



LUNDS UNIVERSITET

Ekonomihögskolan

Institutionen för informatik

Lär känna din kund med blockchain

Möjligheter och utmaningar med blockchainbaserade KYC-system

Kandidatuppsats 15 hp, kurs SYSK16 i Informatik

Författare: Filip Fjellstedt
Isak Larsson

Handledare: Ahmad Ghazawneh

Rättande lärare: Björn Svensson
Benjamin Weaver

Lär känna din kund med blockchain: Möjligheter och utmaningar med blockchainbaserade KYC-system

ENGELSK TITEL: Know your customer with blockchain: Possibilities and challenges with blockchain-based KYC-systems

FÖRFATTARE: Filip Fjellstedt och Isak Larsson

UTGIVARE: Institutionen för informatik, Ekonomihögskolan, Lunds universitet

EXAMINATOR: Odd Steen, Docent, Fil Dr

FRAMLAGD: augusti, 2019

DOKUMENTTYP: Kandidatuppsats

ANTAL SIDOR: 75

NYCKELORD: Blockchain, KYC, DLT, Innovation, Emerging Technology

SAMMANFATTNING:

Det ställs höga krav på finansiella instituts kundkännedomsprocesser för att motverka penningtvätt och finansiering av terrorism. Många av dessa processer kräver mycket manuellt arbete hos både organisation och för kund, som måste upprepa processen hos varje bank de önskar att bli kund. Blockchain kan beskrivas som en decentraliserad databas utan behovet av någon central del som styr nätverket. Istället är alla transaktioner registrerade och verifierade av medlemmarna i nätverket. Syftet med denna kvalitativa studie är att med hjälp av kvalitativa och semi-strukturerade intervjuer av personer med kunskap om blockchain och insyn i den finansiella marknaden samt en litteraturstudie undersöka bankernas och finansbranschens syn på blockchain tekniken och vilka möjligheter och utmaningar som kommer med blockchainbaserade KYC-system. Studien identifierar ett antal möjligheter och utmaningar med blockchainbaserade KYC-system. Möjligheterna identifieras som högre effektivitet, lägre kostnader, mer digitalisering och högre kundnöjdhet samt bättre regelefterlevnad och säkerhet. Utmaningarna identifierades som låg acceptansnivå för blockchain, krav på stora samarbeten och avsaknad av standarder.

Innehåll

1	Inledning	5
1.1	Bakgrund.....	5
1.2	Problemområde	6
1.3	Syfte och frågeställning	6
1.4	Avgränsningar	6
2	Litteraturgenomgång	7
2.1	Definitioner	7
2.1.1	Kundkännedom	7
2.1.2	General Data Protection Regulation (GDPR).....	7
2.1.3	Blockchain	8
2.1.4	DLT	8
2.1.5	Hashing.....	8
2.1.6	Konsensus	9
2.1.7	Privata, konsortium och publika blockkedjor	9
2.1.8	Zero-knowledge proof	10
2.1.9	Ethereum.....	10
2.1.10	Privata vs publika nycklar	10
2.1.11	Emerging technology	11
2.2	Utmaningar med blockchainteknologin.....	11
2.3	Möjligheter med Blockchainteknologin	12
2.4	Blockchain och KYC.....	13
2.5	Innovationsspridning	14
2.5.1	Innovation	14
2.5.2	Innovationsattribut	15
3	Metod.....	16
3.1	Metodval	16
3.2	Urval.....	16
3.3	Genomförandet av intervjuer	18
3.4	Presentation och analys av datainsamling	18
3.5	Validitet och reliabilitet	19
3.6	Etik	19
3.7	Metodreflektion.....	19
4	Empiri	21
4.1	Presentation av respondenter	21
4.2	Blockchain	21

4.2.1	Blockchain idag.....	21
4.2.2	Blockchains framtid inom finansbranschen.....	22
4.2.3	Utmaningar	23
4.2.4	Möjligheter.....	25
4.2.5	Risker med blockchain	25
4.3	KYC.....	26
4.3.1	Utmaningar och problem med dagens KYC-process.....	27
4.4	Hur en blockchainbaserad KYC-lösning kan se ut	28
4.4.1	Fördelar för kunder.....	29
4.4.2	Fördelar för bankerna	29
4.4.3	Utmaningar med implementation.....	30
5	Analys.....	31
5.1	Finansbranschens syn Blockchain.....	31
5.1.1	Blockkedjans framtid inom finansbranschen.....	31
5.1.2	Utmaningar	32
5.1.3	Möjligheter.....	32
5.2	KYC.....	32
5.2.1	Utmaningar och problem med dagens KYC-process.....	32
5.3	KYC och blockchain	33
5.3.1	Hur en blockchainbaserad KYC-system skulle kunna se ut.....	33
5.3.2	Fördelar för kunder.....	34
5.3.3	Fördelar för finansiella institut.....	34
5.3.4	Utmaningar med en implementation	35
6	Slutsats.....	36
6.1	Vidare forskning.....	36
Appendix 1	37
Appendix 2	38
Appendix 3	45
Appendix 4	51
Appendix 5	57
Appendix 6	64
Referenser	72

1 Inledning

1.1 Bakgrund

På senare tid har kraven på banker och finansiella institut ökat när det gäller kundkännedom eller KYC (Know Your Customer) (KPMG International, 2018). Tillräcklig information om kunden behöver samlas in för att kunna motverka penningtvätt och finansiering av terrorism (KPMG International, 2018). Bankerna och de finansiella instituten har ibland svårt att möta kraven och processen är både tidskrävande och dyr och de riskerar dryga böter om kraven inte uppfylls (KPMG International, 2018). Processen kan även bli tidskrävande för kunder då de kan behöva uppge samma information hos olika aktörer vilket kan leda till lägre kundnöjdhet (KPMG International, 2018).

Trots den kritiska betydelsen av dessa processer är dagens KYC-processer präglade av manuella processer och dubbelt arbete som löper hög risk att bli fel och det uppskattas att omkring 80 procent av ansträngningen går till insamling och bearbetning av information och endast 20 procent till att bedöma och övervaka den insamlade informationen för kritisk bedömning (KPMG International, 2018).

Blockchain, eller Blockkedjan, är en teknik som har fått stort genomslag under senare år (Murray, 2018). Den är mest känd som tekniken bakom kryptovalutan Bitcoin men har även många andra användningsområden och tekniken anses vara ett säkert sätt att överföra digitala tillgångar mellan olika parter då den erbjuder ett effektivt och pålitligt sätt att dokumentera och verifiera transaktioner utan behov av mellanhänder (Murray, 2018). Transaktionerna dokumenteras i en huvudbok som distribueras till samtliga deltagare i nätverket vilket gör det svårt att hacka eller manipulera registret (Murray, 2018). Det sägs att tekniken kommer att ha stor påverkan på hur transaktioner kommer att ske över internet i framtiden och många användningsområden har föreslagits bland annat inom finansmarknaden, sjukvården och utbildning (Murray, 2018).

Enligt Kaletovic (2018) spenderade banker omkring 1.7 miljarder dollar på blockchainprojekt år 2017 och en av tio av de 200 deltagande i studien hade en budget för blockchainprojekt på över 10 miljoner dollar. Av dessa institutioner hade 14 procent redan implementerat blockchainlösningar (Kaletovic, 2018).

Furlonger och Valdes (2017) menar att under år 2022 kommer omkring 10 procent av alla företag ha genomgått en radikal transformation med hjälp av blockchain. Det kommer åtminstone finnas en ny verksamhet byggd på blockchain vars värde överstiger USD 10 miljarder (Furlonger & Valdes, 2017). Furlonger och Valdes (2017) förutspår också att omkring år 2030 dess affärsvärde kommer att överstiga USD 3.1 triljoner.

FinTech Network (u.å.) ser Blockchain som en teknik som kan förbättra den kostsamma och tidskrävande kundkännedomsprocessen. Lootsma (2017) ser flera möjligheter att förbättra insamlingen av kundkännedom med blockkedjeteknik. Lootsma (2017) nämner även att det kan främja samarbete mellan olika banker och finansiella institut vilket sparar tid både för

företagen och deras kunder. Moyano och Ross (2017) föreslår ett KYC-system baserat på blockkedjeteknik där kunden kan välja att delge sin information med de finansiella institut som behöver den. Detta skulle innebära att kunden endast behöver uppge sin information en gång och att endast en bank skulle behöva samla in den (Moyano & Ross, 2017). Enligt Moyano och Ross (2017) skulle detta innebära effektivisering, lägre kostnader och en förbättrad upplevelse för kunden.

1.2 Problemområde

Nuvarande uppskattningar visar att kostnader kring riskhantering av finansiell brottslighet överstiger USD 25 miljarder årligen inom banksektorn (KPMG International, 2018). Här spenderar vissa stora finansiella institutioner upp till USD 500 miljoner, enligt Thomson Reuters (2016) och Moyano och Ross (2017), varav den största delen avser KYC.

Blockchain är en teknologi som fortfarande är relativt ung och outforskad (Tapscott & Tapscott, 2016). Den befinner sig fortfarande i ett experimentellt skede och kunskapen runt teknologin är begränsad och det kommer troligtvis ta år innan man vet hur och om blockchain kan komma att förändra banksektorn (Tapscott & Tapscott, 2016). Carson et al. (2018) berättar att bortom hypen har blockchain ett strategiskt värde hos organisationer som möjliggör kostnadsbesparingar. Kaletovic (2018) argumenterar att det är omöjligt att neka att blockchain kommer ha en stor roll i framtiden och berättar att Furlonger och Valdes (2017) skriver att det kommer att gå långsamt men är oundvikligt.

På grund av de manuella och ineffektiva processerna kring KYC och den stora potential och ovisshet som finns runt blockchain är det av intresse att undersöka bankernas och branschens syn på blockchainteknologin för att identifiera utmaningar samt att undersöka möjligheterna med att använda tekniken för KYC-processen.

1.3 Syfte och frågeställning

Syftet med denna uppsats är att undersöka bankernas och finansbranschens syn på blockchainteknologin och möjligheterna och utmaningarna med ett blockchainbaserat KYC-system.

Forskningsfråga:

Vad finns det för möjligheter och utmaningar med ett blockchainbaserat KYC-system?

1.4 Avgränsningar

Vi har valt att avgränsa oss till blockchains användningsområde inom finansbranschen. Studien avgränsar sig till banker och företag som agerar på den svenska marknaden.

2 Litteraturgenomgång

2.1 Definitioner

2.1.1 Kundkännedom

Begreppet KYC är en akronym för 'Know Your Customer', på svenska "kundkännedom" och syftar till processen att samla relevant information om sina kunder för att i möjligaste mån kunna motverka kriminella aktiviteter såsom penningtvätt och finansiering av terrorism (Svenska Bankföreningen, 2017). Företag som verkar inom den finansiella sektorn har särskilda krav på kundkännedom och det kan exempelvis handla om att banker är tvungna att fastställa sina kunders identiteter och samla in information om kunders affärer (Bisnode, u.å.). Det kan också handla om huruvida kunden är en person i politiskt utsatt ställning (Politically Exposed Person (PEP)) eller om den är en på något vis närstående till en sådan person (Bisnode, u.å.).

Dessa processer hjälper till att begränsa cirkulationen av svarta pengar på marknaden och gör det svårare att tjäna stora summor på kriminella aktiviteter (Svenska Bankföreningen, 2017). KYC-processer regleras i Sverige i lagen om penningtvätt och lagen har sin grund i internationella överenskommelser med andra länder där liknande lagstiftning finns (Svenska Bankföreningen, 2017). Förutom att lagen ställer krav på instituts kundkännedom krävs även noggrant bearbetade interna policys för riskhantering (Bisnode, u.å.). Lagen säger att finansiella institut måste granska och rapportera misstänkta transaktioner samt utbilda sin personal inom detta (Bisnode, u.å.).

2.1.2 General Data Protection Regulation (GDPR)

Den 25 maj 2018 introducerades en ny dataskyddsförordning i Sverige och i övriga EU (Datainspektionen, u.å.). Lagstiftningen reglerar hur företag får behandla personuppgifter och har i syfte att dels skydda den enskildes grundläggande rättigheter och friheter och dels att skapa en enighet för skyddet av personuppgifter inom EU (Datainspektionen, u.å.). Den nya förordningen, med dess regelverk, är tillämplig för alla medlemmar inom unionen (Datainspektionen, u.å.). Lagen gäller, i princip, för alla sorters verksamheter som på något vis behandlar personuppgifter och gäller således för myndigheter, föreningar, organisationer, företag och privatpersoner (Datainspektionen, u.å.). Personuppgifter är information som kan, enskilt eller i kombination med andra uppgifter, härledas till en fysisk person (Datainspektionen, u.å.).

Typiska personuppgifter innefattar personnummer, namn, adresser och elektroniska identiteter såsom IP-adresser och cookies (Datainspektionen, u.å.). Personer vars personuppgifter behandlas har ett antal rättigheter som exempelvis att få information om när dennes personuppgifter behandlas, att veta vilka personuppgifter organisationer har om personen och hur de behandlas, att få felaktiga uppgifter rättade och att få sina uppgifter raderade (rätten att bli bortglömd) (Datainspektionen, u.å.). Vid överträdelser av dataskyddsförordningen kan sanktionsavgifter på upp till EUR 20 miljoner, eller fyra procent av bolagets globala omsättning delas ut, beroende på vilket belopp som är högst (Datainspektionen, u.å.).

2.1.3 Blockchain

Blockkedjan är i grunden en distribuerad huvudbok som kopieras till flera noder i ett nätverk (Lootsma, 2017). Huvudboken innehåller alla transaktioner som skett på blockkedjan och dessa läggs till kronologiskt i block (Lootsma, 2017). Transaktionerna övervakas och valideras av de enheter som deltar i blockkedjan och tack vare kryptografi och eftersom huvudboken och dess innehåll inte lagras på ett ställe resulterar det i att den är resistent mot angrepp (Murray, 2018). För att ett nytt block ska skapas krävs konsensus mellan alla, eller en majoritet av, noderna i nätverket (Swanson, 2015).

År 2009 släppte Satoshi den första versionen av Bitcoinprogramvaran som öppen källkod och lanserade nätverket (David Bauman, Lindblom, & Olsson, 2016). I mitten av 2010, efter att ha samarbetat med andra utvecklare för att förbättra den ursprungliga koden, överlämnade Satoshi all kontroll till allmänheten och upphörde att bidra till utvecklingen (David Bauman, Lindblom, & Olsson, 2016). Intresset för Bitcoin har inte slutat växa sedan dess och den underliggande teknologin, blockchain, har börjat implementeras i en rad av nya applikationer bortom kryptovalutor (Crosby et al., 2016).

2.1.4 DLT

Blockchain är en implementation av ett DLT-koncept (Lootsma, 2017). DLT står för ”Distributed Ledger Technology” och används för att hitta konsensus mellan deltagarna i det nätverk inom vilket huvudboken distribueras (Kannengießler et al., 2019). I grunden är en distribuerad huvudbok en databas som delas mellan de olika deltagarna i nätverket (Mills et al., 2016). En ändring i databasen måste godkännas av en eller flera av deltagarna i nätverket (Rückeshäuser, 2017). Man når konsensus i nätverket genom regler som godkänts av samtliga deltagare och detta innebär att nätverket kan validera data utan en tredje part och möjliggör ökad transparens (Rückeshäuser, 2017).

Det mest framstående exemplet som använder sig av DLT är kryptovalutan Bitcoin (Rückeshäuser, 2017). Implementationen som Bitcoin använder är just blockchain men det finns flera andra sätt att använda DLT och man kan till exempel skilja på hur olika implementationer lagrar data och om nätverket är öppet eller slutet (Rückeshäuser, 2017). Bitcoin lagrar data kronologiskt i form av block (Rückeshäuser, 2017).

2.1.5 Hashing

Med en hashfunktion kan man göra om data till en bestämd längd oberoende på längden av den data som ska göras om och i blockchain används så kallade kryptografiska hashfunktioner (Drescher, 2017).

Eftersom en hashsträng kan göras kort kan den inkluderas som text i en blockchaintransaktion (Nofer et al., 2017). Varje block i kedjan innehåller en tidsstämpel, ett hash-värde från föregående block, och ett slumpmässigt nummer för att verifiera hash-värdet (Nofer et al., 2017). Detta garanterar kedjans integritet från första till sista block (Nofer et al., 2017). Hash-värdet är unikt för det block det tillhör och om blockets innehåll förändras, förändras även hash-värdet vilket resulterar i att blocket inte längre passar in i kedjan (Nofer et al., 2017).

2.1.6 Konsensus

I ett blockchainedätverk måste alla deltagarna komma överens om att en transaktion är giltig och detta uppnås genom användningen av olika konsensusalgoritmer (Gupta, 2018). Varje blockchainedätverk fastställer villkoren för en transaktion (Gupta, 2018). Det finns flera olika metoder för att uppnå konsensus i form av olika algoritmer och de vanligaste konsensusalgoritmerna som används bland populära blockchain nätverk inkluderar (Gupta, 2018):

Proof-Of Work (POW):

På Bitcoin-nätverket uppnås konsensus genom sk. Proof-Of-Work (POW) (Gupta, 2018). Det innebär att varje maskin som lagrar en kopia av huvudboken uppmanas att lösa ett komplext pussel baserat på dess version av huvudboken (Gupta, 2018). Maskiner med identiska kopior av sina huvudböcker arbetar tillsammans i lag för att lösa pusslet som de har fått (Gupta, 2018). Det första "laget" att lösa pusslet vinner, och alla andra maskiner uppdaterar sina huvudböcker för att matcha det vinnande lagets och tanken är att majoriteten kommer att vinna för de har mest beräkningskraft för att lösa sitt pussel först (Gupta, 2018).

Proof-Of-Stake (POS):

Proof-of-stake är ett alternativt protokoll för att ge distribuerad konsensus och skydd mot dubbla utgifter (David Bauman, Lindblom, & Olsson, 2016). I ett proof-of-stake-baserat system är det de noder som innehar flest mynt som validerar nya transaktioner till skillnad från POW där noderna med mest beräkningskraft får detta uppdrag (David Bauman, Lindblom, & Olsson, 2016). Argument för detta konsensusystem är att det skulle vara dyrare att attackera eftersom det skulle kräva att någon av angriparna äger majoriteten av mynt, det vill säga att angriparen mestadels skulle skada sig själv (David Bauman, Lindblom, & Olsson, 2016). Ett annat argument till förmån för POS är att det inte är lika beroende av samma mängder beräkningskraft som POW (David Bauman, Lindblom, & Olsson, 2016). Detta är emellertid också akilleshälen för POS (David Bauman, Lindblom, & Olsson, 2016). Eftersom verifieringen av transaktioner i blockchain inte kräver något verkligt arbete står det inget på spel och det finns ingen kostnad för att skapa alternativa historier av huvudboken (David Bauman, Lindblom, & Olsson, 2016).

Tanken med Proof-of-stake är följande: Användare med högre insats i systemet har störst intresse av att upprätthålla ett säkert nätverk (BitFury Group, 2015). Detta på grund av att de kommer att drabbas i högre grad gällande rykte och att priset på kryptovalutan skulle minska på grund av attackerna (BitFury Group, 2015).

2.1.7 Privata, konsortium och publika blockkedjor

Man kan dela upp blockkedjor i tre olika typer av applikationer: publika blockkedjor, privata blockkedjor och konsortiumblockkedjor (Buterin, 2015). Om en blockchain är publik innebär det att vem som helst kan utföra transaktioner i kedjan förutsatt att de är giltiga (Pilkington, 2016; Xu et al., 2016). De kan också delta i valideringsprocessen för att vara med och bestämma vilka transaktioner som godkänns (Buterin, 2015). Blockkedjan är säkrad genom kryptografi och verifikation genom till exempel "proof of work" eller "proof of stake" (Buterin, 2015). Enligt Xu et al. (2016) resulterar användningen av en privat blockkedja till bättre transparens och granskningsmöjlighet, dock offras informationsintegriteten.

I en privat blockchain kan endast medlemmar inom en organisation skriva till kedjan och möjligheten att läsa information från kedjan kan vara öppen för allmänheten alternativt begränsad

till en organisation (Buterin, 2015). Huruvida kedjan är läsbar för allmänheten kan variera beroende på vad den används till (Buterin, 2015).

En konsortiumblockchain kan beskrivas som en variant på en privat blockkedja men med fler parter inblandade och processen för validering och konsensus kontrolleras av ett antal förutbestämda noder (Buterin, 2015). Enligt Lin och Liao (2017) kan man se en konsortiumblockchain som delvis centraliserad. Även här kan möjligheten att läsa information från kedjan vara öppen för allmänheten alternativt begränsad till deltagarna i nätverket (Buterin, 2015). Man kan också tänka sig en lösning som ligger mitt emellan där allmänheten har tillgång till begränsad information i kedjan (Buterin, 2015). Enligt Xu et al. (2016) används en konsortiumblockchain ofta mellan ett flertal organisationer.

Det finns ett antal fördelar med en privat blockchain, organisationen eller organisationerna som använder blockkedjan kan kontrollera och manipulera data (Buterin, 2015). Ett exempel är möjligheten att återkalla transaktioner, vilket resulterar i att kedjan blir mer flexibel (Buterin, 2015). Transaktioner i en privat blockchain är även billigare när det gäller processorkraft då färre noder behöver verifiera en transaktion och den kan även anses säkrare i det avseendet att alla noder är kända (Buterin, 2015).

Det finns även fördelar med publika blockkedjor (Buterin, 2015). Publika kedjor kan limitera utvecklarnas kontroll över kedjan, vilket kan öka tilliten till systemet (Buterin, 2015). Det kan även omöjliggöra manipulation genom utpressning av utvecklaren då utvecklaren inte har möjlighet att kontrollera vissa eller alla delar av kedjan (Buterin, 2015). Att en publik kedja har möjlighet att få ett betydligt större nätverk än en privat kedja kan även medföra fördelar och man kan till exempel tänka sig att en kedja kan innehålla data från olika branscher men som kan tänkas användas i samma situation (Buterin, 2015). Olika resurser skulle kunna utbytas på ett säkert sätt inom samma blockkedja utan behov av en potentiellt dyr tredje part (Buterin, 2015).

2.1.8 Zero-knowledge proof

Zero-knowledge proof, eller nollkunskapsbevis, är en term inom kryptografi som innebär att det går att bevisa att en viss information är korrekt utan att ta del av innehållet i informationen (Guan et al., 2018). Med nollkunskapsbevis är det alltså inte möjligt att få ut någon mer information än huruvida något är korrekt eller ej (Wu & Wang, 2014).

2.1.9 Ethereum

Ethereum är en öppen plattform baserad på blockchain som kan användas för att bygga decentraliserade applikationer och som många andra blockkedjor har Ethereum en tillhörande valuta, Ether (District0x, u.å.; Ethereum, u.å.).

2.1.10 Privata vs publika nycklar

Public key cryptography eller Asymmetrisk kryptering är en typ av kryptering som använder två nycklar, en publik och en privat, för att dekryptera information (Wander et al., 2005). Denna typ av kryptografi används bland annat i olika säkerhetsprotokoll såsom SSL och IPsec (Wander et al., 2005). I Bitcoin används metoden för att utbyta Bitcoins på ett säkert sätt utan ett behov av tredje parter (Pilkington, 2016). Varje transaktion får en digital signatur som

skickas till mottagarens publika nyckel och signeras med hjälp av avsändarens privata nyckel (Pilkington, 2016). För att ägaren ska kunna använda valuta krävs det att ägaren bevisar sitt ägandeskap med sin privata nyckel (Pilkington, 2016).

2.1.11 Emerging technology

En emerging technology definieras som en ny teknologi som är relativt snabbt växande och har potentialen att radikalt förändra socio-ekonomiska (Rotolo, Hicks, & Martin, 2015). Srinivasan (2008) berättar att emerging technologies har potentialen att både skapa nya industrier och transformera existerande. Det enda som är säkert är att det finns en hög grad av osäkerhet associerad med (Srinivasan, 2008).

World Economic Forum (2016b) listade blockchain som en av tio top emerging technologies år 2016 och Murray (2018) förklarar att blockchain är en emerging technology som snabbt växer fram som en säker plattform för alla typer av transaktioner i digitaliserad form. Teknologin är särskilt tilltalande på grund av att den erbjuder ett effektivt sätt att digitalt bokföra permanenta och verifierbara transaktioner mellan två eller fler intressenter utan behovet av en förmedlare (Murray, 2018).

Även Beck och Müller-Bloch (2017) ser blockchain som en ny teknik som bör uppfattas som banbrytande. Vidare förklarar (Beck & Müller-Bloch, 2017) att blockchain emellertid ger etablerade organisationer betydande utmaningar och ifrågasätter hur de ska svara på tillkomsten av denna innovativa teknik samt hur de kan bygga upp de förmågor som är nödvändiga för att framgångsrikt engagera sig i blockchain.

2.2 Utmaningar med blockchainteknologin

Iansiti och Lakhani (2017) berättar att blockchain har potential att helt förändra de grunder som bygger upp våra finansiella system idag. (Iansiti & Lakhani, 2017) menar också att det kommer att ta årtionden innan blockchain har en betydande roll inom den ekonomiska infrastrukturen och att det kommer att ske gradvis. Den huvudsakliga orsaken till detta är att blockchain är en grundläggande teknologi, likt TCP/IP, och kräver mycket stor koordination (Iansiti & Lakhani, 2017).

Blockchain anses ännu vara en ny teknik och enligt Glaser (2017) är det väldigt få som helt och hållet förstår och kan redogöra för dess funktioner. Anledningarna till detta, menar Glaser (2017), är troligtvis att blockchain är en komplex teknik med många komponenter samt att det saknas en god gemensam kunskapsbas, framförallt inom IS-området. Grewal-Carr och Marshall (2016) ser bristen om medvetenhet kring tekniken som en av huvudutmaningarna för blockchain. Denna brist av förståelse för hur blockchain fungerar hämmar både investeringar och utforskning i konceptet (Grewal-Carr & Marshall, 2016). Lin och Liao (2017) nämner vikten av att försäkra sig om att den nya tekniken inte endast skapar ekonomiska fördelar och att det är viktigt att den även inkorporeras i den traditionella organisationen vilket kan vara en utmaning.

