CHALMERS

Blockkedja för säkrare hälsodata och ökad patientsäkerhet

En litteraturstudie om blockkedjeteknikens funktion inom sjukvården

Kandidatarbete inom Elektroteknik

Armin Alami Alamdari
Selin Oguz
Viktor Olafsson
Gustav Rydner

Institutionen för Elektroteknik (E2)
Avdelningen för Signalbehandling och medicinteknik
CHALMERS TEKNISKA HÖGSKOLA
Göteborg, Sverige 2023
www.chalmers.se

Blockkedja för säkrare hälsodata och ökad patientsäkerhet

En litteraturstudie om blockkedjeteknikens funktion inom sjukvården

Kandidatarbete inom Elektroteknik

EENX16-23-47

Armin Alami Alamdari
Selin Oguz
Viktor Olafsson
Gustav Rydner

Institutionen för Elektroteknik (E2)
Avdelningen för Signalbehandling och medicinteknik
CHALMERS TEKNISKA HÖGSKOLA
Göteborg, Sverige 2023
www.chalmers.se

Blockkedja för säkrare hälsodata och ökad patientsäkerhet

En litteraturstudie om blockkedjeteknikens funktion inom sjukvården

Armin Alami Alamdari, Selin Oguz, Viktor Olafsson, Gustav Rydner

Kandidatarbete inom civilingenjörsprogrammet Elektroteknik
Institutionen för Elektroteknik (E2)
Chalmers tekniska högskola
SE-412 96 Göteborg, Sverige 2023
Telefon + 46 (0)31-772 1000

Chalmers digitaltryck Göteborg, Sverige 2023

Sammanfattning

Sjukvården är ett område som blir allt mer digitaliserat. På grund av detta har hacker-attacker ökat och frågor om hur hälsodata ska lagras och skyddas har uppstått. Eftersom hälsodata är integritetskänsligt ökar vikten för säker lagring. Denna litteraturstudie genomförs i syfte att undersöka blockkedjeteknologin, dess funktioner och egenskaper, samt hur den skulle kunna struktureras inom hälso- och sjukvården. Studien undersöker sjukvårdens behov av ett interoperabelt och decentraliserat system, samt dess struktur. Vidare undersöker studien hur användningen av blockkedjeteknologin fungerar med nuvarande lagar som GDPR och patientdatalagen. Litteraturstudien utfördes på aktuell forskning och tidigare prototyper för hur blockkedjeteknologin skulle kunna användas inom sjukvården. Slutsatsen är att blockkedjeteknologin har potential att öka säkrare datautbyte, patientsäkerthet och interoperabilitet inom hälsovården, dock behövs det fortfarande mer forskning kring aspekter som blockkedjors struktur, datalagring på blockkedja och ett stort fokus på interoperabla system.

Abstract

Healthcare is an area that is becoming increasingly digitized. Due to this, hacker-attacks have increased and questions about how health data should be stored and protected have arisen. As health data is privacy sensitive, the importance of secure storage is increasing. This literature review is carried out with the aim of investigating blockchain technology, its functions and properties, as well as how it could be structured within healthcare. The study examines healthcare's need for an interoperable and decentralized system, as well as its structure. Furthermore, the study examines how the use of blockchain technology works with current laws such as GDPR and patient data regulations. The literature review was conducted on current research and previous prototypes for how blockchain technology could be used in healthcare. The conclusion is that blockchain technology has the potential to increase safer data exchange, patient safety and interoperability in healthcare, however, more research is still needed on aspects such as the structure of blockchains, data storage on blockchain and a major focus on interoperables systems.

Ordlista

Ordlistan är till för att underlätta förståelsen av ämnesspecifika begrepp som tas upp i rapporten.

- *Decentraliserad App (DApp):* Blockkedjebaserad applikation
- *Electronic Health Record (EHR)*: Elektronisk journal som lagrar hälsoinformation i digital form
- *Fast Healthcare Interoperability Resources (FHIR)*: En uppsättning regler och specifikationer för utbyte av elektronisk sjukvårdsdata
- *Health Level Seven (HL7)*: Organisation som driver standardarbete inom hälso- och sjukvård och hänvisar till de standarder som de har skapat
- *Interoperabilitet*: Förmågan hos system att ”förstå varandra”
- *InterPlanitary File System (IPFS)*: Ett decentraliserat fildelnings system som använder sig av hashsummor.
- *Patientsäkerhet*: Patientskydd mot fysisk eller psykisk skada av hälso- och sjukvården
- *Proof-of-concept (POC)*: Koncepttest handlar om att demonstrera en produkts genomförbarhet i syfte att bevisa de möjligheter som finns

Innehåll

1 Inledning

Hälso- och sjukvård är ett av de grundläggande sociala systemen som finns i ett samhälle för att behandla patienter, förebygga sjukdomar och hålla en fungerande livsstandard på individ- och samhällsnivå. Enligt Regeringskansliet ska vården vara ”jämlik, jämställd och tillgänglig och erbjudas utifrån behov på lika villkor”[1].

En patient besöker många olika vårdenheter under sin livstid. Under ett besök sammanställs och registreras patientens hälsodata i en journal som även benämns som Personal Health Record (PHR). PHR definerades i rapporten The personal health working group final report av Markle Foundation: ”An electronic application through which individuals can access, manage and share their health information, and that of others for whom they are authorized, in a private, secure, and confidential environment” [2]. Säker delning av hälsodata är en förutsättning för en effektiv och patientsäker vård till exempel för att skicka remisser. Trots vikten av säker delning av hälsodata har många av dagens vårdsystem stora svårigheter med att utbyta information mellan varandra. Vid exempelvis remitteringar och hantering av akuta händelser inom den prehospitala vården är ett effektivt informationsutbyte extra viktigt.

Blockkedja har nyligen introducerats in i medicinbranschen för att lösa säkerhetsfrågor och datasäkerhet. En blockkedja är en ”distributed ledger” (databaser) för att distribuera register för transaktioner mellan parter [3]. Blockkedjans mest lovande funktion är dess decentraliserade struktur som kan exempelvis skydda lagrade elektroniska hälsojournaler (EHR) från skadliga attacker och servicefel eller avbrott på en viktig webbplats [3]. Ett blockkedjebaserat system med decentraliserad arkitektur skulle med största sannolikhet undvika dessa problem. En annan fördel med blockkedjan är att det är väldigt svårt att manipulera lagrade transaktioner på grund av säkerheten för så kallade ”hashfunktionen” och ”proof-of-work” (POW) i blocket. En hashfunktion är en matematisk beräkning som tar in en relativt godtycklig mängd indata, matar den och producerar en utdata av fast storlek som är samma som indatan [4].

Journaler används för att förstå patientens hälsa, följa den över en period och fatta beslut om vilken vård som är lämplig eller behövlig. En journal är integritetskänslig för så kallade “hacker-attacker” genom dataintrång, eftersom den lagrar personlig och känslig information. Sjukvårdens nätverk är uppbyggd på integration av informations- och kommunikationsteknik (IKT) för utbytet av data. Implementering av kommunikationsnätverk och sjukvårdssystem är en förutsättning för en effektiv och patientsäker vård, men det introducerar också sårbarheter [5]. Andra sårbarheter enligt [5] är exempelvis:

- attacker för att stänga ner sjukhussystem, och labb- och kritisk utrustning
- identitetsstöld och försäkringsbedrägeri genom att stjäla eller imitera personlig information

- historik förlust av medicinsk information som är avgörande för behandling av patienter i kritisk situation eller sjukdom

Antalet hacker-attacker har ökat de senaste åren och nyligen utsattes den globala folkhälsan för ett cyberhot i form av ett programvirus, Wannacry, allmänt känt som Ransomware (kryptering av fil som pressas mot pengar i utbyte av filen) [6]. Attacken påverkade mer än 150 länder där hundratals datorer infekterades och attacken hade en mycket specifik inverkan på Storbritanniens National Health Service (NHS). Under fyra dagar var sjukhus runt om i Storbritannien påverkade vilket ledde till att kliniska möten och operationer fick ställas in. Det uppstod kaos bland den administrativa personalen på sjukhus och komplexa medicinska maskiner inaktiverades vilket visade sig vara riskfyllt för patientens hälsa. Även om dödligheten var låg skapades allvarliga osynliga konsekvenser på grund av attacken och NHS uppskattade kostnaden för attacken till minst 92 miljoner brittiska pund. Den totala ekonomiska förlusten kan inte utvärderas men säkerhetsöppningen av sjukhusen kostade cirka 7 miljoner pund inklusive patienters liv, rättstvister och förstörelse av rykte [6].

En ransomware-attack hindrar åtkomst till datafiler genom en ransomware, en typ av skadlig programvara, där systemet kräver en betalning av en lösensumma (ransom) för att få tillbaka datafilerna [7]. Enligt Sophos rapport "The State of Ransomware 2022" listas Sverige som ett av de länder där flest ransomware-attacker per capita sker samt är mest benägen att betala ut lösensumma under en sådan attack [8]. Enligt den svenska krismyndigheten Myndigheten för samhällsskydd och beredskap (MSB) har man enligt internationella insatser visat med rapporter som underlag att organisationer inom hälso- och sjukvårdssektorn varit attraktiva för cyberattacker under covid-19-pandemin [9].

