankerne - billigere. Det er blot

[60] (Kryptos Redaktionen, 2021)
[61] (MyBanker redaktionen, 2019)

et eksempel på, hvorfor det er nødvendigt at se på, hvordan bankerne kan gøre det bedre vha. selvsamme teknologi.

Konkurrencedygtige produkter vedrører primært aktivitets- samt finansperspektivet. Lad os hvordan blockchain yderligere kan optimere forretningsmodellen ift. disse perspektiver.

Aktivitetsperspektivet kan især effektiviseres. Som tidligere redegjort for, kan blockchain forenkle transaktionsformidlinger meget - dette vil betyde et udskift af nøglepartnerne, og nøgleaktiviteter vil især forenkles jf. hvad der tidligere er redegjort for; Ved at udnytte blockchain til infrastruktur, og desuden Smart Contracts, vil man kunne fjerne mange manuelle og tidskrævende mellemled.

Det hænger også sammen med det finansielle perspektiv - nærmere bestemt i omkostningsstrukturen. Forenklingen i aktivitetsperspektivet afspejler sig netop i omkostninger; En banks omkostninger er i høj grad baseret på omfattende og avancerede sikkerheds- og godkendelsesled. Kan disse minimeres, kan omkostningerne ligeledes også.

Alt andet lige vil blockchain altså resultere i en udvidet profitmargin. Man kan herefter vælge at beholde prisniveauerne, således at avancen og overskuddet bliver større. Man kan også sænke prisniveauet som formentligt vil resultere i en stigning i afsætningen, og dermed også omsætningen og til sidst overskuddet.

Et andet vigtigt kriterie ved valg af bank, var det personlige kundeforhold - og her har bankerne en fordel. Danske Bank kan udnytte, at man kan tilbyde samme services billigere, og bruge det ekstra overskud til at forbedre de andre periferiydelser (læs: de personlige kundeforhold) - dette kan på sigt også skabe præference og forøget overskud.

Allerede her ses det hvordan anvendelsen af blockchain kan føre til en række konkurrencemæssige fordele.

God og overskuelige netbank hæfter sig til kundeperspektivet - og blockchain har også mulighed for at forbedre ting indenfor dette.

Blockchain kan forbedre låneprocessen; Såfremt denne kan integreres, så et system selvstændigt og pålideligt kan foretage kreditvurderinger og identitetsbekræftelse, vil man kunne strømline låneprocessen ved at formindske tids- og ressourceforbruget gevaldigt - dette gør forbrugeroplevelsen nemmere, samtidig med at banken sparer tid og penge.

Desuden kan man med blockchain fjerne visse manuelle led (som uddybes i det næste), som tillader at endnu flere services er tilgængelige 24/7 (selvom mange er det i forvejen), netop fordi man kan automatisere.

Gennem opgaven er bl.a. sikkerheden og pålideligheden ved blockchain blevet fremhævet. I Danmark er der dog ikke troværdighedsproblemer til pengevæsenet[62]. Derfor fremgår det også af denne analyse, at det ikke er sikkerheden og troværdigheden ved den distribuerede blockchain, der udgør en potentiel forbedring i forretningsmodellen, men i stedet effektivitets- og optimeringsaspektet ved teknologien.

[62] (Danmarks Nationalbank, 2022)

6. FINANSSEKTORENS FREMTID MED BLOCKCHAIN

Blockchain-teknologien har potentielt mange indgangsvinkler ift. at disrupte finanssektoren; Banker har fulgt en traditionel model i mange århundrede, og blockchain ændrer nu på det.

En måde blockchain kan disrupte branchen på, er noget så simpelt som at vende om på de etablerede aktører og de nye aktører. Gennembrud i teknologien kan være udfordrende for store finansielle virksomheder at håndtere. Modsat kan de mindre virksomheders elasticitet - og ofte også innovative miljø, - nemmere håndtere at integrere og benytte blockchain i sin forretning.

