Evaluering og implementering av Digital Identity Ledger for blokkjede systemer

Jesper Hustad og Fredrik Julsen

2019/07/18

Sammendrag

Dagens autentisering systemer består hovedsakelig av individuelt implementerte identiter (konto som bare fungerer på en nettside) eller identitetsleverandører som har kontroll over mange tjenester (Sign in with Facebook/Google osv.). Dette fører til dårlig sikkerhet og er ikke bra for personvern. Digital Identity Ledger prøver å løse disse problemene ved å gi individet kontroll over sin egen bruker gjennom blokkskjede teknologi. Prosjektet er en fullstendig implementasjon av en nettapplikasjon med grensesnitt mot en egenprodusert Digital Identity Ledger som blir lagret på et Etherium basert nettverket. Dette er gjennomført med en brukervennlig demo som guider brukeren gjennom de nødvendige stegene for å sette opp, produsere, lagre, og verifisere en legitimasjon. En server tjeneste håndterer kommunikasjon med blokkjeden. En smart kontrakt verifiserer at signaturene er gyldig. Brukerundersøkelse viser at de fleste klarer selv å bruke Digital Identity Ledger systemeet gjennom demoen. Prosjektet viser mulighetene Digital Identity Ledger og selv-suveren identitet har som erstatninger for tradisjonelle autentisering metoder.

Abstract

Today's authentication systems mainly consist of individually implemented identities (accounts that only work on one website) or identity providers who have control over many services (Sign in with Facebook / Google etc.). This leads to poor security and is not good for privacy. Digital Identity Ledger tries to solve these problems by giving the individual control over their own user through blockchain technology. The project is a complete implementation of a web application with an interface to a self-produced Digital Identity Ledger that is stored on an Etherium based network. This is done with a user-friendly demo that guides the user through the necessary steps to set up, produce, store, and verify an ID. A server service handles communication with the blockchain and a smart contract verifies that the signatures are valid. User survey shows that most people manage to use the Digital Identity Ledger system through the demo. The project shows the possibilities Digital Identity Ledger and self-sovereign identity have as replacements for traditional authentication methods.

Forord

Denne bacheloroppgaven ble tilbudt av NTNU og vil være fullføringen av bachelorstudiet dataingeniør, bachelor i ingeniørfag ved Norges teknisk-naturvitenskapelige universitet. Prosjektet har vært en lærerik opplevelse der vi fikk bruke spennende ny teknologi og fikk erfaring med fagstoffet generelt. Før prosjektet var vi nysgjerrige på hvordan teknologien fungerte siden dette domenet er relativt nytt og komplekst. Det var derfor en spennende opplevelse å jobbe med oppgaven og vi håper denne rapporten gir nytting informasjon til de interesserte.

Vi ønsker å takke Surya Kathayat som har vært hjelpsom med verdifull tilbakemeldinger gjennom hele prosessen og en uvurderlig ressurs av dyptgående fagkunnskap. Ønsker å takke master studen Anushka Subedi for samarbeidsmøte som var øyeåpnende til mulighetene og verktøyene som vi kunne ta i bruk. Dessuten ønsker vi også å takke programansvarlig Grethe Sandstrak som klarte å være løsningsorientert selv i vanskelige situasjoner og som har gjort Dataingeniør studie til en bedre opplevelse.

J.F. Hustad & F.H. Julsen

- 20 mai 2022 Trondheim

Oppgavetekst

I dette prosjektet vil en blokkjedebasert MVP på Digital Identity Ledger bli utviklet med en pedagogisk og faglig reise for Ola Nordmann.

- Det blir opprettet en identitet når Ola start på universitetet.
- Identiteten hans vil bli oppdatert etter endt utdanning, opp på denne første jobben, når han skifter jobb, når han går inn i en annen universitet for videre studier, når han oppretter sin LinkedIn-konto, og så videre.
- Hans identiteter (og relevante attributter) kan valideres underveis, for eksempel av arbeidsgivere, Finn.no eller akademiske institusjoner.

Konkret oppgave er å evaluere og bruke en eller flere blokkjede teknologier som Ethereum, Corda, Hyperledger, etc. og bygg en nettapplikasjon på toppen av den støttende brukssaken som ovenfor for identitetsoppretting, identitetsoppdatering og senere identitetsbekreftelse.

Når det gjelder oppgaveteksten nevnt ovenfor, er de resulterende forskningsspørsmålene definert som:

- **FS1:** Hvordan kan en Digital Identity Ledger bli implementert
- **FS2:** Hvordan designe en nettapplikasjon for å støtte DIL
- **FS3:** Hvilke blokkjede teknologier er best egnet for DIL

Contents

Figures

Tables

Chapter 1

Introduksjon og relevans

Hva utgjør din identitet? Hva gjør deg til den du er? Hva er det med deg som skiller deg fra andre? Filosofer har kranglet om disse spørsmålene siden begynnelsen av tiden. Identitet er et vanskelig begrep å slå fast.

> Identity is a uniquely human concept. It is that ineffable "I" of self-consciousness, something that is understood worldwide by every person living in every culture. As René Descartes said, **Cogito ergo sum — I think, therefore I am.**
>
> *Christopher Allen [1]*

Det er tydelig at vi er på et vendepunkt med hensyn til hvordan den digitale verden samhandler med den fysiske verden. De eldre systemene i den fysiske verden har ikke holdt tritt med den digitale verdenens økende betydning. Ettersom begge verdene fortsetter å smelte sammen, vil dette måtte endres. Dette gir oss en mulighet til å lage systemer som bygger bro mellom de to. Systemer som opererer med en annen oppfatning av identitet. Hvis vi designer dem godt, vil de tillate oss å redefinere hvordan moderne samfunnet tenker om identitet. Kanskje få oss nærmere det ubeskrivelige "jeg" av selvbevisstheten.

Internettet får stadig større tilgjengelighet, godt over 90% i nord Amerika og nord og vest Europa. [2] Med det har flere folk tilgang på og bruker digitale tjenester. Totalt på sosiale medier er det omtrent 5 milliarder brukere og i 2020 alene har internettbrukere vokst med 8 % og brukere av sosiale medier med 14 %. Imidlertid er det et veldig fundamentalt problem som ennå ikke er løst. Verifiseringen av den virkelige identiteten til de enorme antall internett brukerene er en av disse problemene vi forsatt sliter med. Det er stort problem med falske identiteter og svake verifisering mekanismer for å verifiserer ekteheten til nettidentiteten er fundamentalt utilstrekkelig. På den andre siden, i motsetning til den fysiske verden, er online identiteter så frakoblet at en fysisk identitet blir identifisert av forskjellige fragmenterte identiteter på forskjellige nettsteder. En mulig løsning finnes i selv suveren identitet og blokkjede teknologien. Potensialet er ikke bare å muliggjøre kobling, sikker administrasjon og lagring av digitale identiteter, men også for å gi kompatibelt og manipulasjossikker infrastruktur.

1.1 Rapportens struktur

Rapporten består av 6 kappitler. I introduksjonen er prosjektbeskrivelsen og forskningsspørsmål. 2. Teori og relevant litteratur introduserer det teoretiske grunnlaget i prosjektet. 3. Metode beskriver forskningsmetoden og de forskjellige valgene og implementasjonene som ble tatt. 4. Resultater er de ingeniørfaglige, vitenskapelige, og administrative resultatene fra prosjektet. 5. Diskusjon går gjennom valgene tatt og mulig fremtidlig arbeid. 6. Konklusjon av oppgaven. Samfunnspåvirking er effekten prosjektet kan ha.

1.2 Akronymer og forkortelser

NTNU: Norges teknisk-naturvitenskapelige universitet

FS: Forskningsspørsmål

SSI: Selv Suveren Identitet

EKDS: Elliptisk Kurve Digital Signaturalgoritme

TLS: Transport Layer Security

SSL: Secure Sockets Layer

MVP: Minimum Viable Product/Minimum levedyktig produkt

DIL: Digital Identity Ledger

Chapter 2

Teori og relevant litteratur

For å ha en effektiv diskusjon av digital identitet og dens bruksområder er det nødvending å gjennomgå flere teoretiske konsept. Dette innebærer et bredt utvalg av teknologier, rammeverk, og begrep. Kombinasjonen av forskning og systemutviklings aspektet beskrevet i oppgavens mål krever et stort spekter av konsepter innenfor fagfeltet; et større system-implementerings perspektiv samt smart kontrakters innviklet asymmetrisk krypterings-algoritme.