Bekymmer om patientsäkerhet har ökat, och hälso- och sjukvård sektorn har hittat liknande utmaningar inom flygbranschen [10]. Enligt [10] har flygbranschen sedan långt innan lärt sig att information och klar kommunikation är kritisk för säker navigation av ett flygplan. Piloter måste kommunicera med flygledare om oron om destination och nuvarande omständighet (som mekanisk eller andra problem), och miljöfaktorer (väderförhållande) som kan påverka ändring av rutt. Information är lika avgörande för en säker hälso- och sjukvård, exempelvis så måste en läkare ha tillgång till patientinformation för att erbjuda den vård patienten behöver. Skillnaden mellan arbetsmiljön inom flygbranschen och hälso- och sjukvården är att en pilot har direkt tillgång till information som de behöver för att ta informerade beslut [10]. Inom hälso- och sjukvården finns inte samma IT-infrastruktur. Inom den svenska vården finns det problem mellan datautbytet vid exempelvis en fallolycka i en patients hem. Kommunikationen mellan aktörer är inte effektiv och det grundar sig i att systemen som används inte "förstår varandra" - interoperabilitet saknas.

1.1 Syfte och mål

Syftet är att undersöka hur blockkedjeteknologin fungerar för att stödja säker och interoperabelt utbyte av hälsodata inom svensk prehospital vård. Målet är att

utforska olika alternativ för en decentraliserad app (DApp) så att hälsodata kan utbytas med hjälp av sensordata inom olika miljöer inom den svenska vården.

1.2 Frågeställningar

Utifrån arbetets inledning, genom undersökning av och befintliga lösning ämnar arbetet undersöka följande frågeställningar:

F.1 Hur hade en ideal blockkedja sett ut för att stödja säker och interoperabel utbyte av hälsodata inom den svenska sjukvården?

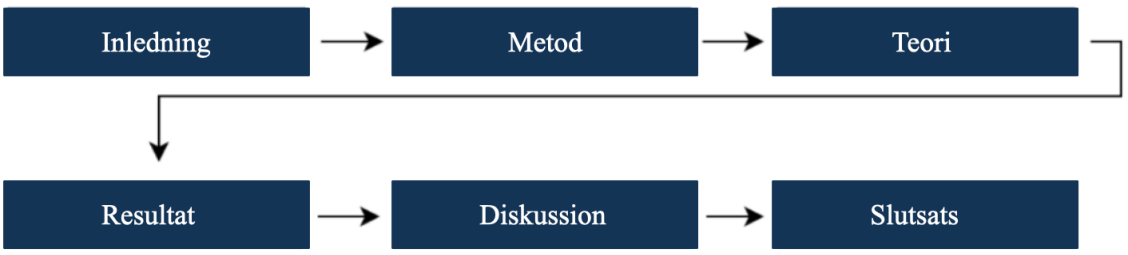
F.2 Hur kan sensordata vid hemmonitorering delas interoperabelt med hjälp av en DApp blockkedja för ökad spårbarhet och säkerhet inom prehospital vård?

1.3 Avgränsningar

I detta projekt ligger fokus främst på den prehospitala vårdkedjan från larmsignal till ankomst till sjukhus. Trots att det finns tillgängliga resurser på Chalmers som sensorer, så kommer fokuset inte att läggas på hur man kan skapa en metod för att omvandla sensordata till en läsbar standard som kan existera på vald blockkedja då det inte finns tid till att göra en ordentlig undersökning av detta. Eftersom rapporten främst är en litteraturstudie kommer fokuset inte vara att skapa en “proof-of-concept” (POC).

1.4 Disposition

Rapporten inleds med en inledning vilket ger en bakgrund av vad rapporten handlar om samt en teoretisk inblick i vilka problem som sjukvården står inför. Därefter beskrivs metodiken och genomförandet av studien. Metoden innehåller två strategier - litteraturstudie och utvecklandet av ”proof-of-concept” (POC). Efter metoden presenteras teorin om den svenska hälso- och sjukvården, hälsodatan inom svensk vård och blockkedjteknologin. Utifrån litteraturstudien presenteras resultatet i resultatdelen av rapporten och slutligen diskuteras det med utgångspunkt från rapportens syfte och frågeställningar i diskussionen. Rapportens struktur illustreras med hjälp av figur 1 nedan.



Figur 1: Rapportens disposition

2 Metod

I detta kapitel beskrivs den metodik som använts i arbetet för att leda till ett resultat och därefter en diskussion, samt hur den tillämpas för att besvara frågeställningarna och uppfylla rapportens syfte. Schematisk illustration över metodiken illustreras med hjälp av figur 1 tidigare i arbetet.

Studien inleddes med formulering av problembeskrivning, och syfte och frågeställningar. Med hjälp av tidigare forskning och studier påbörjades en litteraturstudie för att få en grund och förståelse för området. Figur 2 visar den schematiska implementeringen som genomfördes för att svara på frågeställningar och uppfylla syftet med studien.

Figur 2: Metodiken för studien

2.1 Litteraturstudie

För att få en enkel förståelse över området gjordes en förstudie, bland annat om datadelning, interoperabelt utbyte av hälsodata, hur blockkedjeteknik fungerar, och om rapportens syfte och frågeställningar var relevanta för denna studie. Vetenskapliga teorier som bland annat datadelning, interoperabilitet och blockkedja har sökts genom användandet av nyckelorden och olika kombinationer av dem i sökmotorer som IEEE Xplore, Google Scholar och Elsevier. Nyckelord på engelska som bland annat ”interoperability”, ”blockchain”, ”health data” och ”data sharing” har sökts i sökmotorer. Även boolean operators (boolesk operator) som ”och” användes. Vi värderar källorna på så sätt att vi först kollar vem upphovsmannen är: finns det en angiven författare eller utgivare och kan deras auktoritet verifieras? I nästa steg är det viktigt att tänka på vilket syfte informationen har, vem materialet är skrivet för, hur aktuell informationen är och hur trovärdig källan är.

3 Teori

I detta kapitel definieras de teoretiska områdena i syfte att underlätta förståelsen för kommande delar i rapporten. Det som presenteras är bland annat den svenska sjukvården, delning och lagring av hälsodata, de lagar och regulationer som finns samt blockkedja och dess uppbyggnad.

3.1 Den svenska hälso- och sjukvården

Den svenska hälso- och sjukvården är ett socialt ansvarsfullt system med offentlig skyldighet att skydda alla svenska medborgares hälsa [11]. Hälso- och sjukvårdslagen (1982:763) innehåller mål och riktlinjer som ger tillgång till behovsbaserade tjänster, samt betonar en vision om lika hälsa för alla. Det finns tre grundläggande principer som bör gälla för den svenska hälsovården, dessa är enligt hälso- och sjukvårdslagen (1982:763) följande:

1. Principen om mänsklig värdighet - att alla människor har lika rätt till människovärdighet och oavsett ställning i samhället ska ha samma rättigheter

2. Behovs- och solidaritetsprincipen - att de som har störst nöd till sjukvård har företräde inom sjukvården

3. Kostnadseffektivitetsprincipen - att det ska finnas ett rimligt samband mellan kostnaderna och effekterna vid val av vårdalternativ, mätt i termer av förbättringar av hälsa och livskvalitet

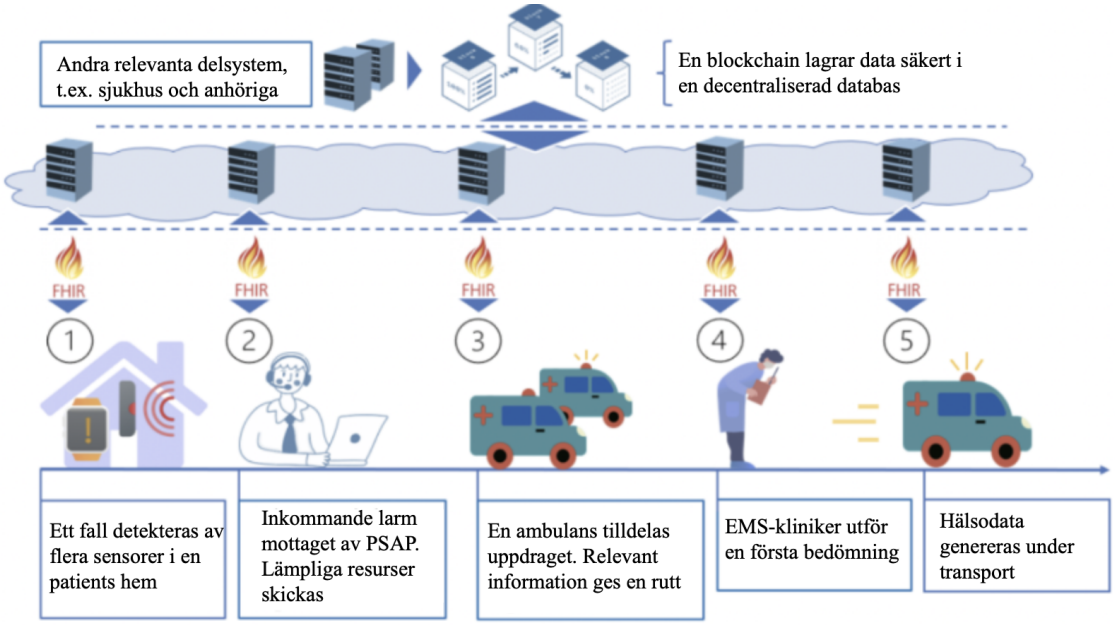
3.1.1 Den prehospitala vården i Sverige och dess användning av hälsodata

Prehospitalt arbete är sjukvård som utförs mellan tidpunkten för vårdbehovets uppkomst och ankomsten till sjukvårdsinrättning, till exempel ambulanssjukvård eller akutsjukvård på olycksplats [12].