Dog vil. etablering og integration af sådanne systemer være forbundet med et højt kapitalkrav - hvorfor det måske alligevel er en opgave for de etablerede og store virksomheder.

Kryptovaluta er som tidligere beskrevet som et meget spekulativt fænomen - specielt i den vestlige verden. Når der i vesten tales om kryptovaluta, tænkes der ofte på kryptovaluta som investering, og ikke som betalingsmiddel som det jo egentlig er.

I Danmark og i vesten er troværdigheden til pengesystemet ikke en udfordring. Dette er dog ikke tilfældet andre steder i verden, især i ulande[63]. Her kan den decentrale valuta være et afgørende redskab ift. at fremme et ustabilt - og ofte korrupt - system. Men fordi blockchain er decentralt, kan man ikke på samme måde kontrollere kryptovaluta på tværs af landegrænser. Det betyder at landene (heri også Danmark) ikke som sådan har kontrol over kryptovalutas eventuelle udbredelse, hvilket kan vise sig at skubbe til det etablerede finansielle system i vesten også.

Dog er det igen vigtigt at huske på, at troværdigheden til det finansielle system er høj i Danmark, og et scenarie som ovenstående derfor på nuværende tidspunkt er mere usandsynligt - men dog ikke umuligt.

[63] (Hansen, 2021)

Den absolutte største potentielle trussel mod finanssektoren som den kendes er DeFi-virksomhederne, som med den rette udbredelse og indtrædelse kan vise sig at vende hele branchen på hovedet.

DeFi kan i princippet gå helt uden om bankerne; Blockchain kan repræsentere den sikkerhed, troværdig og tillid som de centrale aktører i finanssektoren hidtil har repræsenteret, og disse bliver derfor overflødige. Desuden åbner DeFi for i langt højere grad at effektivisere og automatisere.

Med alt ovenstående er det vigtigt at huske på, at der på den anden side er de lovgivende og regulatoriske institutioner, som på mange måder er helt afgørende for teknogiens anvendelse. Lovgivningen på området er stadig uklar, og fremtidige lovgivningsmæssige og regulatoriske rammer kan sætte en stoppe for den brede udbredelse af blockchain.

Det kan ydermere også vise sig, at det slet ikke er bankerne og de private virksomheder som bliver first movers indenfor blockchain. Finanstilsynet og Nationalbanken viser allerede stor interesse for området, og selvom der ikke er horisonten lige nu, kan det tænkes at de kommer i forkøbet med blockchain - således at anvendelsen af denne bliver et generelt markedsvilkår for alle banker.

7. KONKLUSION

Blockchain kan bl.a. bruges som *betalingsinfrastruktur* ifm. transaktioner. Dette er en af de mest oplagte anvendelsesmuligheder. Teknologien kan erstatte traditionelle, centrale afviklings- og clearingsystemer, og kan i stedet håndtere disse opgaver decentralt. Det resulterer i en hurtigere (realtid) og mere effektiv betalingsformidling.

En anden anvendelsesmulig er *intelligente kontrakter.* Disse kan simpelt forstås som automatiserede versioner juridiske kontrakter. En intelligent kontrakt kan programmeres til at udføre de kontraktlige forhold, og kan registreres på en blockchain. Blockchainen sørger for dens pålidelighed og ægthed

Desuden kan teknologiens også anvendes ifm. låneformidling, identitetsbekræftelse, pantsætning, m.v.

Alle medlemmer i et blockchain-netværk har adgang til at se indholdet, men de kan imidlertid ikke forstå det. Blockchain udnytter offentlig-nøgle-kryptering, til at sikre at man kun med den rette nøgle (og dermed rette bemyndigelse) kan forstå indholdet. I praksis gøres dette ved at udnytte egenskaber ved primtal samt moduloregning. Sikkerheden heri består i, at menneskeheden hidtil kun har meget tidskrævende metoder til af primfaktorisere - og dette muliggør en kombination af hhv. en offentlig og hemmelig nøgle.