2.1 Autentisering

Brukerautentisering er essensielt og et krav for dagens tjenester, det er en prosess som bekrefter identiteten til bruker av en dataenhet eller tjeneste på nett. En pålitelig brukerautentiserings-mekanisme er avgjørende for å hindre ulovlig tilgang. Disse tjeneste lagrer sensitiv personlig informasjon (f.eks e-post), selv bank konto forventes å være tilgjengelig gjennom nettverk. Uautorisert tilgang vil da ha alvorlige konsekvenser som tap av penger. Dette understreker hvor viktig det er med godt gjennomført sikkerhet i tjenester. Forskjellige implementasjoner av autentisering beskrives i mer detalj senere i teksten, men viktig å få med seg er kjernekonseptet bak autentisering, det er kategorisert inn i tre hovedgrupper [3].

- **Kunnskaps faktor**
  Noe du *vet* som for eksempel et passord.

- **Iboende faktor**
  Noe du *er* som ditt fingeravtrykk.

- **Besittelse faktor**
  Noe du *har* som engangskoder eller kodegenerator.

Kunnskaps faktor har vært den mest populære og enklest å implementere av de forskjellige hovedgruppene. I nyere tid har det vært stort fokus på å implementere

flere faktorer i autentiseringsystemer, multi-faktor eller to-faktor autentisering. Dette øker sikkerheten ved å gjøre det vanskeligere for et fiendtlig parti å tilegne seg begge faktorene. Enkel autentisering alene er nyttig alene men er en byggestein for å opprette mer avanserte metoder for autentisering.

2.2 Asymmetrisk kryptering

Grunnlegende for dagens mer avansert digital sikkerhet er signaturer og kryptering. Dette beskriver forskjellige måter å garantere informasjonen du mottar er fra riktig parti. Asymmetrisk kryptografi prosessen baserer seg på to nøkler, en offentlig nøkkel og en privat nøkkel for å kryptere og dekryptere meldinger. Det finnes mange protokoller som er avhengige av asymmetrisk kryptering, eksempler på dette er Transport Layer Security (TLS) og Secure Sockets Layer (SSL) som gjør sikre websider med HTTPS mulig [4].

Det finnes flere implementasjoner av asymmetrisk kryptering. De største er elliptisk kurve digital signaturalgoritme (EKDS) eller ECDSA på engelsk, Rivest-Shamir-Adleman (RSA), Pretty Good Privacy (PGP) og Diffie-Hellman. Den brukt i de fleste blokkjeder er EKDS og derfor den fokusert på i denne teksten, men generelle konsepter knyttet til asymmetrisk kryptering er like mellom algoritmene.

Spesielt aktuelt for sertifikater er evnen å signere meldinger. Signaturer garanterer at innholdet i en melding er fra utgiver. Mattematikken bak algoritmen er ikke innenfor rammene av prosjektet, men pseudokode av de forskjellige funksjonene tilgjengeligort av EKDS hjelper å visualisere flyten.

```
privat_nøkkel, offentlig_nøkkel = EKDS_lag_nøkler()
melding = "melding␣som␣blir␣signert"

signert_melding = EKDS_signer(privat_nøkkel, hash(melding))

# hos motakker som ikke har tilgang til privat nøkkel:
gjenopprettet_nøkkel = EKDS_gjenopprett(signert_melding, hash(melding))

if(gjenopprettet_nøkkel = offentlig_nøkkel):
    print("signaturen␣er␣gyldig")
```

For å signere en melding brukes en hash funksjon på innholdet og hashen er signert med den private nøkkelen. En mottaker kan da bekrefte at innholdets signatur er gyldig. Først bruker de også hash funksjonen på meldingen og en gjenopprettings funksjon. Hvis verdiene av den gjenopprettet nøkkel og offentlig nøkkelen er like, vet man at signaturen er gyldig. [5]

2.3 Silo domene modell og sentralisert identitet

Silo domene modellen er individuelt implementerte bruker-identitet av flere tjenster. Identitet domene beskriver bruksområde av tilknyttet tjenester til en bruker-identitet. I en silo modell tilhører hver identitet ett domenene med en tjeneste

som har sin egen identitetsleverandør (se figur 2.1). Hver identitetene hånteres individuelt av tjenesten. Dette fører til en enkel modell der hver bruker har en identitet som lagres av tjenesten. Samtidig trenger brukere å håndtere mange fragmenterte identiteter for hver tjeneste.

Forutsigbart forårsaker denne løsningen at brukere må lage mange identiter for hver tjeneste som alle må huskes. Resultatet er en dårlig brukeropplevelse. Den stadig økende nettbruken globalt [2] forverrer problemet. At brukere må håndtere mange identiteter er upraktisk og skaper dårlig sikkerhetspraksis. Repeterende/-lignende passord betyr at et firma sitt passord sikkerhetsbrudd gjør alle andre identiter blottstilt.

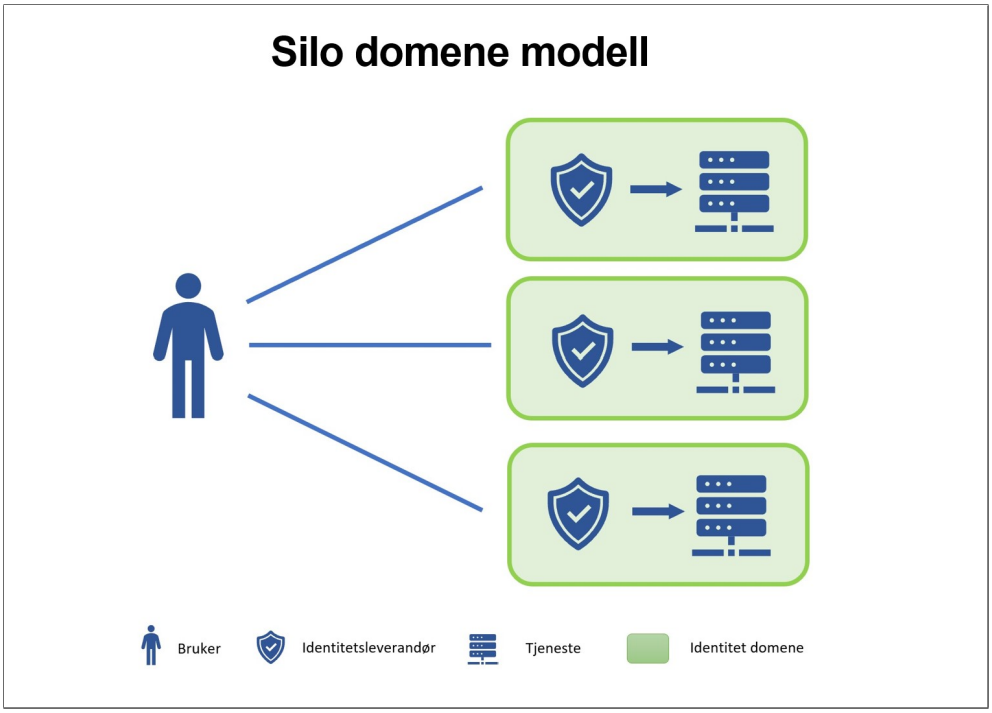

Figure 2.1: Visualisering av silo domene modell

2.4 Føderert identitet

Føderert identitet prøver å løse problemene tilknyttet silo modellen ved å ha identitet domener som tilhører flere tjenester. Brukeren sin identitet kan bruker på flere tjenester. Dette skaper en bedre opplevelse for kunden. Identitetsleverandør (IDL) i denne modellen er et tredjeparti som ikke trenger å være tilknyttet tjenesten.

For å være konkurransedyktig i markedet kan IDL sine tjenester være gratis, da tjenes det på brukerens data istedet. Sosiale medier sin virksomhet baserer seg på å tjene på persondata og de fleste brukere har allerede en konto hos sosiale

medier som gjør dem godt egnet til å ta denne som rollen IDL, men dette svekker brukerens personvern. Den sentraliserte karakteren av identitetsleverandører kan være en svakhet. Om en tjeneste har brukere på en IDL som blir lagt ned mister disse brukerene tilgang til tjenesten.