Den prehospitala vårdkedjan börjar från att patienten slagit larm och pågår genom handläggning, vård på plats, transport ända till överlämning till rätt vårdplats. Den utförs framförallt utanför sjukhus och då av ambulanser och helikoptrar. För att prehospital sjukvård ska fungera krävs ett effektivt samarbete och informationsutbyte mellan olika aktörer och dess system i vårdkedjan. Prehospitala snabbspår har införts för olika patientgrupper för att förbättra omhändertagandet och undvika onödiga väntetider på akutmottagningar [13]. Syftet är att säkerställa att patienterna får den vård och behandling de behöver så fort som möjligt. Snabbspår används för patienter med allvarliga medicinska tillstånd och hjälper till att minimera riskerna för förseningar i behandlingen.

Ett effektivt prehospitalt omhändertagande av patienter är avgörande för patientens positiva utfall i många akuta situationer. För detta krävs ett effektivt utbyte av hälsodata som kan bestå av till exempel sensordata från hemmmonitorering eller

data från patientjournaler. En effektiv delning av hälsodata mellan ambulans och akutmottagning kan bidra till snabbare handledning och därmed kortare väntetid innan behandling. Införandet av snabbare handläggning har resulterat i färre dödsfall och komplikationer av patienter med höftfraktur [13]. Figur 3 [14], som är översatt till svenska, illustrerar de olika stegen som sker vid händelse av en fallolycka inom hemsjukvården. Några av dessa steg i vårdkedjan är sensorer placerade i patientens hem, ambulans och larmcentral (PSAP).



Figur 3: Exempel på hur FHIR och blockkedjor kan hjälpa till att säkra och skapa robusta system för detektering av fallolyckor

Olika regioner i Sverige använder olika patientjournalsystem. Även inom varje enskild region skiljer sig systemen vanligen åt mellan olika aktörer, vilket skapar problem för vårdgivare då man inte alltid ges tillgång till patientens data [13]. Problemet beror på att man vid utvecklandet av systemen inte har prioriterat interoperabilitet mellan olika system [15]. Ambulanssjukvårdens digitala patientjournalsystem hanterar information som exempelvis: kontaktorsak, hämtplats, folkbokföringsadress, behandlingar, kön, ålder, datum, tid för ankomst till sjukhus och avlämning på akutmottagning eller röntgen samt ambulansbehov under de närmaste sex månaderna efter utskrivning från vård.

Patienter i Sverige har åtkomst till sin hälsodata i patientjournaler genom olika internetlösningar men har inte möjlighet att själva ändra informationen i dessa [15]. Dessutom blir en del hälsodata otillgänglig för patienter på grund av brist på interoperabilitet mellan system. Det finns också tillfällen där det inte anses lämpligt för vårdgivare att göra viss information tillgänglig till patienter vilket är en egen debatt i sig. Vill man som samhälle utveckla ett väl fungerande patientjournalsystem

behöver patienter vara med i utvecklingen av dessa för att se till att deras behov blir mötta. För att skapa en patientcentrerad vård behöver man lösa de problem som finns med interoperabilitet så att patienter kan få åtkomst till data som de på pappret ska ha tillgång till.

I takt med att digitaliseringen av sjukvården ökar skulle en konsekvens kunna vara att människor blir oroliga över deras datasäkerhet. Trots detta visar Sveriges befolkning en stor tillit till sjukvården jämfört med andra länder i EU [16]. Patienter som inte litar på sjukvårdens datasäkerhet kan vara mer tvivelaktiga till att ge läkare eller forskningsinstitut tillstånd att hantera datan till att göra nytta för patienten eller sjukvården och skapar ett hinder för sjukvårdens digitalisering. Patientens tillit till datahantering inom sjukvården har visat sig vara en förutsättning för ett effektivt utbyte av hälsodata [16].

En studie från Karolinska Institutet år 2021 [17] visar att svenska patienter är villiga att dela med sig av sin hälsodata, inte bara för egen vinning, men även vid fall då det främst gynnar andra. Det hävdades också att patienterna prioriterade att dela sin hälsodata för sjukvårdens utveckling över att få möjligheten att kontrollera sin egen hälsodata. Studien visade även att patienterna tycker det är viktigare att ha tillgång till datan bakom sin egen behandling över att begränsa andras åtkomst till sin data, vare sig de är behöriga eller obehöriga.

3.2 Hälsodata inom svensk vård för en effektiv och patientsäker vård

Det finns olika lagar och regulationer som skapats för att skydda hälsodata och för att säkra datahanteringen inom den svenska sjukvården. Då hälsodata är integritetskänslig är det viktigt att informationsutbyte sker på ett effektivt och patientsäkert sätt. Genom datadelning kan grupper av vårdspecialister analysera olika fall, dela information och samarbeta vilket kan bidra till utveckling inom sjukvården.

3.2.1 Vilka lagar och regulationer finns på hälsodata i Sverige?

Patienter och deras hälsodata skyddas av lagar och regulationer som sätter krav på ansvariga personer i vårdkedjan. Dataskyddsförordningen (GDPR) är en förordning som är skapad av EU för EU-länder i syfte att skydda data. GDPR sätter skyldigheter på verksamheter att säkra användares rätt till en privat och säker datahantering [18]. Verksamheter har en skyldighet att kunna bevisa att de följer riktlinjerna i GDPR. Några exempel på riktlinjerna inkluderar användarens rätt till att få tillgång till sin data, rätta eventuella felaktigheter i datan och radera den när så önskas [19].

Inom hälso- och sjukvården kompletteras GDPR av Patientdatalagen som ställer ytterligare krav på vårdgivare [20]. Bland annat kan patienten genom sin vårdgivare få tillgång till sin journal och i vissa fall få möjligheten att spärra sina uppgifter. Dessutom är det bara behörig personal som har rätt att få åtkomst till patientens

dokumentation och man säger att den inre sekretessen ska upprätthållas genom tekniska lösningar för behörighetstilldelning och åtkomstkontroll [20]. Det krävs att verksamheter vars produkter eller lösningar som behandlar hälsodata är byggt på ett sätt där det tydligt framgår vem som är behörig och vem som har åtkomst till patienternas hälsodata. Allt ansvar ligger hos den personuppgiftsansvarige att säkerställa användarnas rättigheter. Vidare finns även lagen om hälsodataregister som är riktad åt centrala förvaltningsmyndigheter som ger de ytterligare möjligheter att behandla hälsodata [21]. Bland annat för att framställa statistik, utvärdera hälso- och sjukvård samt för att ge grund till forskningsundersökningar.

3.2.2 Hur lagras hälsodata?

Lagring av hälsodata är ett område som digitaliseras fort [22]. Detta har lett till att frågor om hur datan ska lagras har ökat. Samma sorts data kan lagras på flera olika sätt vilket ökar svårigheterna med effektiv lagring och interoperabilitet. En läkares anteckningar kan till exempel lagras som allt från en ”eXtensible Markup Language” (XML)-fil till en handskriven anteckning. Även bilder och videor kan lagras i olika format, exempelvis kan bilder lagras som antingen jpeg eller png. Detta gör datan svår att strukturera och ökar problemen med interoperabilitet.

Anteckningar och textdokument är vanligen enkla att lagra då dessa kan lagras i rad-och kolumndatabaser och dess data kan vanligtvis kartläggas i fördefinierade områden. Sådan data kallas för ”strukturerad data” och är lättförståeligt för både människor och datorer [23]. Det finns också så kallad ”ostrukturerad data”, detta är data som till exempel bilder och email. Dessa kan inte lagras i rader och kolumner vilket gör dem svårare att söka, strukturera och analysera, samt tar vanligen upp större delen av datasystemens storlek.

3.2.3 Vikten av delning av hälsodata för en effektiv och patientsäker vård

Patienter besöker olika vårdenheter som sjukhus eller vårdcentral under sin livstid vilket innebär att patientens hälsodata lagras på flera vårdenheter. Hälsodata är integritetskänslig då den innehåller personuppgifter, som exempelvis personnumer, adress och sjukdomshistoria, och därför är det ytterst viktigt att utbytet av informationen sker effektivt samt att den är tillgänglig för personer som patienten gett samtycke till.

Hälsodata genereras mer och mer under de senaste åren, och med data från professionella hälsosystem och bärbara enheter (smartwatch och mobil) kan man samla ”big data” för att skräddarsy behandling (precisionsmedicin) för varje unik patient [24]. Enligt [25] definieras big data som ”a term for massive data sets having large, more varied and complex structure with the difficulties of storing, analyzing and visualizing for further processes or results”. Att erbjuda varje patient precisionsmedicin är möjligt om sjukhus, den akademiska världen och sjukvård samarbetar

tillsammans och delar hälsodata för att övervinna ”the valley of death” (dödens dal)* (dödens dal) inom translationell forskning [24]. Trots att patienten kan ge samtycke till delning av hälsodata är vanligtvis sjukhus och akademiska sjukhus ovilliga att dela uppgifter med varandra, detta då akademiska sjukhus vill vara de första som publicerar artiklar om data som de arbetar på genom kliniska prövningar [24].

Datadelning kan även resultera forskningsframsteg genom kombinering (data pooling) och analysering av informationen som fås för att kunna förbättra folkhälsan, patientsäkerheten och främja utvecklingen av läkemedel [27]. Allmänhetens förtroende för kliniska prövningar och slutsatser från dem kan ökas vilket gör den kliniska prövningen mer transparent. Utebliven datadelning kan innebära förlust av biomedicinska forskningsmöjligheter vilket skapar oro bland forskare för bland annat datautvinning och omotiverade rättstvister för att skydda konfidentiell affärsinformation [27].

