Bacheloroppgave

NTNU
Norges teknisk-naturvitenskapelige universitet
Fakultet for samfunns- og utdanningsvitenskap
Institutt for lærerutdanning

Kjetil Gillebo Overaae

Blokkjeder som altseende øyne i digitale arkiver

En undersøkelse av blokkjedeteknologiens potensial til å beskytte digitale arkiver mot uautoriserte dataendringer og forfalskninger

Bacheloroppgave i Arkiv- og samlingsforvaltning
Veileder: Tor Eivind Johansen
Mai 2024

NTNU
Kunnskap for en bedre verden

Kjetil Gillebo Overaae

Blokkjeder som altseende øyne i digitale arkiver

En undersøkelse av blokkjedeteknologiens potensial til å beskytte digitale arkiver mot uautoriserte dataendringer og forfalskninger

Bacheloroppgave i Arkiv- og samlingsforvaltning
Veileder: Tor Eivind Johansen
Mai 2024

Norges teknisk-naturvitenskapelige universitet
Fakultet for samfunns- og utdanningsvitenskap
Institutt for lærerutdanning

NTNU
Kunnskap for en bedre verden

Innhold

Sammendrag

Denne oppgaven undersøker hvordan blokkjedeteknologi kan forbedre bevaring av digitale arkiver og beskytte mot uautoriserte endringer og forfalskninger. Fokuset er på hvordan blokkjedeteknologiens egenskaper som desentralisering, uforanderlighet, transparens og kryptografisk sikkerhet kan brukes til digital arkivering. Metodene som brukes kombinerer litteraturstudier og case-analyser. Litteraturstudien gir en oversikt over eksisterende forskning, mens case-analysene ser på praktiske anvendelser av blokkjedeteknologi. Tre viktige eksempler er: Filecoin, som tilbyr en desentralisert lagringsløsning som blant annet benytter Proof-of-Replication og Proof-of-Spacetime; Archain, som brukes av Statsarkivkomiteen i Tatarstan for sikker dokumentoverføring; og ARCHANGEL, som sikrer dokumenters integritet gjennom et prototypeprosjekt på en desentralisert plattform i Storbritannia. Oppgaven konkluderer med at blokkjedeteknologi har stort potensial til å løse utfordringer innen digital arkivering ved å sikre integritet og autentisitet. Teknologien har flere fordeler som reduserer risikoen for uautoriserte endringer og forfalskninger. Samtidig finnes det utfordringer innen bærekraft og behov for bedre integrasjon med eksisterende systemer som bør løses. Det er derfor nødvendig med videre forskning for å utnytte teknologiens fulle potensial i digital arkivering.

1 Innledning

1.1 Bakgrunn for valg av tema

Det moderne samfunnet genererer enorme mengder digitale data som skal arkiveres for fremtidig referanser, forskning, og bevaring av kulturarv. Digitale arkiveringssystemer står overfor viktige utfordringer som inkluderer sårbarhet for dataendringer, forfalskning, og tap over tid. Med økende digitaliseringen av dokumenter og arkiver blir behovet for å skape sikre og pålitelige arkiveringsmetoder tydelig. Digital arkivering innebærer en rekke prosedyrer og strategier designet for å bevare digitale dokumenter og data slik at deres autentisitet, tilgjengelighet og integritet blir godt bevart over lang tid. Denne oppgaven vil derfor se på feltene for digital arkivering og dokumentasjonsforvaltning med fokus på informasjonssikkerhet og teknologisk nyvinning. Blokkjedeteknologi interessant tilnærming til digital arkivering, med potensial for å overkomme mange eksisterende utfordringer. Blokkjedeteknologiens grunnleggende egenskaper som inkluderer desentralisering, uforanderlighet, transparens og kryptografisk sikkerhet bidrar til at den kan bli en attraktiv løsning for å sikre integritet og autentisitet til arkiverte data.

1.2 Problemstilling

Ved å undersøke problemstillingen "i hvilken grad kan blokkjedeteknologi bidra til å forbedre langvarig bevaring av digitale arkiver og sikre mot uautoriserte dataendringer og forfalskning?" ønsker jeg å utforske blokkjedeteknologiens potensiale til å forbedre digital arkivering, om det kan bidra til feltets fremtidige utvikling, og adressere noen av utfordringene digital arkivering står ovenfor.

1.3 Avgrensninger

Siden blokkjedeteknologi har et bredt spekter av bruksområder og stadig utvikler nye metoder og løsninger, vil denne studien avgrense seg til å undersøke de mest aktuelle bruksområdene som er relevante for langvarig bevaring av digitale arkiver. Fordi teknologien fremdeles er i rask utvikling, vil noen av de nyeste metodene ikke bli vurdert, ettersom de fortsatt kan være under testing eller i en tidlig fase av implementering. Oppgaven inkluderer også juridiske og regulatoriske aspekter ved blokkjedeteknologi og digital arkivering, men den vil ikke dekke alle juridiske implikasjoner globalt. Denne oppgaven vil derfor

hovedsakelig basere seg på eksisterende forskning, dokumenterte case-studier som omhandler anerkjente områder der blokkjedeteknologi brukes til digital arkivering.

2 Teori

2.1 Proveniens, integritet og autentisitet

Prinsippene om proveniens, integritet og autentisitet er viktige deler for å bevare arkivenes verdi over tid. Disse prinsippene sikrer at arkivene forblir pålitelige, autentiske og nyttige for forskning, juridisk bruk, og kulturarv. Provenienssprinsippet omhandler arkivmaterialets opprinnelse. Det understreker viktigheten av å bevare informasjon om hvem som har skapt materialet, når det er skapt og under hvilke omstendigheter. Dette prinsippet hjelper til med å sikre at arkivmaterialet kan spores tilbake til sin opprinnelige kilde, som er avgjørende for å vurdere autentisitet (NOU 2019: 9). Integritetsprinsippet fokuserer på å bevare arkivmaterialets fullstendighet og uforandret tilstand over tid. Det innebærer at materialet ikke bør endres, slettes eller manipuleres på måter som kan gå ut over autentisitet eller konteksten det skal representere. Integritet sikrer at fremtidige brukere kan stole på at arkivmaterialet er et korrekt og fullstendig bilde av det som opprinnelig ble skapt (NOU 2019: 9). Autentisitetsprinsippet handler om å bevare og bekrefte arkivmaterialets ekthet. Det innebærer å sikre at materialet faktisk er det det utgir seg for å være og at det ikke har blitt forfalsket eller endret på en måte som påvirker kildens verdi. Dette oppnås gjennom nøye dokumentasjon av arkivmaterialets «liv» som opprinnelse, bevaringshistorikk og eventuelle endringer som er foretatt (NOU 2019: 9).

2.2 Lovverk

2.2.1 Arkivloven

Arkivloven er en lovgivning som sikrer systematisk bevaring og håndtering av dokumenter og annet arkivmateriale, både for offentlige og private arkivskapere. Loven legger ansvaret på arkivskaperen for å sikre at arkiver blir korrekt behandlet og bevart for fremtiden, og setter standarder for hvordan dette skal gjøres. Loven fremhever at arkiver skal være tilgjengelige for forskning, undervisning og allmennheten, samtidig som konfidensialitet og personvern ivaretas. Arkivloven stiller krav til arkivinstitusjoners rolle for å veilede og overvåke

arkivarbeidet, sikre at verdifulle arkiver overføres til offentlig arkivinstitusjon for bevaring på lang sikt, og å fremme digitalisering og tilgjengeliggjøring av arkivmateriale (Arkivlova, 1992).

2.2.2 Offentlighetsloven

Offentlighetsloven har som formål å fremme åpenhet og transparens i offentlig virksomhet, styrke grunnleggende demokratiske verdier som informasjons- og ytringsfrihet, og legge til rette for bruk av offentlig informasjon. Loven gjelder for statlige, fylkeskommunale og kommunale organer, samt selvstendige enheter hvor det offentlige har stor innflytelse (Offentleglova, 2006).