Blockchain skapar mest värde för organisationer när de arbetar tillsammans och det finns ett problem med att organisationer arbetar i en mer traditionell kontext och utvecklar egna blockkedjor och applikationer (Grewal-Carr & Marshall, 2016). Grewal-Carr och Marshall (2016) anser att detta motverkar syftet med blockchain. FinTech Network (u.å.) och Beck och

Müller-Bloch (2017) anser att dessa problem endast kan överkommas med hjälp av samarbeten mellan organisationerna.

Blockchainteknologin anses också kunna komma med regulatoriska utmaningar. Även om teknologin kan användas för att effektivisera system som motverkar penningtvätt kan regler och lagar gällande detta, och krav på kundkännedom, vara ett hinder för implementering av tekniken, menar Glaser (2017). Enligt World Economic Forum (2016a) skiljer sig processerna mellan olika banker och så även de regionala kraven som ställs på dem. Lin och Liao (2017) menar också att blockchainteknologins decentraliserade karaktär kan komma att göra det svårt för centralbankerna att kontrollera ekonomisk policy och penningmängden. Något som gör att regeringar är försiktiga när det gäller blockchain (Lin & Liao, 2017). Nya policys behöver skapas gällande blockchain (Lin & Liao, 2017).

Det finns även ett antal tekniska utmaningar med blockchainteknologin. Zheng et al. (2018) och Lin och Liao (2017) nämner att en blockkedja kan bli väldigt stor om den används mycket. Eftersom alla transaktioner inom kedjan lagras växer den snabbt vid stort användande och kräver då mer datorkraft och lagringsutrymme för att fungera (Lin & Liao, 2017). Zheng et al. (2018) använder Bitcoin som exempel. På grund av en maxstorlek för blocken kan Bitcoin bara hantera 7 transaktioner per sekund, vilket inte alltid är tillräckligt (Zheng et al., 2018). Även FinTech Network (u.å.), förklarar att en av de största utmaningarna med en bred tillämpning av blockchain är frågan av skalbarhet och att lösa problemen med bland annat transaktionshastigheter.

Även om blockchain anses vara en säker teknik nämner Lin och Liao (2017) att det finns säkerhetsrisker. Om en entitet får kontroll över mer än 51 procent av datorkraften kan det betyda att den får auktoritet att godkänna eller neka nya block och detta resulterar i att entiteten kan modifiera transaktionsdata (Lin & Liao, 2017).

2.3 Möjligheter med Blockchainteknologin

Det finns många eventuella fördelar och möjligheter med blockchainteknologin. Den anses kunna effektivisera många processer då den kan förenkla och samla nödvändig information (European Securities and Market Authority, 2016; World Economic Forum, 2016a; Zheng et al., 2018). European Securities and Market Authority (2016) ser även möjligheter att använda DLT-teknik för att förbättra riskhantering och riskrapportering eftersom tekniken kan möjliggöra insamling av nödvändig information till ett och samma ställe. Detta gör i sin tur att informationen blir mer lättillgänglig för bland annat tillsynsmyndigheter (European Securities and Market Authority, 2016). Eftersom transaktioner på en blockkedja kan göras direkt mellan två deltagare menar Zheng et al. (2018) att det finns stora besparingar att hämta när det gäller serverkostnader och man kan undvika eventuella flaskhalsar som finns på en centraliserad server.

Enligt European Securities and Market Authority (2016) är kostnadsreduktioner en av de största eventuella fördelarna med DLT-teknik. Det kan handla om lägre individuella kostnader för företag eller minskade transaktionskostnader på grund av det minskade behovet av mellanhänder (European Securities and Market Authority, 2016). Även Murray (2018) nämner möjligheten att eliminera mellanhänder eftersom blockchainteknologin på ett effektivt sätt permanent sparar all transaktionshistorik mellan olika parter. Zheng et al. (2018) nämner att blockchainteknologin kan leda till rejäla besparingar och effektiviseringar, som resultat av att

transaktioner kan göras decentraliserat. FinTech Network (u.å.) förklarar att det finns många användningsområden för blockchain hos banker och att varje lyckad implementation bör resultera i snabbare transaktioner, mindre friktion, mer stabilitet och mer transparens. Lyckade implementationer bör också innebära reducerade kostnader och mindre administrativt arbete för både bankerna och dess kunder (FinTech Network, u.å.).

Nofer et al. (2017) menar att tilltron ökar till ett DLT-baserat system eftersom ett DLT-baserat nätverk fungerar även om en eller flera noder slutar att fungera till skillnad från ett centraliserat system. Tilltron till systemet ökar även eftersom användarna inte behöver lita till någon specifik annan deltagare eller några mellanhänder (D Bauman, Lindblom, & Olsson, 2017). Även Zheng et al. (2018) anser att ett blockchainbaserat system ger tilltro eftersom transaktionerna dokumenteras över hela nätverket. Detta gör att det i stort sett är omöjligt att på något sätt manipulera det och även om någon skulle försöka ändra data så måste ändringen verifieras av andra noder, vilket gör att förfalskad data snabbt upptäcks (Zheng et al., 2018). Eftersom alla transaktioner är sparade och tidsstämplade kan användare enkelt verifiera och spåra tidigare transaktioner i nätverket (Zheng et al., 2018). Även Lin och Liao (2017) nämner att tekniken är pålitlig eftersom det är transparent för varje nod i systemet och eftersom transaktionshistoriken sparas för evigt.

2.4 Blockchain och KYC

Thomson Reuters (2016) skriver att blockchain teoretiskt sett skulle kunna leverera den perfekta plattformen för en automatisk KYC-lösning som är säker och pålitlig. Den skulle dessutom kunna effektivisera KYC-processen och driften samt ge en bättre kundupplevelse (Thomson Reuters, 2016). Informationen som kunder ger till banker och finansiella institut kan med stor fördel lagras i en blockchain (Thomson Reuters, 2016). Vidare skulle denna blockchain kunna vara öppen för ett flertal finansiella institut och andra auktoriserade organisationer som exempelvis försäkringsbolag, biluthyrningsfirmor och långgivare (Thomson Reuters, 2016). På så vis skulle dessa organisationer inte behöva utföra KYC-processer för varje ny kund och detta skulle leda till reducerade kostnader för organisationerna samt nöjdare kunder (FinTech Network, u.å.; Lootsma, 2017).

Enligt Moyano och Ross (2017) är ökande kostnader på grund av KYC en av bankvärldens största utmaningar just nu och processen är lång framförallt när det handlar om företagskunder. De föreslår därför ett system baserat på DLT-teknik som ska sänka kostnaden för KYC-processen för finansiella institutioner och det ska även, enligt Moyano och Ross (2017), öka kundnöjdheten.

Anledningen till att använda sig av DLT-teknik är enligt Moyano och Ross (2017) att teknologin tillåter att man delar upp kostnaden mellan de olika finansiella institutionerna som behöver tillgång till informationen. Den tar också bort behovet av att samma process upprepas på nytt när en privatperson eller ett företag blir kund hos ett annat finansiellt institut (Moyano & Ross, 2017). Enligt Moyano och Ross (2017) erbjuder DLT-tekniken ett oföränderligt protokoll över informationen i systemet som inte kan matchas av någon annan teknologi. Ett finansiellt institut som åtar sig en ny kund kan verifiera att KYC-processen har utförts av en annat finansiellt institut om så är fallet och med hjälp av DLT-teknik delas kostnaden upp mellan de institut som tar del av informationen (Moyano & Ross, 2017). Kostnaden för individuell KYC-process blir alltså lägre ju fler institut som tar del av informationen (Moyano & Ross, 2017).

Enligt Moyano och Ross (2017) måste tre krav uppfyllas för att systemet de föreslår ska fungera. De deltagande finansiella institutionerna måste följa samma KYC-regleringar och komma överens om kärnprocesser för att verifiera en kund (Moyano & Ross, 2017). De måste även komma överens om en genomsnittlig kostnad för att genomföra KYC-processen för en kund och reglerande myndigheter måste tillåta att systemet används (Moyano & Ross, 2017). Moyano och Ross (2017) anser att man till en början bör implementera systemet på en nationell nivå, för att sedan kunna inkludera ett flertal länder.

Tanken är att när en bank åtar sig en ny kund genomförs KYC-processen med hjälp av systemets applikation och nödvändig dokumentation sparas på bankens databas (Moyano & Ross, 2017). När ett dokument hanteras av banken skapas en hash som länkar till dokumentet i den distribuerade huvudboken (Moyano & Ross, 2017). Om samma kund senare vill använda en annan bank kan kunden själv ge tillgång till de nödvändiga dokumenten åt den nya banken och den nya banken får nu också lov att spara en kopia av nödvändiga dokument i sin databas. (Moyano & Ross, 2017) Kunden skulle i det här fallet vara ägaren av sin egen information, menar Moyano och Ross (2017), något som är kompatibelt med det paradigmskifte angående konsumentdata som håller på att ske i och med bland annat implementationen av GDPR (Moyano & Ross, 2017).

Enligt Moyano och Ross (2017) skulle systemet ha en central part som fungerar som regulator och underhåller systemet. ”Regulatorn” skulle bli en form av tredje part (Moyano & Ross, 2017). Moyano och Ross (2017) nämner att detta skulle kunna vara en svaghet i systemet då en korrupt regulator skulle kunna orsaka problem med att systemet hackas eller utsätts för insiderbedrägeri. Enligt Moyano och Ross (2017) skulle systemet kunna baseras på en publik blockkedja. Det skulle resultera i att behovet av en tredje part försvann och informationen skulle vara svårare att korrumpas (Moyano & Ross, 2017). Trots dessa fördelar förespråkar Moyano och Ross (2017) användandet av en privat distribuerad huvudbok. Anledningen är att risken för en korrupt tredje part i västvärlden anses låg, dokumenten skulle vara mer lättillgängliga samt att banker inte skulle känna sig bekväma med att spara kundernas privata information på en publik distribuerad huvudbok (Moyano & Ross, 2017).

2.5 Innovationsspridning

Diffusion of innovations, eller innovationsspridning, är en teori grundad av Everett Rogers och publicerades först 1962. Teorin ämnar förklara hur nya idéer eller teknologier sprids och den berör även varför och i vilken hastighet innovationen sprids (Rogers, 2010). Eftersom blockchain är en ny teknik, och framförallt är ny för användning inom KYC, använder vi bland annat denna teori som underlag för att försöka förklara teknikens spridning och acceptans inom finansbranschen.

2.5.1 Innovation

Rogers (2010) definierar innovation som en idé, ett beteende eller ett objekt som uppfattas som nytt av en individ eller organisation. Huruvida en idé är ny eller ej spelar, enligt Rogers (2010), ingen större roll - om den uppfattas som ny är det en innovation. Att någonting anses nytt behöver inte nödvändigtvis bero på ny kunskap (Rogers, 2010). En individ kan ha känt till en innovation tidigare men inte ännu utvecklat en positiv eller negativ inställning till

innovationen (Rogers, 2010). Möjligheten att en innovation skulle kunna ha en positiv inverkan på individen motiverar individen att ta reda på mer om innovationen (Rogers, 2010). När tillräcklig information samlats in kan individen eller organisationen ta beslut om innovationen ska implementeras eller ej (Rogers, 2010). Enligt Rogers (2010) är ”Vad är innovationen?”, ”Hur fungerar den?”, ”Varför fungerar den?”, ”Vilka konsekvenser har den?” och ”Vad är innovationens fördelar och nackdelar för mig?” typiska frågor som ställs angående en ny idé.

2.5.2 Innovationsattribut

Enligt Rogers (2010) finns det fem innovationsattribut som hjälper till att förklara innovationers acceptanshastighet: Relativ fördel (”Relative advantage”), Kompatibilitet (”Compatibility”), Komplexitet (”Complexity”), Testbarhet (”Trialability”), Observerbarhet (”Observability”).

En innovations relativa fördel innebär enligt Rogers (2010) hur mycket mer fördelaktig en innovation uppfattas i jämförelse med den idé den ersätter. Innovationens fördel kan mätas ur ekonomisk synpunkt men även sociala faktorer är viktiga (Rogers, 2010). Enligt (Rogers, 2010) är den objektiva fördelen hos innovationen mindre viktig än den uppfattade fördelen hos individen.

Enligt Rogers (2010) mäts kompatibiliteten utefter hur en innovation stämmer överens med individens värderingar, tidigare erfarenheter och behov. En innovation som är kompatibel med existerande värderingar kommer att accepteras snabbare än en som inte är kompatibel (Rogers, 2010). För att en inkompatibel innovation ska accepteras krävs det oftast att samhället eller individen först accepterar nya värderingar (Rogers, 2010).

Rogers (2010) beskriver att en innovations komplexitet mäts i hur svår innovationen är att förstå eller använda. Innovationer som är enkla att förstå eller använda sprids snabbare än de som är svåra att förstå eller använda (Rogers, 2010).

En innovations testbarhet mäts enligt Rogers (2010) i till vilken grad en innovation kan testas av individen innan den implementeras. Om en innovation går att testa innan den implementeras kan den ofta accepteras snabbare menar Rogers (2010). Anledningen är att innovationen då representerar mindre osäkerhet för individen (Rogers, 2010).

Enligt Rogers (2010) mäts en innovations testbarhet i vilken grad innovationens resultat kan ses av andra. En innovation vars effekter kan ses med lätthet av andra individer har en högre grad av acceptans (Rogers, 2010). Detta är enligt Rogers (2010) för att hög observerbarhet skapar diskussioner om innovationen bland olika individer där den som accepterat innovationen kan dela med sig av sin kunskap om den.

3 Metod

I detta avsnitt förklaras den metod som använts till insamlingen av empirisk data och för bakomliggande teorier i studien. Detta följt av en diskussion varför dessa metoder har valts i syfte till att besvara studiens frågeställning på bästa möjliga vis. Vidare beskrivs studiens validitet och reliabilitet samt en metodreflektion där val av metod vidare motiveras samt kritiseras.

3.1 Metodval

Det tillvägagångssätt som valts för denna intervjustudie är en kvalitativ forskningsansats. Detta då (Jacobsen & Sandin, 2002) menar på att en kvalitativ metod är att föredra när man vill skapa en djupare förståelse för ämnet då metoden kan ge en mer nyanserad bild utifrån respondenternas erfarenhet och kompetens. Därmed var det lämpligt att en kvalitativ metod valdes för denna studie eftersom studien ämnar undersöka respondenternas uppfattning om vilka möjligheter och utmaningar det finns med blockchainteknologi och dess användning för KYC.

De intervjuer som genomförts har varit semistrukturerade vilket betyder att intervjuerna har varit baserade på en uppsättning med frågor som kan komma att variera i ordföljd samt att följdfrågor har ställts (Bryman & Bell, 2017; Jacobsen & Sandin, 2002). Bryman och Bell (2017) beskriver att en av fördelarna med kvalitativa intervjuer är att det ges möjlighet till att nå de mer personliga dimensionerna hos respondenterna och på så vis öka möjligheten att få tillgång till dessa personers handlingar och händelser som ses som relevanta för studien.

Litteraturgenomgången är baserad på akademiska artiklar och journaler samt nationella rapporten och företagsrapporter inom bland annat blockchain, KYC, regtech, innovation och emerging technologies. Sökningarna gjordes främst via Google Scholar, LUBsearch och AIS eLibrary där bland andra följande söktermer användes för att besvara frågeställningen: Vad finns det för möjligheter och utmaningar med ett blockchainbaserat KYC-system? För att hålla en god kvalitet på studien har vi så långt som möjligt valt att använda artiklar och journaler som är kvalitetsgranskade eller "peer reviewed". Enligt (Bryman & Bell, 2017) är en kvalitetsgranskad artikel eller journal granskad och håller den kvalitet som krävs för att den ska bli publicerad.

3.2 Urval

För att på bästa sätt kunna besvara frågan: "Vad finns det för möjligheter och utmaningar med ett blockchainbaserat KYC-system?" söktes personer som har arbetat eller arbetar inom finansiella institut med tidigare erfarenhet av blockchain teknologi och KYC. Bryman och Bell (2017) beskriver detta som ett målinriktat urval där respondenter söks baserat deras relevanta erfarenheter inom ämnet. Förutom personer som jobbar inom finansiella institut söktes även personer som jobbar med att tillhandahålla blockchain-baserade KYC lösningar.

I de flesta fall skapades kontakt med respondenterna genom att mejla eller ringa svenska banker och berätta vad studien skulle handla om och be om hjälp att komma i kontakt med rätt personer inom organisationen.

Nedan finns en kort beskrivning om respektive respondent. Beskrivningen innehåller deras yrkesroller och tidigare erfarenheter samt erfarenheter av blockchainteknologin. Detta för att ge legitimitet till studien i deras samlade erfarenhet och kompetens.

Peter (fiktivt namn)

Peter startade som trainee, för cirka sju år sedan, på en anonym bank och har jobbat på företaget sedan dess. De senaste ett och ett halvt åren har han jobbat i en avdelning som heter digitalisering och innovation och förklarar att avdelningen fungerar som en katalysator för att hjälpa organisationen att bli mer innovativ och digital. Hans roll var under en tid ansvarig för bankens blockchainprojekt. Vidare berättar Peter att han fick ett intresse för blockchain privat omkring år 2012/2013 och har sedan dess hållit sig väldigt bekant med utvecklingen och teknologins framfart under privat tid.

Christian Frisch

Christian började jobba på Nordea år 2013 och var då ansvarig för att bygga upp Nordeas interna konsultavdelning. Efter det blev Christian ansvarig för att driva ett simplificeringsprogram på samma bank som bland annat omfattade att minska antalet system som de arbetade med. Efter det blev Christian Head of Digital Process Redesign och ansvarar för digitalisering av online onboarding. Detta innebar bland annat om KYC-processen och införskaffandet av nya kunder online. Christian är även ansvarig för utvecklingen av digitala lösningar inom bolåneerbjudandet och en avdelning som har product owners. Den liknar han vid gamla tidens projektledare som utför olika typer av effektiviseringar inom banken. Christian berättar också att han har ett brinnande intresse för blockkedjor och kryptovalutor och att det är något han spenderar två till tre timmar per dag på både professionellt och privat. Han berättar att han haft detta intresse i drygt tre år och att det är konsekvenserna för samhället och för banker och företag som driver hans intresse.

Nikos Patsiogiannis

Nikos är chief operating officer för Norbloc. Han är från Grekland och har cirka 15 års erfarenhet av industri & management consulting i Europa och i mellanöstern inom den finansiella sektorn. Han berättar att hans erfarenhet har täckt en mängd olika roller och har jobbat med problem som exempelvis kontroll av att lagstiftning följs, KYC, förbättring av arbetsflöden. Han förklarar att företaget, som är baserat i Stockholm, är ett av de första som erbjuder en KYC produkt som baseras på blockchain teknologin.

Ludvig Öberg

Ludvig blev först intresserad av Bitcoin 2011. 2013 startade han, tillsammans med några andra, Safello som hade som ambition att bli den första professionella och reglerade platsen i Sverige för köp- och sälj av Bitcoin. Idag är det Sveriges största växlingstjänst för kryptovalutor. Efter att ha jobbat som affärsutvecklare hos Safello i två år började Ludvig jobba för Chromaway som är ett företag som utvecklar mjukvara baserat på blockchain. Där har han, bland annat, varit en del av ett projekt där svenska Lantmäteriet, skatteverket och då några svenska banker gick tillsammans för att digitalisera fastighetstransaktionen. Idag har Ludvig en egen byrå där han jobbar som konsult samtidigt som han pluggar på högskola.

3.3 Genomförandet av intervjuer

Intervjuerna byggde på en intervjuguide som användes som stöd för genomförandet av intervjuerna (se appendix 1). Däremot kunde frågorna till viss del variera och följdfrågor kunde ställas för mer utvecklande svar och en djupare förståelse eftersom intervjuerna var semistrukturerade (Bryman & Bell, 2017). Frågorna i sig var av öppen karaktär för få fram respondentens egna erfarenheter och för att kunna nå en djupare förståelse av deras individuella tolkningar (Jacobsen & Sandin, 2002).

Litteraturgenomgången låg till grund för intervjuguiden (se appendix 1) som i sin tur baserades på följande teman: Blockchain, KYC, utmaningar och möjligheter. Mindre förändringar i intervjuguiden gjordes då respondenterna delade med sig av information som inte tagits i aktning innan intervjun men som ansågs vara relevant för studien.

Samtliga intervjuer har genomfört över telefon. Bryman och Bell (2017) berättar att fördelar som kommer till att hålla intervjuer över telefon är att det förenklar möjligheten att nå fram till personer som är svåra att nå fram till genom att de inte behöver avvara lika mycket tid samt kunde anpassa intervjutillfället efter deras scheman.

I intervjuerna började vi med att sammanfatta målet med vår studie och vad vi ville undersöka samt introducerade oss själva. Vi kontrollerade med respondenten att den godkände att vi spelade in intervjun samt klargjorde att respondenten har möjlighet att vara anonym om så önskas. En av respondenterna valde att vara anonym. Till sist ställde vi de frågor som vi behövde för att kunna besvara vår frågeställning. Intervjuerna var mellan 25 minuter och en timme. En av intervjuerna fick göras om från hälften på grund av tekniska problem med inspelningen.

3.4 Presentation och analys av datainsamling

För att kunna återge det respondenten säger så korrekt som möjligt har samtliga intervjuer spelats in. Respondenten informerades om att samtalen skulle spelas in och deras godkännande gavs innan inspelningen påbörjades, för att sedan kunna transkriberas (Jacobsen & Sandin, 2002). Vidare gavs respondenterna möjligheten att vara anonyma om så önskades. Att transkribera intervjuerna har varit en vital del för att i ett senare skede kunna analysera och dra slutsatser utifrån de svar som givits (Jacobsen & Sandin, 2002). Samtliga transkriberingar återfinns bland studiens bilagor (se appendix 2-6).

Analysen av transkriberingarna hölls till att börja med så öppen som möjligt för att inte gå miste om viktig information (Jacobsen & Sandin, 2002). Då intervjuunderlaget var relativt okomplicerat krävdes ingen färgkodning eller liknande sortering. Det var därför relativt enkelt att leta fram de svar och synpunkter som var relevanta och hitta mönster i data från intervjuerna (Jacobsen & Sandin, 2002). Analysen baseras på teorin tillsammans med intervjuguiden och den information från respondenterna som vi ansåg vara relevant för vår undersökning, så utmaningar och möjligheter med blockchainteknologin, hur ett blockchainbaserat KYC-system skulle kunna se ut samt möjligheter och utmaningar med ett sådant system.

3.5 Validitet och reliabilitet

En studies reliabilitet syftar, enligt Jacobsen och Sandin (2002), till hur tillförlitlig och trovärdig den insamlade empirin är. Bryman och Bell (2017) förklarar reliabilitet som huruvida resultaten från en studie kan upprepas med samma resultat eller om studiens resultat har påverkats av slumpmässiga faktorer. Då intervjuerna har varit semistrukturerade och ämnet är relativt nytt finns det en viss osäkerhet kring huruvida en likadan studie skulle få exakt samma resultat. Tillförlitligheten i respondenternas svar kunde också variera på grund av intervjueffekten, som Jacobsen och Sandin (2002) beskriver som att svaren och respondenterna kan ha påverkats av intervjuerna. Däremot så har detta tagits i beaktning innan intervjuerna genomfördes och ett försök till att utföra intervjuerna på ett liknande sätt har eftersträvat. Effekten kan dock inte helt uteslutas. Intervjuerna bokades även in i förväg för att se till att respondenterna hade avsatt tid för intervjun och kunde i och med detta ha möjlighet att ge mer genomtänkta svar, vilket Jacobsen och Sandin (2002) beskriver som planlagda intervjuer.

Bryman och Bell (2017) förklarar validitet som att bedöma om studien har undersökt det man hade som avsikt att undersöka och om resultaten av studien är relevanta i sammanhanget, även kallat intern validering. De frågor vi ställt till respondenterna har varit noga utvalda med koppling till syftet med studien. Då intervjuerna var av semistrukturerad karaktär hade vi möjlighet att ställa följdfrågor om vi var osäkra på om frågan hade uppfattats rätt. På så vis öka chansen att vi fick svar på frågan. Den interna valideringen kunde även uppnås genom att respondenterna fick möjlighet att läsa igenom och korrigera transkriberingarna om de önskade så att ingen missuppfattning av deras svar gjorts.

3.6 Etik

Jacobsen och Sandin (2002) berättar att det bör tas hänsyn till etiska aspekter vid utförandet av en studie för att säkerställa att rapporteringen sker på korrekt vis och nämner tre grundläggande krav för att på bästa vis uppnå detta. Dessa krav är följande; informerat samtycke, rätt till privatliv samt krav på riktig presentation av data (Jacobsen & Sandin, 2002).

Genom att fullständigt informera samtliga respondenter om syftet med intervjun och hur den kommer att användas samt att deltagandet givetvis var frivilligt berörs de två viktigaste aspekterna av vad Jacobsen och Sandin (2002) kallar informerat samtycke. Som tidigare nämnt informerades samtliga respondenter om möjligheten att vara anonym innan intervjuerna genomfördes, därmed säkerställdes deras rätt till privatliv.

Kravet på riktig presentation av data har säkerställts genom att samtliga transkriberingarna finns tillgängliga i rapportens bilagor, respondenten gavs möjlighet att läsa igenom transkriberingarna innan påbörjad analys.