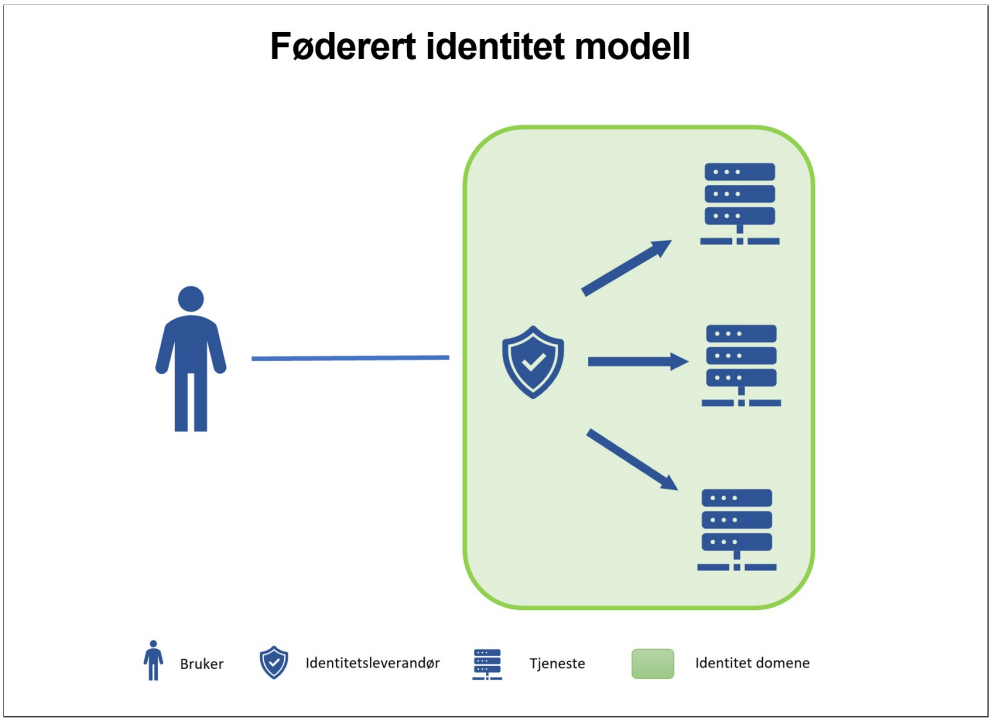

Figure 2.2: Visualisering av føderert identitet modell

2.5 Selv suveren identitet

I motsetning til de tidligere nevnte systemene der identitetsleverandør er i sentrum av identitetsmodellen er selv suveren identitet (SSI) brukersentrisk (se 2.3). Denne løsningen en mer desentralisert og har brukeren i kontroll av identiteten sin. En Digital Identity Ledger (DIL) er en SSI implementasjon der blokkskjeden erstatter registreringsmyndigheten. Den identifiserende faktor (adresse) er knyttet til brukeren gjennom asymmetrisk kryptografi.

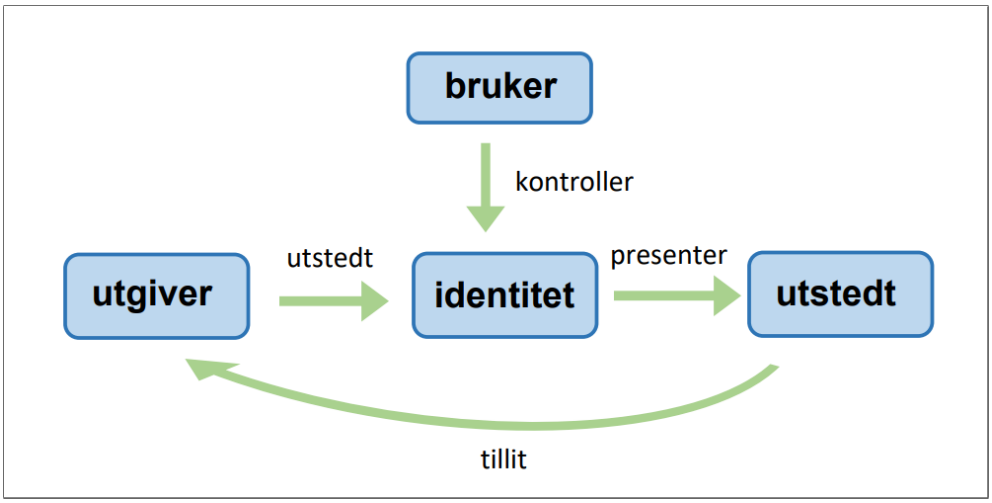

Figure 2.3: Visualisering av føderert identitet modell

2.6 Blokkjeden

For å oppnå et desentralisert nettverk er blokkjeden den mest vellykket løsning til dags. Blokkjeder er beskrevet som digitale "kontobøker" hvor digitale transaksjoner kan registreses i blokker. Kryptografi garanterer at dataen beskrevet i blokkjeden kan stoles på. På grunn av at blokkjeden er distribuert av et peer-to-peer nettverk er det ingen sentral administrator, dette beskrives som å være desentralisert og er et viktig evne for et trygt system.

For å gjennomføre logiske operasjonen i blokkjeden eksisterer smart kontrakter. Smart kontrakter inneholder kode blir kjørt automatisk[6]. Blokkjeder muliggjør smarte kontrakter som er implementert i hovedsak på toppen av blokkjeder. Smart kontrakter inneholder tjenester som tilgjengeliggjøres for alle. Sammenlignet med tradisjonelle systemer er dette nærme en salgsautomat som kan brukes av alle og veksler penger for tjenester. Hver gjennomføring av kontrakten er registrert som en uforanderlig transaksjon i "regnskapsboken". Kontrakten garanterer håndhevelse av reglene og logikken den er basert på som betyr de er egnet for autentisering.

En transaksjon må gjennomføres for å kjøre smart kontrakter på grunn av kostnader med å legge til resultatet i "regnskapsboken" blokkjeden består av. Prisen på transaksjonsen avhenger av prisen på selve blokkjeden, størrelsen på arbeidet gjennomført og mengden data lagret. En viktig evne med smart kontrakter er at de må være deterministisk og ikke-probabilistiske, det betyr at det kan ikke eksistere tilfeldige utfall [7].

Chapter 3

Metode

3.1 Forskningsmetode

Innenfor forskningsmetoder er det viktig å skildre mellom kvantitativ og kvalitativ metoder. *Kvantitativ forskning* forklarer fenomener ved å samle inn numeriske data som analyseres ved hjelp av matematiske metoder da spesielt statistikk. *Kvalitativ forskning* søker å svare på spørsmål om hvorfor og hvordan mennesker oppfører seg på den måten de gjør og er mer fokusert på menneskelig atferd. Prosjektet og arbeidet er systemutvikling. For et slikt prosjekt er valg av teknologi et viktig punkt som må fokuser på i kapitellet.

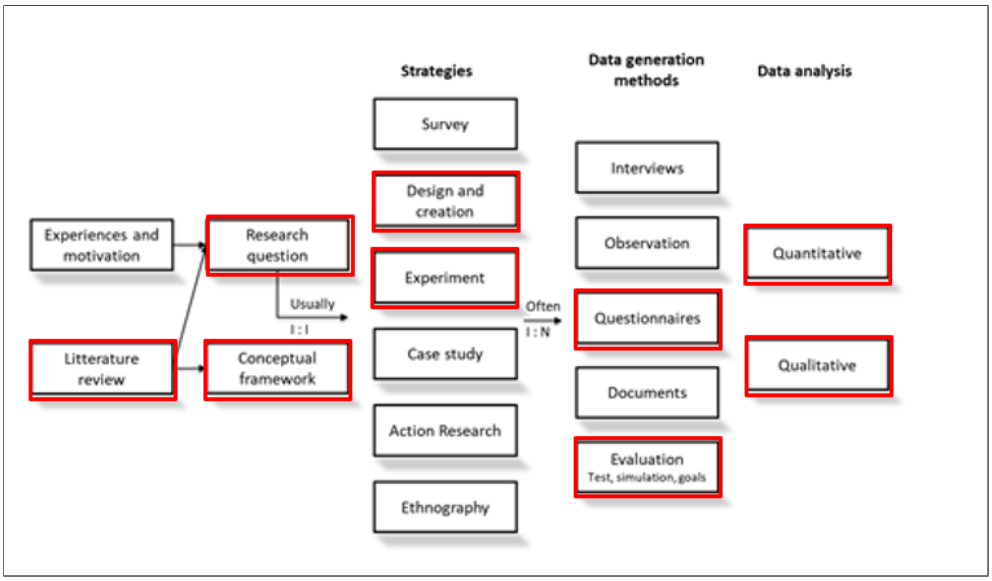

Figure 3.1: Relevante forskningsmetoder uthevet i rødt

For å undersøke spørsmålene i oppgaven er flere metoder brukt 3.1. På grunn av systemutviklings delen av prosjektet er produksjon design og eksperimentering relevante.