2.2.3 General Data Protection Regulation (GDPR) og Personopplysningsloven

Formålet med GDPR er å beskytte fysiske personer med hensyn til behandling av personopplysninger og sikre fri bevegelse av slike data i EU. Forskriften har som mål å gi individer kontroll over sine personopplysninger og forenkle det regulering for internasjonale virksomheter ved å forene reguleringen innen EU (European Parliament and Council of the European Union, 2016). Prinsippene for behandling av personopplysninger under GDPR inkluderer lovlighet, rettferdighet og gjennomsiktighet; formålsbegrensning; dataminimering; nøyaktighet; lagringsbegrensning; integritet og konfidensialitet; og ansvarlighet. Rettighetene til registrerte personer under GDPR inkluderer retten til informasjon, rett til tilgang, rett til retting, rett til sletting (retten til å bli glemt), rett til begrensning av behandling, rett til dataportabilitet, rett til å protestere, og rettigheter knyttet til automatiserte avgjørelser, inkludert profilering (European Parliament and Council of the European Union, 2016). I Norge er personopplysningsloven opprettet for å beskytte enkeltpersoner mot krenking av personvernet gjennom behandling av personopplysninger. Loven gjennomfører EUs personvernforordning (GDPR) i norsk rett og gjelder som norsk lov. Bakgrunnen for loven er den raske teknologiske utviklingen som gjør det lettere å samle inn, bruke og utveksle personopplysninger, samt et ønske om å lette utvekslingen av personopplysninger over landegrenser på en måte som ivaretar personvernet (Personopplysningsloven, 2018**)**.

2.3 Rammeverk og standard for digital bevaring

2.3.1 Noark

Noark (Norsk Arkivstandard) er en norsk standard for arkivdanning og dokumentasjonsforvaltning utviklet for å sikre systematisk behandling av offentlige arkiver. Denne standarden er en veiledning for hvordan offentlige og private organisasjoner kan organisere, bevare og tilgjengeliggjøre elektronisk dokumentasjon over tid. Noark 5 fokuserer på digital dokumentforvaltning hvor hovedformålet er å tilby en strukturert metode for å samle, lagre, og administrere digitale dokumenter. Dette inkluderer alt fra opprettelse og mottak av dokumenter, til klassifisering, lagring, tilgangsstyring, og til slutt avlevering til et arkivdepot for langtidsbevaring (Arkivverket, 2018). I Noark 5 blir det spesifisert metadataelementer for dokumentasjon av arkivverdige dokumenter, som sikrer at informasjonen kan forvaltes, bevares og gjøres tilgjengelig over tid. Det blir også inkludert krav om elektronisk signatur for å verifisere dokumentenes autentisitet og integritet, samt prosedyrer for kryptering og dekryptering av dokumenter for å sikre konfidensialitet og beskyttelse mot uautorisert endring. (Arkivverket, 2018)

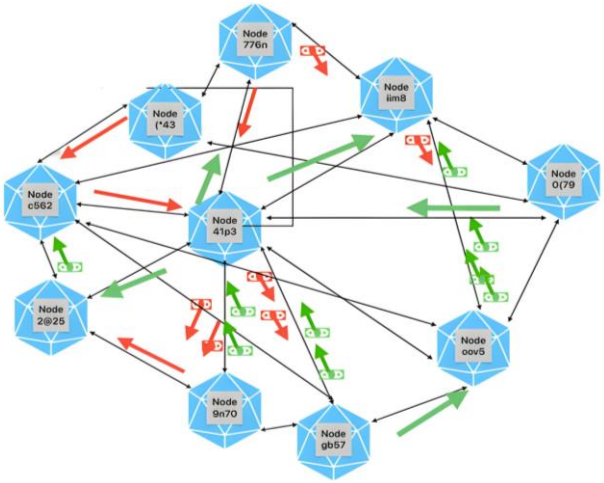
2.3.2 Open Archival Information System (OAIS)

Open Archival Information System (OAIS) er en internasjonal standard som utgjør et teoretisk rammeverk for digital langtidslagring og arkivering. Hovedkonseptene i OAIS-modellen er rettet mot å gi en bedre forståelse av arkivering og langtidsbevaring av digital informasjon. OAIS-modellen omhandler en rekke arkivfunksjoner, inkludert innsamling, arkivlagring, databehandling, tilgang og formidling. Den tar også for seg overføring av digital informasjon til nye medier og formater samt utveksling av digital informasjon mellom arkiver (Consultative Committee for Space Data Systems, 2012).

2.4 Blokkjeder

2.4.1 Blokkjeder, hash-funksjoner og noder

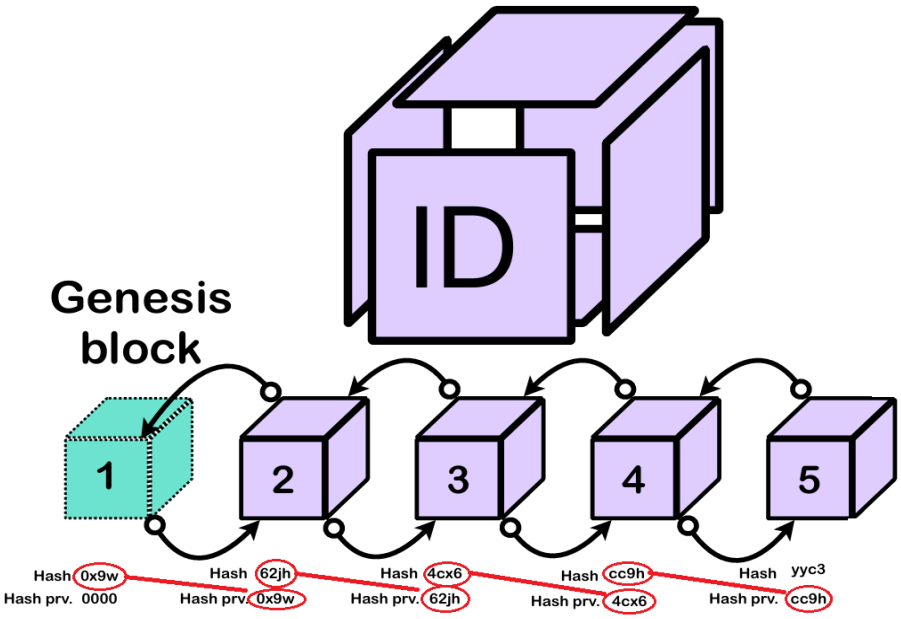
Blokkjedeteknologi, også kjent som "blockchain" på engelsk, representerer en alternativ tilnærming til digital informasjonsoverføring og lagring, kjent for sin sikkerhet, transparens og desentralisering. Teknologien er kanskje mest kjent som grunnlaget for kryptovalutaer som Bitcoin, selv om den også blir brukt på områder der digital sikkerhet og identitetsstyring er relevant. Blokkjedeteknologi baserer seg på distribuert databehandling hvor data lagres over et nettverk av noder i stedet for på en sentral server (Farah, 2018).



Figur 1. Jurci.P.(2024) Enkel illustrasjon som viser hvordan noder i blokkjede-nettverket jobber sammen..

En node i en blokkjede er en datamaskin som deltar i blokkjedenettverket. Nodene er både ansvarlige for å validere og lagre transaksjoner, samt distribuere og synkronisere informasjonen med andre noder i nettverket. Det finnes forskjellige typer noder med ulike roller, men hovedprinsippet er at de alle jobber sammen for å opprettholde sikkerheten og integriteten til blokkjeden (Farah, 2018). For å sikre at ingen enkelt part kan kontrollere eller manipulere dataene, har hver node i nettverket en kopi av hele databasen, og transaksjoner verifiseres gjennom en konsensusprosess blant deltakerne som kalles Proof of Work (PoW). Dette krever at deltakerne, kjent som "miners", løser en kompleks matematisk oppgave som deretter verifiseres av andre i nettverket. Den første som løser oppgaven, får tillatelse til å legge til en ny blokk til blokkjeden og får en belønning i form av kryptovaluta. Når en node løser oppgaven, blir løsningen presentert som "bevis" for arbeidet som er gjort og tillater noden å legge til den nye blokken. Dette sikrer at kun den lengste kjeden av blokker, som representerer majoriteten av nettverkets beregningskraft anerkjennes som gyldig.

Hver "blokk" i en blokkjede inneholder en kryptografisk sjekksum (hash) av den forrige blokken, et tidsstempel og transaksjonsdata. En hash-funksjon tar inn data av hvilken som helst størrelse og produserer en fast størrelse utdata, kjent som en hash. Hver hash er unik og fungerer som et digitalt fingeravtrykk av inndataene. En god hash-funksjon må beregnes raskt og minimere antall kollisjoner. Den mest vanlige hash-funksjonen i blokkjeder er SHA-256 (Secure Hash Algorithm 256-bit). SHA-256 er en del av SHA-2-familien og brukes blant annet i Bitcoin og flere andre blokkjede-prosjekter. SHA-256 er populær på grunn av sin gode sikkerhet, effektivitet og motstand mot kollisjoner (Kuznetsov et al., 2021). Blokkjeder bruker hash-funksjoner til å skape en sikker og uforanderlig kjede av blokker. Hver blokk inneholder en hash av den foregående blokken, som kryptografisk lenker hver blokk til den forrige og dermed danner en kontinuerlig kjede.



Figur 2. Jurci.P (2024) Illustrasjon som viser hvordan hver blokk inneholder en hash av forrige blokk.