3.7 Metodreflektion

Vi fick vid ett tidigt skede bestämma oss för om studien skulle ha ett kvantitativt eller kvalitativt förhållningssätt. Kvantitativ datainsamling har fördelen att resultera i generella slutsatser ofta baserade på siffror och på så vis ofta kan replikeras av andra forskare (Bryman & Bell, 2017). Vi valde en kvalitativ metod då det skapar möjlighet för att undersöka subjektivitet i

form av attityder och motiv inom ett specifikt område (Bryman & Bell, 2017). Detta passade ämnet för studien bättre då vi hade avsikten att skapa en större förståelse för fördelar och nackdelar med blockchainteknologi och dess användning för KYC, samt att vi ville undersöka teorier kring blockchain och jämföra dessa med hur attityden kring dessa såg ut i verkligheten (Jacobsen & Sandin, 2002).

Vi lärde oss att antalet personer som har expertis inom valt forskningsområde är få till antalet och svåra att komma i kontakt med. Därav är antalet respondenter relativt lågt i vår studie. Detta kan komma att påverka trovärdigheten. På grund av detta lade vi stor vikt på urvalet av respondenter och strävade efter en hög kvalitet på samtliga personer.

Den kritik som kan riktas mot valet av semistrukturerade intervjuer har varit de svårigheter som dykt upp i analysen av data, då intervjuerna har påverkats av individuella svar från respondenterna. Detta har påverkat sammanställningen av materialet och gjort det både mer komplicerat att sammanställa och jämföra resultaten, men också tydligt visat på skillnader och likheter i empirin efter genomförd analys.

En viss kritik kan riktas mot att samtliga intervjuer genomfördes över telefon menar Jacobsen och Sandin (2002) att det är lättare att skapa personlig kontakt med respondenten samt avläsa dennes kroppsspråk om mötet sker på plats med personen.

4 Empiri

Syftet med detta avsnitt är att redogöra resultatet från de intervjuer som genomförts. Inledningsvis presenteras samtliga intervjuobjekt som påminnelse om deras roller och erfarenheter, därefter återges en sammanställning av resultaten av studiens intervjuer.

4.1 Presentation av respondenter

Nikos jobbar som Chief Operating Officer på Norbloc. Han har 15 års erfarenhet som industri- och managementkonsult inom finansindustrin i Europa och mellanöstern. Han har hjälpt banker med bland annat regelefterlevnad och kundkännedom.

Ludvig jobbar som konsult, studerar och har även uppdrag kvar på Chromaway, där han arbetat tidigare. Han har tidigare varit med och grundat Safello som nu är Sveriges störst växlings-tjänst för kryptovalutor. Från sin tid på Safello har han erfarenhet av bland annat AML/KYC-system.

Peter som jobbar med digitalisering och innovation på en anonym bank. Han har en teknisk bakgrund och har läst till civilingenjör på KTH. Han har tidigare varit ansvarig för bankens blockchainprojekt.

Christian jobbar som Head of digital process redesign och arbetar för närvarande inom en projektorganisation som jobbar med att förbättra kunders upplevelser av bolåneärenden på Nordea. Han har en bakgrund i informatik och har tidigare jobbat med digitalisering på Nordea och som managementkonsult inom finansbranschen. Christian har också ett stort personligt intresse av Blockchain och kryptovalutor.

4.2 Blockchain

4.2.1 Blockchain idag

I nästa fråga bad vi respondenterna förklara hur banken/organisationen jobbar med blockchain idag. Frågan ställdes för att få en uppfattning av vilket stadie dessa projekt har uppnått.

Peter, som jobbar med digitalisering och innovation, berättar att den anonyma banken har ett antal blockchain projekt igång. Det handlar framförallt om projekt som är i konsortium med andra parter. Han nämner ett projekt som kallas nordic fund ledger, som är i samarbete med de andra storbankerna och går ut på att bygga upp en plattform för att skapa en enighet inom fondhandeln. Han berättar vidare att det finns ett flertal andra projekt som är i produktion, dessa handlar främst om små applikationer som utforskar möjligheterna med blockchain. Han ger ett exempel, ett projekt som handlar om att hålla "a single source of truth" mot större aktörer i andra branscher.

Christian, Head of digital process redesign, börjar med att berätta att de har en del projekt igång, men att mycket av det är konfidentiellt. Det gör att han är begränsad kring vad han kan

delge. Ett projekt som nämns är we.trade. Det är ett projekt där ett tjugotal banker har gått ihop för att utföra transaktioner mellan de olika bankerna. Han berättar att det finns en person som är ansvarig för “emerging technologies” och att blockchain är en stor del av detta. Han förklarar att divisionen jobbar på gruppnivå och att Nordea, som är den största banken i Norden, är uppdelat i olika divisioner i flera länder som alla har olika kulturer. Dock drivs initiativen ute i divisionerna med regelbunden dialog med den blockchainansvarige på gruppnivå. Vidare insinuerar han sin uppfattning av mognadsgraden kring blockchain och säger:

“Vi har en blockkedjefunktion med en person som är ansvarig för hela gruppens blockkedjeinitiativ. Så det vittnar ju lite om var Nordea är i mognadsfasen tror jag och det är inget som reflekterar varken positivt eller negativt med just Nordea, utan jag tror att det gäller hela branschen.” - Christian, Head of digital process redesign

Christian menar också att det finns en intern splittring kring blockchain och dess konsekvenser. Nordea har till och med förbjudit alla anställda att engagera sig i kryptovalutor trots att banken själv driver blockchainprojekt. Det finns alltså inte en gemensam attityd kring kryptovalutor och blockchain. Christian är säker på att majoriteten på Nordea inte känner till blockchainteknologin och gissar att det råder samma okunskap hos andra banker.

Nikos, chief operating officer, förklarar att Norblocs intresse för KYC frågor grundar sig i att de såg att det är ett stort problem och att majoriteten av finansiella institutioner världen över står inför samma problem och att det finns stor potential för förbättring. Samtidigt kan de med hjälp av revolutionära teknologier som blockchain utveckla produkter som är banbrytande i sättet finansiella institutioner kan samla in, lagra, validera och dela KYC-information inom samma grupper och flera olika organisationer. På så vis kan man eliminera dubbelarbete och höja säkerhetsstandarder.

Konsulten Ludvig bekräftar att banker har blockchainprojekt igång där han under sin anställning av Chromaway var delaktig i ett projekt där bland annat svenska banker var involverade för att automatisera fastighetstransaktionen och fastighetstransaktionsflödet. Han berättar att projektet fastnade i huvudsak på grund av bristande lagstiftning där en digital signatur inte ersätter en fysisk signatur i alla delar av lagen i dagsläget.

4.2.2 *Blockchains framtid inom finansbranschen*

Vid frågan om synen på blockchainteknologins framtid inom finansbranschen så svarar både Chief operating officer Nikos och Peter, som arbetar med digitalisering och innovation, att det funnits en stor hype kring konceptet som utlovade lösningar till alla problem som många banker föll för. Därav har de haft det svårt att se den faktiska nyttan teknologin kan bidra med men att nu börjar mognaden öka och användningsområden där teknologin är applicerbar börjar att förtydligas men fortfarande är långt kvar.

”[...] jag tror också den passar idag väldigt bra in under emerging technologies just för att man kan hitta ett sätt att skapa en verktygslåda där nya tekniker också kan vara ett alternativ för att lösa befintliga problem [...] men jag skulle fortfarande säga att vi är långt ifrån en tydlig mognad av blockchain och DLT som koncept och framförallt kanske som, ur ett rent affärsperspektiv så tror jag att mognaden är väldigt låg och förståelsen likaså” - Peter, som jobbar med digitalisering och innovation.

“Sure, so essentially, you know, blockchain is a buzzword in the last, maybe 2 or 3 years, I think we’re very slowly moving from the infant steps to the toddler steps, in the sense that banks gradually start understanding what could be some applicable use cases. [...] in reality there are only a number of use cases that could potentially start being addressed by the banks, and luckily enough, that was also out initial thesis, KYC is one of the most prominent use cases ...” - Nikos Patsiogiannis, Chief operating officer

Även Christian, Head of digital process redesign, håller med om att branschen inte är redo för blockchain och han tror att mognaden kommer att ske väldigt snabbt när den väl börjar få ordentligt fäste.

Christian berättar också att han uppfattar att det råder en kamp mellan centralisering och decentralisering. Han tror att finansbranschen står inför ett liknande hot som musikindustrin gjorde under digitaliseringen av ljudfiler och streamingtjänster som exempelvis Spotify. Christians uppfattning är att banker främst driver centralisering i den utsträckning de är engagerade och att han själv inte stöder det protektionistiska förhållningssättet mot blockchain och kryptovalutor. Samtidigt förstår han varför den attityden dominerar och liknar den okunskap och attityd som fanns mot internets potential när det var ett nytt fenomen.

“Alla banker driver ju centraliseringslinjen i den utsträckning de alls är engagerade. [...] Svårigheten och det som ger långsiktig bärkraft det är ju att försöka hitta hur en öppen blockkedja eller en halvt öppen blockkedja kan tjäna både våra kunder och vi som bankaktörer. Det är väldigt svårt och vi vet inte hur man kan göra det ännu. Men det är mer optimalt att försöka hitta en sån lösning än att kämpa emot och bibehålla kontroll och jag ser i bankbranschen hur den kampen pågår tillsammans med okunskap om vad Bitcoin till exempel och vad blockkedjor över huvud taget är för något och ännu mer vilka potentiella konsekvenser de kan ha för samhället och våra affärsmodeller.” - Christian Frisch, Head of digital process redesign

Konsulten Ludvig anser att finansbranschen var först med att se potentialen med blockchain och att se stora möjligheter med ett decentraliserat nätverk. Han berättar att finansbranschen till en början var väldigt dominant inom blockchain men att en del andra branscher har hunnit ikapp på grund av den rigorösa lagstiftning som lyder inom finansbranschen.

4.2.3 Utmaningar

Vid frågan vilka utmaningar som finns vid implementationen av blockchainteknologin är Peter, som jobbar med digitalisering och innovation, inne på samma spår som Christian, Head of digital process redesign. De menar att blockkedjor bör röra sig mot att vara permission less (public) och att det är den typen av kedjor som Peter ser som det enda alternativet för att kunna leva upp till den nivå av trovärdighet som blockchain teknologin bygger på. Ett problem som även ligger i detta är att hitta ett protokoll som är applicerbart och att det idag inte finns en känd teknik som på effektivt sätt tillhandahåller en permissionless blockchain.

Christian nämner att den största utmaningen just nu är att höja kunskapen kring blockchain teknologin för att över huvud taget kunna identifiera de svårigheter som finns. Det är dessutom svårt att veta när mognadsgraden har blivit tillräckligt hög så att organisationer är på samma nivå och kan fullt ut börja satsa på blockchain projekt. Christian nämner likt Peter att

det finns tekniska utmaningar. Han tar upp exemplet att Ethereum inte kan garantera de transaktionshastigheter som kan komma att krävas samt att när fler människor som använder bitcoins blockkedja ökar väntetiderna och transaktionskostnaderna går upp, då de inte kan hantera mer än 5 till 6 transaktioner per sekund.

En tredje utmaning som Christian ser är lagstiftning kring blockchain och berättar att exempelvis en KYC-process som sparar människors identiteter på en blockkedja aldrig skulle tillåtas under någon lagstiftning. Detta trots att den tekniskt sett skulle vara 100 procent säker.

Nikos, chief operating officer, nämner tre huvudsakliga utmaningar. Den första, som inte har direkt med teknologin att göra men påverkar utvecklingen av den, ligger hos banker internt, är hur snabbt banker kan först förstå blockkedjans användningsområden och hur snabbt de kan ta sig igenom olika mognadsstadier från test till produktion. Han berättar att bankernas förmåga att jobba med innovation och hur snabbt de kan fatta beslut har en stor påverkan på resultatet. Den andra utmaningen han ser är svårigheten att skapa en enlighet hos bankerna och på så vis skapa ekosystem runt blockchain där samtliga parter är överens och eniga över ett tillvägagångssätt. Nikos poängterar den andra utmaningen med att säga:

“If I connect this with my first argument it is quite challenging pushing a big organisation towards a direction to make a decision and start implementing things, you can imagine how, even more difficult, it is to bring 2 or more organisations to work towards the same direction” Nikos, Chief Operating Officer

Den tredje utmaningen som Nikos nämner går även den att knyta till de första två och handlar om svårigheten att skapa en rådande standard. Han berättar att detta är speciellt svårt när det handlar om KYC då det inte finns någon standard inom finansbranschen eller någon annan bransch för den delen. Han menar att det är essentiellt att det finns en standard och utsatta regler för hur KYC processen ska se ut för att en blockchain implementation ska kunna lyckas.

Ludvig, konsult, är inne på samma spår som Nikos när vi pratar om utmaningar som finns för blockchain såsom att få många involverade parter att arbeta tillsammans och hitta en affärsmodell som fungerar. Eftersom blockchain är en sorts infrastrukturs teknik krävs det stora förändringar i både system och i hur arbetsprocesser ser ut. Ludvig anser att det dels finns en generell ovilja för banker att ändra på sina processer, dels att bristen på samarbete har resulterat i att många olika blockchainsystem har utvecklats enskilt hos bankerna som sedan andra banker ej vill ingå i.

“Så det har varit problem med hur man, ja, skapar incitament inom systemen och hur man får folk att koppla ihop sig till ett system. Inom finansbranschen där de är ganska hårda... Ja... man är ganska illvilliga mot varandra så har man problem med att man har gjort massa olika system, ofta inom en bank och sen så har man haft svårt sen att få andra att komma med.” - Ludvig Öberg, konsult.

Ludvig ser även lagstiftning som en stor utmaning då blockchains decentraliserade natur är problematisk för dagens lagstiftning som är utformad för att system har en enskild ansvarig.

4.2.4 Möjligheter

Peter, som jobbar med digitalisering och innovation, Christian, Head of digital process redesign och konsulten Ludvig ser alla tre stora potentiella fördelar med att skapa förtroende med hjälp av blockchain. Det skulle innebära att man inte längre är beroende av olika typer av mellanhänder. Detta skulle vara ett enormt skifte för branschen och ett potentiellt hot mot aktörer som idag agerar som mellanhänder. Peter och Christian anser att banker måste acceptera att det är oundvikligt att teknologin kommer leda till att alla de strukturer som finns idag kommer att bytas ut och gå mot decentralisering. Istället för att kämpa emot det bör hitta nya affärsmodeller som anpassar sig till detta för att kunna dra nytta av den potential som tekniken innebär.

“[...] man får också acceptera det att med den möjligheten så måste också banker hitta ett sätt att förhålla sig till den nya verkligheten, jag tror inte att banker kommer ha det särskilt svårt att göra det egentligen för att jag menar viss av de grejer som man pratar om finns ju kvar, ett banklån löses inte bara för att du kan göra en transaktion gratis, så att, det finns liksom möjligheter för banker att forma om sina affärsmodeller utifrån den enorma möjlighet som finns konceptuellt i blockchain.” - Peter som jobbar med digitalisering och innovation.

“Den största möjligheten är ju egentligen för banker att om de är öppna och kreativa så kan de hitta nya affärsmodeller, nya intäktsmodeller och nya produkter av möjligheterna som blockkedjor erbjuder. Jag vet inte exakt vad det skulle innebära, men jag vet att de finns där. Så det är ju egentligen den största potentiella fördelen.” - Christian Frisch, Head of digital process redesign

Christian ser även möjligheter i att öka säkerheten med hjälp av blockchain samt andra praktiska fördelar som exempelvis minskat pappersarbete.

Även chief operating officer, Nikos, ser stora praktiska möjligheter med blockchainteknologin och de kostnadsbesparingar som kommer i och med det. Det kan eliminera den stora mängd dubbelarbete som sker inom KYC idag, inte bara för finansiella institut utan också för kunderna vilket leder till en ökad kundupplevelse. Detta skulle också leda till att affärer kan ske på ett snabbare och mer effektivt vis och att standarden kommer att öka över hela branschen.

4.2.5 Risker med blockchain

Samtliga intervjupersoner anser att det finns en stor risk med blockchain i dagsläget då teknologin är så pass ny och otestad att det kan vara svårt att se vilka potentiella risker som kan dyka upp i framtiden. Peter, som jobbar med digitalisering och innovation, och konsulten Ludvig nämner också likt det Nikos, chief operating officer, nämnde som en utmaning, det vill säga bristen på standarder. Båda belyser att teknologin är fortfarande så pass omogen att potentiella risker inte har hunnit visa sig och att teknologin måste prövas hårdare för att eventuella risker ska uppenbara sig.

“[...] i dagsläget, och hur utvecklingen ser ut idag, och hur den fungerar finns det enorma risker. Alltså, det tror jag kommer från ett rent mognadsperspektiv, att med tiden och med användning så kommer förstås att de riskerna minska med olika mitigerande effekter som olika aktörer kommer att ha [...] om alla förutsätter att blockchain är helt immutable, att det inte finns några faror i det så kommer det också vara en väldigt stor förvåning sen när

man kanske eventuellt upptäcker att här gick någonting fel.” - Peter, som jobbar med digitalisering och innovation.

“Så bitcoin och Ethereum och liknande kan väl anses vara hyfsat säkra, men det är fortfarande svårt att skriva applikationer till exempelvis Ethereum och vara säker på att det inte finns buggar och liknande. Så det finns inte de här kod standarderna och allt sånt här som skulle krävas för att bygga väldigt säkra applikationer.” - Ludvig Öberg, konsult

Christian, Head of digital process redesign, berättar att den som är tidigt ute med att implementera blockchain riskerar att göra stora misstag som sedan kan undvikas av andra. Detta leder till en form av avvaktande i branschen. En annan risk han tar upp är likt det som nämndes bland de utmaningar som finns det vill säga att banker tappar kontroll och intäkter. Han skiljer på öppna och privata blockkedjor och anser att risken är något högre hos öppna blockkedjor där en större massa behöver skapa förståelse och kunskap och att användarvänligheten kring blockchain idag är väldigt låg.

“[...] om de på något sätt behöver utbilda användare eller få användare att själva använda kedja då kommer det att behöva göras med väldigt intuitiva lösningar, som till exempel när du använder Spotify. Det första E-mail som skickades krävde ju en rymdforskare liksom, och idag gör det inte det.” - Christian Frisch, Head of digital process redesign

Ludvig menar att det framför allt är de privata kedjorna som inte hunnit provas tillräckligt utifrån ett säkerhetsperspektiv och att publika kedjor provas dagligen på grund av dess sammanhang och att de dagligen utsätts för försök att på något vis hackas. Han ser också juridiska utmaningar, som exempelvis det han nämnt tidigare problematiken i att skapa juridiska kontrakt för konsortier.

Utöver att teknologin är ny ser Nikos inga andra direkta risker med blockchain som teknologi. Han berättar att teknologin är tillräckligt skalbar för att kunna leva upp till samtliga krav som banker har gällande bland annat säkerhet och prestanda.

4.3 KYC

Peter, som jobbar med digitalisering och innovation, förklarar att KYC processen är mycket omfattande och att han inte är helt insatt. Banken samlar övergripande in KYC-information bland annat utifrån de krav som ställs av myndigheter. Informationen som samlas in ska ge ett underlag till att bevisa att personer är de personer som de säger att de är och att pengar kommer från de källor som anges. Peter berättar att finansiella verksamheter har en stor tilltro till att blockchain ska kunna skapa nya förutsättningar för KYC. Han nämner projekt som han anser vara bra exempel på en lyckad KYC struktur hos bland annat the royal bank of Canada och Norbloc.

Head of digital process redesign på Nordea, Christian, förklarar att mycket av KYC-processen är digitaliserad idag. Dock finns fortfarande många manuella inslag som exempelvis att anställda måste ringa upp kunder för att komplettera eller klargöra otydlig information. Han berättar också att det är fler manuella inslag på företagssidan jämfört med den hos privatkunder, då processen inte är lika standardiserat samt mer rigorös. Christian tycker att Sverige är

duktiga och har kommit långt inom automatiseringen av KYC och uppskattar att processen som helhet är ca 70 procent automatiserad men att det finns många hundratals personer inom Nordea som jobbar med manuella KYC processer.

Nikos, som tidigare har erfarenhet av rådgivning inom KYC, berättar att det i dagsläget finns stort utrymme till förbättring då att finansiella institut är präglade av dubbelt och manuellt arbete. Han ser avsaknaden av en branschstandard för KYC som ett stort problem som bidrar till detta.

Konsulten Ludvig som byggde ett eget KYC-system under tiden han jobbade för Safello förklarade processen som att kunden fyllde i ett digitalt formulär som inkluderade:

“Identifiera personen då med pass eller ID eller liknande, identifiera adress med någon sorts räkning av något slag, elräkning, hyresräkning eller liknande, svara på frågor om din riskprofil och var pengarna kommer ifrån och vad pengarna ska användas till och liknande.” - Ludvig Öberg, konsult

4.3.1 Utmaningar och problem med dagens KYC-process

Christian, Head of digital process redesign nämner att ett stort problem med dagens KYC-process är att man inte riktigt kan lita på den informationen som man har. Det utförs mycket manuellt arbete i form av uppdatering av kundinformation samt monitorering av transaktioner. Enligt Christian kommer detta med stora personalkostnader. Det är dock inte alla delar av kundkännedomen som är så tids och resurskrävande, för att bli ny kund som privatperson kan det ibland räcka med att svara på ett antal frågor i mobilappen. Den processen är alltså helt digitaliserad och innebär inget manuellt arbete för banken.

Christian ser även att det skulle vara en fördel att bara ha ett system för KYC där informationen är samlad men att han tror att det kommer att bli svårt att lösa. I dagsläget finns det olika system för KYC i de olika länder där Nordea är verksamma. En annan utmaning som Christian ser är i lagstiftningen GDPR. Han nämner att den har blivit mindre eftersom Nordea, och även de flesta andra banker, vad han förstår numera är kompatibla med lagstiftningen. Enligt Christian blir utmaningen blir också mindre av att banker till ganska stor del är undantagna från lagstiftningen, då de har kvar på sig att samla information om kunder som många andra typer av företag inte behöver eller får göra.

Peter, som jobbar med digitalisering och innovation, diskuterar detta utifrån hur en Blockchain-lösning skulle kunna förbättra processen. Ett problem som en Blockchain baserad lösning skulle kunna lösa är att man idag ibland överlämnar information till någon annan och att man då inte riktigt vet hur informationen kommer att användas.

Nikos, chief operating officer nämner att dubbelt arbete är väldigt vanligt när det gäller KYC. Eftersom banker i dagsläget inte delar någon information angående kundkännedom, upprepas liknande eller identiska processer i samma kunds kontakt med olika banker. Detta är en stor kostnad för bankerna och även något som kan skada kundens upplevelse.

Ludvig, konsult, har tidigare erfarenhet av KYC-processen från Safello och vi frågar om vilka utmaningar de stötte på relaterat till KYC. Ludvig upplevde att det fungerade ganska bra i Sverige, men att det framförallt kunde bli utmanande när de behövde identifiera personer med identitet från andra länder. De kunde också ibland få falska identitetshandlingar. Det kunde

också vara en utmaning att avgöra om en transaktion i en kryptovaluta faktiskt görs av den personen som den utger sig för att vara.

4.4 Hur en blockchainbaserad KYC-lösning kan se ut

Christian, Head of digital process redesign, skulle helst se en lösning baserad på en publik blockkedja där kundens identitet och kundkännedom finns registrerad. Kunden skulle då kunna välja vem som ska få tillgång till informationen och när detta ska ske. Antingen skulle kunden eller banken kunna betala en liten kostnad. Christian använder 50 öre som ett exempel för att informationen skulle delas. Han nämner att baserat på vad vi vet idag skulle en sådan lösning vara helt säker ur ett tekniskt perspektiv men att fel uppgifter skulle kunna anges vid till exempel hot eller liknande. Christian menar att om lösningen skulle baseras på en privat blockkedja, som bankerna själva äger, skulle de huvudsakliga fördelarna vara för bankerna.

Peter, som jobbar med digitalisering och innovation, nämner en liknande lösning och tar upp Norbloc och IBMs lösningar som exempel. I grunden skulle lösningen kunna vara en potentiellt global blockkedja där varje person själv styr över sin information och vem som har tillgång till den. Även Peter tycker att framtida lösningar borde baseras på publika blockkedjor. Peter ser inte att lösningar baserade på privata kedjor skulle skilja sig så mycket från bankernas nuvarande system.

Chief operating officer, Nikos, berättar i stora drag om hur Norblocs KYC-plattform fungerar. Då en kund behöver ange information för kundkännedom får kunden en länk till ett digitalt formulär. Om det är en företagskund hämtas även publikt tillgängliga data så att de fälten kan fyllas i automatiskt. Kunden fyller i det som krävs i formuläret och laddar upp andra nödvändiga dokument och signerar sedan med BankID eller liknande. Informationen som kunden har fyllt i kontrolleras och valideras sedan av banken. Om banken beslutar att godta informationen så sparas en hash av informationen på blockkedjan. Kunden har sedan tillgång till en portal där det går att uppdatera informationen. Det går även att be om att få sin data borttagen eller att sluta dela sin information med en viss bank. Om kunden väljer att bli kund i en annan bank finns det möjlighet att dela informationen med den nya banken. Den nya banken kan sedan välja att lita på den första bankens validering av informationen eller utföra sin egen valideringsprocess.

Enligt Nikos är systemet baserat på en privat blockkedja. Anledningen, enligt Nikos, är att de måste kontrollera vem som får ha noder i systemet och vem som får validera information. I det här fallet finansiella institutioner. För att vara kompatibla med GDPR sparas inte kundens data på blockkedjan. Blockkedjan innehåller hashar som pekar på var och på vilken server informationen finns i systemet. Kundens data delas upp i så små bitar som möjligt, krypteras och placeras över flera noder i systemet. Detta resulterar i att bara de finansiella institutionerna som har rätt till informationen kommer åt den.