Data generering kommer fra å evaluere prosjektet imot målene og en spørreundersøkelse.

Kvantitativ data kommer fra spørreundersøkelsen imens den Kvalitativ analysen består av bruksområde hvordan løsningen kan brukes av personer.

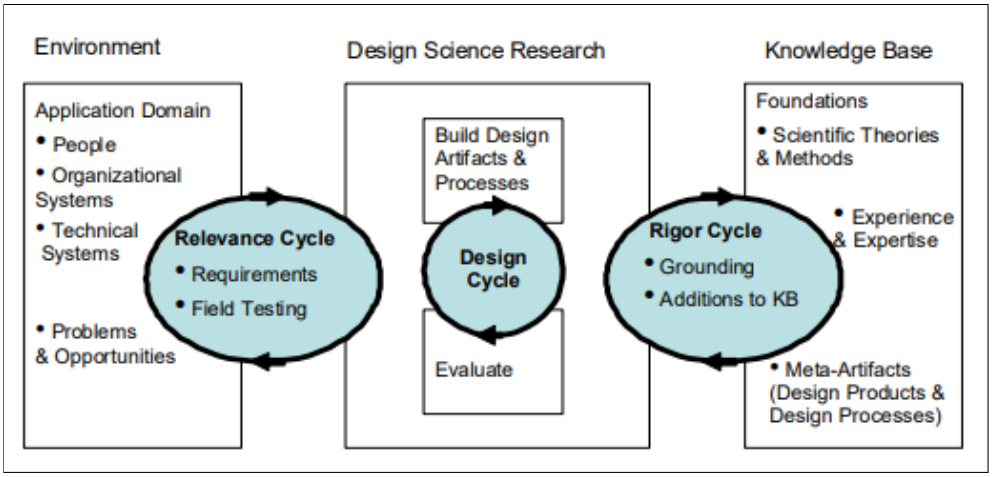

Figure 3.2: Utviklingsforskning modell hentet fra *A Three Cycle View of Design Science Research [8]*

Fagstoffet og utviklingsforskning modeller hjelper utviklingen til å være mer vitenskapelig og strukturer. Den setter en prosess som kan følges for pålitelige resultater i forskjellige utviklingsmiljøer.

Identitet og autentisering er et felt med mye eksisterende forskning som gjør det enklere å evaluere løsningene med disse modellene og rammeverk. Samtidig er mesteparten av disse basert på tradisjonelle autentiseringsmetoder som ikke er relevant for å oppnå målet av en Digital Identity Ledger.

På grunn av tidsrammene til prosjektet er løsningen ikke implementert med ekte brukere for en tjeneste men heller en MVP. Selv vi har om implementasjonen er skapt med fremtidlig utvidelser i baktanke og bred bruksområde er det problemstillinger og forviklinger som ikke blir testet på grunn av at dette er en MVP.

3.2 Valg av blokkskjede

Flere blokkskjeder ble evaluert i arbeidsprosessen. Det er flere mål og kriterer i valget. Kostnader på transaksjoner på være lave slik at løsningen er nyttig og kan brukes for autentisering, hvis det koster 500kr å produsere sertifikat er det ikke en brukbar løsning. Blokkjeden må være relativt populær slik at den støttes i fremtiden, hvis det ikke er nok folk som er på blokkjeden kan den ikke lenger stoles på. Til slutt må smart kontraktene være implementert på en god å sikker måte som kan arbeides med innenfor tidsrammene.

Polygon blokkskjeden er det valget som gjorde det best på disse kriteriene.

Blokkjeden er et såkalt "lynnettverk" som reduserer prisene på tranaksjoner. Polygon kjøres på Etherium nettverket som er det nest største blokkjeden bak Bitcoin. Støtter smart kontrakt språket Solidity som har pålitelige funksjoner for asymmetrisk kryptering og signaturer og enkelt å arbeide med.

3.3 Digital Identity Ledger implementasjon

Det er uenighet i fagområde om hvor legitimasjon skal lagres. De tre forskjellige valgene er i blokkjeden, i en ekstern database, eller lokalt. Disse har alle styrker å svakheter knyttet til seg og den beste løsningen er kanskje en hybrid mellom alle tre. Argumentet imot å lagre legitimasjon i blokkjeden er at det da ikke lenger er privat. Det finnes noen potensielle måter rundt dette problemet som at brukere kan selv kryptere dataen, men det større problemet er at en alltid må tilslutt sjekke blokkjeden for å få den original kilde til sannhet.

3.4 Nettapplikasjon implementasjon

For implementasjonen av nettapplikasjon ble NodeJS basert på javascript brukt. Målet er å skape en fungerende MVP innenfor tidsrammen og Node JS ble derfor valgt for å være best egnet til det målet. Svakheten med Javascript over type safe språk som Java, C#, eller Rust er at det er enklere å introdusere små feil i programmet. Spesielt i større prosjekt er det ønskelig å bruke slike språk. I dette tilfellet i det smale arbeidsområde som oppgaven legger frem oppveier fordelene ulempene.

De statiske websidene er skrevet direkte med html, css, og javascript istedet for å bruke et rammeverk. Det er en generell visdom at frontend rammeverk er foretrukket i utvikling av websider. Men med tanke på kravene til nettsidene, kompleksiteten som medfølger og tidsrammen brukes det ikke.

Chapter 4

Resultater

4.1 Ingeniørfaglige resultater

Dette er resultatene av de forskjellige målene fra første kapittel. Dette inneholder smart kontrakten, arkitektur av systemet og detaljer på implementasjonen av det minimum levedyktig produktet med skjermdumper av grensesnittet.

4.1.1 Smart kontrakt

Smart kontrakter som nevnt i teori kapittelet er kode som kan bli kjørt i blokkjeden. Disse inneholder tjenester som kan bli brukt av alle i blokkjeden. Funksjonaliteten med å verifisere attester er gjennomført av en smart kontrakt som ligger i blokkjeden. Denne er skrevet i programmeringsspråket Solidity som er støttet av Etherium blokkjeden. Smart kontrakten består av to sekjsoner; Credentials event som kan bli publisert og funksjonen createCredentials.

createCredentials verifiserer at meldingen som inneholder sertifikatet er godkjent. Dette gjennomføres ved bruk av en elliptisk kurve digital signaturalgoritme (EKDS). Denne algoritmen lar et parti signere meldinger med sin private nøkkel. Funksjonen kombinerer meldingen med signaturen for å hente ut

```
// SPDX-License-Identifier: MIT
pragma solidity >=0.4.22 <0.9.0;

contract Verifier {

    event Credentials(address signer, string description);

    function createCredentials(string memory _description,
                               uint8 v,
                               bytes32 r,
                               bytes32 s)
    public {
        bytes32 message = keccak256(abi.encodePacked(_description));
        address signer = ecrecover(message, v, r, s);
        emit Credentials(signer, _description);
    }
}
```

4.1.2 Arkitektur av systemet

Den overordnet arkitekturen av systemet består av blokkskjede tjenesten, smart kontrakten, og de to klientene issuer og verifiserer. Disse systemene kommuniserer med hverandre hovedsakelig gjennom http metoder. Viktig for ideen om selv-suveren identitet er at alle funksjonalitetene til blokkjede tjenesten kan byttes ut/er ikke proprietær (se 4.1).