Denne mekanismen sikrer at hvis det blir gjort forsøk på å endre informasjonen i en allerede bekreftet blokk, vil hashen ikke samsvare med den originale hashen lagret i kjeden. Dette vil umiddelbart føre til en uoverensstemmelse i nettverket som skal være lett å oppdage (Nakamoto, 2008). Hvis flere noder genererer en gyldig blokk samtidig, vil en demokratisk konsensus løse konflikten. PoW er en oppgave som består i å finne et tilfeldig tall (nonce) som sammen med transaksjonsinformasjon skaper en gyldig SHA-256-hash (L'Hutereau et al., 2019). Prosessen er tidkrevende og krever store mengder datakraft, noe som gjør forsøk

på å manipulere blokkjeden kostbart og så godt som umulig. Dette sikrer nettverket mot spam og angrep ved å gjøre det kostbart og tidkrevende å utføre. For å lykkes med et dobbeltsvindelangrep må en ond node kontrollere 51 % av nettverkets datakraft. Justeringsmekanismer sikrer en konstant regulering av vanskelighetsgraden i å finne en gyldig hash (L'Hutereau et al., 2019).

2.4.2 Tillatelsesfrie og tillatelsesbaserte blokkjeder

Tillatelsesfrie blokkjeder betyr det samme som offentlige blokkjeder, samtidig som tillatelsesbaserte og private blokkjeder betyr det samme. Valg av blokkjede avhenger av hva den skal brukes til, og man må velge blant de tilgjengelige typene. Hvordan blokkjeden er satt opp, påvirkes av faktorer som ytelse, kostnad, fleksibilitet, samt lagring, beregning og grad av desentralisering (Farah, 2018). Offentlige og tillatelsesfrie blokkjeder er tilgjengelige for alle. Hvem som helst kan delta i transaksjoner og bidra til konsensusprosessen for å legge til nye blokker. Disse systemene benytter ofte Proof of Work (PoW), som krever at noder løser komplekse kryptografiske oppgaver, eller Proof of Stake (PoS), som er mindre beregningstungt, for å oppnå konsensus (Farah, 2018). Med flere deltakere reduseres risikoen for et 51 % angrep. Tillatelsesbaserte blokkjeder er vanligvis laget av organisasjoner for spesifikke forretningsformål og integreres ofte med deres eksisterende systemer. Organisasjoner kan også velge blokkjeder der et utvalg av betrodde medlemmer må godkjenne transaksjoner. I helt private blokkjeder har en sentral enhet rettighetene til å skrive og endre data (Farah, 2018).

2.4.3 Smartkontrakter

Blockchain 2.0 gjorde det mulig å lage smartkontrakter som automatiserer transaksjoner gjennom digitale, selvutførende avtaler. Ideen ble først lansert av Nick Szabo i 1993, men det var ikke før Ethereum at infrastrukturen var på plass for å ta i bruk konseptet. Smartkontrakter er satt opp med forhåndsdefinerte vilkår, regler og straffer, og de bruker et avansert programmeringsspråk på blokkjeden. Når data som oppfyller de spesifikke betingelsene blir mottatt, utføres kontraktene automatisk. Alle noder på nettverket kan se disse kontraktene, og hvis vilkårene ikke er oppfylt, sendes det en feilmelding. Bruken av smartkontrakter har potensiale til å redusere transaksjonskostnader betraktelig i mange ulike bransjer (Upadhyay et al., 2021).

2.4.4 InterPlanetary File System (IPFS)

InterPlanetary File System (IPFS) er et distribuert peer-to-peer filsystem designet for å gjøre internett raskere, sikrere og mer åpent. Det fungerer ved å lagre filer i et nettverk av noder, slik at brukere kan laste ned filer fra nærmeste node i stedet for en sentral server, noe som reduserer ventetid og øker hastigheten (Benet, 2014). IPFS adresserer filer basert på deres innhold, ikke hvor de er lagret, noe som sikrer at filene er autentiske og uendret fra originalen. Systemet bruker også en teknologi kjent som Merkle DAG for å organisere filer og tillate effektiv versjonskontroll. Dette gjør det mulig å opprette en webløsning hvor lenker ikke går tapt og innhold forblir tilgjengelig selv om enkeltnoder går ned. IPFS viser et desentralisert internett der brukere har mer kontroll over deres data, og der informasjon kan deles effektivt uten avhengighet av sentraliserte tjenester (Benet, 2014).

3 Metode

I dette kapittelet presenteres metoden som har blitt benyttet i denne studien om blokkjedeteknologi i digitale arkiver, og eventuelle bidrag for sikring mot uautoriserte dataendringer og forfalskning ved langvarig bevaring. Metoden kan betraktes som et verktøy for innsamling, analyse og verifisering av kunnskap. For å sikre kvaliteten på dette arbeidet, må vi opprettholde intellektuelle standarder som ærlighet og sannferdighet, i tillegg til å foreta en systematisk vurdering av våre egne tanker og forståelse (Dalland, 2020). Problemstillingen krever en detaljert og god forståelse av både de teknologiske egenskapene til blokkjedeteknologi, samt arkivariske krav og behov ved langvarig bevaring. Gjennom en kvalitativ tilnærming kombinerer denne studien litteraturstudie og case-analyser for å utforske i hvilken grad blokkjedeteknologi kan bidra til å forbedre langvarig bevaring av digitale arkiver. Denne metodologiske tilnærmingen er valgt for å fange opp perspektiver både innenfor datasikkerhet og arkiv.

3.1 Litteraturstudiet

Litteraturstudien utgjør en bred del av denne studien, ettersom den gir et teoretisk rammeverk og en oversikt over eksisterende kunnskap om blokkjedeteknologiens potensial innen langtidsbevaring av digitale arkiver. Litteraturstudien vil systematisk gjennomgå relevant forskning, whitepapers og juridiske dokumenter. Med en definert søkestrategi vil datainnsamlingen innebære systematisk søk og nedlasting av artikler, rapporter og

dokumenter. Til innsamlingen blir det brukt kombinasjoner av nøkkelord som "blokkjedeteknologi og arkivering", "blokkjede og digital integritet", "blokkjedeteknologi og dataautentisering", samt spesifikke teknologier og standarder innen blokkjedeteknologi. Søkene vil utføres i akademiske databaser som Google Scholar, IEEE Xplore og JSTOR. Utvalget er blitt basert på kriterier om at artiklene må være skrevet på skandinaviske språk eller engelsk, være relevante for oppgavens problemstilling og gi informasjon om enten direkte bruk av blokkjeder i digitale arkiver eller indirekte bruk i andre fagområder som kan oppfylle arkivenes behov (Dalland, 2020).

3.2 Case-Analyse

Case-analysen vil utforske bruken av blokkjedeteknologi i praktiske scenarioer innen bevaring av digitale arkiver. Den vil involvere detaljert studie av tre utvalgte eksempler hvor blokkjedeteknologi har blitt forsøkt brukt eller aktivt brukt for dette formålet. Case-utvelgelsen blir basert på relevans for problemstillingen, tilgjengelighet av data og potensialet for å forstå hvordan teknologien kan bidra i digital arkivering. Analysen av casene vil fokusere på aspekter ved teknologi, organisasjon og reguleringer ved bruk, i tillegg til eventuelle utfordringer, løsninger og lærdom. Datainnsamlingen består av relevante rapporter, prosjektbeskrivelser og andre tilgjengelige materialer relatert til de utvalgte prosjektene. Dataanalysen vil bruke en tematisk tilnærming for å identifisere mønstre, likheter og forskjeller mellom de studerte casene i forhold til problemstillingen. Analysen presenterer hvert prosjekt detaljert med tilhørende eksempler for å støtte funnene.

3.3 Kildekritikk

Kildekritikk innebærer å sikre troverdighet og faglighet i skriftlige arbeider gjennom nøye litteratursøk som er relevant for problemstillingen, og ved å begrunne og analysere den valgte litteraturen i oppgaven. Dette krever en undersøkelse av kildenes opphav for å bekrefte deres gyldighet. Deretter må innholdet i kildene vurderes og analyseres i forhold til oppgavens problemstilling. Tidspunktet for publiseringen må også vurderes for å sikre at informasjonen er aktuell (Dalland, 2020, s. 143).