Konsulten Ludvig ser en lösning där kunden endast behöver ladda upp sina dokument upp svara på frågor en gång. Kunden signerar sedan med sin privata nyckel och informationen skulle sedan kunna delas med de aktörer som behöver den. Enligt Ludvig skulle man till och med kunna använda "zero-knowledge proof" för att kunna bevisa att en bank har verifierat ens identitet. Detta utan att den data som faktiskt innehåller känslig information behöver delas mellan banker. Ludvig menar att det kan vara svårt att dela kundens data mellan banker på

grund av banksekretessen. Ludvig tror att det nog skulle vara bäst att använda en privat blockkedja eftersom det skulle bli dyrt med många transaktioner på en publik kedja.

4.4.1 *Fördelar för kunder*

Christian, Head of digital process redesign, nämner ett antal fördelar med blockchainbaserat KYC-system så som han beskriver det. Han menar att det skulle underlätta för kunden när de behöver legitimera sig och uppge nödvändig kundinformation förutsatt att det kan göras behändigt och intuitivt. Han nämner också att kunderna kan känna sig säkra, då tekniken bakom skulle vara väldigt säker. Även möjligheterna för kunderna att äga sin egen information ser Christian som en fördel då integriteten är mycket viktig.

Nikos, chief operating officer, säger att processen för kunderna blir fullt digitaliserad och snabbare. De behöver inte heller uppge samma information till flera aktörer. Kunderna kan även uppdatera sin information på ett ställe då alla banker som har fått tillgång till kundens information får då ta del av den uppdaterade informationen. Enligt Nikos leder detta till en bättre upplevelse för kunden

Även Ludvig tror att kundkännedomsprocessen skulle kunna göras mer digitaliserad och effektiv för kunden med hjälp av blockchain. Han ser det också som en fördel att kunden endast skulle behöva svara på frågor och ladda upp nödvändiga dokument till en aktör för att sedan kunna dela detta med fler aktörer som behöver verifiera kunden. Enligt Ludvig skulle detta även kunna innebära fördelar för kundens integritet och kunden skulle själv kunna ha större kontroll över sin identitet.

4.4.2 *Fördelar för bankerna*

Christian, head of digital process redesign, nämner effektivisering som en fördel med ett KYC-system baserat på blockchain. Hanteringen av kundens data skulle kunna gå betydligt snabbare. Även god regelefterlevnad ser han som en fördel eftersom systemet skulle kunna följa reglerna till 100 procent. Med anledning av detta riskerar man inte att få böter från Finansinspektionen. Christian säger även att man skulle kunna lita på informationen i en större utsträckning.

Nikos, chief operating officer, nämner också effektivisering som en fördel. Eftersom man inte behöver upprepa hela processen för KYC, då en kund redan utfört den hos en annan bank, finns det möjlighet att spara mycket tid. Det leder till mindre manuellt arbete och lägre kostnader. Precis som Christian nämner han regelefterlevnad som han ser skulle kunna förbättras över hela marknaden eftersom man har möjlighet att skapa en mer komplett bild av kunden.

Peter, som jobbar med digitalisering och innovation, ser möjligheten att vidare digitalisera som en fördel. En helt digitaliserad lösning skulle kunna leda till nya processer, nya idéer och nya affärsmodeller. Han ser även att det skulle vara lättare att garantera kundens identitet.

Den största fördelen som Ludvig ser för bankerna med en KYC-system baserat på blockchain är besparing.

”Man lägger ju hur mycket som helst på compliance och massa manuella kontroller. Då skulle man kunna automatisera mycket av det här och att det

räcker med att en eller några aktörer gör den här kollen så kan alla andra dela den datan...” – Ludvig Öberg, konsult.

Ludvig nämner även att det skulle kunna leda till ett bättre samarbete mellan bankerna för att lättare kunna upptäcka misstänksamma transaktioner och beteenden hos kunder. Detta kan enligt Ludvig vara svårt idag eftersom bankerna inte delar kundinformation.

4.4.3 Utmaningar med implementation

Christian, head of digital process redesign, ser en utmaning i att blockchainteknologin är ny och inte ännu brett accepterad. Han jämför blockchain idag med internet och E-mail på 90-talet. Eftersom tekniken inte var mogen förstod man inte vad man skulle använda den till. Christian ser även att det pågår en konflikt mellan privata och publika kedjor. Han ser blockkedjetekniken som ett hot mot mellanhänder eftersom tekniken kan reducera behovet av mellanhänder. Christian nämner att eftersom banker är mellanhänder i många aspekter så kan det även ses som ett hot mot banker.

Peter, som jobbar med digitalisering och innovation, säger att det nog finns ett stort antal utmaningar med att implementera en KYC-lösning baserad på blockchain. Han nämner att det kan vara svårt att bygga något som alla tror på för att få med tillräckligt många aktörer. Peter säger även att det kan vara svårt att garantera säkerheten. ”... det måste vara något som kräver ett sådant enormt engagemang av många olika parter skulle jag säga.” – Peter, som jobbar med digitalisering och innovation

Nikos, chief operating officer, ser tre huvudsakliga utmaningar. Den första han nämner är svårigheten för bankerna att ta sig från en teoretisk fas till faktisk produktion. Enligt Nikos beror detta på att blockchain är ett relativt nytt koncept för bankerna och att de kan vara långsamma när det gäller att börja använda ny teknik. Den andra utmaningen Nikos nämner är svårigheten att samla tillräckligt många aktörer för att kunna bygga ett ekosystem som drar fördel av blockchainteknologin. Enligt Nikos är den största anledningen till att man använder blockchain att man på ett säkert sätt kan dela data mellan aktörer. Om inte tillräckligt många aktörer deltar blir teknikens fördelar mindre tydliga. Den tredje utmaningen som Nikos nämner är att det saknas standarder för KYC mellan olika marknader. Han nämner att till exempel formulär och procedurer för att verifiera information skiljer sig mellan bankerna. Nikos säger att man behöver få bankerna att komma överens om en standard för KYC, men att detta, framförallt utan att standarder sätts av myndigheter, kan vara en stor utmaning.

Konsulten Ludvig ser utmaningar i hur infrastrukturen ska byggas upp, vem som ska ha tillgång till vad och vem som ska sköta systemet. Han tror även att det kan bli en utmaning att komma fram till hur systemet ska finansieras. Han ser också en risk i att många kommer att försöka undvika att genomföra KYC-processen eftersom den är kostsam och i stället välja att outsourca uppgiften till en annan aktör som använder sig av systemet. Enligt Ludvig måste det därför finnas en incitamentsstruktur vilket är något som han ser som en utmaning. Han tror även att den juridiska delen kan bli svår att hantera och nämner till exempel GDPR och rätten att bli bortglömd.

5 Analys

Här kommer den insamlade empirin analyseras och jämföras med den insamlade data som avsnitt tre presenterar. Inledningsvis presenteras en allmän vy kring blockchain teknologin och fortsätter med att presentera de utmaningar och problem som är involverade i dagens KYC process. Avslutningsvis presenteras hur en blockchain baserad KYC lösning kan se ut samt vilka fördelar och utmaningar som kommer med detta.

5.1 Finansbranschens syn Blockchain

5.1.1 Blockkedjans framtid inom finansbranschen

Iansiti och Lakhani (2017) berättar att blockchain har potentialen att helt förändra de grunder som idag bygger upp våra finansiella system. Rogers (2010) förklarar att en innovation som är kompatibel med existerande värderingar kommer att accepteras snabbare än en som inte är kompatibel. Då blockchain har förmågan att förändra många grundläggande funktioner, och påverkan av teknologin kommer vara stor, kommer det att ta årtionden innan blockchain har en betydande roll inom den ekonomiska infrastrukturen och att det kommer att ske gradvis (Iansiti & Lakhani, 2017). Blockchain är en komplex innovation som kan vara svår att förstå. Rogers (2010) förklarar att innovationer som är enkla att förstå eller använda sprids snabbare än de som är svåra att förstå eller använda. Det tog cirka trettio år för protokollen TCP/IP att gå igenom alla dess utvecklingsfaser (Iansiti & Lakhani, 2017). Christian, head of digital process redesign, likt Iansiti och Lakhani (2017), liknar blockkedjans potential till förändring med den hos TCP/IP och internet och tror även han att utvecklingskurvan kommer se liknande ut. Till skillnad från Iansiti och Lakhani (2017), som tror att utvecklingen konstant kommer ske långsamt och gradvis, tror Christian att när de första långsamma stadierna har passerat så kommer utvecklingen och adoptionen ske blixtsnabbt.

Peter, som jobbar med digitalisering och innovation, och Nikos talar om att det har varit svårt för banker att få ett grepp om blockchain och se dess potential och att konceptet har varit omringat av en hype som har varit vilseledande. Carson et al. (2018) förklarar att blockchain fortfarande är en omogen teknologi vars marknad är under uppkomst och att det inte finns några tydliga framgångsfaktorer än. Många av de satsningar som finns inom blockchain idag kommer inte se någon avkastning på investerat (Carson et al., 2018). Christian menar att finns en form av avvaktande i branschen på grund av denna osäkerhet och risk.

Carson et al. (2018) skriver att bortom hypen har blockchain ett strategiskt värde hos organisationer som möjliggör kostnadsbesparingar utan att organisationen löper risken att förlora sin funktion som mellanhand. På lång sikt har teknologin förmågan att skapa helt nya grunder för nya affärsmodeller (Carson et al., 2018). Både Peter och Christian ser stora möjligheter och utmaningar för banker att anpassa sina affärsmodeller utifrån den möjlighet som konceptuellt finns i blockchain. Kaletovic (2018) argumenterar att det är omöjligt att neka att blockchain kommer ha en stor roll i framtiden och Furlonger och Valdes (2017) berättar att det kommer att gå långsamt men att det är oundvikligt.

5.1.2 Utmaningar

FinTech Network (u.å.), förklarar att en av de största utmaningarna som står framför en bred tillämpning av blockchain är frågan om skalbarhet det vill säga att lösa problemen med bland annat transaktionshastigheter. Både Peter, som jobbar med digitalisering och innovation, och Christian ser också tekniska utmaningar där Christian nämner transaktionshastigheter som en av de huvudsakliga medan Peter nämner att det idag inte finns någon teknik som på ett effektivt vis tillhandahåller en permissionless blockchain.

Grewal-Carr och Marshall (2016) ser bristen om medvetenhet kring tekniken som huvudutmaningen för blockchain och denna brist av förståelse för hur blockchain fungerar hämmar både investeringar och utforskning i konceptet. Christian nämner i intervjun, likt Grewal-Carr och Marshall (2016), att höja kunskapen kring blockchain tillhör de största utmaningarna och det är svårt att veta när mognadsgraden har blivit tillräckligt hög så att organisationer som är på samma nivå kan börja satsa fullt ut på blockchainprojekt. Grewal-Carr och Marshall (2016) nämner också att blockchain skapar mest värde för organisationer när de arbetar tillsammans. Dessutom finns det ett problem med att organisationer arbetar i en mer traditionell kontext och utvecklar egna blockkedjor och applikationer (Grewal-Carr & Marshall, 2016). (Grewal-Carr & Marshall, 2016) anser att detta motverkar syftet med blockchain och FinTech Network (u.å.) och Beck och Müller-Bloch (2017) anser att dessa problem endast kan överkommas med hjälp av samarbeten mellan organisationerna. Nikos instämmer att organisationer bör gå ihop konsortium och tillsammans skapa lösningar och ser det som en stor utmaning. Ludvig instämmer också och ser problem i att banker har svårt att samarbeta på grund av rädslan över att konkurrenter har mer att vinna.

5.1.3 Möjligheter

Peter, Christian och Ludvig talar alla om hur blockchain kan skapa förtroende mellan organisationer utan att vara beroende av en tredje organisation som intermediär. David Bauman, Lindblom, och Olsson (2016) förklarar att transaktionskostnader minskas när behovet av mellanhänder elimineras och att blockchain fungerar i sin helhet som den betrodda parten i transaktionen. FinTech Network (u.å.) förklarar att det är tydligt att det finns många användningsområden för blockchain för banker och att varje lyckad implementering bör resultera i snabbare transaktioner, mindre friktion, stadigare, mer transparens och oföränderlighet. Lyckade implementeringar bör också innebära reducerade kostnader och administrativt arbete för både bankerna och dess kunder (FinTech Network, u.å.).

5.2 KYC

5.2.1 Utmaningar och problem med dagens KYC-process

Två av respondenterna, Christian, head of digital process redesign och Nikos, chief operating officer, nämner att mycket manuellt arbete och personalkostnaderna är utmaningar med dagens KYC-process. Nikos nämner också att mycket dubbelt arbete utförs. Detta på grund av att processen måste upprepas varje gång en person eller ett företag blir kund i en ny bank. Deras svar är i enighet med Moyano och Ross (2017) som identifierar stora kostnader som ett stort problem med KYC idag.

Nikos beskriver att det dubbla arbetet och det faktum att kunder behöver göra om samma process varje gång skadar kundens upplevelse. Moyano och Ross (2017), FinTech Network (u.å.) och Thomson Reuters (2016) hävdar alla att en blockchainbaserad KYC-lösning skulle kunna leda till en bättre kundupplevelse.

Peter nämner att man idag ger ut personlig information till bankerna utan att riktigt vara säker på hur informationen kommer att användas. Han säger att detta skulle kunna avhjälpas med ett blockchainbaserat KYC-system. Moyano och Ross (2017) hävdar att detta skulle vara möjligt i ett sådant system där kunden skulle få större kontroll över sin information.

Både Ludvig och Christian nämner svårigheten med att veta om den information och de dokument som skickas in till banken vid KYC-processen är korrekt. KPMG International (2018) uppskattar att endast ungefär 20 procent av arbetet med KYC-process går till att faktiskt bedöma informationen som samlas in vilket ökar risken för att felaktig information godkänns.

5.3 KYC och blockchain

5.3.1 Hur en blockchainbaserad KYC-system skulle kunna se ut

Samtliga respondenter har en liknande bild över hur ett blockchainbaserat KYC-system skulle kunna se ut. Gemensamt för alla respondenter är att de ser ett system där kunden har möjlighet att dela med sig av sin information till de banker eller finansiella institut som behöver den. Detta är ett sätt att slippa att upprepa KYC-processen för varje nytt finansiellt institut som de vill bli kunder hos. Detta är helt i linje med den typen av system som Moyano och Ross (2017) och FinTech Network (u.å.) beskriver.

Nikos, cheif operating officer på Norbloc, berättar att för lösningen som de utvecklat fyller kunden i sin information och laddar upp nödvändiga dokument i ett digitalt formulär. Förutsatt att banken validerar och godkänner informationen skapas en hash av informationen på blockkedjan. Kundens information sparas alltså inte direkt på blockkedjan. Detta system liknar det som Moyano och Ross (2017) beskriver där även de förespråkar att endast hashar som länkar till informationen ligger på blockkedjan. Konsulten Ludvigs förslag skiljer sig något ifrån detta då han ser att man skulle kunna använda sig av nollkunskapsbevis eller ”zero knowledge proof” för att undvika att bankerna skickar potentiellt känslig kundinformation mellan varandra. Med nollkunskapsbevis är det möjligt att bevisa att information är korrekt utan att ta del av den Guan et al. (2018). Ett finansiellt institut skulle då kunna få bevis för att ett annat har genomfört KYC-processen med en viss kund, utan att ta del av kundens information enligt Ludvig.

Respondenterna är dock inte överens om vilken typ av blockkedja som bör användas. Christian, head of digital process redesign, och Peter, som jobbar med digitalisering och innovation, förespråkar båda en publik blockkedja. Christian menar att om en privat blockkedja skulle användas skulle det huvudsakligen vara en fördel för de finansiella instituten men inte för kunden. Peter menar att en lösning baserad på en privat blockkedja inte skulle skilja så mycket från bankernas nuvarande system. Ludvig tror att det skulle vara bäst att använda en privat blockkedja. Detta med hänsyn till att en publik kedja skulle bli för dyr att driva på grund av en stor mängd transaktioner. Även Nikos anser att en privat blockkedja passar bäst och förklarar att det är just en privat blockkedja som Norblochs lösning använder sig av.

Anledningen är, enligt Nikos, att de måste kunna kontrollera vem som får vara en del av systemet och vem som får validera information. Moyano och Ross (2017) ser fördelarna med en publik blockkedja men förespråkar ändå en privat sådan. Anledningen enligt Moyano och Ross (2017) är att kunna ha större kontroll och för att kunna dela kostnaden mellan deltagarna i systemet vilket är i likhet med vad Nikos menar på.

5.3.2 *Fördelar för kunder*

Samtliga respondenter är överens om att ett blockchainbaserat KYC-system skulle kunna underlätta för kunden. Christian, head of digital process redesign, Nikos, cheif operating officer och Ludvig, konsult, nämner alla att KYC-processen skulle kunna göras effektivare och lättare från kundens perspektiv. Detta stämmer överens med vad Moyano och Ross (2017), FinTech Network (u.å.) och Thomson Reuters (2017) skriver. Enligt respondenterna blir kundens upplevelse bättre eftersom det skulle vara möjligt att, till större del, digitalisera processen. De menar också att kunderna enbart skulle behöva genomföra den en enda gång för att sedan kunna dela informationen med samtliga anslutna finansiella institut.

Både Christian och Ludvig nämner ökad integritet som en fördel. Kunden skulle till större del ha kontroll över och äga sin egen information vilket de båda ser som en fördel. Moyano och Ross (2017) menar att ge kunden kontroll över sin egen data är en fördel som är kompatibel med dagens syn på integritet som håller på att skifta i och med till exempel införandet av GDPR.

Christian ser även att ett blockchainbaserat KYC-system skulle göra att kunderna kände sig säkrare eftersom tekniken bakom är mycket säker. Detta är i enighet med Zheng et al. (2018) och Lin och Liao (2017) som anser att blockchainteknologin är säker och pålitlig eftersom den är anpassad för att direkt upptäcka förfalskade eller korrumpade data samt håller hög transparens.

5.3.3 *Fördelar för finansiella institut*

Christian, head of digital process redesign, Nikos, chief operating officer och konsulten Ludvig nämner alla effektivisering som en fördel för de deltagande finansiella institutionerna i ett blockchainbaserat KYC-system. Detta är i enighet med vad Moyano och Ross (2017), Thomas Reuters (2017), Fintech network (2017) och Lootsma (2017) beskriver. Christian förklarar att datahantering skulle kunna gå betydligt snabbare och att man i större utsträckning skulle kunna lita på informationen. Även Peter, som jobbar med digitalisering och innovation, säger att det skulle bli lättare att garantera kundens identitet.

Enligt Nikos och Ludvig kommer effektiviseringen medföra stora besparingar. Ludvig säger att mycket resurser läggs på KYC idag och att man med ett blockchainbaserat KYC-system skulle kunna automatisera många av de dyra processerna. Detta är i enighet med vad Moyano och Ross (2017), Thomson Reuters (2017), FinTech Network (u.å.) och Lootsma (2017) skriver. Enligt Rogers (2010) kan en större relativ fördel, till exempel ur ekonomisk synpunkt, leda till snabbare acceptans av tekniken.

Christian och Nikos nämner båda att systemet skulle kunna möjliggöra högre grad av regellevnad eftersom man skulle kunna skapa en mer komplett bild av kunderna. Även Ludvig nämner att ett blockchainbaserat KYC-system skulle kunna förbättra samarbetet mellan bankerna och därigenom skulle man lättare kunna upptäcka misstänksamma beteenden hos

kunder. Enligt Svenska Bankföreningen (2017) är detta huvudsyftet med kundkännedomspromessen.

5.3.4 Utmaningar med en implementation

Christian, head of digital process redesign och Nikos, chief operating officer, menar att en utmaning med att implementera ett blockchainbaserat KYC-system är att blockchain är en ny teknik som ännu inte är brett accepterad inom finansbranschen. Detta är i enighet med vad Iansiti och Lakhani (2017), Glaser (2017) och Grewal-Carr och Marshall (2016) skriver. Glaser (2017) menar att detta kan bero på att blockchain är en komplex teknik med många komponenter. Detta kan enligt Rogers (2010) göra att tekniken accepteras långsammare.

Nikos, Peter, som jobbar med digitalisering och innovation, och konsulten Ludvig, ser en utmaning i att få ett fungerande samarbetet mellan deltagarna i systemet. Peter säger att det skulle krävas ett stort engagemang från flera aktörer och att det kan vara svårt att få alla deltagare att tro på lösningen. Även Nikos nämner att det kan bli utmanande att samla tillräckligt många aktörer och säger att blockchainteknologins fördelar blir mindre tydliga utan tillräckligt många deltagare i systemet. Nikos säger också att det saknas en standard för KYC-processen, något som Moyano och Ross (2017) listar som ett krav för att ett blockchainbaserat KYC-system ska fungera.

Christian nämner att blockchainteknologin kan ta bort behovet av mellanhänder. Detta nämner även European Securities and Market Authority (2016) och Murray (2018). Enligt Christian så kan bankerna se detta som ett hot, eftersom de i många aspekter fungerar som mellanhänder.

Ludvig säger att den juridiska biten kan bli en utmaning, så som till exempel att få systemet förenligt med GDPR och rätten att bli bortglömd.

6 Slutsats

Syftet med uppsatsen var att redogöra för finansbranschens syn på blockchainteknologin och utmaningarna och möjligheterna med ett blockchainbaserat KYC-system. Detta gjorde vi genom att försöka svara på frågan:

- Vad finns det för möjligheter och utmaningar med ett blockchainbaserat KYC-system?

Baserat på vår studie har vi identifierat ett antal möjligheter och utmaningar med ett blockchainbaserat KYC-system.

Baserat på insamlade data ser vi att de huvudsakliga utmaningarna med blockchainteknologin handlar om att tekniken är ny och att förståelsen för den är låg inom finansmarknaden, vilket hämmar investeringar och implementationer.

De huvudsakliga möjligheter som har identifierats med blockchainteknologin är effektivisering, besparingar, transparens och möjligheten att skapa förtroende mellan organisationer utan behovet av mellanhänder.

Baserat på den data som samlats in ser vi att dagens KYC-process är långsam, dyr och har ofta många manuella inslag. Den behöver även upprepas för samma person eller företag, varje gång personen eller företaget väljer att bli kund i ett nytt finansiellt institut.

Möjligheter med ett blockchainbaserat KYC-system har identifierats som högre effektivitet, lägre kostnader, mer digitalisering och högre kundnöjdhet. De finansiella instituten skulle kunna hålla högre regelefterlevnad och erbjuda bättre säkerhet.

Utmaningar med att implementera ett blockchainbaserat KYC-system har identifierats som låg acceptansnivå på grund av ny och komplex teknik, krav på ett stort samarbete mellan många aktörer och avsaknad av standarder.

6.1 Vidare forskning

Vår studie är utförd i Sverige och involverar 4 aktörer på den svenska marknaden. På grund av det relativt låga antalet respondenter kan resultaten inte generaliseras. Vi har inte tagit hänsyn till andra länders KYC-processer eller syn på blockchainteknologin och om studien skulle utföras i ett annat land kan den ge ett annorlunda resultat. Därför behövs ytterligare forskning för att kunna generalisera resultaten.

Appendix 1

Intervjufrågor

- Kan du berätta lite om dig själv, dina tidigare erfarenheter och din roll inom företaget? (Vad har du för erfarenhet av Blockchain/DLT?)
- Hur jobbar ni med Blockchain/DLT idag?
 - Om det finns nuvarande projekt: Berätta gärna lite om projektet.
 - Om det finns framtida planer: Berätta gärna lite om framtiden för blockchain/DLT inom företaget.
 - Om det inte finns några planer: Vad är anledningen till att ni inte planerar att använda blockchain/DLT?
- Hur ser du på Blockchain/DLTs framtid inom finansbranschen i stort?
- Vad ser du som de största utmaningarna med att implementera Blockchain/DLT?
- Vad ser du som de största möjligheterna med att implementera Blockchain/DLT?
- Vad ser du för risker med Blockchain/DLT teknik?
- Hur ser er KYC-process ut idag?
- Vad ser du som de största utmaningarna/problemen med KYC idag?
- Tror du att Blockchain/DLT teknik kan hjälpa till att förbättra KYC-processen och lösa några av de eventuella problem som finns idag?
- Hur tror du att en sådan lösning skulle kunna se ut?
 - Vilken typ av blockchain/DLT tror du skulle passa bäst för en sådan lösning?
- Vad skulle det kunna innebära för fördelar för kunder?
- Vad skulle det kunna innebära för fördelar för verksamheten?
- Vad ser du för utmaningar med att implementera en sådan lösning?
- Nu när du vet vårt syfte med uppsatsen, vilka frågor tycker du att vi har missat att ställa?
- Får vi ta kontakt med dig igen om vi skulle behöva ställa någon fråga vi missat?

Appendix 2

Intervju Peter

Du får gärna börja berätta lite såhär om din roll inom banken och tidigare erfarenheter och så helt enkelt

Peter: Ja absolut, så att jag heter Peter, varit i banken i snart 7 år, började som management trainee där för sju år sedan, har en teknisk bakgrund, eh, civilingenjör från KTH. Har senaste 1,5 åren i banken jobbat specifikt med vår avdelning som heter digitalisering och innovation, vilken är en ganska liten enhet, vi är 5 personer, blir snart 6 och jobbar egentligen som en katalysator att hjälpa organisationen i stort att bli mer innovativ, bli mer digital. Och så pratar vi mycket om transformationsfrågor, pratar mycket om hur banken ska arbeta, så det blir mycket omvärldsbevakning och kommunikation inkluderat i det. Men min roll där specifikt har tidigare varit ansvarig för våra blockchain projekt och på senare tiden mer och mer lämnat över den rollen till vår head of emerging technologies som idag driver den frågan medans jag mer fokuserar på (någonting partnerskap ~2:30) hur vi arbetar med tredjepart, startups, scaleups och så vidare

Isak: Okej,

Har du någon tidigare erfarenhet av blockchain innan den här rollen så att säga?