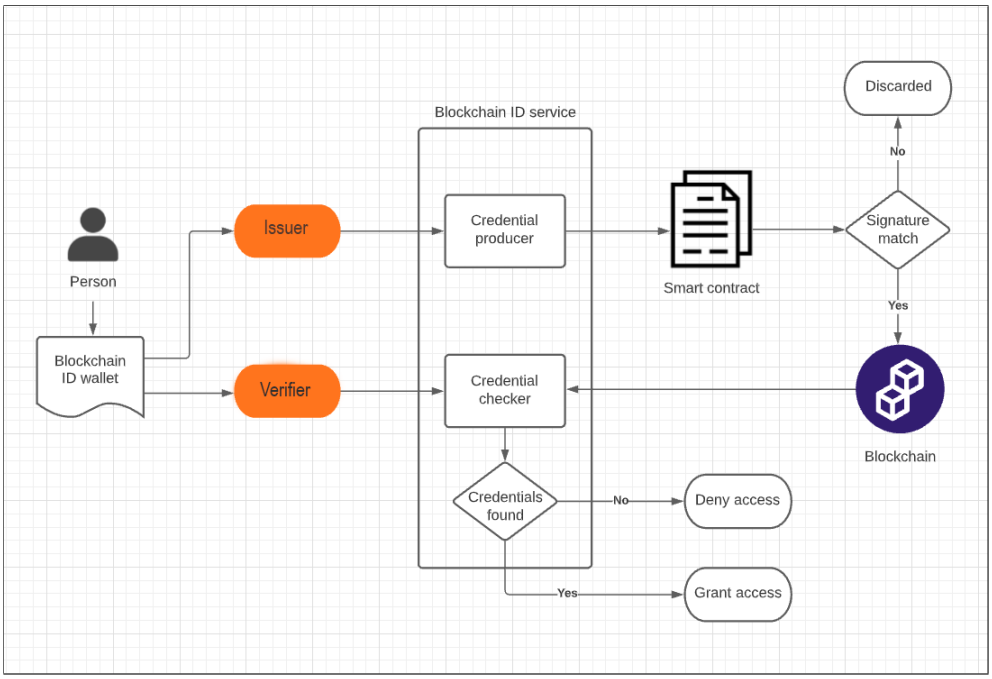

Figure 4.1: Overordnet arkitektur/flyt av systemet

4.1.3 Minimum levedyktig produkt

Dette er det helhetlig systemet som beviser det teoretiske konseptet i en virkelige verden applikasjon. For å gjøre konseptene mer håndgripelige er sidene basert eksisterende tjenester som eksempel på bruksområde for teknologien. Issuer er representert som et universitet (NTNU) og verifiserer er en jobb webside (Finn.no).

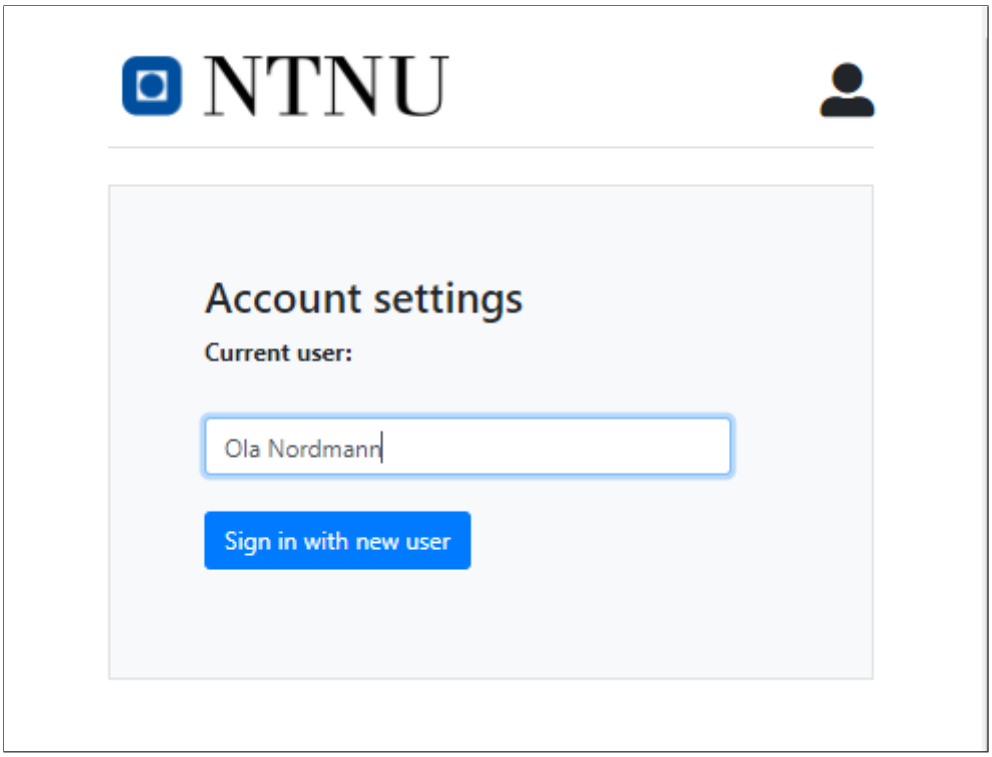

Figure 4.2: Issuer webside innloging

Denne websiden (se 4.2) skal representere en issuer. Den blå knapper med teksten "Sign in with new user" er en name string som brukes videre. Dette er ikke ekte brukere, men istedet en representasjon av innlogging.

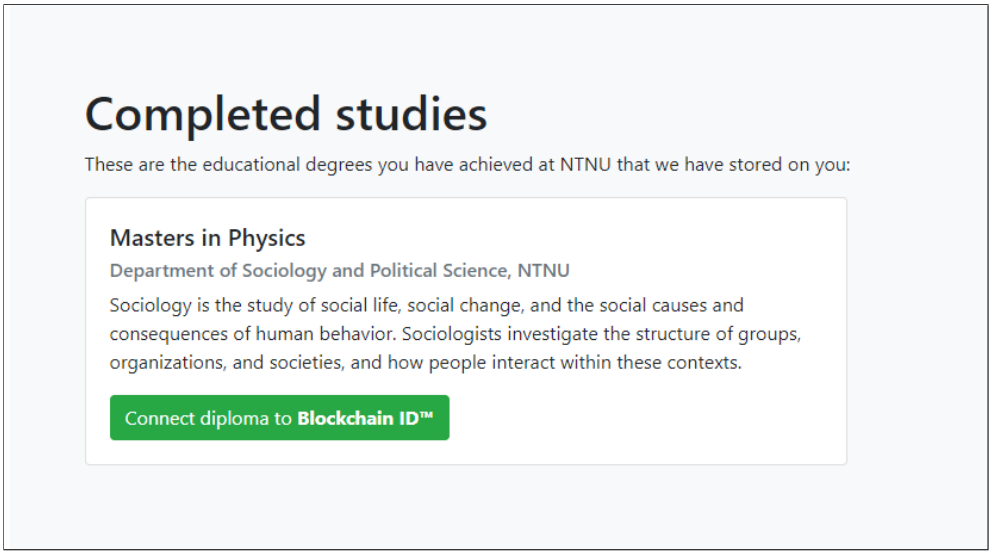

Figure 4.3: Issuer bruker fullført studier

Etter å ha trykket på "sign in with new user" vises en representasjon av brukerens fullførte studier. Her er det mulig og trykke på den grønne knappen "Connect diploma to Blockchain ID" for å laste opp vitnemålet i blokkskjeden som sin egen selv-suveren identitet. Teoretisk er det NTNU som signerer med sin private nøkkel i dette steget vitnemålet (se 4.3).