4 Resultater

4.1 Filecoin

Filecoin whitepaperet introduserer et desentralisert lagringsnettverk som benytter blokkjedeteknologi for å tilby en markedsplass for lagring. Dette nettverket er designet for å erstatte sentraliserte lagringstjenester med en desentralisert modell. Her betaler kunder med Filecoin for lagring og distribusjon av data, hvor igjen minere tjener Filecoin-tokens ved å tilby lagringskapasitet (Protocol Labs, 2017). Systemet er unikt ved at det tilbyr en incitamentsmekanisme for lagring basert på verifiserbar lagringskapasitet. Filecoin benytter seg av taktikker som Proof-of-Replication (PoRep) og Proof-of-Spacetime (PoSt) for å garantere dataintegritet og tilgjengelighet. PoRep-verifikasjonsmekanismen forsikrer at en unik og fysisk uavhengig kopi av dataene er lagret, mens PoSt-mekanismen verifiserer at disse dataene har blitt bevart gjennom en definert tidsperiode. Disse prosedyrene er utformet for å beskytte mot typiske sikkerhetstrusler som Sybil-angrep, outsourcing-angrep og genereringsangrep, som alle representerer potensielle risikoer for lagringssystemets pålitelighet og sikkerhet (Protocol Labs, 2017). Ved å kombinere disse mekanismene sikres det at data ikke bare blir kopiert på en pålitelig måte, men også opprettholdt over lengre tid. Dette er med på å styrke systemets integritet og brukernes tillit. Filecoin har etablert to desentraliserte og verifiserbare markeder, hvor ett er for lagring og ett er for henting av data. Disse markedene garanterer at transaksjoner gjennomføres som avtalt og at betalinger utløses kun når tjenestene er levert. Dette skaper en økonomisk modell hvor minere får incentiver til å tilby pålitelig og sikker lagringskapasitet (Protocol Labs, 2017). Nettverkets konsensusmekanisme er designet for å sikre at en miners innflytelse er direkte knyttet til mengden av lagring de faktisk bidrar med. Dette skal bidra til å motivere til økte investeringer i lagringskapasitet fremfor ren datakraft for utvinning. Dette sikrer at nettverket verdsetter og belønner nyttig lagringsplass framfor simpel beregningskraft.

Filecoin-nettverket består av tre hovedtyper av noder: klientnoder, lagringsminernoder og gjenfinningsminernoder. Disse nodene brukes ved lagring (storage) eller henting (retrieval) (Protocol Labs, 2017). Ved lagring vil en klientnode sende en lagringsforespørsel ved å legge inn en bestilling i lagringsmarkedet. Lagringsminere tilbyr lagringsplass ved å legge inn tilbud. Når en klientbestilling matcher et minertilbud, vil dataen bli lagret hos mineren. Mineren må regelmessig generere og sende inn PoRep og PoSt til blokkjeden for å bevise at de fortsatt lagrer dataene. Hvis dette ikke blir gjort, vil de miste en del av sitt innskudd. Ved

henting vil en klientnode sende en hentingsforespørsel ved å legge inn en bestilling i gjenfinningsmarkedet. Gjenfinningsminere tilbyr å levere data ved å legge inn sine tilbud. Når en klientbestilling matcher et minertilbud, blir dataen sendt til klienten. Dataen sendes i deler hvor klienten betaler mineren i mikrobegalinger for hver del som mottas (Protocol Labs, 2017).

4.2 Archain

Archain presenterer et arkivsystem basert på blokkjedeteknologi, utviklet for Statsarkiv-komiteen i Tatarstan republikken i Russland. Systemet integrerer blokkjede som en primær komponent for å lagre transaksjoner relatert til dokumentoverføring til arkivet på en sikret måte. Etter krav fra kunden blir det benyttet en tillatelsesbasert blokkjedemodell (Permissioned blockchain model). Hovedmålet med Archain var å utforske muligheten for å anvende blokkjedeteknologi i arkivprosesser og skape en programvareprototype for overføring av dokumentasjon til et arkiv (Galiev et al., 2018). Systemet er utformet med tanke på kundens spesifikke restriksjoner, inkludert behovet for et betrodd senter for tildeling av roller innenfor nettverket. Dette inkluderer roller som administrator, deltaker, og ekspert hvor hver enkelt har sitt spesifikke ansvar og nøkler for å signere blokker og transaksjoner (Galiev et al., 2018). Dette sikrer at tilgangsrettigheter og oppgaver distribueres på en kontrollert måte, opprettholder nettverkets sikkerhet og effektivitet. I tillegg tilfredsstiller systemet kravet om å bruke russiske kryptografiske standarder, noe som betyr at det benytter seg av spesifikke teknologier og krypteringsmetoder som følger russiske nasjonale sikkerhetsretningslinjer (Galiev et al., 2018). Blokkjedeteknologi blir beskrevet som en form for distribuert databehandling spesielt utformet for håndtering av transaksjoner, der hver transaksjon blir kronologisk lagret i et felles register. Dette oppsettet tilbyr en innebygd beskyttelse mot fjerning eller modifisering av data. I motsetning til tradisjonelle databaser som MySQL Cluster, vil blokkjedeteknologien oppnå sikkerhet direkte gjennom sin egen protokoll. I prosjektet blir blokkjeder gruppert og analysert i henhold til datatilgang, og det diskuteres offentlige, private, åpne og lukkede blokkjedemodeller. Prosjektet legger vekt på bruk av elektroniske digitale signaturer og hashing-algoritmer fra "Stribog"-serien, spesifikt GOST R 34.10-2012 for digitale signaturer og GOST R 34.11-2012 for hashing (Galiev et al., 2018). Disse standardene brukes for å garantere autentisiteten, integriteten og ikke-benektelse (non-repudiation) av digitale meldinger eller dokumenter, noe som sikrer at innholdet er ekte, uendret og anerkjent av avsenderen (Dolmatov & Degtyarev, 2013). Systemet er designet for

å forebygge, identifisere og motstå ulike typer angrep som kan modifisere, slette eller urettmessig tilføre poster i databasen. Hele livssyklusen til et dokument, fra opprettelse til arkivering, er strengt regulert gjennom sekvensielle statusendringer, beskyttet med signaturer fra nøkkelpersonell (brukere, eksperter og administratorer). Dette sikrer en grundig validerings- og autentiseringsprosess for dokumentene før de blir inkludert i arkivet (Galiev et al., 2018). Prosjektet kartlegger en rekke sikkerhetsrisikoer samt strategier for å adressere disse, inkludert angrep rettet mot modifisering, sletting og uregelmessig tillegg av databaseposter. Det blir spesielt understreket hvor viktig det er å verifisere systemets integritet og raskt oppdage skadelige aktiviteter. Som forsvar mot disse risikoene foreslår dokumentet løsninger som inkluderer effektiv hash-beregning for omfattende filer mellom etterfølgende poster, for å opprette en kontinuerlig og verifiserbar rekkefølge av poster. Dette tiltaket er videre forsterket ved en egen metode for å skape en "hemmelig fil" som er utledet fra blokkjedens data (Galiev et al., 2018). Archain-nettverket bruker tre typer noder. Administratornoden administrerer systemet og legger til nye dokumenter etter godkjenning fra eksperter. Den validerer og signerer transaksjoner, i tillegg til vedlikehold og kommunikasjon med andre noder. Ekspertnoden vurderer og godkjenner dokumenter før de legges til i blokkjeden, og undersøker dokumenter for å sikre at de inneholder nødvendige metadata og er korrekt formalisert. Brukernoden skaper og laster opp dokumenter til nettverket og interagerer med systemet via en klientapplikasjon for å sende dokumenter til vurdering. Nettverket fungerer slik at når en bruker laster opp et dokument, sendes det til en ekspertnode for vurdering. Eksperten godkjenner dokumentet, som deretter signeres og sendes til administratornoden. Administratornoden legger dokumentet til i blokkjeden, sammen med en kryptografisk signatur som bekrefter integriteten. Alle noder i nettverket kan verifisere integriteten av dokumentet ved å sjekke signaturen og transaksjonshistorikken i blokkjeden (Galiev et al., 2018). Archain viser blokkjedeteknologiens rolle i å takle grunnleggende utfordringer innen digital arkivering med tanke på langvarig bevaring, dokumentautentisering og hindring av uautoriserte endringer og forfalskninger.