På baggrund af ovenstående har blockchain mulighed for at optimere bankers forretningsmodel på flere punkter. For det første er det indlysende, at banken kan minimere deres omkostninger ved at benytte blockchain i sin infrastruktur; Dvs. udskifte dyre og tidskrævende mellemled som afviklings- og clearingsystemer. Dette vil også forbedre værditilbuddet, idet aktivitetsoptimeringen afspejler sig i de ydelser kunderne benytter sig af - f.eks. overførsler i realtid.

Desuden vil man kunne strømline låneprocessen ved at benytte blockchain til kreditvurdering og identitetsbekræftelse - både til fordel for kunderne og banken.

Blockchain har desuden også potentialet til helt at disrupte finanssektoren. Den sikkerhed og pålidelighed som banker og mellemmand hidtil har repræsenteret,

bliver trodset og overflødiggjort af blockchainens decentrale struktur. Det kan resultere i en komplet forandring af det finansielle system.

Dog er reguleringen og lovgivningen på området stadig uklar, hvilket potentielt kan hæmme blockchains videre anvendelse og udbredelse.

Også selvom blockchain ikke revolutionere hele branchen, åbner det alligevel op for nye muligheder for nye indtrængere. Disse kan udgøre en væsentlig trussel mod de etablerede aktører - og blockchain vil disrupte markedet den vej i gennem.

8. KILDELISTE

chirag. (2023. januar 2023). *Blockchain technology for KYC: The Solution to Inefficient KYC Process*. Hentet fra Appinventiv: https://appinventiv.com/blog/use-blockchain-technology-for-kyc/

Christensen, T. B. (25. 04 2017). *Her er pengeinstitutterne med de bedste netbanker.* Hentet fra Finanswatch: https://finanswatch.dk/Finansnyt/Pengeinstitutter/article9528745.ece

Damsgaard, J. (2021). *Blockchain business - Ægte, sporbart og uerstatteligt.* København K: Djøf Forlag.

Danmarks Nationalbank. (23. juni 2022). *Nye former for digitale penge.* Hentet fra Nationalbanken: https://www.nationalbanken.dk/da/publikationer/Documents/2022/06/ANALYSE_nr%208_Nye%20former%20for%20digitale%20penge.pdf

Danske Bank. (20. maj 2021). *Danske Banks mobilbank vinder global pris for bedste brugeroplevelse.* Hentet fra Danske Bank: https://danskebank.com/da/news-og-insights/nyhedsarkiv/news/2021/20052021#:~:text=Danske%20Banks%20mobilbank%20er%20k%C3%A5ret,funktioner%20s%C3%A5som%20kontoopg%C3%B8relse%20og%20abonnementsstyring.

Danske Bank. (1. januar 2022). *Danske Banks Prisliste.* Hentet fra danskebank.dk: https://www.danskebank.dk/PDF/PRISER-VILKAAR-FAKTAARK/Konti/Prisliste_for_kundepakker_produkter_services.pdf

Danske Bank. (2023). *Inverstor Relations.* Hentet fra Danske Bank: https://danskebank.com/da/investor-relations

Danske Bank. (2023). *Konti.* Hentet fra Danske Bank: https://danskebank.dk/privat/produkter/konti

Danske Bank. (2023). *News & Insights.* Hentet fra Danske Bank: https://danskebank.com/da/news-og-insights

Danske Bank. (2023). *Om Os.* Hentet fra Danske Bank: https://danskebank.com/da/om-os

Danske Bank. (2023). *Strategisk Retning.* Hentet fra Danske Bank: https://danskebank.com/da/baeredygtighed/strategisk-retning

Erlandsen, M. K. (2005). *Introduktion til Kryptologi.* Hentet fra math.au.dk: https://math.au.dk/fileadmin/Files/matlaererdag/2005/kryptologi.pdf

Finanstilsynet. (26. januar 2022). *Blockchain-teknologi kan udgøre en effektiv infrastruktur til betalingstjenester.* Hentet fra Finanstilsynet: https://www.finanstilsynet.dk/-/media/Nyhedscenter/2022/Blockchain-som-infrastruktur-til-betalingstjenester.pdf

Hansen, L. B. (7. juni 2021). *Nu vil det første land acceptere bitcoin som officielt betalingsmiddel, men det er ikke uden problemer.* Hentet fra TV2 Nyheder: https://nyheder.tv2.dk/business/2021-06-07-nu-vil-det-foerste-land-acceptere-bitcoin-som-officielt-betalingsmiddel-men-det

Jensen, K. B. (2020). SRP i, med og om MATEMATIK.