Inom cancervården är även datadelning nödvändig. Grupper av läkare från olika specialiteter bildar ”tumor boards” där de under regelbundna träffar analyserar cancerfall, delar information och i samarbete utvecklar effektiva behandlings- och vårdplaner för varje patient [28]. Enligt forskningsprofessor Jack W. London är delning av data inom cancerforskning den ”heliga graal” för de som arbetar inom cancerbiomedicinsk informatik då det ses som en möjlighet för ett forskningsföretag att effektivisera forskningen och öka upptäcktsgraden [29].

3.2.4 Administrativt stöd för samordning av hälso-IT-insatser

Enligt Regeringens skrivelse 2005/06:139: ”Nationell IT-strategi för vård och omsorg” är IT ett av de viktigaste verktygen för förnyelse och utveckling av vård- och omsorgsverksamheterna [30]. Användning av IT kan stödja förbättring av patientsäkerhet, vårdkvalitet och tillgänglighet. Dagens IT-stöd har begränsningar och brister som följande:

1. Landsting och kommuner använder IT på olika sätt och infrastrukturen är ojämnt utvecklad inom ramen för verksamheter vilket bland annat kan leda till svårigheter med informationsutbyte och med att skicka hälso- och kvalitetsregister

2. Det saknas möjligheter för patienter att få information som rapporterats om sin behandling och de har begränsade möjligheter att enkelt få service och vård med hjälp av elektronisk kommunikation

3.2.5 Hinder för datadelning för en effektiv och patientsäker vård

I den tekniska infrastrukturen inom hälso- och sjukvård finns det utmaningar som problematiserar säker informationsutbyte mellan institutioner, därför är en säker infrastruktur nödvändig. De främsta utmaningarna är relaterade till integritet, säkerhet

*The valley of death, inom biomedicin, är lovande grundforskningsresultat som inte lyckas ingå i kliniska prövningar och får därför inte chansen att utvecklas till terapier för patienter [26].

och interoperabilitet. För det första är hälsodata integritetskänslig och riskeras för dataexponering då data lagras i ett offentligt moln (cloud storage). Sedan använder de nuvarande systemen centraliserad arkitektur som kräver ett centraliserat förtroende. Även frågor och uppgifter som rör effektiv integrering av hälsodata och interoperabilitet mellan system inom hälso- och sjukvården är utmanande [31]. Hinder inom den tekniska infrastrukturen leder till olika begränsningar så som följande:

Säkerhets- och integritetsproblem

Medicinsk identitetsstöld används för att fakturera för eller få tillgång till medicinska tjänster genom patient- eller läkaridentifikationsinformation [32]. Medicinsk identitetsstöld skiljer sig från ekonomisk identitetsstöld där man istället använder personnummer och kreditkortsnummer för bedrägerier. Federal Trade Commission (FTC) uppskattade 3% (ca 250,000 incidenter per år) av identitetsstölder som medicinska. Enligt en annan statistik presenterad av World Privacy Forums (WPF) så är ”gatuvärdet” av ett stulet personnummer 1 amerikansk dollar (USD) till skillnad från ett stulet medicinskt identifieringsnummer som är värt 50 USD.

Brist på förtroende för digital hälsa

Frågor och aspekter inom integritet och dataskydd lyfter fram etiska utmaningar vilka är relaterade till trovärdigheten hos digital hälsa. Digital teknik används mycket inom vården och därför är det viktigt att undersöka bestämningsfaktorerna och hindren för att förlita sig på digital hälsa. Identifiering av faktorer relaterade till förtroende kan underlätta utvecklingen av nya hälsotjänster samt ge svar på patienters behov och förväntningar [33]. Faktorer som undersökts kan även beaktas vid utvärdering av nya och befintliga digitala hälsotjänster.

Brist på interoperabla datastandarder

Syftet med standarder är att olika system ska fungera tillsammans interoperabelt, att de ”förstår varandra”, för att förbättra patientvården. Exempelvis, när en patient förs in på ett amerikanskt sjukhus finns det en standard som inte är standardiserad mellan sjukhus, och varje sjukhus har olika processer vilket kan leda till tidig död hos patienten [34]. Det skapar förvirring då sjukvårdsenheter följer olika standarder [34]. Eftersom kommunikationsmedlen inte är enhetliga eller standardiserade är sökandet efter en hög patientvård och säkerhet meningslöst då standarder är byggda och lagrar data på olika sätt.

3.3 Interoperabilitet inom hälsodata och standarder

Interoperabilitet är viktigt för hälsodata och standarder då det säkerställer att information kan delas mellan olika sjukvårdssystem patientsäkert. Det möjliggör effektivare samspel och kommunikation då vårdpersonal enkelt kan komma åt hälsodata och dela den till olika anläggningar eller leverantörer. Interoperabelt datautbyte

kan leda till analysering av data för forskare och vårdpersonal för att identifiera trender och mönster som kan leda till utvecklandet av nya behandlingar och ökad patientresultat.

3.3.1 Interoperabilitet och dess betydelse inom delning av hälsodata

IEEE definierar interoperabilitet som “the ability to exchange data and to make use of these data within the receiving system” [35]. Enligt The European Interoperability Framework (EIF): ”European Interoperability Framework - Implementation Strategy (Annex 2)” kan interoperabilitet delas in i fyra olika kategorier i form av rättslig, organisatorisk , semantisk och teknisk nivå.

Rättslig nivå

Rättslig nivå av interoperabilitet handlar om säkerställning av samarbetande mellan organisationer under rättsliga ramar, policyer och strategier. För detta kan det krävas att lagstiftningen inte hindrar inrättandet av europeiska offentliga tjänster inom och mellan länder inom EU samt att det finns tydliga överenskommelser vid hur skillnader i gränsöverskridande lagstiftning ska ske [36].

Organisatorisk nivå

Organisatorisk nivå av interoperabilitet är till för offentliga förvaltningar som tillsammans för gemensamma överenskommelser och fördelaktiga mål ska kunna anpassa sina affärsprocesser, ansvar och förväntningar [36]. Det handlar om utbytet av information och anpassning av affärsmodeller och information, eller dokumentation och integration. Genom gemenskapskrav ska tjänster göras tillgängliga, lätt identifierbara och användarfokuserade.

Semantisk nivå

Semantisk nivå av interoperabilitet är till för säkerställning av att utbytt data och information bevaras i sitt exakta format och att mellanparter förstår utbytet [36]. Denna nivå omfattar semantiska och syntaktiska aspekter som följande:

- Den semantiska aspekten avser dataelementets betydelse och förhållandet mellan dem, vilket inkluderar vokabulärer och schemans utveckling för beskrivning av databyte, och säkerställning av att kommunicerade parter förstår dataelementet likaså
- Den syntaktiska aspekten avser beskrivning av information i sin exakta form och att den utbyts i termer av grammatik och format

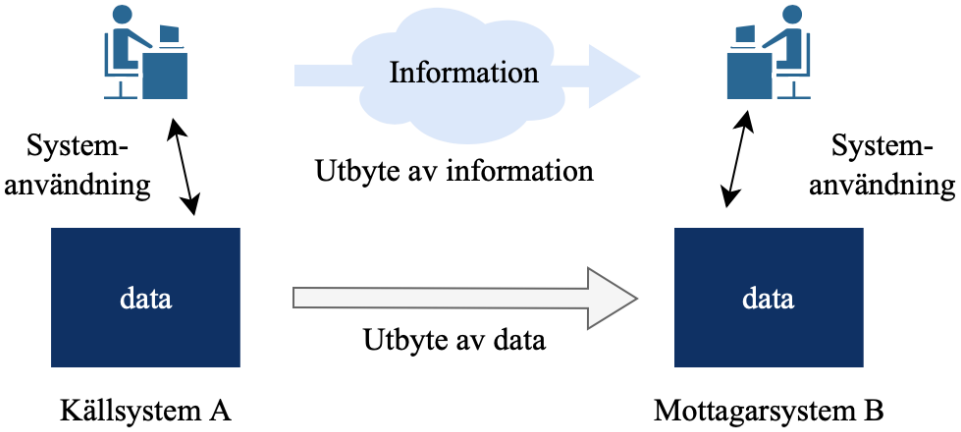
Teknisk nivå

Teknisk nivå av interoperabilitet inkluderar applikationer och infrastruktur som kopplar samman system och tjänster [36]. Det innefattar bland annat specifikationer inom gränssnitt, anslutnings- och dataintegreringstjänster, och datautbyte. Applikationer och informationssystem för offentlig förvaltning har historiskt sett utvecklats underifrån och upp (bottom-up) i ett försök att lösa domänspecifika och lokala problem. Detta resulterar i ”sönderdelade” delar inom informations- och kommunikationsteknik vilka inte är enkla att samarbeta med. Detta skapar hinder för interoperabilitet på teknisk nivå på grund av den offentliga förvaltningens omfattning och den ”sönderdelade” karaktären hos IKT-lösningar.

Genom att uppnå högre nivåer av interoperabilitet, så som juridisk och organisatorisk nivå, kan följande fördelar uppnås:

- Operativ effektivitet kan uppnås med system som är interoperabla, vilket sparar på tid och administrativa uppgifter som exempelvis manuell inmatning av information från fax [37]
- Möjliggör utbytbarhet för konsumenter - de kan ersätta en produkt med en annan tillverkat av ett annat företag vilket betyder större marknadsstorlek, och lägre enhetskostnader och konsumentpriser [38]

En interoperabel datadelning kan illustreras med hjälp av figur 4 nedanför som har översatts till svenska från artikeln [39]. I figuren har systemanvändaren till vänster information som systemanvändaren till höger är i behov av, vilket även är tillgängligt för den. Interoperabilitet uppnås om mottagarsystem och systemanvändarna förstår informationen som utbyts och att de kan använda informationen.