4.3 ARCHANGEL

ARCHANGEL er et forskningsprosjekt som ble initiert for å utforske bruk av blokkjedeteknologi (Distributed Ledger Technology, DLT) for å sikre integriteten av digitale dokumenter lagret i offentlige arkiver. Prosjektet er et samarbeid mellom University of Surrey, The National Archives, og Open Data Institute (ODI) i Storbritannia. Hovedmålet er å

skape en desentralisert plattform som kan garantere dokumenters opprinnelse og uforanderlighet over tid (Collomosse et al., 2018). ARCHANGEL skiller seg ut ved å adressere de spesifikke utfordringene knyttet til den digitale transformasjonen i samfunnet, og hvordan disse påvirker langtidslagring av arkivmateriale. Mens tidligere arbeid i feltet ofte har fokusert på teoretiske rammeverk for dokumentbevaring, som Records Continuum Model, utvikling av standarder og teknologier for beskrivelse, katalogisering og søk i arkiver, slik som Discovery og Archives Portal Europe-prosjektet, tar ARCHANGEL fatt i utfordringen med å bevare digitalt arkivinnholds langtidsintegritet (Collomosse et al., 2018). Ved å bruke blokkjedeteknologi foreslår ARCHANGEL en plattform for å verifisere integriteten og proveniensen av digitale dokumenter både under arkivets forvaring (kurasjon) og ved dokumentets utlevering (presentasjon). ARCHANGEL utnytter en desentralisert struktur ved hjelp av blokkjedeteknologi for å beskytte integriteten til digitale dokumenter oppbevart i offentlige arkiver. Plattformen bruker, i likhet med Archain, en tillatelsesbasert blokkjede. Dette begrenser hvem som kan bidra med innhold til kjeden til kun autoriserte operatører eller automatiserte prosesser (Collomosse et al., 2018). Dette bidrar til å sikre at kun verifisert og godkjent informasjon blir lagt til, og opprettholder dokumentenes autentisitet og sikkerhet over tid. Systemets innhold er beskyttet gjennom bruk av kryptografiske bevis. Sikkerheten i blokkjeden oppnås ved at dataen i blokkene er uforanderlige, da hver ny blokk hashes for å inkludere hashene til de foregående blokkene. Dette sikrer at innholdet forblir sikret, og at blokkjeden er offentlig åpen for verifisering av dokumenter fra arkivet (Collomosse et al., 2018). Når dokumenter tas imot av systemet, starter en prosess for å trekke ut innholdsbevis, som er et slags digitalt fingeravtrykk av dokumentets innhold. Dette fingeravtrykket, sammen med nøkkelinformasjon om dokumentet, blir deretter låst fast og bevart innenfor blokkjeden. Første skritt i deponeringen av et dokument er å finne ut hva slags type innhold dokumentet består av. Dette gjøres med et spesialverktøy som identifiserer filformatet. Deretter blir innholdsbevis hentet ut på en måte som avhenger av filformatet ved hjelp av en prosess kalt innholdshashing (Collomosse et al., 2018). Med denne metoden kan hvem som helst, når som helst, sjekke dokumentets originalitet og historikk ved å hente opp og sammenligne innholdsbevis med det som allerede er sikret i blokkjeden. Dette kan sammenlignes med å ha et sikkert arkivskap hvor du kan dobbeltsjekke at ingen har tuklet med dokumentene dine ved å sammenligne notatene dine med det som er på filene. ARCHANGEL har blitt brukt som en prototype på Ethereums offentlige testnett (Rinkeby), hvor det benytter en konsensusmodell som tillater verifisering av dokumentenes proveniens og integritet. Dette illustrerer plattformens praktiske bruk og

evne til å integrere med eksisterende blokkjedeteknologier for å tilby en løsning som er både sikker og transparent (Collomosse et al., 2018). Nodene som brukes i ARCHANGEL består av arkivnode og offentlig node. Arkivnoden representerer arkivene som deltar i systemet og legger til nye dokumenter i blokkjeden. Denne validerer dokumenter, genererer kryptografiske signaturer og opprettholder konsensus med andre arkivnoder. Den offentlige noden tilbyr verifikasjonstjenester til allmennheten. I tillegg tillater den brukere å verifisere integriteten og opprinnelsen til dokumenter ved å sammenligne kryptografiske signaturer. Bruksscenarioer som Collomosse et al. (2018) beskriver inkluderer håndteringen av dokumenter fra offentlige undersøkelser, slik som etterforskningen av 7. juli-terrorangrepene i Storbritannia eller Chilcot-undersøkelsen. Disse dokumentene, som blir oppbevart i det britiske nasjonalarkivet, kan ofte være unntatt offentlighetens innsyn i mange, mange år. Med ARCHANGEL blir det mulig for slike arkiver å sikre dokumentenes digitale fingeravtrykk i blokkjeden i det øyeblikket de blir arkivert. Dette lar hvem som helst sjekke at dokumentene ikke har blitt endret når de til slutt blir offentliggjort (Collomosse et al., 2018). Denne verifiseringen tillater hvem som helst å bruke de samme metodene for innholdshashing som ble brukt ved opprinnelig arkivering for deretter å sammenligne disse hashene med de som er lagret i blokkjeden (Collomosse et al., 2018). Dette sikrer at selv om dokumentene holdes utenfor offentlig rekkevidde i lang tid, kan deres autentisitet og opprinnelse bekreftes når de endelig blir tilgjengelige for offentligheten. Et annet scenario innebærer en universitetspublisering av en studie om klimaendringer, inkludert en DOI til støttende data som er åpent utgitt. Disse dataene kan hasjes inn i innholdsevidens og lagres i ARCHANGEL DLT sammen med en hash av koden som er nødvendig for å gjenskape hashen ved publiseringstidspunktet (Collomosse et al., 2018). Hvis forskningens integritet blir utfordret kan universitetet selv flere år senere bevise at forskningsdataene matcher de som ble deponert ved utgivelsestidspunktet. Scenariene illustrerer hvordan ARCHANGEL kan bevare integriteten til dokumenter over lang tid og fremhever betydningen av teknologisk verifisering av autentisitet i en tid der digital forfalskning blir stadig mer avansert. Dette styrker tilliten til offentlige arkiver og sikrer at digital informasjon som for eksempel forskningsdata eller offisielle undersøkelsesdokumenter, kan bevares og verifiseres som ekte i fremtiden. Tidlige tilbakemeldinger fra personer involvert i arkivvitenskap viser interesse for hvordan ARCHANGEL håndterer langtidsbevaring av digitale dokumenter. Disse tilbakemeldingene understreker en videre anerkjennelse av behovet for innovative løsninger for å beskytte arkiver mot uautoriserte endringer og forfalskninger (Collomosse et al., 2018). Dette tyder at det fremdeles er god bevissthet rundt utfordringene digital arkivering står

overfor og en vilje til å utforske nye teknologier for å sikre arkivenes integritet og pålitelighet over tid. ARCHANGEL-prosjektet viser potensiale for å sikre integriteten av digitale arkiver gjennom bruk av blokkjedeteknologi. De tidlige evalueringene indikerer at plattformen kan styrke tilliten til offentlige arkiver ved å tilby en teknologisk basert garanti for dokumenters integritet (Collomosse et al., 2018).

5 Diskusjon

5.1 Bruksområder og Implementering av blokkjeder

Blokkjede-teknologi har skapt en rekke initiativer for å utvikle peer-to-peer databaser uten en sentral autoritet og brukes til mange forskjellige applikasjoner. Lemieux (2016) påpeker at mange blokkjede-løsninger som hevder å være arkivsystemer i realiteten bare lagrer hasher av oppføringene og ikke selve dataene. Dette skaper usikkerhet om hvorvidt disse metodene kan garantere at dataene forblir autentiske og tilgjengelige på lang sikt (Lemieux, 2016). For å sikre autentisiteten av data, er det viktig at de opprinnelige dataene lagres i en sikker form. Dette gjør det mulig å utføre hashing på nytt og sammenligne resultatene med de opprinnelige hashene som er lagret på blokkjeden. Ved å lagre de hashede dataene separat, kan man senere verifisere integriteten ved å matche den nye hashen med den som er lagret på blokkjeden (Lemieux, 2016, s. 15). Deloitte (2018) skriver at det finnes nesten 100 internasjonale prosjekter som undersøker bruk av blokkjeder i offentlig sektor. Mange av dem var da fortsatt under utvikling, og få var fullstendig implementert. Det blir også skrevet at blokkjeder kan gi tidlige fordeler i områder som olje- og gassregnskap, digital identitet, eiendomsregister, pasientdata, toll og avgifter, politiattester, fiskekvoter, mattilsyn og aksjeeierbøker. Disse bruksområdene viser hvordan teknologien kan være nyttig på områder som inkluderer lovpålagt arkivering (Deloitte, 2018). Samtidig blir det argumentert for at offentlig sektor i Norge allerede har løst mange av de problemene blokkjeder kan adressere med eksisterende registre og IT-løsninger (Deloitte, 2018). Selv om blokkjeder gir en stabil datastruktur som kan være nyttig for arkivering, kan det være vanskelig å oppdatere metadata og bevare forbindelsene mellom dokumenter i samme samling. Disse forbindelsene endrer seg når dokumentene er aktive og blir først stabile når dokumentene er inaktive (Stancic & Bralic, 2021). Når det gjelder digitale signaturer, har TrustChain blitt introdusert som en blokkjede-basert modell som bevarer gyldigheten av informasjon selv etter at sertifikatene

har utløpt. Dette gjør det mulig å bevare digitale signaturer over lang tid ved å oppgradere modellen for å bevare hele sertifiseringskjeden (Stancic & Bralic, 2021). For å sikre at dataene kan oppdateres uten å bli endret, foreslås et system som kombinerer blokkjeden med en egen database for metadata. Dette gjør det mulig å endre metadata når det trengs og gjør det enklere å søke etter informasjon sammenlignet med å søke direkte på blokkjeden (Stancic & Bralic, 2021). ARCHANGEL-prosjektet har utviklet en prototype som lar arkivinstitusjoner laste opp metadata til en privat Ethereum testbed (Bell et al., 2019). For å få innsikt i praktisk bruk og blokkjedens potensielle fordeler for arkivsektoren blir prototypen testet av flere arkivinstitusjoner for å forstå hvordan den kan passe inn i forskjellige teknologiske miljøer og integreres med andre prosesser (Bell et al., 2019).