Peter: Ehm, ja alltså jag började, ska väl inte säga jobba med, men jag började titta på blockchain 2012-2013 där någonstans i egentligen privat perspektiv och höll väl egentligen därefter mig väldigt bekant med vad som hände i den delen av världen om man säger så, och sen så har jag som sagt jobbat med det i kanske ungefär i ett år helt (ord? 3:16) också, men ska vara tydlig med att jag har betydligt mer kompetens kring de affärsrättsliga perspektiven snarare än de väldigt hardcore tekniska även om jag har en ganska god förståelse för de tekniska också

Isak: Okej,

Hur jobbar banken med blockchain eller annan DLT teknik idag har ni någonting igång?

Peter: Ja vi har ett antal projekt som vi är framförallt i konsortium, där vi är med, största idag skulle jag säga är nordic fund ledger, som är ett samarbete mellan de svenska storbankerna kring att bygga upp ett, en plattform på vilken man kan skapa en enlighet inom fondhandeln, eh, så där är vi med och är det projekt som vi har drivit hårdast internt. Sen har vi ett antal case som vi också har drivit under ganska lång tid nu som ligger i produktion men som vi inte brukar prata om, rent, vad det är för något och det handlar egentligen om väldigt små applikationer som vi testat att använda, jag skulle kalla det en ren blockchain teknik för att göra vissa saker, för att hålla single source of truth mot kanske lite större aktörer i andra branscher.

Isak: Okej!

Vad tror du om framtiden för blockchain inom banken?

Peter: Ja, det är en jättebra fråga, jag tror att den är väldigt aktuell just nu, historiskt har de sagt att krypto har varit den biten av blockchain, om man nu vill dra in det under samma tak, som banker har hållit sig ifrån, också tror de att det funnits en hype vilket som jag helt

håller med om att även banker föll för där jag tror att blockchain har beskrivits som en silver bullet vilket det förstås inte är, har aldrig varit och kommer aldrig bli heller, men jag tror också den passar idag väldigt bra in under emerging technologies just för att man kan hitta ett sätt att skapa en verktygslåda där nya tekniker också kan vara ett alternativ för att lösa befintliga problem, om man kollar på framtiden för det så tror jag att det kommer vara just en teknik bland många som har potential att lösa problem som kanske tidigare varit betydligt svårare eller mer komplexa att lösa, men jag skulle fortfarande säga att vi är långt ifrån en tydlig mognad av blockchain och DLT som koncept och framförallt kanske som, ur ett rent affärsperspektiv så tror jag att mognaden är väldigt låg och förståelsen lika så.

Isak: Okej!

Vad ser du om man kollar mer på generella blockchain lösningar och den tekniken, vad ser du som de största utmaningarna med att implementera dem?

Peter: Jag skulle säga att generellt så, jag står fast vid att, egentligen den blockchain implementation, om vi tar bort DLT från ekvationen tills vidare, den blockchain implementationen som jag har sett och tycker fungerar bäst egentligen är ju bitcoin fortfarande, och jag tror att det talar ganska mycket för vad jag också tror man behöver ha i framtiden för att verkligen kunna bygga vidare på det här på ett effektivt sätt, alltså, de permission chains som vi ser idag, som exempelvis den som facebook lanserade nu, om man läser deras whitepaper vilket jag tycker är en ganska bra sammanfattning, alltså libras whitepaper, så beskriver de att idag finns det ingen känd teknik som på effektivt sätt tillhandahåller en permissionless blockchain, vilket jag tror egentligen är den enda framtiden för att på ett effektivt sätt skapa den här trovärdigheten som blockchain som koncept egentligen bygger på, varför jag nämner bitcoin är för att jag tycker att det verkligen fungerar, men det har funnits live så pass länge och har ändå en så hög användningsgrad men med då problematiken som finns i, exempelvis proof of work, och hur man löser det i en helt permissionless kedja ser jag inte som helt uppenbart, och jag tror att det är väldigt få som ser det som uppenbart. Var det svar på frågan eller driftade jag lite där?

Isak: Jodå det tycker jag att det var, absolut, om vi då vänder på det där:

Vad ser du som de största möjligheterna med implementationen, vad ser du som de största fördelarna?

Peter: De största möjligheterna jag ser, och jag är väldigt pragmatisk i det att en helt, att skapa trust internationellt eller globalt för den delen mellan 2 individuella parter... anonymitet skapar ju förutsättningarna för att egentligen byta ut alla de strukturer för trust som vi har idag, som banker, som i vissa fall om man har... alltså att kunna, att göra transaktioner helt oberoende av en tredje part är ju en fundamental skillnad i hur vi som människor egentligen ser på transaktioner eller utbyte av någon typ av vara eller tjänst och så vidare, så att möjligheterna är enorma, men det förutsätter väldigt mycket större mognadsgrad tekniskt utifrån hur blockchain ser ut idag, jag skulle säga att det kluriga som bank är att, man får också acceptera det att med den möjligheten så måste också banker hitta ett sätt att förhålla sig till den nya verkligheten, jag tror inte att banker kommer ha det särskilt svårt att göra det egentligen för att jag menar viss av de grejer som man pratar om finns ju kvar, ett banklån löses inte bara för att du kan göra en transaktion gratis, så att, det finns liksom möjligheter för banker att forma om sina affärsmodeller utifrån den enorma möjlighet som finns konceptuellt i blockchain.

Isak: Alright,

Ser du några risker med tekniken? Med säkerhetsperspektivet tänker jag

Peter: Ja, jag alltså i, jag skulle säga att idag, i dagsläget, och hur utvecklingen ser ut idag, och hur den fungerar finns det enorma risker. Alltså, det tror jag kommer från ett rent mognadsperspektiv, att med tiden och med användning så kommer förstås att de riskerna minska med olika mitigerande effekter som olika aktörer kommer att ha, men i dagsläget är de största riskerna förstås från ett bankperspektiv ligger mycket i KYC som till viss del går att lösa, absolut, men som inte har någon standardisering, i den riktiga världen finns det någon typ av standard för hur vi identifierar oss och hur vi visar var pengar går och kommer ifrån och den biten medans det kanske den här världen är lite mer vilda västern. Och det säger jag verkligen med en förståelse för att det här är någonting som kommer att utvecklas och ha förändrats över tid också. Och jag menar, jag är mycket väl medveten om att det finns en betydligt mycket större spårbarhet i exempelvis bitcoin än vad det gör i cash, men jag bara konstaterar att för en bank rent processmässigt så är det extremt stora risker associerade med att hantera kryptovalutor, och ska kolla på risker för DLT blockchain än mer en krypto, för jag vill verkligen vara noga med att hålla isär dem då kanske man pratar mer om mognaden och egentligen, över tid kommer det fram nya sätt att, så att säga, skapa, jag vill inte säga fel, men att hitta ett sätt att kringgå de strukturer som finns och där kanske vi inte har hunnit komma till en punkt där vi har börjat se att liksom det förbättras genom att vi upptäcker fel i det, men som med all ny teknik finns det ju bara risker i att den är ny liksom. Där eventuellt skulle jag också vilja säga att, ur ett, blockchain per se, är väl en teknik som också i och med att den bygger på förtroende, så är det mycket som kan liksom gå fel om vi kommer till en punkt att den inte skulle fungera, det kan man jämföra med att om alla litat på att bankerna gör som de ska, så är pengar säkra i bankerna, men om banken inte gör som de ska kan man också förlora pengar. Och det är liksom samma sak här, om alla förutsätter att blockchain är helt immutable, att det inte finns några faror i det så kommer det också vara en väldigt stor förvåning sen när man kanske eventuellt upptäcker att här gick någonting fel.

Isak: mm... mm..

Du nämner KYC där också, det kanske vi skulle ha börjat introducera, men det är precis det vi vill titta på egentligen att, hur, om man kan liksom förbättra KYC processen, och den biten med hjälp av blockchain och DLT teknik så att vi tänkte gå in lite på det här nu, vi vet inte hur insatt du är det, men vi vill fråga ungefär hur ser KYC processen ut hos er idag?

Peter: Oj, då kan ni få ett typ föreläsning på 3 timmar av vår compliance avdelning, men väldigt övergripande: vi samlar in KYC från samtliga av våra kunder utifrån den standard och lite därtill som krävs från myndigheter, mer insatt än så, alltså det beror helt på vad ni vill veta, men vi har en skyldighet mot, liksom, myndigheter att göra vissa saker mot våra kunder, att ta reda på viss information, för att egentligen försäkra oss om att grundläggande att de är vem de säger att de är, och att pengarna framförallt kanske då, kommer från de ställen där de säger att de kommer ifrån. Jag vet att det är väldigt generellt, men det är inte alls mitt område, och jag har väldigt stor respekt för att det är ett väldigt komplext område, så jag vill inte heller säga något till er som är fel.

Isak: Nä, nä jag förstår,

Har du någon inblick i utmaningar eller om det finns några problem med den processen idag?

Peter, Ja ja, absolut, vi säger såhär; utifrån att jag som tidigare då jobbade specifikt med blockchain så har definitivt en bild av att man inom framförallt kanske finansiella verksamheter har haft en ganska stor tilltro till att DLT eller blockchain ska kunna skapa nya

förutsättningar för en bättre KYC, jag brukar alltid hänvisa till, jag vet inte om de har gått vidare från pilotstadiet nu men i Kanada så har RBC, Royal Bank of Canada, gjort en jättebra jobb med att bygga upp en struktur för att kunna hålla KYC, och jag menar, om man kollar här i Sverige så har företag som Norbloc, som jag också tycker har byggt ett föredömligt system för att egentligen samla data på ett sätt som gör att kunderna äger sin egen data, och därmed också kan styra vilka företag och vilka institutioner som ska ha information om dig som kund. Så att, jag menar, och de problemen man löser där bygger ju väldigt mycket på det här att, som kanske idag handlar om att man lämnar över information till någon annan som man inte vet vad de gör med den, ur ett KYC perspektiv så vill du ha en viss specifik information som du som kund kanske bara vill lämna ut till vissa trovärdiga parter, där kan man ju då återigen skapa trust över en transaktion som i det här fallet är transaktion av data egentligen till en ny part. Och förstås viktigt i det här som vi kanske har i Sverige genom exempelvis BankID är ju det här med att du också kan garantera på ett sätt digitalt att du är du, och det tror jag också är viktigt inom KYC så att man pratar mycket, när man pratar bank digitalisering så pratar man mycket om att digitalisera processer och där det krävs det ju också någon form av identifiering som inte varit möjligt tidigare så man måste komma in och visa sitt ID eller leg, vilket man nu potentiellt sett skulle kunna göra helt digitalt.

Isak: mm...

Om du kan utveckla lite på hur du tror att den lösningen skulle se ut

Peter: Ja precis, där tror jag, om man kollar på typ Norbloc eller på caset IBM och RBC i Kanada så får man en ganska bra bild av vad det skulle se ut, och grundläggande är det liksom en blockkedja som potentiellt sett skulle kunna vara global, där egentligen, varje person får ett identifierbart block som de själva styr över och själva krypterar varpå man liksom kan välja vem man ska ge en publik nyckel av informationen till.

Isak: mm..mm.. Alright,

Är det blockchain eller DLT teknik som är bäst anpassat för det här? Eller är det en av många olika tekniker som skulle kunna användas?

Peter: ja det är skitsvårt att säga förstås, jag menar det är ju såhär, en annan databasteknik skulle egentligen kunna vara lika bra men det jag tycker i det här sammanhanget känns relevant är det här att om man ser en utveckling av blockchain där vi faktiskt har en möjlighet att bygga någonting globalt utan att ha den påverkan som exempelvis proof-of-work har, så tror jag verkligen att man kan se en tydlighet i att, eller förlåt, kanske inte en tydlighet, man kan se en stor vinning i att alla då kanske skulle kunna vara sin egen nod, kan det drivas via en mobiltelefon? Att min mobiltelefon är min identitet, alltså, att det finns mycket såhär att, jag kan egentligen inte uttala mig om hur det kan se ut i framtiden men jag tror att det finns en potential här, och i konceptet i sig självt som definitivt skulle kunna vara det som är nyckeln till att lösa det här problemet. Men med det sagt så tror jag inte att blockchain idag egentligen är en hållbar lösning för det här. Men att man kanske måste bygga på DLT vilket som jag ser egentligen som en ganska, det är en begränsning av blockchain som koncept, jag menar, pratar man permission, kommer vi alltid komma fram till att då är det någon av de etablerade agenterna som har trust idag som kommer att fortsätta ha den rollen och då tycker jag att på ett sett förbigår hela blockchain.

Isak: mm.. Du var lite inne på det tror jag men

Blockchain, vad är det för typ av blockchain, är det en privat eller en publik kedja som ni är mest intresserade av?

Peter: Ja, jag ser det som en förutsättning att vi måste gå mot publika kedjor, för att jag tror att det är den enda trovärdiga sättet att hantera information på, att alla har ett eget ansvar för sin egen data. Och jag menar, med det sagt så kan ju fortfarande en permissionless kedja utvecklas till någonting som blir i princip permissioned för att stora aktörer liksom, tar ett ytterligare ansvar, det kan vara en stat, det kan vara ett företag eller.. Whatever, men grundförutsättningen är att det är en öppen, man kan nästan jämföra det med en öppen marknad där man i princip får ta ett individuellt ansvar att det här ska fungera över tid, till skillnad från då permission chains där man etablerar, som jag var inne på lite tidigare då, att de parter som idag har trust är de som ska ha det i framtiden, och jag ser inte riktigt hur det skiljer sig då från att vi har ett centralt databas hos exempelvis en bank som vi har kring våra pengar idag.

Isak: alright,

Om man tänker på en sådan här lösning, vad tror du att de största fördelarna skulle vara för kunderna? Ur ett kundperspektiv?

Peter: Det där är också en jättebra fråga, för att faktum är att det behöver inte vara bra för kunderna för i sådana fall kan man som kund upplever det som ganska bekvämt att det finns en central part som man kan lita på, som hanterar någonting, och mycket av det här bygger på att man skapar en ytterligare komplexitet i livet som då för vissa människor som då måste ta ett eget ansvar för exempelvis då, att man ska hålla sin privata nyckel säker och alla sådana här saker som ökar komplexiteten, och det tror jag också att vi kommer behöva se en lösning på för att folk, om man bara kollar på bitcoin idag, alltså jag har själv varit involverad i ett ganska bra tag och det har alltid varit komplicerat om man inte litar på coinbase eller de stora aktörerna då är det ganska komplicerat att hålla sina pengar säkra, till skillnad från en bank liksom där du i princip idag är garanterad att dina pengar är säkra och du kan få tillbaka dem från staten om banken skulle gå i konkurs, så det är mycket sånt som jag tror, liksom, fallerar just att man inte har den upplåten trogenhet man har i sin traditionella(lite otydligt, 21:24) finansiella marknader.

Isak: Alright,

Om man kollar från andra hållet, för verksamheten eller för bankerna vad är de största fördelarna där?

Peter: Det är jättesvårt att säga, men, det är klart att, de största fördelarna, jag vet inte om det finns några direkta fördelar som kommer av blockchain eller DLT om jag ska vara helt ärlig, det är ju som att säga vad är de största fördelarna med machine learning, det är svårt att definiera utan att ha en kontext att sätta det i

Isak. Ja, jag tänker då att om vi tänker oss en sån här lösning då, att det skulle gå, till och med globalt då som vi talade om tidigare

Peter: jaha, så du tänker rent KYC mässigt?

Isak: Ja, precis om vi tänker oss någon form av DLT lösning på KYC

Peter: ja, jag förstår, och då är framförallt fördelarna att vi kan garantera att våra kunder är de personer som de är, att vi kan bygga en helt digitaliserad lösning också, och jag tror att det innebär också att banker kan också skapa nya affärsmodeller utifrån att vi kan liksom, skapa nya processer, nya idéer, inte bara att det digitaliserar identiteter vilket jag kan tycka bankID

är utan också digitaliserar, alltså gör en transformation av processer och skapar nya möjligheter med det som då är möjligt med en sådan global KYC funktion på en blockchain

Isak: Okej!

Så vad ser du för utmaningar med att implementera en sådan här lösning?

Peter: heh... Allt! Alltså det är skitsvårt... Jag vet inte vart man ska börja, men det finns väl en miljard utmaningar, bara att bygga någonting som alla tror på, och som alla skapa en kritisk massa, garantera säkerhet, det är liksom ett sånt projekt som att åka till månen 2.0 liksom, det måste vara något som kräver ett sådant enormt engagemang av många olika parter skulle jag säga..

Isak: mm...

Men tror du att det skulle kunna börja på nationell nivå, eller bara inom en ...

Peter: Ja men då tycker jag att man landar återigen i permissionless permissioned frågan, att är det då permissioned att bara lokala aktörer får verka, och i sådana fall hur utvecklar man det över tid, och ifall då bara vi i sverige har en permissionless kedja kan kina komma in och totalt äta upp den då, jag tror att det finns mer komplexa frågor här än vad man kanske har stött på tidigare

Isak: mm. mm, alright, ja, men då tror jag att vi har täckt rätt mycket där, eller vad tycker du, Filip?

Filip: Ja absolut jag tror att vi har fått våra huvudsakliga frågor besvarade, ursäkta att jag har suttit så tyst här det är bara det att kvaliteten för mig är väldigt, väldigt dålig och det har varit lite utmanande att hänga med i vad som sägs...

Isak: Ja vi hoppas att det blir bra på inspelningen,

Men nu när du vet vad vi syftar till att besvara med uppsatsen, tycker du att det är några frågor som vi missat att ställa? Eller något ämne vi ska titta extra på?

Peter: Ja men, det är kanske rent, ur ett tekniskt perspektiv, hur, eller såhär; tvärtom, en av frågorna man kan ställa sig är om det här är tekniskt möjligt, är det här feasible? Ett annat perspektiv är ur ett affärsperspektiv, vilka intressen finns det idag? eh, kanske rent volontärt eller jag tänker vilka aktörer som är aktiva på den här marknaden just nu, vilka intressen finns där som kan påverka negativt utvecklingen mot den här riktningen? Och svaret vet jag inte om jag har, men jag kan tänka mig att det finns andra kanske mer dominanta banker där ute som hellre ser att det här är något som de tillhandahåller, en väldigt, så att säga, altruistisk lösning, och mycket av det som blockchain bygger på är ju den altruism som har funnits i, får nästan säga såhär, hackerkretsar tidigare, det finns ju en viss tilltro till någon typ av anarki som jag tror att många institut och institutioner idag i världen inte alls subscribar till, och jag tror att den komplexiteten kan vara större än någon tekniskt eller ekonomisk utveckling

Isak: så att acceptansen bland banker och inom branschen då helt enkelt att alla ska...

Peter: Ja inte bara banker, nu tog jag det som ett exempel eftersom att jag själv jobbar inom bank men vi är så pass små att vi har inte mycket att säga till om där, men jag tror att det handlar i större utsträckning om, alltså, regeringar och liksom det vi ser nu när svenska ministrar går ut och uttalar sig om libra, det är ändå ett privat företag, vad skulle hända om man

bygger en helt altruistisk lösning där alla ska lösas i form av KYC, jag vet inte, jag tror att det är svårt att hitta en modell som fungerar där.

Isak: alright, perfekt, då är vi ganska nöjda där tror jag

Peter: Vad skönt

Isak: stort tack för att du ställde upp, och så självklart är det något som du vill lägga till eller ta bort eller så så är det bara att höra av dig, och vi kommer höra av oss angående anonymitet och så hur du vill göra, det kan vi ta senare, och om du vill titta igenom citat eller liknande om vi använder några

Peter: Ja gärna, det brukar alltid vara bra om det finns något som jag känner att jag vill förtydliga, och om ni har några fler frågor eller om inspelningen behöver något förtydligt, och stor lycka till!

Isak och Filip: Tack och hej!

Appendix 3

Intervju 1 - Christian Frisch

Isak: Vi kanske ska börja med att berätta lite, vi vill titta på hur Blockchain eller DLT teknik kan komma att förbättra KYC/kundkännedomsprocessen. Det är vår huvudfrågeställning och vi vill se hur svenska banker då framförallt och också branschen ser på möjligheterna.

Isak: Du får gärna börja med att berätta lite om dig själv, dina tidigare erfarenheter och din roll inom Nordea just nu.

Christian: Ja. Min bakgrund om vi börjar med studierna är en magister i informatik precis som ni håller på med och även en magister i finansiell ekonomi och utöver det har jag också tagit en executive MBA ungefär tio år efter att jag avlade mina examina. De första tio åren spenderade jag som managementkonsult och det gjorde jag framförallt i London och i Norden. Jag har alltid varit med i projekt som har haft anknytning till banker och försäkringsbolag och inom den typen av projekt så har jag varit specialiserad på strategier och att ta fram olika target operating models för hur ett företag ska vara konstruerat för att bäst möjligt vara effektiva. Dels i sättet de utför sina processer på och dels hur de förklarar sin strategi. Efter att jag gjorde det så flyttade jag till Nordea och då... Ja i och för sig innan när jag var student på Handels så var jag med och startade ett konsultbolag, Sveriges första sånt här student consulting som ni känner till. Och jag var engagerad i småbolag och jag tog ett avbrott och jobbade i Frankrike och sådär. Det var som sagt under studietiden. Men sen började jag på Nordea 2013 och då var jag ansvarig för att bygga upp Nordeas interna konsultavdelning och när jag hade gjort det i två-tre år så var jag ansvarig för att driva ett simplificeringsprogram på Nordea. Man kan säga att det var ett projekt med 500 personer som syftade till att göra allt vi arbetade med på Nordea på ett enklare sätt och ett mindre komplicerat sätt. Så det omfattade bland annat att minska antalet system som vi arbetade med, vi har ju över 10 000 olika system på Nordea i Norden. Och att rationalisera produktutbudet vi hade över 3000 produkter vid det laget och så vidare. Sen så har jag varit ansvarig för digitalisering på Nordea där vi digitaliserar, alltså det är ju jag och många andra som är ansvariga för det, men mitt ansvarsområde var att digitalisera online onboarding vilket innebär att den processen när vi får nya kunder online, och det är ju bland annat KYC-processen då, och även ansvarig för att utveckla våra digitala lösningar inom bolåneerbjudandet. Nu på senare tid så har jag arbetat 100 procent med vår homejourney hub som är en agil projektorganisation med ungefär 150 personer som alla arbetar med att förbättra kundernas upplevelser när de har bolåneärenden hos oss, så allt ifrån den processen när de funderar på att köra en bostad, till de har fått ett lånelöfte och sen gör en låneansökan och sen äger sin bostad och är regelbundna bostadsägare helt enkelt. Då har jag team i Polen och de nordiska länderna då som arbetar med detta. Sen så ansvarar jag också för en avdelning som har product-owners, man kan likna det med gamla tidens projektledare som utför olika typer av effektiviseringar i banken. Och sen utöver det så har jag ett brinnande personligt intresse för blockkedjor och kryptovalutor. Och det är någonting som jag spenderar två till tre timmar per dag på både professionellt och som amatörperson och det har jag gjort nu i snart tre år. Det som intresserar mig där då är konsekvenserna för samhället och för banker och företag egentligen. Så det är väl i korthet min historia.

Isak: Perfekt. Hur jobbar Nordea med Blockchain och DLT idag? Är det några projekt igång eller så? Hur ser det ut där?

Christian: Vi har ju projekt där en hel del saker är konfidentiella.

Isak: Ja jag förstår.

Christian: Så jag är begränsad i vad jag kan yttra mig om, men jag kan ju börja med att säga att vi har en person som är ansvarig för blockkedje... eller egentligen är personen ansvarig för emerging technologies så nya typer av teknik eller teknologier kan man säga och där i är blockkedjor en stor del men det är inte det enda syftet med den personens tjänst. Det är en enhet som jobbar på grupp nivå, vilket innebär att... För Nordea är uppdelat i olika divisioner, en division är ju vår verksamhet för privata kunder, sen har vi en annan verksamhet en annan organisation med annan kultur för företag...

Isak: Förlåt, nu hör jag dig väldigt dåligt tyvärr.

Christian: Jag är ute och går, så ni får helt enkelt... Hörs det bättre nu?

Isak: Jag hör tyvärr knappt alls...

Filip: Det låter väldigt... Där nu är du tillbaka!

Christian: Det kanske var någon forma av störning bara. Vi provar. Det är bara att avbryta om det är nått som...

Isak: Ja, absolut.

Christian. Jo men så, vi har olika divisioner helt enkelt och sen har vi en tredjedel som är en profession banking som håller på med egentligen alla transaktioner, alla former av betalnings-transaktioner och så har vi även wealth management som är en verksamhet som riktar sig till high networth individuals och mindre bolag som ändå har väldigt stora tillgångar. Det här är som olika bolag, Nordea är ju den största banken i norden vi har olika kulturer i respektive land och vi har olika kulturer mellan de här olika divisionerna. Och också olika ledningsgrupper egentligen och olika styrning och så vidare. Vi har en blockkedjefunktion med en person som är ansvarig för hela gruppens blockkedjeinitiativ. Så det vittnar ju lite om var Nordea är i mognadsfasen tror jag och det är inget som reflekterar varken positivt eller negativt med just Nordea utan jag tror att det gäller hela branschen. Det är en väldigt omogen bransch, men när den väl blir mogen så kommer det ske över en natt. Det kommer bli som en ketchup effekt tror jag. Den här personen driver våra blockkedjefrågor på Nordea och han gör det i samarbete med de här divisionerna. Så jag sitter i verksamheten för våra privata kunder och mycket små enmans-/tvåmansbolag. Jag jobbar nu med bolån... (går inte att höra) ... blockkedjelösning. Jag vet inte om ni känner till Chromaway?

Filip: Jo.

Isak: Jo.