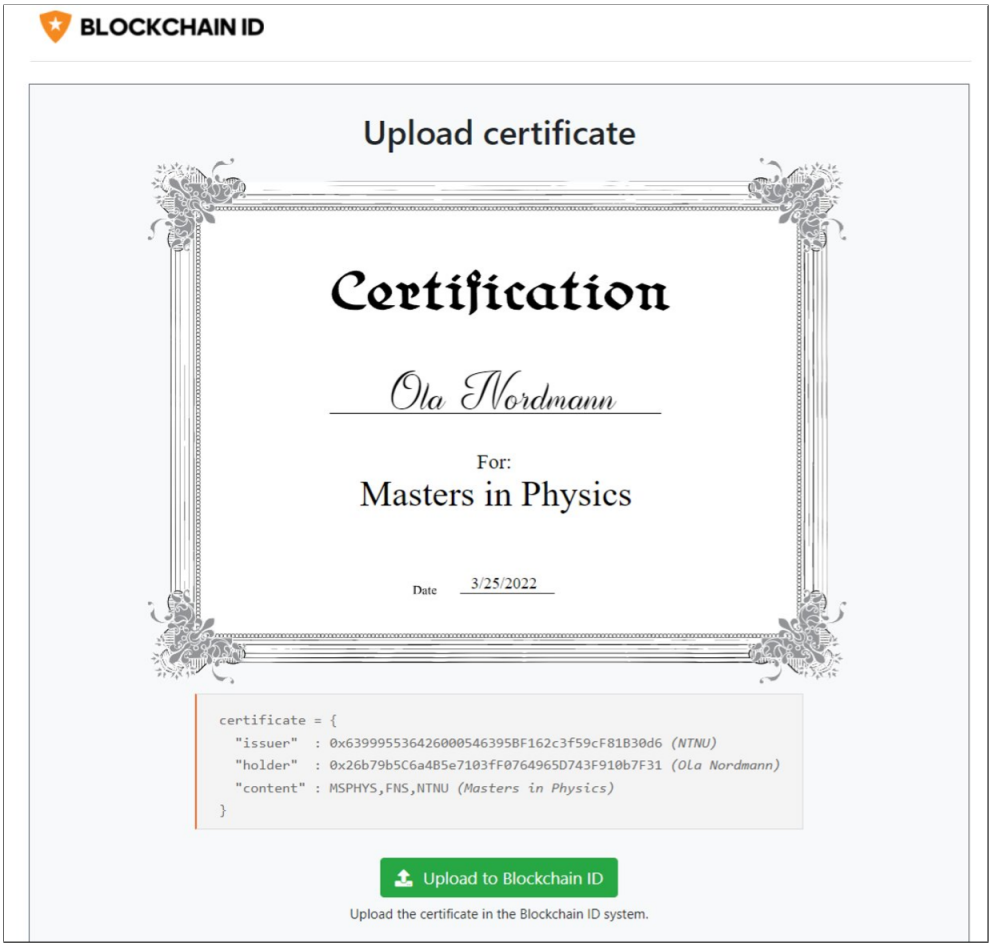

Figure 4.4: Opplasting av sertifikat

Neste steg represter blokksjede tjensten "Blockchain ID". Her er vitnemålet visualisert digitalt for å gi en intuitiv forståelse av hva som blir oppnådd, en skeuomorfisme tilnærming der det digitale representerer sitt fysisk motstykke (se 4.4).

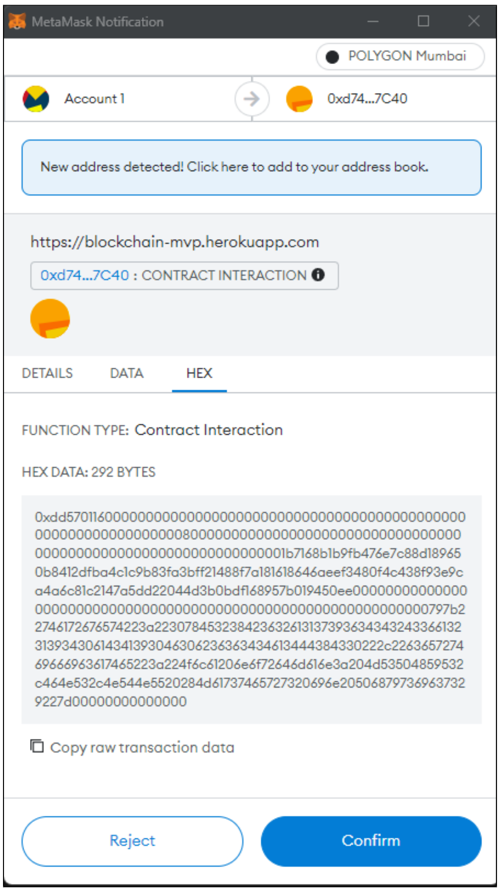

Figure 4.5: Blokkjede lommebok transaksjon forespørsel

Etter å ha trykket på "Upload to Blockchain ID" knappen sendes et forespørsel til brukerens lokale blokkjede lommebok. I eksempelet er dette nettleser utvidelsen MetaMask. Her blir brukeren spurt om de ønsker å fullføre transaksjonen som sender det NTNU signerte vitnemålet til smart kontrakten.

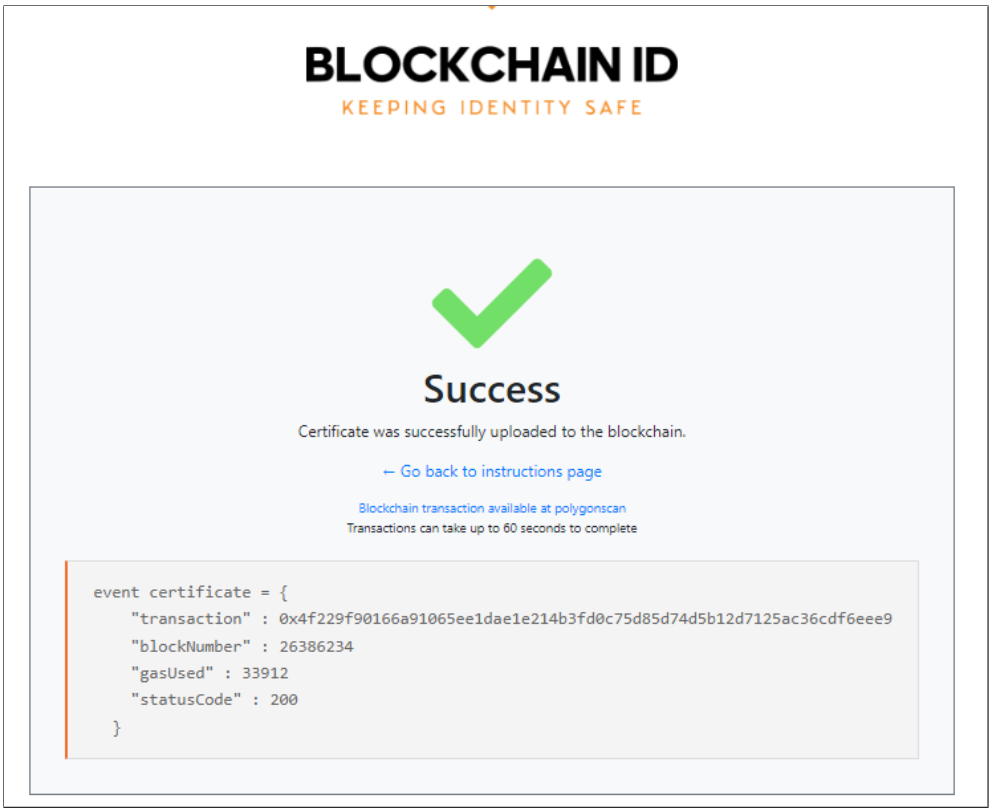

Figure 4.6: Smart kontrakt suksess

Hvis brukeren godkjenner transaksjonen tar det noe sekunder for transaksjonen å gå gjennom blokkjeden før det kommer en suksess skjerm. Her vises det informasjon om brukt gass (kostnaden) i transaksjonen, blokk nummer og transaksjon ID.