Figur 4: Interoperabel datadelning

3.3.2 EHR - Interoperabilitets påverkan på patientsäkerhet

Interoperabilitet av EHR definieras enligt den Internationella standardiseringsorganisationen (ISO) som “the ability of two or more applications being able to communicate in an effective manner without compromising the content of the transmitted EHR” [40]. ISO/TC 215, internationella organisation för standardiseringens tekniska kommitté för hälsoinformatik (HI), har mål att uppnå interoperabilitet och kompatibilitet mellan sjukvårdssystem som är oberoende. Enligt ISO är utvecklandet av nationella och internationella standarder för EHR-interoperabilitet viktigt för delning av hälsodata mellan personal inom hälso- och sjukvården i en samarbetande miljö, delning av hälsodata mellan organisationer inom företag, regionalt eller nationella hälsosystem [40]. Detta gäller även utanför nationella gränser och framförallt stöd för interoperabilitet mellan programvara från leverantörer.

3.3.3 Översikt av interoperabilitetsstandarder

För interoperabilitet inom hälsovården finns det främst tre olika standarder som används för klinisk och hälsodata; HL7 v2/v3, Clinical Document Architecture (CDA) och HL7 Fast Healthcare Interoperability Resources [41]. Alla dessa är skapade av företaget HL7 och är menade för olika användningsområden.

HL7 v2 är en framstående interoperabilitetsstandard då den har varit i bruk sedan 1987. Det används av stora delar av världen inklusive 95% av sjukvården i USA [42]. Standarden är designad för att skicka olika hälsodata i form av meddelanden skrivna i hierarkiskt format uppdelat i olika element [41]. Varje element har olika attribut som används för att beskriva dessa effektivare som bland annat längd av elementet, vilken sorts data attributet består av och om elementet behöver ett giltigt värde för att meddelandet ska kunna skickas. HL7 v3 är en standard vars mål är att vara allomfattande och kunna användas av alla olika sjukvårdssystem. V3 är baserat på en egen metodik ”Message Development Framework” (MDF), som senare utvecklades till ”HL7 Development Framework” (HDF). Då v2 systemet redan användes av stora delar i världen när v3 kom ut på marknaden, ersattes det inte av v3 vilket var förhoppningen, utan det används mer i nya områden som inte redan täcks av v2.

CDA är till skillnad från HL7 v2 och v3 en standard som specificerar strukturen av kliniska dokument. Målet är att alla sorters kliniska dokument ska implementeras och vara läsbart både av dator samt människa [41]. Detta sker genom att använda det strukturerade märkspråket XML. XML är användbart då det är lätt att använda och kan innefatta semantik vilket behövs då alla kliniska dokument inte är skrivna utifrån strukturerade format, till exempel anteckningar från en läkare [43]. Ett CDA dokument är uppbyggt av en rubrik och dokumentets kropp. Kroppen består av text i till exempel PDF eller Rich Text Format medans rubriken innehåller dokumentets metadata och dokumentinformation. Detta kan vara till exempel dokumentets författare och vilken patient som dokumentet innefattar [41]. Markeringar inom XML-dokument gör att en dator kan extrahera information från dokumentet medans det fortfarande är läsbart för en människa.

FHIR är en standard som är baserad på HL7 v2 men med ett större fokus på tillägg och den så kallade ”80/20 regeln” [41]. Detta betyder att FHIR ska täcka 80 % av dess användningsområden och de resterande 20 % ska kunna läggas till som tillägg. FHIR byggs främst upp av ”resurser” vilket kan representeras av filtyper som XML och JSON. Ett exempel på en resurs kan vara en patientresurs där kopplat till resursen är namn, kontaktinformation och anhöriga [44]. En uppsättning kategoriserade fördefinerade resurer ges av FHIR. Varje FHIR-resurs har olika attribut som antingen är referenser till andra resurser, baser för flera attribut eller är direkt olika datatyper. Vissa attribut kan vara flera olika datatyper. FHIR är en hierarkisk standard där alla element utgår från ett ”rotelement” som är designade för att tillåta tillägg.

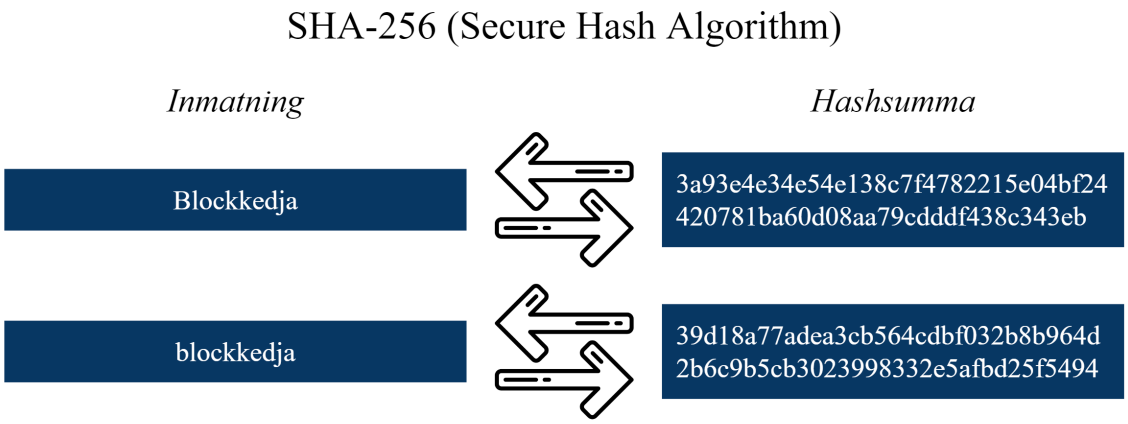
OpenEHR (uttalat ”OpenAir”) är en standard utvecklad av företaget med samma namn designad för förvaring av hälsodata [45]. OpenEHR förvarar hälsodata i ett personcentrerat hälsosystem med lite fokus på datautbyte då andra standarder som HL7 fokuserar på det. Standarden är baserad på fyra olika delar; ”Referensmodeller”, ”Archetype” formalismer, ett ”Query Language” för archetypes och APIs. Genom att använda referensmodeller och archetype formalismen kan archetypes och ”templates” utvecklas som modeller för klinisk data. Query språket används för att utveckla ”queries” som kan be om information från ”archetypes” istället för att ta det från fysisk hälsodata. OpenEHRs APIs används för att få tillgång till de flesta funktioner inom standarden.

3.4 Översikt av blockkedja

Som tidigare beskrivet så finns det många komplexa problem och krav kring delning av hälsodata inom Sverige. Lösningen till detta är fortfarande ett aktivt forskningsområde och en potentiell lösning vi skall diskutera är blockkedja. Blockkedjor erhåller gynnsamma egenskaper så som decentralisering av information för säkrare förvaring och delning samt autonomi över informationen i anslutning till befintlig lag [46]. Detta tack vare faktumet att blockkedja tillåter en att bedriva en manipuleringssäker och oföränderlig kontinuitet av transaktioner över ett distribuerat nätverk med hjälp av kryptografi.

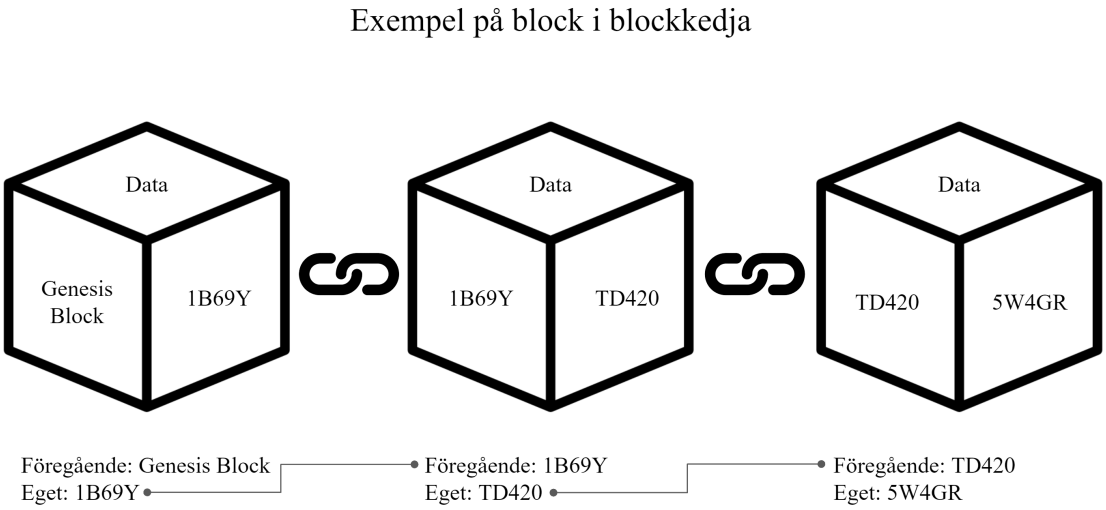
3.4.1 Struktur av blockkedja

I en blockkedja förvaras information i form av data i en transaktion [47]. Information om transaktioner är bevarad i så kallade ”block” och dessa block är kopplade kedjevis i en ”kedja”, därmed namnet blockkedja. Information om vem som har haft åtkomst eller ändrat information förvaras också i blocket bland transaktionerna. Innehållet i ett block är krypterat med hjälp av en hashfunktion. En hashfunktion kan ta original information och representera det i ett unikt krypterat men standariserat format som sedan kan återvandlas tillbaka till originalet. I figur 5 nedan kan vi se exempel på en hashfunktion där den tar en inmatning och omvandlar det till en hashsumma. Hashsumman kan då omvandlas tillbaka till ursprungliga inmatningen.