Christian: Ja, de håller ju på... de har gjort en pilot nu med lantmäteriet och jag har för mig att det är SBAB och även några mäklare. De har testat att göra, till exempel köpa en bostad via blockkedja. Om vi till exempel skulle vilja testa något liknande, så är det jag som kan driva det, men att jag har en viss regelbunden dialog med vår blockkedjeansvariga på grupp nivå

men initiativen drivs ändå ute i divisionerna. Så att så ser själva strukturerna ut på Nordea. Så att officiellt är jag inte blockkedjans ansvarig, utan det är en person som heter Ville Sointu och om ni vill så kan ni säkert intervju honom också så kan jag förmedla hans kontaktuppgifter om det skulle vara aktuellt.

Isak: Absolut, det skulle varit toppen.

Christian: Precis. Vad var nu frågan förresten? Hur vi arbetar med detta på Nordea?

Isak: Exakt.

Christian: Ja, sen har vi ju ett annat samarbete och det är ju när vi är ett tjugotal banker tror jag att det är som har gått ihop för att testa We-trade. För att testa transaktioner mellan bankerna. Det samarbete är vi med i, men det vet Ville mer om än vad jag vet. Men i princip så har vi... Vi är engagerade i blockkedjor. Det finns en intern splittring kring blockkedjornas konsekvenser. Vi har till exempel en ansvarig person för riks och regelefterlevnad som i jag tror det var två år sedan, eller det kan ha varit mars 2018 förresten som gick ut och förbjöd alla anställda att engagera sig i kryptovalutor. Samtidigt så har vi ett konferensrum som... Alltså alla våra konferensrum har ju namn och ett av dem heter Bitcoin. Samtidigt så driver vi interna projekt kring blockkedjor så att vi är... det finns inte en gemensam attityd mot kryptovalutor och blockkedjor och jag skulle nog säga, eller jag vet att majoriteten på Nordea vet inte om vad blockkedjeteknologin är för något. Det gäller ju i princip alla banker också.

Isak: Ja, alright. Om vi tar lite om din syn på Blockchain och DLT... Inom banken har du talat lite om men också så här i finansbranschen i stort. Vad tror du att det kommer att hamna i här, om man ser lite framåt?

Christian: Jag tror att det är ett krig mellan decentralisering och centralisering. Där Bitcoin är det yttersta exemplet på en decentraliserad blockkedja där som ni vet då ingen kan påverka, ingen kan styra, ingen kan manipulera. I alla fall så är det så i teorin. (ohörbart)... situationen, även om det skulle vara exakt som idag, så kommer det bli det i framtiden ju fler noder som ansluts till kedjan. Det här är ju både ett hot och en möjlighet. Som jag ser det så står finansbranschen inför samma utmaning som musikbranschen gjorde innan Spotify kom, eller som CD-skivorna, vad ska man kalla den branschen för? Ja, CD-skivbutikbranschen på 80-talet, som ersattes av digitala filer, det kan man också likna vid dagen penningssystem som ersätts av digitala pengar istället. Det är ingen som riktigt vet var det kommer att hamna i slutändan men som jag ser det så pågår den kamp mellan centraliserade och privata eller decentraliserade aktörer. Alla banker driver ju centraliseringslinjen i den utsträckning de alls är engagerade. Som ni kanske hört så har ju J.P. Morgan skapat sin egen kryptovaluta som ju då inte är öppen för allmänheten och även om den skulle vara öppen och tillgänglig för allmänheten så är det de som har kontrollen. Personligen så tycker jag att det här protektionistiska förhållningssättet inte är positivt så i den bemärkelsen stödjer jag personligen inte bankernas attityd till kryptovalutor och blockkedjor sen förstår jag varför man kan ha den attityden. Svårigheten och det som ger långsiktig bärkraft det är ju att försöka hitta hur en öppen blockkedja eller en halvt öppen blockkedja kan känna både våra kunder och vi som bankaktörer. Det är väldigt svårt och vi vet inte hur man kan göra det ännu. Men det är mer optimalt att försöka hitta en sån lösning än att kämpa emot och bibehålla kontroll och jag ser i bankbranschen hur den kampen pågår tillsammans med okunskap om vad Bitcoin till exempel och vad blockkedjor över huvud taget är för något och ännu mer vilka potentiella konsekvenser de kan ha för samhället och våra affärsmodeller. Det är också naturligt med tanke på att det är en ny teknologi och det är ingen som vet dess implikationer till fullo och det är samma sak, internet tog ju över 30 år

innan det började anammas. Jag tror att det var (ohörbart) som startade och i Sverige, och vi var rätt tidiga tillsammans med Israel på 90-talet så började det här komma mass-adoption. Som många andra i kryptokommunityt så jämför jag dagens attityd och mognadsgrad med den som var då på 90-talet där internettekniken var omogen i många aspekter. Det fanns många olika protokoll till exempel. Idag är det ingen som ifrågasätter TCP/IP utan det bara existerar det är ingen som bryr sig om andra protokoll, medans i kryptobranschen så har vi ju alla möjliga plattformar, Eos, Neo, Blockchain, Ethereum, whatever you name it. Alla dom kämpar ju om att ta dominerade position som the protokoll på blockchain. Det var ju också många i början av 90-talet som inte förstod poängen med internet och när de förstod på poängen, till exempel att informationen kunde delas fritt, så såg de genast negativa konsekvenser och då sa de till exempel Va?! Det är ju bara kriminella, då kommer man ju kunna ta reda på recept på hur man tillverkar bomber eller så kan man kolla på barnporr. Nej det vill vi inte ha, det måste vi begränsa. Sen var det ju vissa företag som insåg att det inte går att stoppa och det här är antagligen en positiv sak mer än vad det kan ha negativa konsekvenser, så därför ska vi ta kontroll över det här och skapa våra egna interna intrapages och sedan ska vi låta folk gå igenom de sidorna. Yahoo ville ju ha en portal där alla skulle... Det var fönstret mot internet liksom. Och precis, det finns ett... Allt som skedde då ser jag idag med kryptovalutor och blockkjedjor.

Filip: Ja, det låter ju precis som det här med att, det ser man ju hela tiden historiskt. Men tryckpress, man kan även se det med dagens stora tidningar att de har tappat trafik mot mindre källor på Youtube till exempel.

Christian: Precis.

Filip: Vi skulle väl komma till nästa fråga som vi tänkte ställa, vad du skulle se som de största utmaningarna med att implementera blockchain och DLT-teknik generellt och det låter ju som att det är det som är den stora svårigheten. Men har du någon annan svårighet som du kan tänka på också?

Christian: Ja, den andra svårigheten är ju att bemöta all okunskap så att folk förstår över huvud taget vad som kan göras och vilka utmaningar som finns. Jag tror att när folk kommer förstå det det är då det kommer bli en ketchupeffekt och den kommer ju att spås på av till exempel Facebook Libra coin, eller att Nike ger ut en coin, eller att Samsung också engageras i det hela. Så det kommer ju att explodera det hela tror jag och då kommer ju de här utmaningarna hanteras automatiskt. Men jag tror att den stora utmaningen med detta är ju att när folk inser att det är intressant att det finns väldigt stor potential för även om man i det läget bestämmer sig för att nu ska vi satsa fullt ut, Nordea går ut och bygger en blockkjedja baserad på Ethereum som är 60 procent decentraliserad och viss kontroll behåller vi tillsammans med andra banker. Även om vi skulle säga visst, vi kör, fullt mandat då skulle vi liksom inte riktigt veta hur ändå, för det skulle ju krävas att andra aktörer har samma mognadsgrad och de har dom inte. Så att det är en stor utmaning. Sen finns det naturligtvis tekniska utmaningar som i början på internet, jag vet inte om ni ens var med då, men man hade modem som lät som bara den när man kopplade upp sig. Man kunde gå in på Mc Donalds och det enda den bestod av det var Mc Donalds logga, och det tog ju dessutom tre minuter innan man kunde se den här loggan. Då undrade alla vad sjutton ska vi med det här till? Det är ju helt meningslöst. Vi befinner oss lite där idag också, att Ethereum är inte garanterad tillräckligt många transaktioner till exempel, så det är ju också en av utmaningarna och att över huvud taget hitta rätt affärsmodell kring detta. En annan stor utmaning är ju lagstiftning kring det här. Om man till exempel använder KYC-processen via en blockkjedja, vi kan hitta på att det finns en blockkjedjeaktör som är öppen vars tjänst innebär att man lägger alla människors identiteter på blockkjedjan, det finns inte en lagstiftning idag som skulle godkänna det. Även om man

tekniskt sätt skulle kunna göra det 100 procent säkert. Det finns ingen användarvänlig teknik som skulle möjliggöra en sådan tjänst för normala människor. Vi får tänka på att Sverige är ganska utvecklat med vår infrastruktur. Om vi till exempel tar BankID så är vi tillsammans med Norden ganska enastående i det i jämförelse med till exempel Indien och många andra länder i världen och det finns fortfarande människor i vårt samhälle som inte kan använda och inte använder Mobilt BankID. Så om vi skulle vilja få dem att använda identiteten i KYC-processen, det är en jätteutmaning.

Isak: Mmm okej. Om vi vänder lite på det och om man kollar på de största möjligheterna med att implementera en blockkedja, och då kollar vi ganska så generellt både med kanske valutator, KYC som vi tittar på, och liknande. Vad ser du att den här tekniken har i bankbranschen, vad är de största möjligheterna med den så att säga?

Christian: Ja... Det beror ju lite på utgångspunkten man har i centralisering och decentralisering, men om jag tar min personliga privata utgångspunkt, inte Nordeas hållning så ser ju jag att fördelen med de här blockkedjorna är att man tar bort makten från mellanhänder. Vars värde och bidrag till processen de är mellanhänder i är utnyttjat, antingen genom höga priser eller onödigt form av maktutövande. Det blir ju ett enormt avbrott för branschen som leder i slutändan till fördelar för kunderna. För alla privatpersoner i princip, så det är ju liksom fördelen. Sen är det ju rent praktiska fördelar som att man kan minska pappersarbete, man behöver inte hålla koll på sin säkerhet på samma vis, för förhoppningsvis så kan man lita på blockkedjans säkerhet. Man kan göra information som man själv äger mer tillgänglig som att när jag utsätts för reklam på webbsidor så får jag en del av intäkterna som webbsidan får. Eller om jag har en olycka när jag är på semester i Thailand, så kan läkaren med mitt godkännande ta del av hela min journal och historik i sjukvårdsammanhanget då. Så det är ju enorma möjligheter med det här. Jag ser inte lika lätt möjligheterna för centraliserade aktörer. Dels för att de är utmanade generellt av de första orsakerna jag beskrev, dels för att ja hur ska jag säga... dels för att jag tror egentligen inte att blockkedjetekniken nödvändigtvis kommer att fungera när den är centraliserad för att risken att det bara är en decentraliserad databas är väldigt överhängande. Så därför ser jag mer fördelar för individer än företag, eller rättare sagt än mellanhänder. Företag har enorma möjligheter, men just mellanhänder vilket banker är, men bara i transaktionsfrågor. Inte nödvändigtvis när man pratar om bolån eller så. Det är klart att bankerna tillhandahåller väldigt viktiga tjänster men om vi tar exempel på en utlandsbetalning till exempel, där banker kan ta enorma summor för att göra en betalning mellan företag, och dessutom tar det lång tid och man är dessutom beroende av banken. Den verksamheten är ju kraftigt hotad. Så att ja... Men det är klart att det vi ser nu är banker som går ihop och försöker skapa betalningssystem på blockkedjan och det kan fungera, det är det vi inte vet. Om det fungerar så är det ju en möjlighet att göra transaktioner billigare och snabbare och säkrare. Så det kan ju vara en fin möjlighet i bankvärlden.

Isak: Mhm, ja... Om vi tittar lite på risker med den här tekniken, jag förstod det som

Nordeas... Att det var lite delat där...

Christian: Ja, får jag bara lägga till en sak där på möjligheterna?

Isak: Absolut.

Christian: Den största möjligheten är ju egentligen för banker att om de är öppna och kreativa så kan de hitta nya affärsmodeller, nya intäktsmodeller och nya produkter av möjligheterna

som blockkedjor erbjuder. Jag vet inte exakt vad det skulle innebära, men jag vet att de finns där. Så det är ju egentligen den största potentiella fördelen.

Isak: Ja, alright... Vad ser du rent generellt med tekniken d", vad ser du för risker här?

Christian: Ja... Risken här den som går ut tidigt riskerar att göra misstag som andra kan undvika sen. Så genom att gå ut först nu så kanske det innebär onödiga risker, och jag tror att vi ser det, det är någon form av avvaktande in branschen också. Men som sagt var när första aktörerna har gjort sitt, då kommer det att bli en ketchupeffekt. Men en annan risk, eller många risker kan man ju relatera till många av de här utmaningarna som jag har beskrivit innan. Så en risk är ju till exempel att man tappar intäkter och att man tappar kontroll. Och sen så finns det någonting...

Appendix 4

Intervju 2 - Christian Frisch

Isak: Jag tror att där inspelningen slutade fungera där hade vi pratat lite om blockchain rent generellt och din syn på det, jag tror att vi var på... Den senaste frågan var vad du ser för risker med blockchain-tekniken ur ett generellt perspektiv.

Christian: Just det. Okej, då såg jag om vi nu ska sammanfatta lite grann. Jag har för mig att jag såg... En risk är okunskap hos befolkningen. Det kräver... det är ju någonting helt nytt och folk, en stor association som många gör men i alla fall digitala valutor såsom bitcoin, det är ju att det är luft och vad är det och så. De tänker de inte på att sina egna pengar är det också, det är bara siffror och de tänker inte heller på att det finns ingen backning för den svenska kronan. Om man kollar på den penningmängd och den reserven som finns hos riksbanken så stämmer de inte överens, och de har de inte gjort sedan 1973 när vi övergav Bretton Wood systemet. En risk är att sprida kunskap och den kunskapsöverföringen kommer att ta tid och det gäller även blockkedjor när vi pratar DLT, när de är kontrollerade men där är risken något lägre, eftersom de företag som håller på med det behöver inte utbilda hela allmänheten. Där är det ju lite mer av en teknologisk satsning, men det som jag ser som den stora potentialen som kan förbättra för samhället och för människor som individer och medborgare det är ju öppna blockkedjor, eller halvöppna blockkedjor. Som också kan integrera med privata naturligtvis, men det är det där jag ser den största potentialen. Då är risken i alla fall kunskap, men det gäller även på DLT sidan. En annan risk är ju att tekniken inte är modern ännu. Den är i alla fall inte så pass mogen som den behöver vara om man kommer till mass adoption. Bitcoin är fullkommet mogen som det är idag, men när det kommer tillräckligt många människor som använder bitcoins blockkedja då ökar väntetiderna och transaktionskostnaderna går upp, och det är för att de inte kan hantera mer än 5-6 transaktioner per sekund. Så det är också en... kunskap är en risk och den andra risken ser jag kring teknologin begränsningar eftersom att det är en ny teknik. Ett tredje område är UI och UX alltså själva användarupplevelsen i sammanhanget blockkedjor. Om igen så är den risken större på öppna kedjor än vad den är på privata DLTs men den finns på båda områdena och vad jag menar med det är helt enkelt att det är inte användarvänligt och intuitivt idag att till exempel köpa bitcoin och om vi tittar på till exempel Vchain som är en annan valuta som har ett avtal med BMW att erbjuda information om en BMW bil via blockkedjan och sedan låta användare och BMW och mekaniker och vem det nu är ladda upp information och sedan få betalt i Vchain och sedan tanka ned information och betala i Vchain valutan. Det kan till exempel vara om du köper en begagnad bil så vill du veta att den är krockfri, ingen har mixtrat med mätaren eller någonting och skulle det då vara en BMW så skulle du kunna kolla det med hjälp av Vchain och BMW kan ju samla in statistik och allting och sen kan man ju dessutom koppla den Vchain lösningen med självkörande bilar och hur de kan kommunicera med varandra för att minska köerna som går som liksom tåg och så vidare, men alla olika tillämpningsområden av DLT och öppna kedjor är väldigt komplexa idag och svåra att förstå som en normal människa och det är upp till företagen att göra dem förståeliga och jag vet inte om bankerna kommer att kunna ta fram en blockkedjelösning som möjliggör att det internt betalas med valutor, om det nu är det incitamentet de vill använda för det är inte säkert att de behöver ett incitament för företag att verifiera

blockkedjetransaktioner när det är en privat blockkedja eller en blockkedja mellan tio banker till exempel. Men om de på något sätt behöver utbildade användare eller få användare att själva använda kedja då kommer det att behöva göras med väldigt intuitiva lösningar, som till exempel när du använder Spotify. Det första E-mail som skickades krävde ju en rymdforskare liksom, och idag gör det inte det. Sen ett annat område, eller det kanske också hör till okunskap mest men det är att det är väldigt många som när de börjar intressera sig för blockkedjor säger att de förstår inte blockkedjor och jag förstår inte vad det är liksom. Det är ju väldigt obehagligt naturligtvis, man vill ju inte förlita sig på någonting man inte förstår och ekonomin är ju liksom central när det gäller trust så att sen är klart... Men då missar de ju till exempel att de inte förstår hur E-mail fungerar heller, men de använder ju det varje dag och det är just att få den där användarvänligheten som E-mail är i jämförelse med tekniken bakom E-mail. Så det är väl de tre områdena som jag kommer på rakt av så.

Isak: Ja men perfekt. Då går vi in lite på den här KYC delen då. Bara kort igen, om du vill sammanfatta lite hur er KYC process ser ut idag, vad det innebär.

Christian: Ja, den är ganska digitaliserad skulle jag säga men den är ju inte hanterad via en blockkedja. Det finns manuella inslag i den processen där vi har människor som ringer upp kunder för att komplettera information eller klargöra otydlig information och sådär och det är ju framförallt på privatsidan. Om vi tittar på företagssidan så är den mer manuell eftersom att det inte är lika standardiserat med våra företagskunder, men där är den också väldigt rigorös. Jag tror inte att det finns så många banker kvar i Sverige och Norden som inte är ganska bra på att hantera KYC idag, för att det är sånt fokus från finansmyndigheter och terrorister och omvärld och allting så det är svårt liksom... Jag vet inte hur många människor på Nordea som jobbar med det, men det är många hundratals. Så att processen är väl ja, vad kan den vara, 70 procent automatiserad och digitaliserad.

Isak: Ja alltså automatiserad, då tänker du på centrala... Kreditupplysning och liknande och sedan är resterande som kunden måste svara på själv då helt enkelt?

Christian: Ja precis och automatiserad då menar jag ju att mänskliga händer inte är involverade och med digitaliserad menar jag att det kan göras digitalt eller via telefon.

Isak: Okej, perfekt. Vad ser du som de största utmaningarna eller problemen med det systemet som finns idag och den KYC-insamlingen som finns idag?

Christian: Det ena är att vi inte riktigt kan lita på det. Om man hade en blockkedja, allra helst en publik blockkedja, där till exempel du kunde ha hela din identitet registrerad och du valde när och vem någon ska få access till den. Och att du när du gör det kanske betalar 50 öre varje gång och att banken betalar 50 öre. Eller att du betalar du inte betalar men banken gör det liksom. En sådan lösning skulle ju vara... Vad vi vet idag i alla fall skulle en sådan lösning vara 100 procent säker tekniskt sett. Men sen kan ju en användare bli utsatt för hot eller vad som helst som gör att dem, ja... Men själva lösningen skulle vara 100 procent säker. Vad var det vi pratade om, möjligheter eller vad sa du.

Isak: Ja, eller egentligen de största utmaningarna med KYC idag så som dagen ser ut.

Christian: Ja, största utmaningen idag är att man inte riktigt kan lita på den informationen man har. Bankerna gör ju en uppdatering årligen och vi gör ju också liksom monitorering av transaktioner och ser vi att det går stora belopp utomlands till svartlistade länder då är det klart att det kommer ett samtal från banken, men det är ju en stor personalkostnad, det är ju ändå en stor manuell process vid de tillfällena. Men när du ansöker om bolån och blir kund hos oss, då är det ju liksom jag vet inte vad det kan vara, tio frågor som du svarar på i mobilappen liksom, det är ju 100 procent automatiserat och digitaliserat. Det är ju en utmaning liksom att få den processen mer effektiv och till lägre kostnad och färre människor involverade, alltså färre personal involverade. Sen är det ju också så att den informationen är ju lagrad på många olika platser, för SE-banken tror jag inte att det är ett jätte issue att de har många olika KYC-databaser. Men om de skulle kunna rationalisera så att det bara hade ett system eller fem system som höll på med KYC det skulle de nog tycka om, men det är svårt. Om man tittar på Nordea så är det ju näst intill... Nej omöjligt är det inte för det håller vi på med hela tiden men att centralisera KYC-hanteringen det är någonting som många banker vill göra. Idag har ju Nordea en KYC-lösning i Sverige, en i Norge, en i Danmark och så vidare. Så det är ju... Man vill ju ha en central databas och sådär om det är möjligt. Och sen är en annan utmaning GDPR, men den utmaningen börjar bli mindre nu för att dels är de flesta vad jag förstår, inklusive Nordea, compliant med den lagstiftningen och sen är det ju det där tåget som är passerat och alla klarade att ta emot det på hållplatsen och nu går det bra igen. Nu är det klart att det ändå är en utmaning för kunderna måste ju kunna ta bort in data och det är klart att vi behöver ju säkerställa det. Samtidigt så är banker undantagna från GDPR i ganska stor utsträckning för att vi är tillåtna att hantera all nödvändig information om kunder. För vi behöver ju även information som andra företag till exempel en resebyrå aldrig någonsin skulle tillåtas att samla in om det inte var med kundens godkännande. Men vi har alltså möjlighet att samla och använda information som inte nödvändigtvis har godkänts av kunden på det sättet som jag tror att... eller vanlig GDPR-lösningar.

Isak: Jag precis, då har du varit inne ganska mycket på kommande frågor här också. Du nämnde att det skulle kunna vara en lösning med en publik blockkedja där man kunde välja att dela med sig av sin information då till olika banker till exempel. Vad tror du skulle vara den huvudsakliga fördelen för kunden då till exempel, men en sådan lösning?

Christian: De skulle ju kunna... De skulle ju alltid behöva legitimera sig på samma sätt. Det skulle ju gå mycket mer effektivt. Du skulle ju i princip aldrig behöva ta upp legget. De bara tar ut sin mobil och trycker på en knapp om man då dessutom då kan göra den användarvänligt som man har lyckats med Mobilt BankID till exempel, det är ju behändigt och intuitivt. Men bakom mobilt bankid så är det mycket komplex teknik, så det är ju... samma sak kan ju hända då i blockkedjesammanhang. Sen så tror jag att en annan fördel skulle vara att kunderna verkligen kan känna sig säkra med det. Det är ju väldigt säkert... så ja...

Isak: Mm, om vi kollar på....

Christian: Ursäkta, en annan fördel är naturligtvis att de själva kan äga sin information, jag vet vem som har rätt till den och inte, och den integriteten är ju enormt viktig

så det är ju liksom väldigt fundamentalt i det här. Jag tror att det finns någon mer sak... nä, det försvann.

Isak: Okej, vi tar det sen om det skulle komma fram. Om vi då kollar på fördelar för verksamheter och bankerna, vad har vi för huvudsakliga där?

Christian: Nej men de skulle kunna effektivisera hanteringen otroligt mycket och de skulle kunna göra alltså de... Ett, de riskerar inga böter från finansinspektionen för att de skulle vara 100 procent regelefterföljande liksom, så att det är ju en sak. Och ja, jag tror att jag skulle säga effektivisering och de skulle också kunna lita på informationen i högre utsträckning än idag. Det tror jag skulle vara två riktigt stora fördelar, men.... Ja, precis.

Isak: Ja, perfekt. Om vi då kollar på de största utmaningarna... Vi kan ta också om vi tänker på... Är det liksom en publik kedja då? Alla liksom... det ska vara ett gemensamt system för samtliga banker eller företag som behöver kundkännedom helt enkelt?

Christian: Ja precis, för det är ju såhär att om bankerna använder sin egna KYC-lösning på en privat blockkedja som de äger då kommer det 100 procent fördelar för bankerna och 0 procent för kunderna, för då kommer bankerna uppfylla sina behov och det är klart att då kan det bli mer effektivt för kunderna, för de kanske inte behöver svara på frågor en gång om året eller varje gång de blir ny kund så det kanske är mer än 10 procent, men om du däremot har din identitet som du äger oavsett om du interagerar med en bank eller en myndighet eller ja... bokar flyg till exempel eller vad det än är, det är klart att det är mycket mer effektivitet och ja, behaglig upplevelse liksom. Det är ju enklare för kunden och faktum är att vi identifierar dem flera gånger om dagen i olika sammanhang, och det kan vara allt från du vet när vi hyr en hyrbil till när vi gör ett bankärende, och det är klart, den processen skulle ju kunna effektiviseras så att du kanske inte ens behöver identifiera dig, utan att du på blockkedja kan ge en del adresser eller myndigheter aktörer tillgång till din information alltså utan att de behöver fråga dig, för att du har Karolinska till exempel, sjukvården som har tillgång till din journal. Det har du godkänt och det gör du bara en gång.

Isak: Ja, det låter smidigt. Då ska vi se... Är du kvar här?

Christian: Jag är kvar.

Isak: Vad bra, det blev lite märkligt tyst bara. Slutligen, vad ser du för huvudsakliga utmaningar med att försöka implementera en sån här lösning då?

Christian: Ja, men en sak som vissa förespråkar i den öppna världen om man säger så, för visst hann vi gå igenom att det är en kamp mellan privata och öppna blockkedjor?

Isak: Ja det gjorde vi kanske ja...

Christian: För det är ju en jättestor grej. Som jag ser det så är det lite grann jämförbart med eller väldigt mycket jämförbart med internet och E-mail. När det här började sprida sig, för det var väldigt många människor som sa att det här ska vi förbjuda därför att det är bara kriminella som vill gå ut på nätet på dark-web och allt vad det är. Sen var det folk som sa ja det är väl bra men inte för mig, vad ska jag med det till?