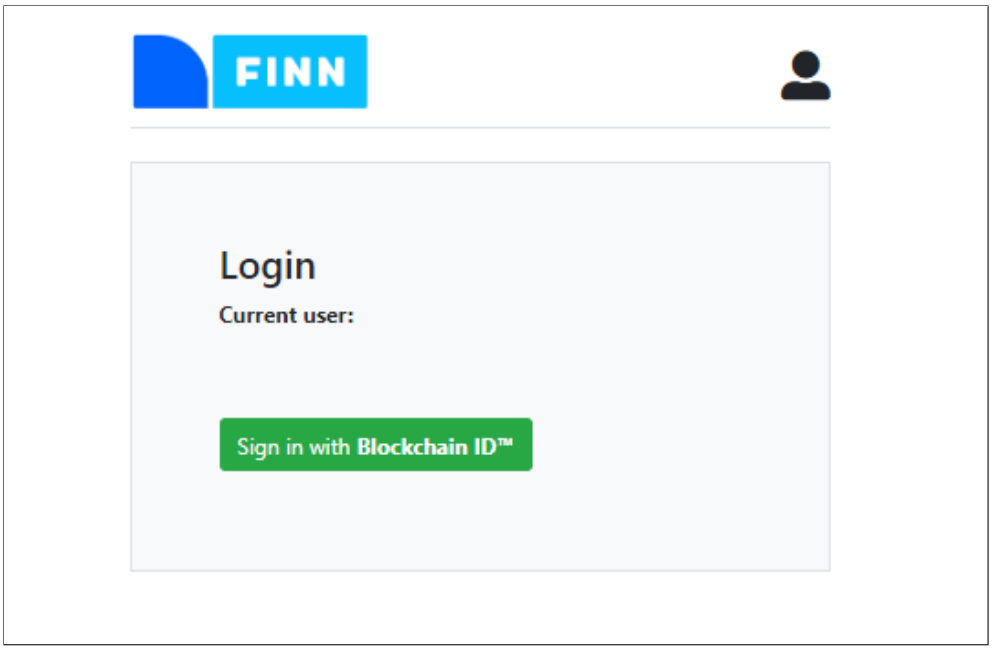

Figure 4.7: Issuer webside innloging

Det neste steget er å verifisere at bruker har vitnemålet tilknyttet sin identitet. Dette er representert i jobb søknad siden Finn. Når bruker trykker på "Sign in" knappen hentes brukerens blokkjede lommebok adresse. Med adressen hentes brukerens vitnemål med blokkjede-tjenesten sitt API /getCredentials (se 4.7).

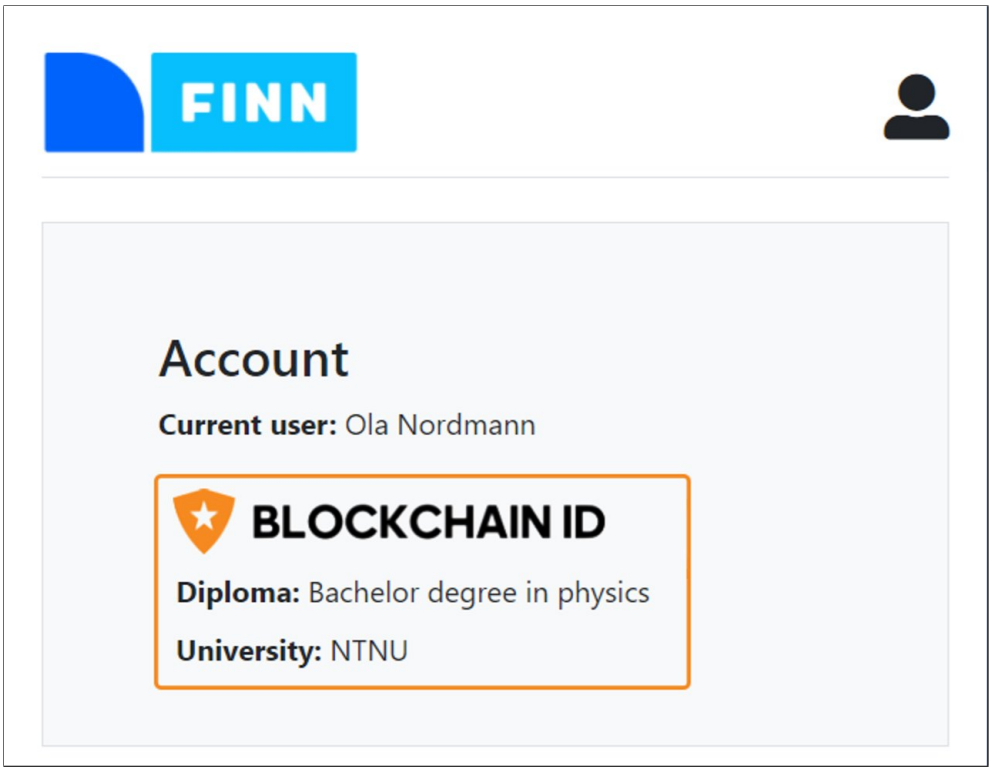

Figure 4.8: Issuer webside innloging

Brukerens vitnemål er hentet med blokkjede tjenesten og vises (se 4.8).

4.2 Vitenskapelige resultater

En veisperre for implementasjonen av selv suveren identitet (SSI) er brukervennlighet. Fordi dette er ny teknologi som ikke har blitt bredt tatt i bruk trengs det en oppsettelse prosess før den kan tas i brukt. For å forsikre at systemet og demoen oppnår dette målet av brukervennlighet ble en spørreundersøkelse gjennomført. Disse spørmålene handlet om brukeren opplevelse av demo-en og deres generelle tanker på bruken av SSI.

- **S1:** Klarte du å laste opp sertifikatet på det desentraliserte nettverket (første del)
- **S2:** Klarte du å verifisere ditt desentraliserte sertifikatet på jobb nettsiden? (andre del)
- **S3:** Hvor viktig er personvern for deg når du bruker digital identitet (konto, log in, osv...)? Ikke viktig 1 - 5 Veldig viktig
- **S4:** Ønsker du å bruke et slikt system som vist i demoen for sertifisering og validering? Nei, aldri 1 - 5 Ja, gjerne
- **S5:** Støtter du bruk av Selv-suveren identitet? Nei, ønsker ikke å bruke det 1 - 5 Ja, vil bruke det oftere

- **S6:** Hvordan var din opplevelse med bruk av smart kontrakter og blockchain i demoen.

Ut ifra spørreundersøkelsen klarte alle brukere å produsere sertifikat, og 6/7 klarte å hente sertifikatet sitt igjen. Spørsmål 3 om hvor viktig personvern hadde et gjennomsnitt resultat på 4.1/5. Fra S4 & S5 med henholdsvis gjennomsnitt 4.1/5 og 4/5 er det generisk støtte for SSI i tjenester. Med S6 hadde 3/7 vanskeligheter med å forstå konseptene bak systemet, dette var ikke et hovedmål for oppgaven men viser at kommunikasjonen kunne blitt implementert bedre.

Table 4.1: Svar fra deltakere

S1	**S2**	**S3**	**S4**	**S5**	**S6**
Ja	Ja	4	4	4	Forstod ikke helt hva som skjedde
Ja	Ja	4	5	3	Vanskelig i starten, men ellers greit
Ja	Ja	3	4	5	Enkelt system å bruke
Ja	Ja	4	5	5	Enkelt system å bruke
Ja	Jeg hadde noen problemer	5	3	3	Forstod ikke helt hva som skjedde
Ja	Ja	4	4	5	Enkelt system å bruke
Ja	Ja	5	4	3	Enkelt system å bruke

4.3 Administrative resultater

Dette GANNT diagrammet beskriver arbeidsprosessen og hva som har blitt fokusert på gjennom prosjektet. Arbeidskontrakt, Gannt-diagram, møtereferat og timelister med statusrapport er lagt til i vedlegg.