5.2 Sikkerhet, sporbarhet og integritet

Avhengighet av tredjeparts lagringsorganisasjoner, mangel på åpenhet, risiko for manipulering og ødeleggelse av data er utfordringer ved digital arkivering som trenger konstant tilsyn. Selv om digital arkivering har forbedret noen av prosessene, har det også introdusert nye sikkerhetsrisikoer. Ved hjelp av et sikkerhetssystem basert på kryptografi blir blokkjeder introdusert som et forsvar mot disse utfordringene. Ved å legge til en kryptografisk signatur av dataene blir hver blokk gjort sikker mot manipulasjon. Blokkjeder benyttes også for en desentralisert og transparent måte å administrere arkiver på, hvor teknologien sporer endringer og eierforhold av dokumenter (Dimas et al., 2022). Distribuerte registre gir flere muligheten til å forvalte informasjon som kan forbedre kvaliteten på data. Denne teknologien kan også føre til bedre samarbeid mellom offentlige og private aktører og gi enkeltpersoner større kontroll over egne data (Deloitte, 2018). En annen viktig utfordring er å sikre at teknologien har lang levetid og evne til å integreres med eksisterende arkivsystemer. Teknologi basert på kryptografi har ofte en begrenset levetid på rundt 20 år før den kan bli sårbar for nye angrep (Bell et al., 2019). Det finnes flere forskjellige fremgangsmåter for å bruke blokkjeder til å bevare sikkerhet, sporbarhet og integritet. For eksempel blir sikkerheten i ARCHANGEL oppnådd ved at transaksjonsdata blir lagret permanent via peer-to-peer distribusjon og konsensuskontroll. I tillegg vil flere arkiver fra forskjellige nasjoner bidra til en felles blokkjede for å sikre at ingen enkelt institusjon har kontroll over dataene (Collomosse et al., 2018). Sporbarhet i ARCHANGEL blir ivaretatt ved at hver handling som utføres på et dokument registreres i blokkjeden og inneholder hash av dokumentinnholdet og tilhørende metadata. Dette gjør det mulig for alle å verifisere

dokumentene ved å sammenligne hashene med de opprinnelig registrerte verdiene (Collomosse et al., 2018). Sikkerheten i Filecoin bevares ved at dataene krypteres fra ende til ende slik at lagringstilbyderne ikke har tilgang til dekrypteringsnøklene. I tillegg bruker systemet bevis for replikasjon og tidsrom for å vise at dataene er kopiert til separate fysiske lagringsenheter (Protocol Labs, 2017). Sporbarhet sikres ved at lagringstilbydere må sende inn bevis for lagring til blokkjeden. Disse bevisene er offentlig tilgjengelige, slik at alle i nettverket kan sjekke dem uten å se de lagrede dataene. Bevisene danner en logg som kan revideres senere for å bekrefte at dataene faktisk ble lagret i riktig tidsperiode (Protocol Labs, 2017). Archain har utviklet spesifikke sikkerhetsprotokoller for å forhindre vanlige angrep på databasen. Dette inkluderer prosedyrer for å oppdage og varsle om integritetsbrudd, og spesielle algoritmer for å verifisere at data ikke har blitt endret uten autorisasjon (Galiev et al., 2018). Men (2020) beskriver et system som kombinerer blokkjede-teknologi med IPFS (InterPlanetary File System) og en distribuert database for å lagre og beskytte digitale arkiver. I eksempelet som er beskrevet, brukes en privat blokkjede for å lagre adresser og digitale fingeravtrykk av filene. Dette skaper en desentralisert og uforanderlig hovedbok som sikrer at dataene ikke kan manipuleres. Digitale filer og deres attributter lagres kryptert i en privat IPFS-klynge. Tilgangskontrollen utføres ved hjelp av smarte kontrakter (chaincode) som blir brukt på Hyperledger Fabric 1.0.3-plattformen. Systemet utnytter samtidig fordelene med blokkjede-teknologi, IPFS og smarte kontrakter for å skape et sikkert digitalt arkivsystem (Men, 2020).

5.3 Regulerings- og Juridiske Forhold

I Norge pålegger Arkivloven at offentlige institusjoner sikrer arkivmateriale med rettslig, forvaltningsmessig og forskningsmessig verdi. Alt fra offisielle dokumenter og korrespondanse til digitale databaser må bevares på en måte som over tid opprettholder integritet og tilgjengelighet. Loven krever at materialet blir ivaretatt slik at det forblir pålitelig og autentisk, og at data er tilgjengelige for fremtidige generasjoner (Arkivlova, 1992). Samtidig setter NOARK 5 strenge krav til frysing av metadata og dokumenter i arkivsystemer, med mål om å sikre autentisitet, pålitelighet, integritet og anvendelighet av arkivdokumenter (Arkivverket, 2018). Det er et uttrykt behov for å forstå hvordan blokkjede-baserte poster skal håndteres under gjeldende lover, spesielt i forhold til hvordan de brukes som bevisføring i retten (Lemieux, 2016). For å regulere bruken av blokkjeder er det derfor nødvendig med konkrete regelverk og juridiske rammer (Dimas et al., 2022). Samtidig har

det vært økende støtte for innføringen av tekniske standarder relatert til blokkjedeteknologi. Standarder som fokuserer på bruk av blokkjeder for arkivering kan bidra til å sikre at teknologien fortsetter å bygge på eksisterende løsninger og krav for arkivering (Lemieux, 2016). Blokkjedeteknologi kan tilpasses gjeldende regelverk, men det er behov for avklaringer spesielt knyttet til personvern. Internasjonalt samarbeid kan være nyttig for å etablere bærekraftige reguleringer (Deloitte, 2018). Blokkjeder kan fortsatt brukes til å sikre metadata for personopplysninger under GDPR. Ved å for eksempel ødelegge dekrypteringsnøklene, kan man oppfylle GDPRs krav om retten til sletting (L'Hutereau et al., 2019). Samtidig kan forskjellige land være underlagt forskjellig lovgivning og regulering. For eksempel er Archain utviklet i samsvar med russisk lovgivning, og vil derfor primært følge russiske databeskyttelseslover. Disse lovene kan ha forskjellige krav og reguleringer sammenlignet med GDPR. Slik regelverket gjelder nå, vil Archain være underlagt GDPR om systemet skal behandle data om EU-borgere, selv om det er basert i Russland. GDPR gjelder for alle organisasjoner som behandler personopplysninger om individer i EU uansett hvor organisasjonen er basert (European Parliament and Council of the European Union, 2016).

5.4 Bærekraft

Det høye energiforbruket forbundet med Bitcoin-mining er en av de mest omtalte utfordringene med blokkjede-teknologi innen bærekraft. Dette kommer av at mining krever betydelig datamaskinkraft og ofte involverer bruk av energikilder med høye karbonutslipp. Det er derfor viktig å vurdere miljøpåvirkningen av blokkjede-teknologi. Selv om The International Energy Agency (IEA) anslår at Bitcoin-mining bruker mindre enn 1/40 av 1 % av globalt elektrisitetsforbruk, bidrar det likevel til klimagassutslipp (Rana et al., 2019). I tillegg genererer Bitcoin-nettverket store mengder elektronisk avfall på grunn av behovet for spesialisert maskinvare som fort kan bli utdatert (Rana et al., 2019). En annen faktor som må vurderes er de økonomiske og ressursmessige kostnadene. Teknologien krever store mengder datakraft og kan være kostbar å vedlikeholde. Dette kan utgjøre en risiko for finansiell ustabilitet hvis kostnadene ikke er bærekraftige. For eksempel kan mindre institusjoner slite med å opprettholde nødvendig infrastruktur (Dimas et al., 2022). Kostnaden for metadata-lagring i en blokkjede øker lineært med antall dokumenter, og valideringstiden er avhengig av blokkjedens genereringstid for nye blokker. Denne lineære økningen kan føre til skalerbarhetsproblemer etter hvert som datamengden vokser. For å motvirke dette kan bruk av mekanismer som proof-of-authority bidra til å redusere ressursforbruket. Samtidig må

slike løsninger vurderes mot behovet for desentralisering og sikkerhet (L'Hutereau et al., 2019). Typiske blokkjeder har flere kjente problemer med datalagring, noe som krever integrasjon av nye tredjepartsprotokoller siden avgiftene er for høye for lagring på kjeden. Dette fører til at tilgang til innhold alltid vil koste samtidig som at innholdet aldri lagres permanent. Ettersom det er en eksponentiell vekst i behovet for datalagring blir det nødvendig med desentraliserte lavkostnadsprotokoller som kan skaleres (Williams & Jones, 2018). For å løse noen av disse utfordringene introduserer Arweave en ny blokkjede-lignende struktur kalt Blockweave. Denne strukturen tilbyr skalerbar on-chain lagring på en kostnadseffektiv måte. Når mengden data i systemet øker, vil mengden hashing som trengs for konsensus reduseres. Effekten av dette er at kostnadene for datalagring også reduseres (Williams & Jones, 2018).