Varför ska jag gå in på www.mcdonalds.com och så tar det 5 minuter att ladda ned den sidan och det jag ser när jag laddar ned det, är en McDonalds logga. Det är klart att, vad sjutton ska jag med det till? Om jag vill ha McDonalds, då går jag in och beställer en hamburgare och äter den där ifrån. Inte ska jag gå in på en hemsida i alla fall. Faktum är att det ju var fullt logiskt om man ser det på det sättet som folk gjorde då på 92 liksom, så vi är ju väldigt mycket där också med blockkedjor idag. Vissa ser förstås möjligheterna men andra ifrågasätter det.

Isak: Precis, så du tänker dig att folk måste vänja sig vid tekniken och liksom ta till sig den?

Christian: Ja, det är det jag menar. Samtidigt som det som var poängen som jag inte riktigt sa det är att det pågår en strid mellan de som har intranätsidor och de som är helt öppna som att du själv kan gå in på vilken webbsida du vill. Det var ju ett försök i början av de som sa att det här är för kriminella, när de började förstå att shit det här är ju något som vi måste anamma och våra konkurrenter har ju webbsidor och nu har ju till och med Burger King lagt ut sin meny på webbsidan så det är inte bara en logga. Då började man ju liksom försvara och tycka om vi kan äga all internettrafik så att alla går via vår internetportal och sen går ut det vore ju jättebra, för då kan vi ge... Då har vi massa möjligheter att marknadsföra oss och sälja varor och tjänster och sånt där och så kan de gå ut till andra konkurrenter sen. De gjorde allt för att man skulle använda... Det fanns ju Yahoo och AOL-portaler och sånt där och det föll ju platt. Men ett tag så kämpade företag på det sättet att behålla kontrollen och jag ser litegrann att det är många banker och andra företag som kämpar för att behålla sin kontroll för att den största fördelen med en blockkedja är att den minskar behovet att lita på din motpart, du behöver inte lita på din motpart när du använder bitcoin, det är... Så är det bara liksom och det är klart att det eliminerar eller kraftigt reducerar behovet av mellanhänder. En bank är i väldigt många aspekter, inte alla, men i väldigt många aspekter så är det en mellanhänder och det är ju ett enormt hot mot banker. Då försöker man ju bemöta detta genom att skapa sina privata blockkedjor och såhär och det är möjligt att det fungerar eller att det kommer att bli någon hybridvariant tillslut men det är en utmaning och det pågår ett krig mellan DLT och öppna kedjor. Det kriget är extremt småskaligt, det är fel att säga ett krig egentligen men jag ser de tendenserna överallt.

Isak: Alright, bra. Då tror jag att vi har det hela här. Det är rätt så bra sammanfattat.
Christian: Sen har det kommit ut nu i dagarna att det är 6 nordiska banker som startar ett bolag för nordisk kundkännedom.

Isak: Ja jag såg det imorse här faktiskt, så det är ju spännande. Det stod inte vilken teknik de skulle använda, men...

Christian: Nej och jag tror inte att det är blockkedja, men det är klart att när det finns ett sånt bolag och det finns 6 banker som backar upp det då är ju nästa steg inte lika stort att ta om man vill ha det på en blockkedja som det skulle vara att idag göra en blockkedja av det och det är ju en liten intressant sak. Men de som förespråkar de hävdar ju, eller många av dem hävdar att sådana här försök, till exempel de här sex bankerna, om de skulle skapa en blockkedja så är den dömd till att haverera som en KYC-lösning för att de måste lita på varandra, och de kan inte riktigt det och det är inte tillräckligt många oberoende aktörer som bekräftar transaktionerna varje gång de görs, så det är ett jätteproblem. Sen är det också så att en enskild individ av de här 6 företagen kommer plötsligt att vilja utveckla en viss feature kring den här blockkedjan

medan en annan enhet vill utveckla en annan feature. Då kommer man att få olika agendor och olika utvecklingsbehov och det kommer att bli en utmaning när det då är en gemensam plattform. Så att det är ju, med den kunskapen jag har idag, om jag vore liksom en allsmäktig härskare och bestämde då skulle jag satsa i första hand på en öppen publik blockkedja för identiteter som främst kontrolleras av individen men som kan tas över av myndigheter till exempel om någon åker i fängelse så skulle myndigheten på något sätt kunna liksom påverka informationen. Men det kanske är svårt om den är öppen, den kanske måste vara halvöppen en sådan lösning. Men jag skulle satsa på det mycket, mycket mer än att bygga ihop en KYC-lösning för 6 banker liksom, den kommer inte att vara lika säker den kommer inte att vara lika effektiv för samhället men däremot för bankerna, men även det kommer att utmanas efter några års användande.

Isak: Perfekt, det ska bli spännande att följa. Stort tack för att du ställer upp igen.

Christian: Ja, absolut.

Appendix 5

Intervju Nikos Patsiogiannis:

Filip: Thank you for participating in our study, of course

Nikos: sure

Filip: And i guess we will go straight into it

Nikos: Would you like to just give me some background on who you are and what you do before we jump into the questions?

Filip: Absolutely! So my name is Filip Fjellstedt, and i am currently doing the system sciences, or informatics, bachelor at lund university. So this is the bachelor thesis we are working on, which is the final part of the program. Currently I'm living in Paris with my girlfriend so I'm doing this on distance. I had a break from the program and started working, since then I've quit my job and resumed the program to get my bachelors degree.

Nikos: Okey, that's good, two questions: what is the topic of your thesis and how you came across norbloc?

Filip: In the thesis we want to explore how blockchain can be used to improve, especially swedish banks and financial institutes KYC processes and what kind of possibilities, we want to .. otydligt.. And like, the the general view on blockchain.

Nikos: Okey, Cool. So, how can I help you today?

Filip: Alright, let's see here. Well the first question is the same question to you, if you could tell us a bit about yourself, your role within the company, how you got there, etc..

Nikos: So very briefly about myself, like I said, my name is Nikos, I'm from Greece, I'm the chief operating officer of Norbloc, My background is about 14-15 years of industry and management consulting experience in europe and the middle east, all of which have been spent in financial services, so i have worked in.. from both sides of the table, having covered roles within the industry. I have advised banks and insurance companies on a variety of issues like regulatory compliance, KYC, cross improvement and operations. So regarding Norbloc, Norbloc is, obviously a swedish based company, it was founded in 2016, we're headquartered in Stockholm, and we are... Essentially we are the premier blockchain KYC provider in europe and potentially globally. So essentially we are developing regulatory technology appli..(clicking noise), We are developing software in order to address specific regulatory challenges. In KYC, we though it's a very interesting problem to tackle for the reason that it's a problem that is being widely..eh.. faced, a majority of financial institutions across the world have similar or even the same challenges around KYC, and this, you know, gives a lot of space to improve. At the same time, with the introduction of technologies like blockchain we can develop products which are quite pioneering, in the way that banks and financial institutions in general can potentially capture, validate, store and share KYC information within

same groups or across multiple organisations, eliminating duplication of efforts and increasing security standards.

Filip: Alright, Can i just ask you again Isak to lower the volume on your speakers a little bit to reduce eco

Isak. Ofcourse, Is this better?

Filip: let me see... test test... Yes now it seems to be fine

Filip: So you answered my next question by describing what kind of products you offer, so i'd like to ask your personal view on the future of blockchain or DLT technology future within banking and the financial industry at large

Nikos: Sure, so essentially, you know, blockchain is a buzzword in the last, maybe 2 or 3 years, I think we're very slowly moving from the infant steps to the toddler steps, in the sense that banks gradually start understanding what could be some applicable use cases. Obviously, you know blockchain is not the answer to every potential problem or challenge, and I think in the last, maybe 24 months, we've experienced a lot of noise around blockchain like, you can do this with blockchain or you can do the other with blockchain but in reality there are only a number of use cases that could potentially start being addressed by the banks, and luckily enough, that was also out initial thesis, KYC is one of the most prominent use cases for the use. So generally speaking I think that banks, at least the global banks, they have understood and appreciated blockchain as a technology, they have narrowed down the, you know, the scope of the use cases and applications that could potentially start testing technologies like blockchain and essentially, you know ,now we are moving towards to... oh, Many of them, they have conducted a series of proof-of-concept and pilots in order to assess results and to, you know, see what's the benefits that this kind of technology brings, and now they're ready to move to the next step of production projects. I mean, we have already witnessed some real production cases, especially in the trade finance, but also KYC is one of the fastest growing areas with regards to blockchain that we are currently witnessing.

Filip: Alright, I imagine that you have overcome quite a few challenges already, what do you think is the biggest ones currently on implementing a blockchain based KYC system?

Nikos: I would say that there are 3 kinds of challenges, first one is internally within the banks, as I said, blockchain started out as an exotic thing which banks started, you know, slowly and gradually exploring and trying to understand what they can do with that, so one of the biggest challenges in the beginning was, and still is, you know, how we move from test phase, the pilot phase, the proof-of-concept phase to the production phase. That has to do with the decision making within the banks, that has to do with how quickly banks are adopting innovation, and how quickly banks can test and really fail or proceed to the next step, these are, you know, internal challenges that financial institutions have which are irrelevant to blockchain but obviously affects the curve of adaptability of blockchain. So that's the first one.

The second one is obviously something that relates to challenges with regards to bringing many parties together and create ecosystems around blockchain, the reason for variation of using blockchain technology is to have a safe and alterable way in sharing data, essentially. In storing and sharing data in a decentralized manner. Which means that by definition you need multiple counterparties or stakeholders to get aligned. If i connect this with my first argument it is quite challenging pushing a big organisation towards a direction to make a decision and

start implementing things, you can imagine how, even more difficult, it is to bring 2 or more organisations to work towards the same direction, agree on a common framework or operation, agree on common standards, and so on and so forth. So I think this is the second biggest challenge we are facing, which is not to align very big organisations, and push them or guide them towards the same direction at a decent phase, not even fast, but a decent phase.

The third and final reason, again, it connects to the other two, it is essentially how you are creating common standards. So there are many, many areas within financial institutions, and KYC is one of them where there's not a single standard that applies across a single market or even worse, across multiple markets. So, for example with KYC there's no, let's say, single questionnaire, there's no single way of validating KYC data, there's no, you know, standard operative procedures, so you can say that said bank has this kind of KYC fills and documents that they capture, and say Swedbank has a different set, okay, maybe there's a significant overlap most of the times to the extent of 80 to 90 percent, but again, these are not the same, which means you need to bring to big organisations and agree on this common standard, and agree on the standard operating procedures. And unless these are imposed by an authority that could be, so, like, a top to bottom approach, which is like the law, or how regulation works, when we work vice versa so when we operate from a bottom up approach where the participants need to agree on a common framework, that can be especially challenging

Filip: Alright, I understand, what do you see as the greatest possibilities for improvement by implementing blockchain technology regarding KYC?

Nikos: Yeah, I mean, obviously one of the things we are witnessing is that banks appreciate.. You know.. A number of things, they are appreciating the cost efficiencies they can achieve using blockchain, and the cost efficiencies essentially comes because of the elimination of the duplication of efforts, so if one, for example, in the KYC example, if one party has already validated a client the other party doesn't need to conduct a full KYC procedure from scratch, so essentially you're eliminating the double effort, or similarly if, you know, a client updates his or her information with one bank, he or her doesn't need to go and update the information to every bank, because the same validating information is being disseminated across the ecosystem. So these are, you know, operational and cost efficiencies, so operational efficiencies that creates essentially cost efficiencies. These are, you know, the upsides that the organisations get. At the same time, they offer much better customer experience, because the client doesn't need to go on and on to, you know, all the various parties that they bank with in order to, for example, update their information, they can essentially reusing or recycling already validated data, which means that the whole business happens faster, in a faster manner and the client doesn't need to produce and reproduce and submit and resubmit the same data and the same documents. And finally, you know, the whole compliance standards of the market are increased, because we're on a single level, sorry, at a market level we're creating a single view for the same client. So, when we have a client, we create a single interface between financial institutions and the client and all financial institutions because they're sharing the same validate data, they share, you know, the same standards and the same information which means that they create a single view for a client, so it's not that one bank has this kind of information and another bank has another set of information and nothing reconciles. So everyone has the same information about the client and this increases by definition the compliance standards across the market.

Filip: Alright, and can you see any current risks involving the technology?

Nikos: Risks, i mean, from a technology perspective I don't see any risks in the sense of, you know, obviously it's a newly tested technology, there are multiple providers around that and, you know, all providers need to meet a very high standard, i mean, security and performance standards that banks require. But the technology is scalable enough and it can meet the requirements. In the sense of, you know.. A possible risk could be the time that will be required to adopt this kind of technology, but, every new thing has its own... eh.. It takes its own sweet time until it becomes mainstream. I think that if it took us maybe about 3 years to pass through this initial stage, of the initial orientation around the technology, I think that the subsequent stages of maturity will be much faster.

Filip: Yes i could see that, and, could you walk us through the processes and how your product works?

Nikos: yes, sure, so let's assume that we have, for simplicity purposes, let's say that we have two banks in a market and we have one client, right? That could be either an individual or more interestingly a corporate.. Right? a corporation, that is owned by multiple stakeholders and has multiple beneficial owners. So essentially, when you want to start a banking relationship you go to bank A and you provide.. You know... bank A says hello, we need you to provide this kind of information about yourself and about the sources of your assets, of your funds and so on and so forth. And if you are a company they will want to have some visibility around the beneficial owners, so who owns this corporation. So in the traditional world you need to go and find a utility bill, you need to find all this kind of information like passport copies or ID copies and so on and so forth. And you know, maybe in Sweden, some of these things have been automated through bankID but I can assure you that in the majority of the world, in a majority of places around the world things are still pretty manual and people really need to submit hard copies of their passports or IDs or utility bills or other proof. In our case, we are creating a fully digitized onboarding journey, where, essentially the client expresses an interest to open a bank account, the client receives a link, opens a form, an electronic form, with all of the KYC data that he or she needs to submit. If we are talking about a corporation, we are integrating this questionnaire with publicly available data. So for example, we can integrate with corporate registries and we can pre populate publicly available information. In this way we are achieving two things, the first thing is that we are saving time for the client because we are already completing, maybe 30 or 40 percent of the data required and also we are avoiding any typing errors down the line. The client submits the rest.. Completes the rest of the data missing, uploads any kind of proof that is required, like as i said, passports, IDs, whatever is needed there, in any kind of format, then electronically signs the applications through bankID and submits this form to the bank. The bank then receives that, internally collaborates, you know, there's an internal workflow where multiple KYC officers collaborate for .. (ice?)... principles in order to review and validate the clients data, we integrate our application with other data sources so that they can.. In order to enable KYC officers to cross check the validation of the data provided. So for example we hit politically exposed and sanctioned databases and other negative news databases, whatever its clients require in order to conduct a robust KYC. And we enable the KYC officer to end up in an educated decision on whether to accept or not to accept the specific KYC profile or the specific client based on the KYC profile. From the moment that the KYC officer has validated the information, once the information has been validated only then the information, or a hash of this information, will be stored on the blockchain, right?

Filip & Isak: right

Nikos: So one of the main challenges that blockchain has, is that, whatever you store on blockchain, doesn't mean that the information is necessarily correct or valid, but whatever you store you can assure yourself that it can never be altered. But if you store garbage, all you will assure is that the garbage will not be altered and this is not necessarily good. This means that essentially you need a robust framework of validating the KYC information in the non blockchain world before the information is stored on the blockchain.

Filip: Got it,

Nikos: So once this information, or hashes of this information has been stored on the blockchain, from that very moment the client has an independent portal where he or she can update the information, he or she can exercise any GDPR related rights, for example, revoke access to data or request to delete their data. And finally they can move to other financial institutions, so bank B, and instead of providing again from scratch all the information, when bank B will send that link that I described in my example, that link, that form, will be a 100 percent or 95 percent completed from the data already validated from bank A. So essentially the client has already saved time because he or she doesn't need to refill the form because the data is already there, maybe they will update some data but not necessarily, and they submit this data to bank B, and bank B can see that this data is already validated by bank A. So in that case it's up to bank B to decide whether they trust bank A, so that they will not conduct any KYC and move to the next step, so essentially they are eliminating the duplication of effort, the data has already been validated. Or if they partially trusts, they can do some, lets say, a risk based approach where they can check a few fields in order to gain the confidence that the information is correct. Does it make sense?

Isak: mm

Filip: Absolutely

Nikos: Excellent

Filip: And is the blockchain.. Mm.. What type of blockchain is it? Is it a public or private?

Nikos: It's a private blockchain, it's always a private blockchain because we need to ensure who participates with the node and who makes the validation of the data. So essentially we are controlling who participates and essentially the ones who participates are only the financial institutions who has nodes. In terms of what protocol we use, we claim that we are protocol agnostic, so in essence we can integrate with any mainstream blockchain protocol out there. However, at this stage we are mostly working with hyperledger fabric.

Isak & Filip: Alright,

Fråga8:

Isak: So you mentioned GDPR and that it was compatible with that, that people could delete their data, how does that work? From my understanding most blockchains, you can't really go back and delete data without actually breaking the chain, so how does that work?

Nikos: Right, that is a very good question. So essentially there's two elements. The first one is that, as I said, we are not storing any client data on the blockchain, but we are storing hashes of the data on blockchain. Which means that we are storing pointers of where the data sits across the ecosystem of servers that we are providing to the participants, so the data is being broken into the smallest possible pieces, and is then being encrypted, right?

Isak: Right

Nikos: Or essentially encrypted and then broken, and we are essentially sending these pieces across the ecosystem, across multiple nodes and servers in the system, and only the bank or banks that they have a direct relationship with that client are able to decrypt and read the specific data. So on the blockchain, we are only storing hashes of the pointers of where the data sits in order to be able to decrypt, to reconstruct and decrypt the data. Now, with regards to GDPR, essentially through the independent client portal that we are providing, what we do is that we are creating a new entry on the blockchain where the client states to the bank a request to delete their data, right?

Isak: mm

Nikos: And that proof remains there and cannot be altered for future use, and the bank has the responsibility to go back and delete the data, we can not do that from their servers

Filip & Isak: mm, okey

Isak: So the data is actually stored on the banks' servers and not server that you run?

Nikos: There's actually a middle layer, another layer which is called drill, which is not on blockchain, where we are, as I said, eh, we encrypt and allocate pieces of the data across, and we have proprietary technology developed where we can instantly decrypt the data and unlock the data, should the conditions provide the necessary requirements. So if you meet the requirements, which means that, for example, if you are a client of Swedbank, your information can be instantly decrypted by you and Swedbank.

Isak: Okey!

Filip: Alright, so, the next questions you already touched on, but maybe if you could repeat a little bit, what would be the greatest benefits, both for the end customers and for your clients using your product?

Nikos: I think I covered most of them, but I can summarize the benefits. The benefits for the banks is that there's an elimination of the duplication of efforts and manual labor, which means that the banks can allocate and use less resources for KYC in a more effective manner which means they create high cost efficiencies. At the same time customers has a better customer experience because the whole thing is fully digitized, it's faster, they do not need to submit and resubmit the data, they can update their data with one bank and propagate all these updates automatically and instantly to all participating banks without having to go to each bank separately. And ultimately the compliance, the level of compliance across the market is getting enhanced.

Filip: Great, thank you. Now that you know more about what we intend to explore with our thesis, do you think there's any questions which we have not asked you that we should have asked or is there anything else you'd like to add in general?

Nikos: In general, I think.. No, any other questions.. No. I think for a thesis like yours you have covered the majority of things, in terms of benefits, in terms of risks and in terms of scope of project. I think what's critical in all this noise around blockchain is to identify all the most important use cases, which have the applicability. In the financial services world, my personal view is that KYC and trade finance are the most prominent ones in the coming period, Norbloc is already working on production grade kind of projects, so we are going to have production, you know, live projects in a couple of months with major institutions. In trade finance we have witnessed big platforms like for example we trade in Europe and some others. I believe anything related to money exchange will take a bit more time, for the very reason that, you know, when we are talking about having money in the middle, the level of risk is even higher. So I think that the level of scrutiny by the participating banks will be even higher and take more time until they feel the necessary comfort to proceed towards that route. Finally, there's a number of interesting DLT based use cases outside the financial services, I'm not sure if you are looking at those as well, for example anything related to food tracking, or anything related to containers tracking, I think that's something that's already happening and I think it will actually become mainstream in a very short amount of time. I think that Deloitte, check with Deloitte, they do have some very interesting material that you could potentially look and leverage.

Isak: mm

Filip: mm, thank you

Isak: We forgot to mention, I hope it is alright that we transcribe and use this interview in our study, and if you'd like to be anonymous and Norbloc as well that's fine of course, that's up to you really

Nikos: We don't mind for a reference, however would like to see the transcript or the text in advance just to make sure that whatever we have said reflects, properly reflects what we have said.

Isak: Yes of course, certainly, we will send that to you

Nikos: Excellent, so, unless you have any questions, thank you very much for your time and let me know if you need anything else, just give me a shout guys

Filip & Isak: great thank you very much

Nikos: Take care guys

Filip: You too, take care

Appendix 6

Intervju Ludvig Öberg

Isak: Vi kanske ska börja lite med att... Vad vi undersöker är möjligheten och hur marknaden ser på att använda blockchainteknik för KYC, det vill säga kundkännedomssinsamling, och liksom utformningen av den typen av system. Så vi pratar både med banker och andra aktörer inom branschen och folk som är kunniga inom blockchain. Så att...

Fråga 1:

Isak: Du får gärna börja berätta lite om dig själv, dina tidigare erfarenheter och vad du gör just nu och din relation till blockchain.

Ludvig: Mmm, javisst! Ja, det började med att jag snubblade in på, att hitta bitcoin år 2011, och började jobba med det på heltid 2013 där jag grundade en firma som heter Safello tillsammans med några andra som nu är Sveriges största växlingstjänst för kryptovalutor, och där har jag lite erfarenhet av att jobba med och designa AML/KYC system. Vår tanke var att vi skulle vara den första professionella och reglerade platsen i Sverige där du kunde köpa och sälja bitcoin. Tidigare har det ofta varit hobbyprojekt och liknande som inte varit registrerade hos finansinspektionen och kanske inte följt alla regler precis som man skulle. Men vår ambition var att göra det. Så vi har varit registrerade med finansinspektionen från vår första dag då och, ja, gjort allt det där. Så där jobbade jag som affärsutvecklare i två år, mot sen 2015 gick jag med i en firma som heter Chromaway, som också är en startup, som utvecklar blockkedjeteknik mjukvara skulle man kunna säga, som utvecklar olika produkter, ah, olika plattformar helt enkelt som man kan bygga blockchain applikationer ovanpå, och även bygger några blockkedje applikationer, det kändaste projektet eller vad man ska säga är nog det med svenska Lantmäteriet då, där jag var del av projektet, där det var svenska lantmäteriet, några banker, skatteverket, några konsulter och liknande som gick tillsammans för att digitalisera fastighetstransaktionen och fastighetstransaktionsflödet. Så det projektet var nog huvuddelen av när jag jobbade på Chromaway. Nu jobbar jag lite som konsult, egen byrå samtidigt som jag pluggar, jobbar bland annat kvar lite på Chromaway, men har lite andra utbildnings- och workshop-uppdrag och liknande. Så det är väl en liten snabb summery.

Isak: Okej, perfekt! Då ska vi se..

Fråga 2:

Isak: Om du tittar liksom på blockchain eller DLTs framtid inom finansbranschen lite generellt, vad tror du om det så att säga?

Ludvig: Ja, jag brukar förklara blockchain som att man har tagit inspiration från bitcoin, för bitcoin är ju grunden i allt, och man har tagit inspiration från bitcoin för att bygga och använda det för andra applikationer, så den här idén med decentraliserat nätverk och liknande har man tagit inspiration från och då var det ju först finansbranschen som började, för att man såg att bitcoin, det är ju en valuta, kan man då ha andra sorters tillgångar på en blockkedja? Man kanske kan registrera aktier eller guld eller vad det nu kan tänkas vara, så började man bygga innovationer inom det, men nu skulle jag säga att finansbranschen som först var väldigt dominant inom

blockchain har blivit omsprungna just därför att det är så mycket regler och så många olika aktörer som måste godkänna system innan de kan sättas live. Och då har andra industrier till exempel inom supply chain blivit större för att där kan man snabbare gå till live eftersom att det finns mindre regleringar, men för en bank är det en väldigt stor process att försöka byta ut några IT-system.

Isak: Mmmm.. nu ska vi se, hör ni mig här?

Ludvig: Ja!

Filip: jada

Fråga 3:

Isak, Vad bra, det blev så tyst här.. Perfekt, då har du varit involverad med Lanmäteriet där med implementation av blockchain system. Vad har varit de största utmaningarna med att implementera den här tekniken? På en generell nivå men du får såklart nämna problem som ni stötte på där.