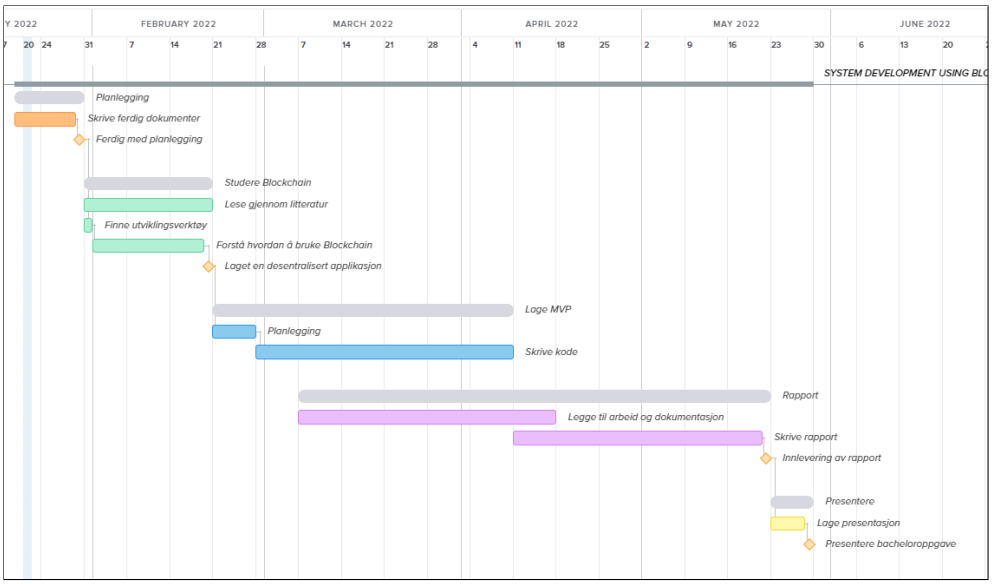

Figure 4.9: Gannt diagram

Chapter 5

Diskusjon

Forstå resultatene i forrige kapittel og evaluere dem ut ifra problemstillingen og sluttproduktet.

5.1 Ingeniørfaglige resultater

Prosjektet var velykket i å produsere det tekniske systemet av en Digital Identity Ledger og nettapplikasjon som ble satt fram i oppgaven. Implementasjonen kan kan bli utvidet til å fungere med andre identiteter og bruksområde enkelt. Mange valg måtte tas der det handlet om å veie alternativene. Løsningen fungerer godt for målet som har prøvd å bli løst innenfor rammene gitt.

5.1.1 Smart kontrakt

Smart kontrakten implementasjon fungerer for verifisering av signaturer og lagring av events. Blokksjeden Polygon fungerer godt slik at teknologien kan implementeres i et produkt. At alle credentials må lagres i blokkjeden er en svakhet med implementasjonen. Fremtidlig arbeid kan se på andre måter på å lagre denne informasjonen på. Å lagre informasjonen lokalt i lommeboken er en spennende måte å løse problemet på og er noe en fremtidlig implementasjon kunne brukt.

5.1.2 Arkitektur av systemet

Arkitekturen fungerer godt innenfor rammene av problemstillingen. Det er lett oversiktlig og følger prinsippene av minste mulig implementering. Noe som ble diskutert men ikke valgt er å gjennomføre transaksjonen fra tjeneste siden. På denne måten hadde det ikke vært nødvending for brukere å skaffe seg penger før de kan laste opp vitnemålet. Ut ifra brukertestene er steget å få penger inn på kontoen det vanskeligste med prosessen. Da kunne man istedet bruke enkle blokkskjede lommebøker.

5.1.3 Minimum levedyktig produkt

Nettsidene er godt oversiktlig og visualiser de forskjellige aspektene i prosessen. Innenfor tidsrammene av prosjektet er en MVP alene akseptabelt, men med mer tid hadde det vært av interesse å faktisk koble systemet opp til eksisterende infrastruktur slik som en universitets side. Da hadde prosjektet fått en virkelig applikasjon og bruksområde. Dette krever da mer sikkerhet og er heller passende for en større gruppe. Valget å bruke NodeJS fungerte godt fordi det gjorde utvikling prosessen raskere. Dette betydde at det tok kort tid å teste ut nye ideer.

5.2 Vitenskapelige resultater

Spørreundersøkelsen inkluderte 7 deltakere, flere svar hadde gitt flere vitenskapelige resultater og vært mer verdifult. Det er vanskelig å forsikre at resultatene hadde skalert godt med en større spørreundersøkelse. Flere sprøsmål om personens alder og kunnskap hadde også gitt godt tiltrengt kontekst på det reelle vanskelighetsnivået. Undersøkelsen ble delt til personer med god teknologiske ferdigheter som kan påvirke resultatene.

Samtidig er det også en suksess på grunn av at blokkjede og bruk av blokkjede lommebøker er noe de fleste har veldig lite erfaring med. At denne MVPen klarte å få de aller fleste til å samhandle med slik nyskapende teknologi viser at demoen er godt utviklet og kjernekonseptet bak fungerer godt. Noen nettlesere har allerede blokkskjede lommeboken bygd inn, men disse hadde websiden vært enda enklere å bruke

5.3

Chapter 6

Konklusjon

Dagens autentisering systemer er sentraliserte. De fleste kontoer baserer seg bare på brukernavn og passord som øker faren for å bli hacket og føderert identitet modellen respekterer ikke brukerens personvern. Når samfunnet blir mer og mer digitalisert er det viktigere enn noen gang at alle eier sin egen identitet. Konseptet bak Digital Identity Ledger er en logisk løsning til de mange eksisterende problemene. Problemstillingen er å implementere en nettapplikasjon med grensesnitt som beviser brukbarhet av Digital Identity Ledger for legitimasjon. I prosjektet er det implementert systemarkitektur mellom klient, tjeneste og blokkjede, smart kontrakten som verifiserer signaturer fra blokkskjeden, og et effektiv brukergrensesnitt som visualiserer de forskjellige systemene. Selv om dette er ny teknologi som fortsatt ikke er veldig godt støttet er funksjonaliteten fortsatt på plass, så viser spørreundersøkelsen at systemet er brukervennlig, pålitelig og lar brukeren samhandle med Digital Identity Ledger. Dette er et Minimum levedyktig produkt som tilgjengeliggjør Digital Identity Ledger systemet på en enkel og effektiv måte.

Samfunnspåvirkning

Digital Identity Ledger teknologi har som effekt å digitalise identitet. Dette er viktig for mange grunner. Når ting er digitalisert kan systemer være mer objektive. Personens erfaring kommer da mye mer frem istedenfor for at fokuseet blir på personens kjønn eller rase.

Mangel på identitet er et stort problem verden over. Uten ID blir det vanskelig å ta i bruk finansielle tjenester. Digital ID kan hjelpe alle med å få ID. Dette fører til økonomisk styrking. Verdens Banken estimerer at i lav inntekt land mangler 45% av kvinnener en grunnleggende ID. Dette er fordi det finnes flere adkomstbarrierer for å skaffe seg ID. Digital ID kan derfor være med å redusere forskjeller i slike land.

Fra et miljømessig perspektiv er blokkjede generelt en versting når det kommer til klimafotavtrykk. I dette prosjektet brukes Polygon som er en mye mer effektiv blokkjede. Dette betyr at kostnadene er heftig redusert og klimaavtrykket er også redusert.

Bibliography

[1] C. Allen, *Life with alacrity*, Apr. 2016. [Online]. Available: http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html.

[2] *Fn internettbrukere*, 2020. [Online]. Available: https://www.fn.no/Statistikk/internettbrukere.

[3] T. H. Nätt and S. Johan Knapskog, *Autentisering*, 2019. [Online]. Available: https://snl.no/autentisering.

[4] I. Hassan, *Introduksjon til kryptering - hioa*, 2019. [Online]. Available: https://www.cs.hioa.no/~solvese/Undervising/Matematikk1000/DAFE1000_V19/IntroVeke/Gjesteforelesning_Kryptering.pdf.

[5] D. Johnson, A. Menezes and S. Vanstone, 'The elliptic curve digital signature algorithm (ecdsa),' *International journal of information security*, vol. 1, no. 1, pp. 36–63, 2001.

[6] B. K. Mohanta, S. S. Panda and D. Jena, 'An overview of smart contract and use cases in blockchain technology,' in *2018 9th international conference on computing, communication and networking technologies (ICCCNT)*, IEEE, 2018, pp. 1–4.

[7] Y. Wang, A. Bracciali, T. Li, F. Li, X. Cui and M. Zhao, 'Randomness invalidates criminal smart contracts,' *Information Sciences*, vol. 477, pp. 291–301, 2019.

[8] A. R. Hevner, 'A three cycle view of design science research,' *Scandinavian journal of information systems*, vol. 19, no. 2, p. 4, 2007.