Figur 5: Exempel på hashfunktionen SHA-256. Notera hur minsta ändring ger fullständigt olika hashsummor

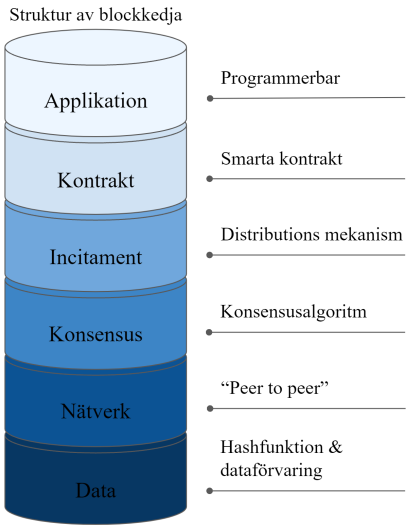
Varje block består av tre delar. Det har sin data i form av tidstämplade transaktioner, sitt egna unika digitala fingeravtryck i form av en hashsumma som representerar innehållet i blocket och slutligen hashsumman av föregående blocket som kedjar dem ihop. Detta gäller för alla block förutom det första som kallas för ett genesis block då det inte har ett tidigare block att kedja till som vi kan se i figur 6 nedan.



Figur 6: Exempel på hur en rudimentär blockkedja skulle kunna se ut

I och med att dessa block är kedjade ihop med hjälp av hashsummor lämpar det sig att vara en manipuleringssäker metod för att förvara information. Då hashfunktions egenskapen förhindrar insättning av ett nytt block i mitten av en kedja eller ändring av ett befintligt block utan att fullständigt förändra hashsumman av blocket och bryta kedjan. Blockkedja har många parametrar som kan justeras för att anpassa den för många olika användningsområden och säkerhetskrav. Strukturen av en blockkedja kan delas upp i sex olika lager som visas i figur 7 nedan [46].

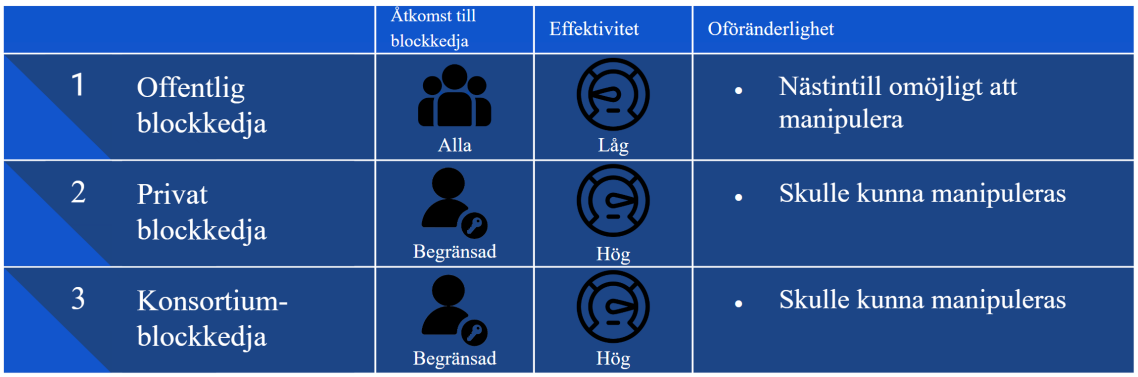
Applikationen utgör den programmerbara delen som användare interagerar med. Med hjälp av smarta kontrakt, kod som befinner sig på blockkedjan, kan man låta blockkedja utföra autonoma och oföränderliga instruktioner som möjliggör olika funktioner att utföras säkert. Med val av olika distributionsmekanismer kan man ge incitament för användare att adoptera systemet. Med hjälp av konsensusalgoritmer kan man nå en konsensus i ett distribuerat miljö. Kommunikation mellan olika partier möjliggörs av ett ”Peer-to-Peer” (P2P) nätverk där datorer agerar som noder i ett icke-hierarkiskt nät. Slutligen utgörs basen av data och hur man krypterar den med hjälp av hashfunktioner samt hur man förvarar den. Utifrån strukturen ovan är det huvudsakligen fyra parametrar man skall ha i åtanke när man designar en blockkedja. Dessa parametrar kan beskrivas med hjälp av fyra koncept val av delad liggare, konsensusalgoritmer, dataförvaring och smarta kontrakt.



Figur 7: Struktur av blockkedja visualiserat i rangordning från det ytligaste till det mest grundliga lagret [46]

3.4.2 Delad liggare - hur och vem har tillgång till blockkedja

En delad liggare är ett digitalt system för att registrera transaktioner över ett flertal separerade noder i ett nätverk där flera transaktioner kan hända i olika noder samtidigt. Inom blockkedja använder delade liggare ett P2P datornätverk och diverse konsensusalgoritmer för att kunna dela med sig av identisk information mellan alla noder inom ett nätverk på ett koordinerat och icke-konfliktväckande sätt. Detta tillåter för decentraliserad delning av information där man inte har en central auktoritet som kan leda till ”Single Point Of Failure” (SPOF), vilket är en stor fördel jämfört med traditionella centraliserade system [48]. Ett kliniskt exempel på en SPOF är när ett nödvändigt dokument ligger på en central databas i ett sjukhus och vid fallet att tillgång till det äventyras vid exempelvis olycka eller misstag är det svårare att få tag på för andra. Om det hade varit på ett decentraliserat system hade det varit lika lätt för alla sjukhus med rättigheter att ha åtkomst till det, samt en större grad av redundans vid fall av massiv fallering av systemet.



Figur 8: Jämförelse mellan olika modeller av delade liggare [46]

I figur 8 ovan går det se att det finns tre huvudsakliga paradigmer för blockkedja. Dessa är offentliga liggare, privata liggare och konsortiumliggare som används i respektive typ av blockkedja [49].

Offentliga blockkedjor

Offentliga blockkedjor använder sig av en offentlig liggare, detta innebär att alla deltagare i nätverket kan se informationen på kedjan samt kan delta i dess acceptering av ny information och modifiering [49]. Inom sjukvård kan denna sortens blockkedja vara svår att implementera då man arbetar för det mesta med känslig och privat data. Det kan vara komplikationer med att göra data fullständigt privat utan att obehöriga kan extrahera detaljer på en offentlig blockkedja. En risk är att yttre aktörer utanför sjukvården blandar sig in i blockkedjan och om det blir tillräckligt många kan de påtvinga oönskade ändringar i form av en 51% attack då man har nästintill fri kontroll över blockkedjan [50]. Denna blockkedja är fullständigt decentraliserad i sin natur och låter användare interagera med den genom en tillståndslös modell. De två huvudsakliga exemplen på offentliga blockkedjor är Bitcoin [51] och Ethereum [52] som används för det mesta inom finanssektorn och är så anpassningsbara till en sjukvårdsmiljö.

Privata blockkedjor

Trots att blockkedja oftast används för att undvika centralisering kan det finnas värde i att ha någon sorts form av central auktoritet som överser vem som kan ha tillgång till en blockkedja. Privata blockkedjor är baserade på en privat liggare vilket innebär begränsad tillkomst till att visa och ändra på information [49]. En central auktoritet bestämmer vem som får se och göra ändringar. Dessutom går acceptering av förändringar genom en auktoriserad grupp noder utvald av den centrala auktoriteten. Privata blockkedjor kan exempelvis låta en patient personligen överse sin blockkedja och ändringar som görs på den. En privat blockkedja går lättare att göra ändringar på, till och med ta bort något. Privata blockkedjor låter en ha positiva kvalitéer så

som transparens och spårbarhet samtidigt som man får bättre kontroll över vem som har tillgång till innehållet.

Konsortium-blockkedjor

En form av medelväg erbjuds av konsortium-blockkedja där man kan välja om informationen skall vara tillgänglig för alla att se eller inte, men ändringar och acceptering av ändringar lämnas till bestämda grupper eller agenter [49]. Detta kan vara passande i en miljö där ett flertal behöver se och ha tillgång till kritisk information men endast pålitliga aktörer så som läkare och patienter har tillgång till att göra ändringar av blockkedjan. Förmågan att ändra på blockkedjan fördelas mellan utvalda auktoriteter för att uppnå bättre kollektiva val med mindre bias.

3.4.3 Konsensusalgoritmer - en lösning till frågan om hur man kommer överens

Utifrån vilken liggare man väljer uppstår problemet om hur man skall acceptera förändringar i ett decentraliserat och autonomt system såsom blockkedja. Generellt stöter man på två problem när man försöker acceptera ny information till blockkedjan, dessa två problem är ”Byzantine Generals Problem” (BGP) och problemet med dubbel spendering. Konsensusalgoritmer kan hjälpa en att undvika felaktiga dubbla transaktioner som kan störa validiteten och finaliteten av liggaren [53].

BGP kan förenklat beskrivas genom att granska en hypotetisk Byzantinsk armé, där ett flertal generaler har omringat en stad och skall komma överens om en gemensam stridsplan med hjälp av meddelanden [54]. Problemet är då att bland generalerna finns det en eller flera förrädare som vill sabotera attacken genom att sprida falska meddelanden. Vid fallet att man använder oförfalskbara skrivna meddelanden är problemet lösbart för vilket nummer av lojala generaler eller förrädare som helst. Det finns flera förhållningssätt till att lösa detta problem och uppnå en konsensus i en blockkedja som alla har olika fördelar och nackdelar. Lösningar till BGP finns då i algoritmisk form och kallas för konsensusalgoritmer. Dessa algoritmer används för att säkert acceptera ny information på en blockkedja. Konsensusalgoritmer som kan lösa BGP problemet är så kallade ”Byzantine Fault Tolerance” (BFT) algoritmer och är passande i opålitliga miljöer där man kan ha illvilliga noder [55]. Det finns också konsensusalgoritmer som inte uppnår BFT men ändå kan nå konsensus under förhållandena att det inte finns illvilliga noder i nätverket och att åtminstone hälften av noderna är tillgängliga, i detta fall är det kallat ”Crash Fault Tolerance” (CFT).