5.5 Fremtidig utvikling

Blokkjeder har potensial til å løse mange av de nåværende problemene i digital arkivering, men det er viktig med videre forskning og vurdering av teknologiens langvarige effekter (Dimas et al., 2022). Beslutningstakere må derfor ha kjennskap til både fordeler og utfordringer med blokkjeder og sikre at teknologien inkluderer grunnleggende prinsipper for arkiv (Dimas et al., 2022). Forslaget om å bruke TrustChain-teknologi for digitale arkiver er et viktig skritt for å utforske ny teknologi samtidig som viktige prinsipper fra arkivvitenskapen blir beholdt. Fremtidig testing vil utforske hvordan TrustChain-systemet fungerer, hvor godt det presterer, og hvor godt det kan håndtere vekst. Samtidig vil det utføres samarbeid med arkivinstitusjoner for å bygge et nettverk av pålitelige noder (Stancic & Bralic, 2021). I tillegg bør det fokuseres på utvikling av mindre energikrevende metoder for å validere blokker i blokkjeden for å gjøre teknologien mer bærekraftig. For å oppnå sterk bærekraft må utfordringer knyttet til energiforbruk, regulatoriske rammer, og teknologiske utfordringer løses. Videre forskning og innovasjon er nødvendig for å utnytte det fulle potensiale til blokkjede-teknologien samtidig som negative miljøpåvirkninger minimeres (Rana et al., 2019). ARCHANGEL Prosjektet har vist arkivenes vilje til å engasjere seg i og utforske nye teknologier som blokkjeder for å forbedre fagområdet (Green et al., 2018). ARCHANGEL har sett på flere muligheter for fremtidig utvikling av prosjektet. For øyeblikket utføres innholdshashing ved hjelp av binære hashing-algoritmer som SHA-256, men det er planer om å spesialisere hashing for spesifikke dokumenttyper som PDF-er og til og med bilder og videoer (Collomosse et al., 2018). I fremtiden vurderer også ARCHANGEL

å bruke smarte kontrakter ikke bare for å legge til data i blokkjeden men også for å søke og verifisere dokumenter (Collomosse et al., 2018). Filecoin-teamet planlegger å stadig forbedre systemet for å håndtere flere brukere og mer data. De vil gjøre teknologiene Proof-of-Replication (PoRep) og Proof-of-Spacetime (PoSt) mer effektive og mindre ressurskrevende (Protocol Labs, 2017). For å gjøre Filecoin enklere å bruke, vil de forbedre brukergrensesnittet og lage det enklere for folk uten teknisk bakgrunn å bruke nettverket. Dette inkluderer å utvikle bedre verktøy og dokumentasjon for både brukere og utviklere. Det vil også være fokus på å forbedre sikkerheten og personvernet i Filecoin. Dette innebærer å utvikle bedre kryptografiske metoder og mekanismer for å beskytte data mot uautorisert tilgang og manipulasjon (Protocol Labs, 2017). Archain ble laget for eksperimentell bruk hvor testing og tilbakemelding skal bidra til å forbedre systemet. I fremtiden planlegges det nye funksjoner og forbedringer for å gjøre systemet mer effektivt, brukervennlig og sikkert (Galiev et al., 2018). Dette inkluderer oppdaterte algoritmer, bedre brukergrensesnitt og økt sikkerhet mot nye trusler. Videre utvikling innebærer også å inkludere flere avdelinger og håndtere flere typer dokumenter ved å distribuere programvaren til hele Republikken Tatarstans arkivsystem (Galiev et al., 2018).

6 Oppsummering og konklusjon

Denne studien har utforsket hvordan blokkjedeteknologi kan forbedre langsiktig bevaring av digitale arkiver og beskytte mot uautoriserte dataendringer og forfalskninger. Behovet for sikre og pålitelige digitale arkiver øker i et samfunn som produserer enorme mengder digitale data. Digitale arkiver står fremdeles overfor utfordringer som risiko for datamanipulering, forfalskning og tap over tid. Blokkjedeteknologi, kjent for desentralisering, uforanderlighet, transparens og kryptografisk sikkerhet, kan møte disse utfordringene. Teknologien bruker et nettverk av noder for å verifisere og lagre transaksjoner, som skaper en sikker og uforanderlig kjede av blokker. Denne mekanismen sikrer at endringer i arkivmaterialet er lett å oppdage. Gjennom casestudier av Filecoin, Archain og ARCHANGEL-prosjektet har vi sett praktiske eksempler på bruk av blokkjedeteknologi i arkivering. Filecoin er et desentralisert lagringsnettverk som bruker blokkjedeteknologi for å tilby en markedsplass for lagring, og bruker Proof-of-Replication og Proof-of-Spacetime for å sikre dataintegritet og tilgjengelighet (Protocol Labs, 2017). Archain er et arkivsystem utviklet i Tatarstan, Russland, som benytter en tillatelsesbasert blokkjede for å sikre dokumentoverføringer og

bruker russiske kryptografiske standarder (Galiev et al., 2018). ARCHANGEL er et britisk prosjekt som bruker blokkjedeteknologi for å sikre integriteten av digitale dokumenter i offentlige arkiver, og benytter en desentralisert struktur og kryptografiske bevis for å verifisere dokumenters opprinnelse og uforanderlighet over tid (Collomosse et al., 2018). Blokkjedeteknologi har stort potensial til å forbedre langsiktig bevaring av digitale arkiver ved å tilby høy sikkerhet og pålitelighet. Teknologiens evne til å skape en uforanderlig og verifiserbar kjede av transaksjoner gjør den godt egnet til å sikre dokumentenes integritet og autentisitet. De praktiske eksemplene viser lovende resultater, og det er viktig å merke seg at teknologien fortsatt er under utvikling. Videre forskning er nødvendig for å løse juridiske, regulatoriske og tekniske utfordringer, spesielt med hensyn til personvern og energiforbruk. Fremtidig utvikling bør fokusere på å gjøre blokkjedeteknologi mer bærekraftig og kompatibel med eksisterende arkivsystemer. Et godt samarbeid mellom teknologiske utviklere, arkivinstitusjoner og juridiske myndigheter vil være viktig for å oppnå en vellykket implementering av teknologien. Gjennom kontinuerlig utvikling og tilpasning kan blokkjedeteknologi bidra til å håndtere det økende behovet for sikker digital arkivering.