Kryptos Redaktionen. (8. juni 2021). *Decentralized Finance (DeFi) – Informationer, oversigt og udbydere.* Hentet fra Kryptos.dk: https://kryptos.dk/defi-decentralized-finance/

Kryptos Redaktionen. (3. maj 2021). *Hvad er Smart Contracts?* Hentet fra Kryptos.dk: https://kryptos.dk/smart-contracts/

Lorenzen, E. W., Jørgensen, M., Carstensen, J., & Frandsen, J. (2017). *Talmængder*. Hentet fra MAT stx grundforløb: https://matstxgrundforlob.systime.dk/?id=846

MyBanker redaktionen. (29. 4 2019). *Etik og værdier fylder mere når der skal vælges ny bank.* Hentet fra MyBanker: https://www.mybanker.dk/artikler/etik-og-vaerdier-fylder-mere-naar-der-skal-vaelges-ny-bank/

Nordgaard, P. (27. Oktober 2017). *Vil du forstå Smart Contracts på fem minutter?* Hentet fra LinkedIn: https://www.linkedin.com/pulse/vil-du-forst%C3%A5-smart-contracts-p%C3%A5-fem-minutter-peter-nordgaard/

Osterwalder, A., & Pigeneur, Y. (2012). *Business Model Generation.* København K: Gyldendal A/S.

Portilla, D. L., Kappos, D. J., Ngo, M. V., Rosenthal-Larrea, S., Buretta, J. D., Fargo, C. K., . . . Moore-LLP. (28. januar 2022). *Blockchain in the Banking Sector: A Review of the Landscape and Opportunities*. Hentet fra Harvard Law School Forum on Corporate Governance:

https://corpgov.law.harvard.edu/2022/01/28/blockchain-in-the-banking-sector-a-review-of-the-landscape-and-opportunities/

Riber, P. (2007). *Kryptering.* Århus: Systime A/S.

Rosenstand, C. (2017). *Digital Disruption.* Aalborg Ø: Aalborg Universitetsforlag.

Stinson, D. R. (2002). *Cryptography - theory and practice.* Boca Raton: Chapman & Hall/CRC.

Østergaard, B. R., Mortensen, R., Marquart, S. S., Bregendahl, M., & Haase, M. (2017). *Marketing - en grundbog i afsætning*. Hentet fra Systime: https://marketing.systime.dk/

9. BILAG

9.1 BILAG 1 - HASH-FUNKTIONER

Blokkene i en blockchain er kædet sammen på sådan en måde, at man ikke kan ændre i de foregående blokke og deres data. Dette gøres i praksis vha. et hash-nummer, som udledes baseret på nogle kryptografiske hashfunktioner, og kan sammenlignes med et fingeraftryk; Hver blok har sit eget unikke hash-nummer (fingeraftryk), og efterfølgende blokke har altid en reference til den foregående bloks hash-nummer.

Hashfunktionerne bestemmer hash-nummeret baseret på indholdet af blokkene i den pågældende blockchain - og samme data vil altid føre til samme nummer. Ændres indholdet, ændres hash-nummeret ligeledes også, og kæden går i stykker - netværket vil derfra opdage en uautoriseret ændring og forhindre den.[64]

[64] (Damsgaard, 2021)

9.2 BILAG 2 - OM PRIMTAL

De fleste er bare en smule bekendte med primtal, men lad os for god ordens skyld opfriske definitionen.