Det finns många olika algoritmer och lösningar för att nå konsensus. De två främsta sorterna av konsensusalgoritmer är lotteribaserade som används av den största blockkedjan, Bitcoin, i form av ”proof-of-work” och röstbaserade algoritmer exempelvis ”proof-of-stake” som nu används i Ethereum [56]. Proof-of-work är resurskrävande och används mest i samband med incitament-mekanismer som att ge kryptovaluta

i gengäld för att man utför arbete i form av matematiska beräkningar kallat ”mining”. Utifrån ett kliniskt perspektiv finns det möjlighet att ha en kryptovaluta som incitament för adaption och användning av ett system men detta kan leda till etiska komplikationer och friktion i systemet vilket kan göra det långsammare i en miljö där sekunder kan räknas. Generellt används dessa konsensusalgoritmer i fullständigt opålitliga miljöer som i offentliga blockkedjor. Lotteribaserade konsensusmekanismer kan erbjuda bättre skalbarhet för större system där det är en nod som blir utsedd ”vinnare” för att överföra informationen om det nya blocket till resten av nätverket. Detta kan dock leda till att man stöter på två vinnare samtidigt och att blocket går igenom en ”fork” och delas i två. Detta måste då lösas vilket gör att det tar längre tid att nå finalitet, blockkedjans slutgiltiga tillstånd. Till skillnad från lotteribaserade når röstbaserade konsensusalgoritmer finalitet snabbare, men detta till en kostnad av skalbarhet. Ju mer noder man har i ett nätverk desto mer data måste skickas runt för att den skall valideras av alla noder. Man måste därför oftast välja mellan hastighet och skalbarhet.

Det finns många konsensusalgoritmer att välja på utifrån de behov man har av en blockkedja. Det finns algoritmer för att praktiskt besvara på BGP exempelvis i form av ”Practical Byzantine Fault Tolerance” (PBFT) som inte kräver lika mycket komputationella resurser som proof-of-work [57]. Andra blockkedjor som vill undvika datadelning vid verifiering av konsensus för att maximera prestanda kan använda sig av exempelvis ”proof-of-authority” där ens förmåga att uppdatera en blockkedja är bunden till verifierade identiteter med godtycklig auktoritet [58]. Konsensusalgoritmer behöver inte endast verifiera ändringar gjorda av människor utan kan också användas för att verifiera ändringar som skickas in av sensorer, exempelvis signaler från medicinska sensorer, vilket kan användas för att monitorera data spårbart och säkert [59]. Olika konsensusalgoritmer passar olika situationer och därför kan det vara värt att kombinera flera olika konsensusalgoritmer för att skapa en hybrid konsensusalgoritm [60]. En skräddarsydd hybrid konsensusalgoritm kan erbjuda en mer heltäckande lösning i en blockkedja.

3.4.4 Lagring av information ”on eller off-chain”

Även om information kan förvaras direkt på blockkedjan, så kallat ”on-chain”, är det inte alltid passande att göra det då det är varken tekniskt eller finansiellt praktiskt i många fall [61]. Det kan försämra effektiviteten och prestanda av en blockkedja. Istället kan det vara bättre att förvara information så kallat ”off-chain” där man förvarar huvudelen av informationen i ett separat system med pekare till önskad information på blockkedjan. På så sätt kan man minimera kostnader och maximera prestanda genom att förvara så lite information som möjligt på blockkedjan. Fördelarna med blockkedja kan också appliceras till off-chain beroende på val av förvaringmetod. Genom att använda ”Distributed Hash Tables” kan man bevara de positiva egenskaperna av blockkedja även vid off-chain förvaring.

En relevant teknologi till off-chain förvaring av information inom sjukvård är ”Inter-

Planitary File System" (IPFS) [62]. IPFS är från grunden ett protokoll designat för att decentraliserat förvara versionerad fildata. När en fil läggs till i IPFS delas den upp i krypterade 256 kb-paket och sprids ut på ett flertal noder inom IPFS-systemet. IPFS returnerar också ett "Content ID" (CID) i form av en hashsumma som man sedan kan använda för att hämta filen. IPFS har då liknande egenskaper till blockkedja i att den är motståndskraftig till SPOF-attacker tack vare sin decentraliserade natur och att den enkelt detekterar förändringar i filer då CID är baserat på hashfunktioner och minsta ändring ändrar CID fullständigt.

3.4.5 Smarta kontrakt för smartare lösningar

Smarta kontrakt är i grunden kod som är inbyggd i blockkedjan som tillåter en att autonomt utföra funktioner när vissa kriterium är bemötta [63]. Detta låter en utföra kontrakt eller andra operationer utan att ett tredje parti inblandas. Smarta kontrakt kan användas för att säkert och privat utföra kod, exempelvis vid monitorering av en patients vitala signaler från bärbara sensorer. Smarta kontrakt är passande då det möjliggör för mätsensorer att skicka data direkt till blockkedjan [64]. Ytterligare har smarta kontrakt funktionella interoperabilitetsförmågor och kan integreras med olika tekniska system. Smarta kontrakt låter en ha bättre kontroll över hur data förvaras på blockkedjan i och med att kod automatiskt utförs när förbestämda kriterium möts. Exempelvis förmågan att enkelt ange livslängd på vad som skall förvaras på en blockkedja. Det finns en stor potential till vad smarta kontrakt kan göra som frigör en från behovet att ha ett tredje parti som utför känsliga operationer.

3.4.6 Befintliga blockkedjors designer och egenskaper

Bitcoin

Bitcoin är en blockkedja som är kopplad till kryptovalutan med samma namn. Det skapades 2009 för att vara ett alternativ till traditionella valutor [51]. Blockkedjan är proof-of-work där varje nytt block skapar en ny bitcoin som delas upp baserat på arbetet som olika användare utfört för att skapa det. Användardata skyddas genom att de offentliga nycklarna hålls hemliga medan resten av blockkedjan är öppen.

Ethereum

Ethereum är likt Bitcoin i och med att det är en blockkedja som i början av sitt liv använde proof-of-work för att legitimera nya noder och är direkt kopplad till en kryptovaluta med samma namn [52]. Detta har senare i 2022 bytts ut mot proof-of-stake efter att Ethereums energiförbrukning ökade [65]. En annan skillnad mellan Bitcoin och Ethereum är Ethereums implementation av smarta kontrakt i sin algoritm. Smarta kontrakt tillåter att användare kör program på blockkedjan och kan lagra samt hämta information på denna.

Hyperledger

Hyperledger är till skillnad från Ethereum och Bitcoin en blockkedja som inte är baserad på en kryptovaluta [66]. Detta gör att den är användbar för forskning och projekt där man vill undvika att ha en kryptovaluta kopplad till ens projekt. Det finns flera olika Hyperledger projekt med olika användningsområden. Dessa projekt kan ha olika konsensusmekanismer, programmeringsspråk, öppenhet och mer. Bland dessa finns till exempel Hyperledger Fabric, Sawtooth, Ursa och Aries som alla fokuserar på olika användningsområden.

FHIRChain

En prototyp på en blockkedja för EHR är så kallade FHIRChain där konsensusmekansimen ”proof-of-FHIR” testades [67]. För att göra detta användes ett privat Ethereum-testnät och tre separata smarta kontrakt. För att verifiera användare användes så kallade ”digital health identities”. DAppen kunde notifiera användare vid händelser och hade en konsensusmekanism som var baserad på om block hade en korrekt FHIR-standard.

HealthChain

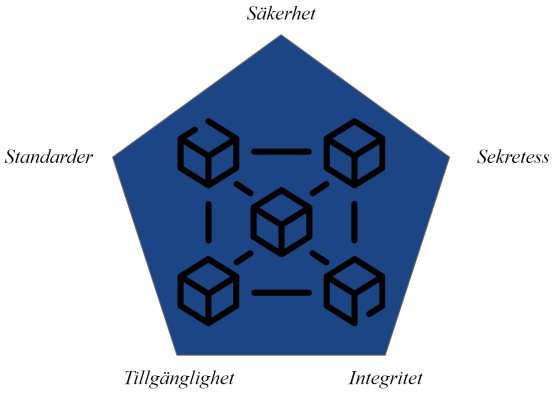
HealthChain är en annan prototyp för att lagra hälsodata på en blockedja. Blockkedjan som användes är Hyperledger Fabric och konsensusmekanismen var den så kallade BFT [68]. Detta gjorde den säker för patientens hälsodata genom att verifiera vad patienten vill dela innan datan laddas upp på blockkedjan.

4 Resultat

I detta kapitel diskuteras det potentiella strukturella upplägg och användningsområden för en DApp inom den svenska sjukvården. Vilka krav som kommer behövas bemötas av den kommer detaljeras och hur en DApp kan potentiellt uppfylla dem. Grundläggande riktlinjer för hur man skulle potentiellt kunna utveckla en DApp och vilka teknologier som är tillgängliga för användning kommer också att beskrivas.