Litteraturliste

Arkivlova. (1992). *Lov om arkiv.* (LOV-1992-12-04-126) Lovdata. https://lovdata.no/dokument/NL/lov/1992-12-04-126

Arkivverket. (2018). Noark 5 versjon 5.0: Spesifikasjon. https://www.arkivverket.no/forvaltning-og-utvikling/noark-standarden/noark5-standarden

Bell, M., Green, A., Sheridan, J., Collomosse, J., Cooper, D., Bui, T., Thereaux, O., & Higgins, J. (2019). *Underscoring archival authenticity with blockchain technology*. Insights, 32, 21, 1-7. https://doi.org/10.1629/uksg.470

Benet, J. (2014). *IPFS - Content addressed, versioned, P2P file system* (Draft 3). Hentet fra: https://arxiv.org/pdf/1407.3561.pdf

Collomosse, J., Bui, T., Brown, A., Sheridan, J., Green, A., Bell, M., Fawcett, J., Higgins, J., & Thereaux, O. (2018). *ARCHANGEL: Trusted archives of digital public documents*. ACM. https://doi.org/10.1145/3209280.3229120

Consultative Committee for Space Data Systems. (2012). *Reference model for an Open Archival Information System (OAIS)*. CCSDS 650.0-M-2. Magenta Book. https://public.ccsds.org/pubs/650x0m2.pdf

Deloitte. (2018). *Distribuert sannhet: Potensial og barrierer for blokkjeder i norsk offentlig sektor*. Deloitte Norge. Hentet fra: https://www.regjeringen.no/no/dokumenter/distribuert-sannhet/id2593790/

Dimas Wijaksono, S., Hadi Trianto, R., Febri Ikhtiarman, A., Amalia, R., & Jannah, F. (2022). Execution of Blockchain in The World of Archive. *Blockchain Frontier Technology*, *2*(1), 64–71. https://doi.org/10.34306/bfront.v2i1.115

Dolmatov, V. (Ed.), & Degtyarev, A. (2013). *GOST R 34.10-2012: Digital signature algorithm* (RFC 7091). Internet Engineering Task Force. https://doi.org/10.1742-6596/1550/6/062021

European Parliament and Council of the European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data,

and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union, L 119*, 1-88. https://eur-lex.europa.eu/eli/reg/2016/679/oj

Farah, N. A. A. (2018). Blockchain technology: Classification, opportunities, and challenges. *International Research Journal of Engineering and Technology (IRJET), 5*(5), 3423-3426. https://www.irjet.net/archives/V5/i5/IRJET-V5I5423.pdf

Green, A., Bell, M., Sheridan, J., Collomosse, J., Bui, T., Brown, A., Fawcett, J., Thereaux, O., & Tennison, J. (2018). *304.2 Using blockchain to engender trust in public digital archives.* iPRES 2018: 15th International Conference on Digital Preservation, Boston, USA. https://doi.org/10.17605/OSF.IO/KEFJ8

Kuznetsov, A., Oleshko, I., Tymchenko, V., Lisitsky, K., Rodinko, M., & Kolhatin, A. (2021). Performance analysis of cryptographic hash functions suitable for use in blockchain. *I. J. Computer Network and Information Security, 13*(2), 1-15. https://doi.org/10.5815/ijcnis.2021.02.01

Lemieux, V. L. (2016). *Blockchain technology for recordkeeping: Help or hype?* Social Sciences and Humanities Research Council of Canada. Hentet fra: https://www.researchgate.net/publication/309414276_Blockchain_for_Recordkeeping_Help_or_Hype

L'Hutereau, A., Burihabwa, D., Felber, P., Mercier, H., & Schiavoni, V. (2019). Blockchain-based metadata protection for archival systems. *Proceedings of the IEEE 38th Symposium on Reliable Distributed Systems (SRDS 2019)*, 44-53. https://doi.org/10.1109/SRDS47363.2019.00044

Lo Duca, A., Bacciu, C., & Marchetti, A. (2020). The use of blockchain for digital archives: A comparison between Ethereum and Hyperledger. *Umanistica Digitale, 8*. https://doi.org/10.6092/issn.2532-8816/9959

Men, R. (2020). Research on access control method of digital archives based on blockchain. *Journal of Physics: Conference Series, 1550*(062021). IOP Publishing. https://doi.org/10.1088/1742-6596/1550/6/062021

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. Hentet fra: https://bitcoin.org/bitcoin.pdf

NOU 2019: 9 (2019). *Fra kalvskinn til datasjø: ny lov om samfunnsdokumentasjon og arkiver*. Departementets sikkerhets- og serviceorganisasjon, teknisk redaksjon.

Offentleglova. (2006). *Lov om rett til innsyn i dokument i offentleg verksemd*. (LOV-2006-05-19-16). Lovdata. https://lovdata.no/dokument/NL/lov/2006-05-19-16

Personopplysningsloven (2018). *Lov om behandling av personopplysninger*. (LOV-2018-06-15-38). Lovdata. https://lovdata.no/dokument/NL/lov/2018-06-15-38

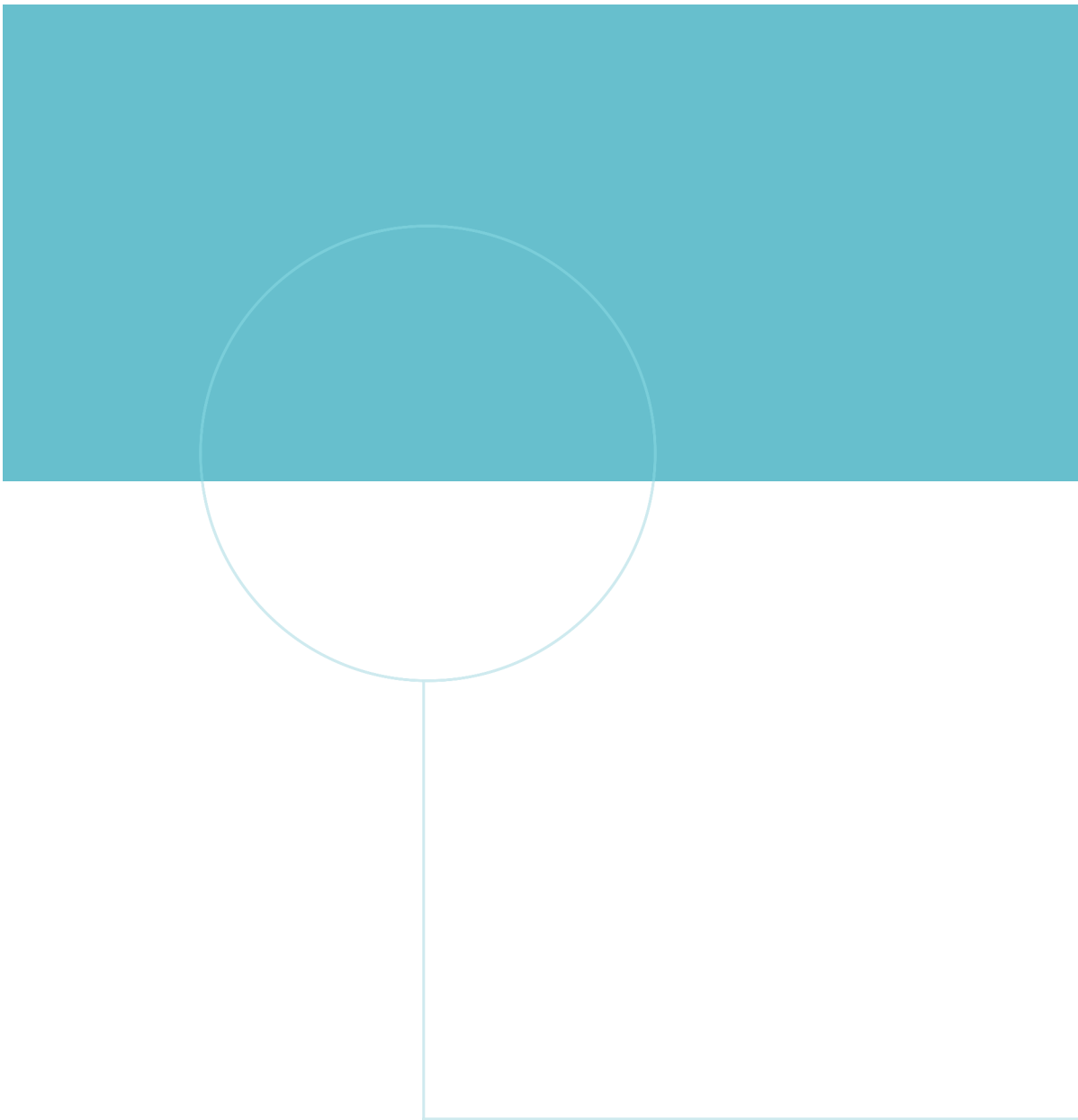
Protocol Labs. (2017). *Filecoin: A decentralized storage network*. Hentet fra: https://filecoin.io/filecoin.pdf

Rana, R. L., Giungato, P., Tarabella, A., & Tricase, C. (2019). Blockchain applications and sustainability issues. *Amfiteatru Economic, 21*(Special Issue No. 13), 861-870. https://doi.org/10.24818/EA/2019/S13/861

Stancic, H. & Bralic, V. (2021). *Digital Archives Relying on Blockchain: Overcoming the Limitations of Data Immutability*. Computers 2021. https://doi.org/10.3390/computers10080091

Upadhyay, A., Mukhuty, S., Kumar, V., & Kazancoglu, Y. (2021). Blockchain technology and the circular economy: Implications for sustainability and social responsibility. *Journal of Cleaner Production, 293*, 126130. https://doi.org/10.1016/j.jclepro.2021.126130

Williams, S., & Jones, W. (2018). *Arweave Lightpaper*. Version 0.9. Hentet fra: https://whitepaper.io/document/627/arweave-whitepaper



NTNU

Kunnskap for en bedre verden