Ludvig: Största problemet skulle jag säga är att blockkedjeteknik är en sorts infrastrukturteknik, det är inte något man bara kan lägga på på sin nuvarande verksamhet och få ut allt av det, utan det är en väldigt stor förändring som man behöver göra ofta i hur man jobbar, hur delar data och liknande och det kräver också att flera parter samarbetar för att uppnå en gemensam infrastruktur för att dela data eller processer. Så det räcker inte med att ett företag har ambitionen att göra någonting de måste också hitta andra parter som de kan integrera det här systemet med då, och där finns det även problem med att... ja.. Det finns en generell ovilja att ändra processer och liknande men även att det är svårt att skapa affärsmodeller som fungerar. Man har problemet med att om man sätter upp ett konsortium eller en blockkedja då, och det är någon som måste ta själva investeringskostnaden i början och då måste de på något sätt få tillbaka de pengarna, men är det för tungt och de gynnar för mycket för de som startade systemet, då motverkar det näteffekten för då vill inte andra konkurrenter eller andra personer på marknaden komma med i det här systemet, för då tycker de att de som skapade det tjänar för mycket pengar, och frågar varför ska vi då gå med, till exempel med banker då, skulle Nordea skapa ett nätverk så kanske SEB inte vill gå med och liknande. Så det har varit problem med hur man, ja, skapar incitament inom systemen och hur man får folk att koppla ihop sig till ett system. Inom finansbranschen där de är ganska hårda.. Ja.. man är ganska illvilliga mot varandra så har man problem med att man har gjort massa olika system, ofta inom en bank och sen så har man haft svårt sen att få andra att komma med. Det har varit nu på lite senare tid som man haft lite större branschöverskridande med till exempel en bankförening och liknande som man faktiskt fått det att funka i Sverige, men i andra länder som inte har något liknande organ har haft det väldigt svårt att faktiskt få igång någonting. Och sen så även juridiska problem då, ehm, all den juridik inom IT-system är baserade på att det finns en ansvarig, om något händer, går systemet ner, går något fel så är det den som är ansvarig för att, ja, leverera och fixa det, men så fungerar det inte riktigt med blockkedjor utan där är det något slags delat ansvar där alla och ingen är ansvariga. Och det blir ganska svårt både från ett business och ett juridiskt perspektiv. Bland annat hade vi då i Lanmäteriet-fallet så hade vi.. Fastnade vi egentligen på att.. Själva lagfarts överföringen krävs inom jordabalken krävs att den ska vara en fysisk signatur, så till exempel då digitala signaturer inte är en liknelse med fysiska signaturer i alla delar av lagen än i Sverige. Så även

ifall det teoretiskt sätt skulle vara möjligt, genom liksom civila(?) kontrakt så är sista biten där med lagfarten som satte stop. Men där finns det även inom EU förslagen av E-id, att man ska likställa då fysiska och digitala signaturer och det tror jag kommer vara viktigt för just blockkedjeteknik att kunna träda i kraft.

Fråga 4:

Isak: Mm, okej, om vi då tittar på de generella största möjligheterna då med blockchainteknik, vad ser du som de största där?

Ludvig: Ja, jag brukar säga att blockkedjeteknik är bra om man är flera aktörer som inte fullt litat på varandra och om man kanske har då en tredjepart som nu har gjort en tjänst till exempel ett clearinghus eller liknande som egentligen inte levererar så mycket värde, utan de har en stark näteffekt som egentligen tvingar alla att använda dem, men egentligen kanske de är lite för dåliga, lite för dyra eller liknande och då finns det möjlighet att man kan skapa ett distribuerat nätverk istället som klipper ut den här mellanhanden då. Så ja, om det då kanske är data som är strukturerad, processer som är strukturerade och som måste återupprepas hela tiden så att man kan programmera det, själva processtrukturen eller vad man ska kalla det.

Fråga 5:

Isak: Mm, alright, om vi tittar på risker med blockchainteknik, vad ser du där?

Ludvig: Ja det är ju fortfarande en väldigt ny teknik, väldigt otestad, även de system som har kommit längst fram inom just privata blockkedjor då är väldigt otestade, publika blockkedjor har ju fördelen att de är publika och blir konstant testade och folk försöker konstant ta sönder dem. Så bitcoin och Etherrum och liknande kan väl anses vara hyfsat säkra, men det är fortfarande svårt att skriva applikationer till exempelvis Ethereum och vara säkra på att det inte finns buggar och liknande. Så det finns inte de här kod standarderna och allt sånt här som skulle krävas för att bygga väldigt säkra applikationer. Och sen så finns det även problemet med det juridiska, hur man ska bygga upp dessa konsortier där avtal är någon sorts foundation man ska bygga upp och liknande. Och där kan det finnas både juridiska- och IT-säkerhetsrisker då. Och det är väl kanske en av de större riskerna. Hur man hanterar privata nycklar och liknande för att säkra de här systemen är väl inte heller något om är särskilt utarbetat än, och det finns alltid risk i att någon kan korrumpiera systemet på så sätt. Men det beror kanske lite på vilken sorts IT-säkerhetsnivå man jämför med.

Fråga 6:

Isak: Perfekt, om vi då går in lite mer på vårt andra fokus då som är KYC, vad vet du om KYC processen idag och hur den brukar se ut?

Ludvig: Ja, jag vet ju lite om det sen jag startade Satello och det är huvudsakligen: Identifiera personen då med pass eller ID eller liknande, identifiera adress med någon sorts räkning av något slag, elräkning, hyresräkning eller liknande, svara på frågor om din riskprofil och var pengarna kommer ifrån och vad pengarna ska användas till och liknande. Så det är ungefär en bild av det vi gör.

Fråga 7

Isak: Och rent tekniskt där då, för er del, var det något digitalt formulär som kunderna fyllde i då, eller hur såg det ut?

Ludvig: Ja, exakt, så vi använde dels då mobilt bankID, vi hade som möjlighet att ladda upp pass eller ID-kort, man laddade upp en räkning digitalt och svarade på ett formulär helt enkelt

Fråga 8:

Isak: Vad tyckte du var de största utmaningarna eller problemen med den processen där, eller var kan man förbättra den så att säga?

Ludvig: Jag tror att inom Sverige hade vi det hyfsat bra, där funkade det ju som det skulle på så sätt att BankID funkade ganska bra. Det vi hade problem med däremot var att säkerställa ID-kort och liknande som inte var från Sverige. Där det kan till exempel vara pass från Tyskland som hade hundra års duration. Där det kan vara egentligen bara en pappersbit, där är det väldigt svårt. Det är ju inte ett felaktigt pass men det är ju kanske inte det man skulle vilja på kvalitén och liknande. Även då kanske Photoshoppade bilder och liknande där de inte... Fake och liknande, det finns ju verktyg där ute men jag skulle säga att de var ganska undermåliga så de slutade med att vi byggde mycket av systemen själva istället. Sen så även problem med kryptovalutor är kanske att det är svårt att avgöra om pengarna som kommer in, alltså den kryptovalutan som kommer in, är från den personen som den faktiskt säger att den är, alltså ingen kompis som kommer in och säljer Bitcoin via oss och så och liknande. Där har vi börjat utveckla system för våra Bitcoin-transaktioner och liknande men det är fortfarande en utmaning inom branschen.

Fråga 9:

Isak: Alright. Tror du att det skulle förbättra någonting om man byggde ett KYC-system på Blockchain, skulle det lösa några av de här problemen eller hur ser du på det?

Ludvig: Ja alltså får man tillräckligt stor användning av ett sådant system så skulle man ju kunna lösa... det är ju egentligen onödigt att alla gör KYC och ställer samma frågor om och om igen. I teorin skulle man ju då bara kunna ladda upp sitt ID-kort och sin elräkning eller vad det nu är och bara svara på de här frågorna en gång och då skulle de svaren då kunna delas med de aktörerna som behöver dem när man registrerar sig för en ny tjänst. Det skulle ju vara mycket bättre användarupplevelse. Man skulle ju även kunna hjälpa varandra, den här kunden hade ett konstigt beteende hos oss, det kanske behöver ytterligare uppföljning eller liknande. För nu är det ju väldigt silo liksom alltså om det görs skumma grejer på Swedbank, då får de inte berätta om det för en annan bank så det kan sättas i system om du skickar transaktioner mellan väldigt många banker så kan inte omfattningen eller att det är konstiga transaktioner kanske är svårare att upptäcka än om man skulle ha någon sorts sätt att dela det här på. Men samtidigt finns det ju banksekretess och integritet som man måste tänka på.

Fråga 10:

Isak: Mmm. Vad tror du att just Blockchain-tekniken skulle tillföra i ett sånt system?

Ludvig: För mig är det just det här att det kanske kan hjälpa med integritetsbiten, att istället för att ha en central databas där alla ID-system ligger i som idag med Mobilt BankID det är ju en autentiseringsserver som har alla publika nycklar och alla certifikat och matchar dom till personnummer och tas den ned så är det ju då problematiskt, för då kan man inte identifiera att det här certifikatet faktiskt är kopplat till det här

personnumret och då fallerar systemet. På liknande sätt i till exempel Indien där de har ID-system baserat på fingeravtryck och irisscanning och liknande så var ju det systemet blev hackat och allt det här läckte. Om hemligheten till liksom där du kan bevisa din identitet läcker så kollapsar ju hela systemet egentligen då går det ju inte att identifiera sig längre på det sättet, då får man hitta ett annat sätt. Så det är ren IT-säkerhetsmässigt att man skulle kunna säkra det. Det andra är integritetsmässigt att med Blockkedja så skulle man i teorin kunna ha att du är ansvarig för din egen identitet så att du kan signera med dina privata nycklar att jag attesterar att jag loggar in på Nordea eller liknande. Nordea skulle i sin tur kunna attestera att den här publika nyckeln, den representerar Ludvig Öberg och sen med hjälp av då instruktion eller till och med zero knowledge proof så skulle man kunna bygga ett system där det bara är dom jag vill ska se som ser den här informationen och jag själv väljer selektivt vilka jag vill dela den med. Eller till och med zero knowledge proofs nya kryptografi att man skulle kunna ställa frågor eller matematiskt bevisa någonting utan att visa datan så du skulle kunna bevisa att Nordea till exempel har godkänt min identitet utan att visa exakt detaljerna över exakt hur det skett eller liknande. Så det är ju såhär med liksom någon sorts distribuerad identitet men också tror jag att det finns ett syfte av att aggregera, för att som Mobilt BankID eller liknande funkar nu det är ju liksom PKI infrastruktur där du har liksom Mobil BankID företaget och dom ger ut certifikat till alla banker och sen kan bankerna med certifikat då ge ut undercertifikat men problemet där är att om du byter bank eller liknande då måste du helt byta certifikat och då måste de oftast göra den här processen om igen bankerna, så det man inställer skulle kunna göra det är att du själv äger din privata nycklar och att andra personer attesterar att du är den du är, det behöver inte bara vara banker utan det skulle kunna vara skatteverket, det skulle kunna vara polisen, det skulle kunna vara sociala medier, vänner och liknande, att de attesterar att du är den du är och det ger en aggregerad bild över din identitet. Så att din identitet inte är så nära kopplad med en bank specifikt utan istället något som du själv äger liksom.

Fråga 11:

Isak: Okej. Ja, och det har du varit inne lite på nu, hur du tror hur en sån här lösning skulle kunna se ut. Men om du vill sammanfatta det lite kanske, och är det en privat eller publik blockkedja som du tror skulle vara bäst för detta?

Ludvig: Mmm, det finns ju vissa som har någon idé om att det ska vara en distribuerad databas där all data ska finnas och så ska det liksom skickas runt mellan bankerna, men det är ganska svårt ur banksekretesssynpunkt, hur det skulle funka med pass och liknande. Det känns som att det bara skulle sluta med att någon lyckas ta sig in eller lyckas korrumpna någon av aktörerna i systemet och dra ut all information så att det läcker, så det känns som en ganska dålig idé. Jag är väl mer inne på det här att man har kedjor av attesteringar att man med hjälp av transaktioner då pekar på den här personen, har de gjort den viss KYC-koll på till exempel Ludvig Öberg då då. Nordea har gjort en passkontroll på Ludvig Öberg och sen kan jag ge ut den här informationen då då, med hjälp av att ja, publicera min transaktion så att jag kan säga till SEB "kolla här vad Nordea gjorde". Det är egentligen en kedja av attesteringar och det är själva individen är själv ansvarig för sin egen identitet. Det är väl så som jag ser att det skulle vara bästa att bygga. Jag tror att en privat blockkedja är vad som är mest troligt att det skulle vara på för att man kanske skulle kunna mer kontroll och för att man skulle kunna bygga upp sina egna incitament och det blir ganska dyrt att ha sådana system om det blir många transaktioner på en publik blockkedja. Det känns som man kan få en tillräckligt hög säkerhetsnivå med säg 30

till 40 aktörer, banker och skatteverket och liknande, att man skulle kunna bygga ett sånt system.

Fråga 12:

Isak: Alright, ja. Vad skulle det innebära för huvudsakliga fördelar för kunder så, alltså de som uppger sin information, privatpersoner. Eller företag kan det ju också vara såklart, men liksom för själva kunden, vad skulle de största fördelarna vara?

Ludvig: Jag tror att man skulle kunna digitalisera mycket mer, jag tror att man skulle kunna, istället för att upprepa och uppge samma dokument till massa olika personer, så skulle man istället kunna ge till en person och om alla andra litar på att den personen har gjort ett bra jobb så skulle man då kunna bara dela den attestationen eller den specifika datan, så man skulle inte behöva upprepande gånger göra KYC, och man kanske skulle kunna koppla bort lite från det här publika infrastrukturen som finns med BankID och att det ska vara bundet till bankerna. Man skulle istället kunna tillåta andra aktörer som också behöver KYC eller inloggning data eller liknande ta del av det här systemet.

Fråga 13:

Isak: Okej, om vi då kollar på fördelarna för verksamheten, alltså företagen som samlar in datan, vad ser du där?

Ludvig: Ja där är det väl största då besparing. Man lägger ju hur mycket som helst på compliance och massa manuella kontroller. Då skulle man då kunna automatisera mycket av det här och att det räcker med att en eller några aktörer gör den här kollen så kan alla andra dela den datan, så det ju kunna finnas ett värde i att man även skulle kunna ha den som är mest effektiv och den som är bäst på att göra det skulle kunna göra de här kontrollerna och sen kan alla andra då möjligtvis få köpa den här tjänsten eller liknande, eller hur man nu skulle bygga upp incitamentet. Men man skulle kunna få en bättre mer effektiv marknad där man inte behöver spendera jättemycket tid att göra exakt samma sak som alla andra gör och massa upprepat arbete.

Fråga 14:

Isak: Ja, vad tror du, om man skulle implementera en sån lösning som vi har talat om här då, med många aktörer som kan komma åt informationen efter kundens godkännande, vad tror du att det skulle vara för utmaningar med att faktiskt implementera den lösningen?

Ludvig: Dels är det väl IT-säkerhetsmässigt som man skulle bygga upp systemet, vem skulle få tillgång till vad? Vem skulle faktiskt drifva systemet? Och även incitamentsstrukturen, hur skulle affärsmodellen se ut? Vem skulle betala för att bygga för systemet, hur skulle det finansieras och liknande? Hur skulle man... ja. Det finns ju en risk med att bygga ett sånt här system att alla bara vill undvika att göra KYC-kontrollen och bara outsourca det så det måste finnas något slags incitament för att göra det, du får betalt, säg varje gång någon använder din KYC-data, eller vad det nu skulle kunna vara, måste finnas incitament så att det inte missanvänds och liknande. Sen så tror jag att det är väl att få ihop tillräckligt många aktörer för att det ska bli effektivt är väl det som är svårt, men lyckas man med det så skulle det kunna funka, även just den här data-sekretess biten och det juridiska är väl det som är utmanande, jag vet inte hur planen skulle se ut. Ett problem till exempel som vi stötte på i Lantmäteriet fallet är GDPR. Rätten att bli bortglömd till exempel, hur löser man det i ett

blockkedjesystem, hur löser man det i ett system där hela poängen är att man inte ska kunna ta bort data i efterhand? Där finns det några idéer som är presenterade om hur man skulle kunna lösa det. Man skulle till exempel kunna ha en hash av en data till exempel, eller att man skulle kunna använda till exempel att kryptera datan och kasta nyckeln. Räknas det då som att datan är kvar? Det finns ingen som kan komma åt den, men det är tekniskt sett kvar. Så det finns sådana aspekter som inte riktigt är testat ännu med GDPR, men som kanske skulle kunna lösa just det problemet.

Fråga 15:

Isak: Mmm, alright. Ja då har vi väl gått igenom de flesta frågorna här. När du vet lite mer om vad vi nu liksom tittar på, är det någon fråga som du tycker att vi missat att ställa?

Ludvig: En grej jag har tänkt på är att helst vill man ju få sådana här system att fungera internationellt. Det är väl det som kanske är det största problemet, att varje finansinspektion har ju auktoritet i sitt eget land, så hur... Det skulle vara en svårighet kanske att skala upp det här, för alla länder har väl... Ja, det finns ju en viss synergi juridiskt inom EU och liknande, men det finns ju även skillnader för varje land, så det är just det, hur får man såna här privata blockkedjor som på något sätt ska spela med det juridiska systemet att funka globalt? Man vill ju att såna här system ska funka för alla, det är ju då man får verkliga skaleffekter och nytta av det.

Isak: Okej, vad har du själv för tankar om det, hur tror du att man skulle kunna...

Ludvig: Ja, det är ju svårt för att ett sånt här system bygger ju på något sätt på tillit. Du måste ju lite på den som har gjort KYC. Om det är någon skum italiensk bank som en svenska bank inte litar på, då gör det ju ingen skillnad vad systemet säger, de kommer ju fortfarande inte kunna använda den datan då, utan då får man försöka bygga standarder på hur en sån här KYC-koll ska göras som så många som möjligt tycker är bra och att man kanske har någon form av whitelist eller liknande, att ja Nordea via godkänner alla som har gjort KYC-kontroll på den här listan, men vi har den här blocklist som inte godkänns till exempel och liknande, att man skulle kunna ha någon form av självreglerande system där de som missanvänder och inte gör de här KYC-kontrollerna bra utan bara försöker göra liksom minimal effort för att känna pengar och liknande, de skulle bli blacklistade. Det blir något slags tillitsystem där bara de som sköter sig, ja... Det är ju lite på så sätt som banksystemet i miniversion gör idag, vi har ju sett alla storbanker som har problem med att de inte har skött sina kontroller ordentligt så jag vet inte nödvändigtvis om det skulle vara ett unikt problem för det här systemet men det är i alla fall något som man borde tänka på i designen av systemet.

Isak: Ja, perfekt. Är det något mer du har tänk på Filip som du tycker att vi borde komplettera med?

Filip: Nej, jag tycker att vi fått bra och tydliga svar på det vi ville veta.

Isak: Mmm jag håller med, absolut. Perfekt, men då är vi nog klara. Tack så jättemycket Ludvig för din tid.

Ludvig: Inga problem, och är det något mer så får ni gärna skicka ett mail om ni kommer på någon fråga i efterhand eller liknande.

Isak: Absolut, det gör vi gärna.

Filip: Superschysst, och vi kan ju även skicka när uppsatsen börjar ta ordentlig struktur och form om du skulle vilja titta igenom om du tycker att vi representerar det du säger korrekt.

Ludvig: Ja super. Lycka till!

Isak: Tack så mycket, ha det fint.

Filip: Ha det fint.

Ludvig: Hej då!

Isak & Filip: Hej då!

Referenser

- Bauman, D., Lindblom, P., & Olsson, C. (2016). *Blockchain decentralized trust*. Retrieved from https://entreprenorskapsforum.se/wp-content/uploads/2016/10/NaPo_Blockchain_webb.pdf
- Bauman, D., Lindblom, P., & Olsson, C. (2017). *Blockchain*. Paper presented at the Decentralized Trust, Näringspolitiskt Forum Rapport.
- Beck, R., & Müller-Bloch, C. (2017). Blockchain as radical innovation: a framework for engaging with distributed ledgers as incumbent organization.
- Bisnode. (u.å.). Vad är KYC? Och hur kan ditt företag förhindra terrorism? Retrieved from <https://www.bisnode.se/kunskap/vara-tankar-om/vad-ar-kyc/>
- BitFury Group. (2015). *Proof of stake versus proof of work*. Retrieved from <https://bitfury.com/content/downloads/pos-vs-pow-1.0.2.pdf>
- Bryman, A., & Bell, E. (2017). *Företagsekonomiska forskningsmetoder* (Upplaga 3 ed.): Liber.
- Buterin, V. (2015). On Public and Private Blockchains. Retrieved from <https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/>
- Carson, B., Romanelli, G., Walsh, P., & Zhumaev, A. (2018). Blockchain beyond the hype: What is the strategic business value. *McKinsey & Company*.
- Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. *Applied Innovation*, 2(6-10), 71.
- Datainspektionen. (u.å.). Dataskyddsförordningen (GDPR). Retrieved from <https://www.datainspektionen.se/lagar--regler/dataskyddsförordningen/>
- District0x. (u.å.). What Is Ethereum? Hämtad från <https://education.district0x.io/general-topics/understanding-ethereum/what-is-ethereum/>.
- Drescher, D. (2017). *Blockchain basics*: Springer.
- Ethereum. (u.å.). Ethereum is the foundation for a new era of the internet. Retrieved from <https://www.ethereum.org/beginners/>
- European Securities and Market Authority. (2016). *Discussion Paper The Distributed Ledger Technology Applied to Securities Markets*. Retrieved from https://www.esma.europa.eu/sites/default/files/library/2016-773_dp_dlt.pdf
- FinTech Network. (u.å.). *Four Blockchain Use Cases for Banks*. Retrieved from https://blockchainapac.fintecnet.com/uploads/2/4/3/8/24384857/fintech_blockchain_report_v3.pdf
- Furlonger, D., & Valdes, R. (2017). Practical blockchain: a Gartner Trend Insight Report. In Glaser, F. (2017). Pervasive decentralisation of digital infrastructures: a framework for blockchain enabled system and use case analysis.
- Grewal-Carr, V., & Marshall, S. (2016). Blockchain: Enigma. Paradox. Opportunity. *Deloitte, UK, Tech. Rep.*
- Guan, Z., Si, G., Zhang, X., Wu, L., Guizani, N., Du, X., & Ma, Y. (2018). Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities. *IEEE Communications Magazine*, 56(7), 82-88.
- Gupta, M. (2018). *Blockchain for dummies* (2 ed.). Hoboken: John Wiley & Sons, Inc.
- Iansiti, M., & Lakhani, K. R. (2017). The truth about blockchain. *Harvard Business Review*, 95(1), 118-127.
- Jacobsen, D. I., & Sandin, G. (2002). *Vad, hur och varför: om metodval i företagsekonomi och andra samhällsvetenskapliga ämnen*: Studentlitteratur.

- Kaletovic, D. (2018). Banks Spent \$1.7B On Blockchain Last Year. Retrieved from <https://www.nasdaq.com/article/banks-spent-17b-on-blockchain-last-year-cm978640>
- Kannengießer, N., Lins, S., Dehling, T., & Sunyaev, A. (2019). What Does Not Fit Can be Made to Fit! Trade-Offs in Distributed Ledger Technology Designs. *Trade-Offs in Distributed Ledger Technology Designs (January 10, 2019)*.
- KPMG International. (2018). *Could blockchain be the foundation of a viable KYC utility?* Retrieved from <https://assets.kpmg/content/dam/kpmg/xx/pdf/2018/03/kpmg-blockchain-kyc-utility.pdf>
- Lin, I.-C., & Liao, T.-C. (2017). A Survey of Blockchain Security Issues and Challenges. *IJ Network Security, 19(5)*, 653-659.
- Lootsma, Y. (2017). Blockchain as the Newest Regtech Application—the Opportunity to Reduce the Burden of KYC for Financial Institutions. *Banking & Financial Services Policy Report, 36(8)*, 16-21.
- Mills, D. C., Wang, K., Malone, B., Ravi, A., Marquardt, J., Badev, A. I., . . . Kargenian, V. (2016). Distributed ledger technology in payments, clearing, and settlement.
- Moyano, J. P., & Ross, O. (2017). KYC optimization using distributed ledger technology. *Business & Information Systems Engineering, 59(6)*, 411-423.
- Murray, M. (2018). An Examination of the Blockchain, the Emerging Technology that Promises to Transform Digital Tracking of Assets.
- Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. *Business & Information Systems Engineering, 59(3)*, 183-187.
- Pilkington, M. (2016). 11 Blockchain technology: principles and applications. *Research handbook on digital transformations, 225*.
- Rogers, E. M. (2010). *Diffusion of innovations*: Simon and Schuster.
- Rotolo, D., Hicks, D., & Martin, B. R. (2015). What is an emerging technology? *Research Policy, 44(10)*, 1827-1843.
- Rückeshäuser, N. (2017). Typology of distributed ledger based business models.
- Srinivasan, R. (2008). Sources, characteristics and effects of emerging technologies: Research opportunities in innovation. *Industrial Marketing Management, 37(6)*, 633-640.
- Svenska Bankföreningen. (2017). Känn din kund. Retrieved from <https://www.swedishbankers.se/foer-bankkunder/penningtvaett/kaenn-din-kund/>
- Swanson, T. (2015). *Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems* Retrieved from <https://allquantor.at/blockchainbib/pdf/swanson2015consensus.pdf>
- Tapscott, D., & Tapscott, A. (2016). *Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world*: Penguin.
- Thomson Reuters. (2016). Thomson Reuters 2016 Know Your Customer Surveys Reveal Escalating Costs and Complexity Retrieved from <https://www.thomsonreuters.com/en/press-releases/2016/may/thomson-reuters-2016-know-your-customer-surveys.html>
- Thomson Reuters. (2017). *A Blockchain Enabled KYC Solution: New Horizon or False Dawn?* . Retrieved from https://www.refinitiv.com/content/dam/marketing/en_us/documents/white-papers/kyc-blockchain-white-paper.pdf
- Wander, A. S., Gura, N., Eberle, H., Gupta, V., & Shantz, S. C. (2005). *Energy analysis of public-key cryptography for wireless sensor networks*. Paper presented at the Third IEEE international conference on pervasive computing and communications.
- World Economic Forum. (2016a). *The future of financial infrastructure*. Retrieved from http://www3.weforum.org/docs/WEF_The_future_of_financial_infrastructure.pdf

- World Economic Forum. (2016b). *Top 10 Emerging Technologies of 2016*. Retrieved from http://www3.weforum.org/docs/GAC16_Top10_Emerging_Technologies_2016_report.pdf
- Wu, H., & Wang, F. (2014). A survey of noninteractive zero knowledge proof system and its applications. *The Scientific World Journal*, 2014.
- Xu, X., Pautasso, C., Zhu, L., Gramoli, V., Ponomarev, A., Tran, A. B., & Chen, S. (2016). *The blockchain as a software connector*. Paper presented at the 2016 13th Working IEEE/IFIP Conference on Software Architecture (WICSA).
- Zheng, Z., Xie, S., Dai, H.-N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services*, 14(4), 352-375.