Definition 3.1: *Primtal* er kendetegnet ved, at disse kun har 1 og sig selv som divisorer.[65]

Eksempel 3.2:

- 5 er et primtal, da det kun har 1 og 5 som divisorer
- 6 er ikke et primtal, da det udover 1 og 6, også har 2 og 3 som divisorer
    - Her kaldes 2 og 3 for trivielle divisorer[66]
- 19 er et primtal, da det kun har 1 og 19 som divisorer

Man kan primfaktorisere tal. Dette gøres ved at omskrive tallet til et produkt af *ikke-trivielle* faktorer

Definition 3.3: Et tal n *primfaktoriseres* ved at omdanne det til et produkt udelukkende af primtals-faktorer, dvs.:

$$n = p_1 p_2 \dots p_n$$

Hvor samtlige p_n er primtal. [67]

Eksempel 3.4:

$4 \cdot 5 \cdot 2$ er en faktorisering af 40, men ikke en primfaktorisering, da en af faktorerne, 4, ikke er et primtal. Lad os forsøge at beregne den rette primfaktorisering:

Først divideres 96 men det laveste primtal der ikke efterlader en rest. Her der det 2 da $96 \$ 2 = 0$:

[65] (Riber, 2007)
[66] (Riber, 2007)
[67] (Riber, 2007)

$$\frac{40}{2} = 20$$

Da 20 ikke er et primtal, gentages første skridt - det ses at den rette divisor stadig er 2:

$$\frac{20}{2} = 10$$

10 er heller ikke et primtal, processen gentages - stadig med 2:

$$\frac{10}{2} = 5$$

Det ses at forholdet mellem 10 og 2 er et primtal, vi kan stoppe her.

Da multiplikation er det modsatte af division, kan vi betragte samtlige divisorer som faktorer og opstille den rette primfaktorisering:

$$2 \cdot 2 \cdot 2 \cdot 5 = 2^3 \cdot 5$$

BEMÆRK Man kan i praksis ikke primfaktorisere et primtal p. Dette fordi p kun har divisorerne 1 og p. Derfor vil den eneste teoretiske primfaktorisering være:

$$1 \cdot p = p$$

[68]

Man vil ved algoritmen i Eksempel 3.4 hurtigt se at beregningen ved større tal hurtigt vil blive meget tidskrævende.

Definition 3.5: To tal $a, \in \mathbb{N}$ er *indbyrdes primiske* hvis kun 1 går op i begge tal.[69]

[68] Bearbejdet eksempel fra (Riber, 2007)
[69] (Erlandsen, 2005)

Eksempel 3.6: F.eks. er 11 og 12 *indbyrdes primiske,* da 1 er de eneste divisor der går op i begge tal, mens 12 og 16 *ikke* er indbyrdes primiske, da både 1, 2 og 4 går op i begge tal.[70]

[70] Bearbejdet eksempel fra (Erlandsen, 2005)

9.3 BILAG 3 - MODULOREGNING

Sætning 3.7: *Givet* $n, p \in \mathbb{Z}$ *hvor* $p \neq 0$ *findes* $q, r \in \mathbb{Z}$ *hvor* $0 \leq r \leq p$*, så:*

$$n = pq + r$$

[71]

Altså at p går q gange op i n med r rest.

Definition 3.8: Sætning 3.7 fortæller at moduloregning, altså division med rest, kan lade sig gøre. Derfor menes der med notationen:

$$n \$ p = r$$

hvor $ siges modulo, at ved division $\frac{n}{p}$ efterlades r rest (fra Sætning 3.7).[72]

Eksempel 3.8: Haves f.eks. $n = 11$ og $p = 5$, vides det at 5 går to gange op i 10 med én til rest. Notationen fra sætning 3.7 vil da være:

$$n = 11, p = 5, q = 2, r = 1$$

altså:

$$11 = (5)(2) + 1$$

Og derfor:

$$11 \$ 5 = 1$$

[73]

[71] (Erlandsen, 2005)
[72] Notation $ fra (Riber, 2007), definition fra (Erlandsen, 2005)
[73] Bearbejdet eksempel fra (Erlandsen, 2005)