4.1 Krav

Utifrån det som tagits upp i inledningen och teorin går det att framställa krav som måste uppnås för att facilitera ett säkert och interoperabelt utbyte av hälsodata inom den svenska sjukvården. Dessa krav kan beskrivas med hjälp av fem hörnstenar som ligger till grund för de problem som den svenska sjukvården ställs inför. De fem hörnstenarna utgörs av säkerhet, sekretess, integritet, tillgänglighet och standarder, se figur 9 nedan. Ett system som byggs med dessa fem hörnstenar i åtanke har grunden för att uppfylla behoven av den moderna svenska sjukvården. I dagens sjukvård är det tydligt att det ännu inte finns en heltäckande lösning. Den svenska sjukvården fallerar oftast på en eller flera av dessa hörnstenar i olika delar av landet. I många fall används en kombination av olika lösningar, oftast med dålig interoperabilitet vilket leder till ökad komplexitet av problemet men också behovet på en lösning.



Figur 9: De fem hörnstenarna

4.2 Blockkedja som lösning

Blockkedjeteknologi är en potentiell lösning då den besitter önskvärda egenskaper i sin natur som möjliggör decentraliserad förvaring och distribution av många olika sorters data. Blockkedjans decentraliserade natur bidrar till dess säkerhet. Det låter den undvik svagheter av traditionella lagringsmetoder såsom centraliserade databaser eller servrar, som är båda sårbara till dataintrång och attacker. Hälsodata kan lagras distribuerat på en blockkedja där varje nod i ett nätverk har en kopia av blockkedjan.

Detta gör det svårare för angripare att manipulera eller ändra på data samt ökar tillgängligheten för auktoriserad personal som är i behov av datan då det eliminerar öde öar av information.

Blockkedja i sin natur är transparent och möjliggör enkel spårbarhet av förändringar och hantering av data genom att jämföra hashsummor. Detta underlättar verifikation att datahantering sker enligt befintliga regelverk såsom GDPR, för att uppehålla datans integritet. Det som möjliggör detta är blockkedjors rötter inom kryptografi vilket tillåter för säker förvaring och delning av data med ytterst sekretess. Krypterad data kan förvaras med begränsad åtkomst av endast auktoriserad personal och med hjälp av privata eller konsortium blockkedjor.

Blockkedja är inte endast ett sätt att förvara data på, då en mängd olika funktionaliteter kan möjliggöras med hjälp av smarta kontrakt. Kod som kan användas för att ge patienten kontroll över sin egen hälsodata samt hur, när och vem data delas med. Smarta kontrakt kan också användas för att göra blockkedjan anpassningsbar till många olika standarder för ökad interoperabilitet. Möjliga fall är att viss data har begränsad livscykel och tas bort efter en viss tid. Dessutom kan det låta blockkedjan autonomt ta emot och förvara signaldata från externa enheter och sensorer med exempelvis känslig data om en patients välmående.

4.3 Teoretisk struktur

Kraven som var detaljerade tidigare utgörs av behoven från flera olika aktörer inom den svenska sjukvården. Från patienter vars hela data är kritisk för sjukhus och kliniker för att kunna låta vårdpersonal i form av läkare och sjuksköterskor erbjuda effektiv vård till forskare och myndigheter som inte behöver alla detaljer för att kunna utföra sitt jobb. Olika aktörer har olika behov av hur mycket av en patients data de behöver tillgång till. En patient bör själv ha tillgång till hela sin egna data samt kontroll över vem den delas med. Till skillnad kan lägre tillgångsnivåer behövas av andra aktörer, exempelvis forskare som kan nöja sig med anonymiserad data. Det är då viktigt att ha möjligheten att kontrollera vem som har tillgång till blockkedjan därför är det passande att använda antingen privata eller konsortium-blockkedjor. Inom sjukvård är tid en kritisk resurs, mer i vissa områden än andra. Exempelvis inom den prehospitala vården i fallet av att man har en patient i ambulans kan sekunder räknas och då är det nödvändigt med låg latens på dataöverföring. Val av konsensusalgoritm som når finalitet snabbt är då kritisk exempelvis proof-of-authority, oftast är det på bekostnad av att man inte har BFT utan får nöja sig med CFT. Dock för förvaring av information i en hospital miljö kan BFT med hjälp av exempelvis PBFT vara önskat för ökad säkerhet trots att konsensusalgoritmer som uppfyller det oftast inte når finalitet snabbast. Potential för hybrid konsensusalgoritmer finns för att ge det bästa prestanda för många olika situationer.

För smidig användning av en blockkedja är det tydligt att bra prestanda är kritisk. Idag är många konsensusalgoritmer baserade på att man röstar fram rätt version

efter att data har delats med tillräckligt många noder. En flaskhals bildas i hur mycket data som kan delas och till hur många noder. Därför är det fördelaktigt att lagra en del av datan off-chain för att avlasta blockkedjan, vilket kan göras på exempelvis IPFS. Blockkedjas decentraliserade natur skapar en datakonflikt med existerande regelverk som GDPR. Detta beror på att strukturen som blockkedja är baserad på gör den svår att anpassa efter vissa behov. Det finns därför utrymme för reformer hos regelverk för att lösa denna konflikt. Den kan också lösas genom att utnyttja intelligent användning av smarta kontrakt. Smarta kontrakt låter blockkedja ha stor potential för flexibilitet och skapar möjligheten att samverka med många olika typer av standarder. Smarta kontrakt möjliggör för autonom hantering av data enligt regelverk. Samtidigt möjliggörs säker och spårbar insamling av sensordata inom prehospital sjukvård som lagras på blockkedjan. Nedan sammanställs resultatet i en punktlista på riktlinjer som kan användas som utgångspunkt för utveckling av en DApp.

- Privat blockkedja i form av Hyperledger Fabric
- Skräddarsydd hybrid konsensusalgoritm
- Off-chain lagring med hjälp av IPFS
- Smarta kontrakt för praktisk funktionalitet och koppling till sensorer

5 Diskussion

I detta kapitel diskuteras val av metod, det som tidigare lyfts i teori och resultat, och hur studien har besvarat frågeställningarna, anknytning till tidigare forskning och studier.

5.1 Metoddiskussion

Kandidatarbetet har främst varit baserad på att utföra en litteraturstudie, vilket har både sina för- och nackdelar. Metoden är effektiv då den ger en förståelse för befintlig kunskap, men beroende på ämnesområde kan man behöva inkludera ny information som är aktuell. Arbetet kunde delvis ha genomförts som en intervju- eller enkätstudie för att få en inblick i de problem. Exempelvis problem inom delning av hälsodata som personal inom sjukvården upplever där man hade kunnat få möjligheten till att ställa följdfrågor och fördjupa sig inom ämnet.

Initialt valdes ämnet datadelning inom sjukvården, men det är väldigt brett då flera landsting har olika infrastruktur. En generalisering skulle vara alldeles för komplicerad. Beslut om att byta ämnet till datadelning inom prehospital vård togs av författarna efter diskussion med handledare.

5.2 Resultatdiskussion

Vi hade två frågeställningar inför arbetet, det ena handlar om att bestämma en struktur för en blockkedja som skulle användas för att stödja säkert och interoperabelt utbyte av hälsodata inom svensk sjukvård. Det vi kom fram till i resultat var att det är effektivare att använda Hyperledger istället för att programmera en egen blockkedja. Anledning för detta är att Hyperledger redan är en etablerad blockkedja som är både lättanvänd och att dess egenskaper stämmer överens med den struktur vi kom fram till i resultat.

Användningen av en privat blockkedja var användbar för att skydda hälsodata genom att begränsa åtkomst till information till endast de användare med auktoritet, som nämns i 3.4.2. Den förbättrade möjligheten att göra ändringar på blockkedja är också nödvändig då hälsodata ska kunna raderas eller ändras uteefter behandling och användares vilja. Att använda Hyperledger gör också att vi undviker energiproblemen som kommer med proof-of-work samt kan undvika det monetära incitamentet som behövs för proof-of-stake. Som nämns i 3.4.4 är metoden att lagra IPFS-länkar på blockkedjan en lösning för hur man lagrar större data på blockedjan. Detta lägger dock till en ny bristpunkt då man behöver tillförlita sig på ett extra system istället för att bara använda blockkedjan.

FHIR-standardens användning för delning och lagring av data är fördelaktig då ett blockkedjebaserat system behöver fungera för många olika system och användas till flera olika användningsområden. 80/20-regeln gör att FHIR överträffar andra

standarder då resurser som behövs av specifika system inte behöver belasta alla system som använder blockkedjan utan bara dem som behöver använda samma resurser.

Vårt POC visar på en rudimentär metod för hur hälsodata kan lagras på blockkedjan för ökad patientsäkerhet. Vidareutveckling av den skulle kunna inkludera koppling till en extern sensor för att automatiskt omvandla sensordata till FHIR-format och ladda upp det på blockkedjan så som nämns i 3.4.5

5.3 Etiska och sociala aspekter

De etiska och sociala aspekterna av datadelning inom sjukvården är viktiga att ta hänsyn till. Delning av hälsodata kan leda till mer effektiva behandlingar och även framsteg, utveckling och forskning inom den medicinska världen. Tillgänglighet av data kan leda till fler kliniska prövningar och bättre resultat för patienter, och en övergripande förbättring av sjukvården.

Hälsodata rör frågor kring integritet och säkerhet. Tanken av att det kan finnas risk att obehörig part får tillgång till personlig information eller att denna används i skadlig eller utnyttjande syften är oroväckande för en patient. Därför kan en patient vara obekväm med att ge samtycke och dela sin personliga hälsodata. Potentiell diskriminering eller förvärring av befintliga ojämlikheter inom sjukvården kan även uppkomma.

Generellt sett är det viktigt att hitta en balans mellan delning av hälsodata och dess fördelar, och behovet av att skydda patienters integritet och säkerhet. Genom robusta dataskyddspolicyer och kommunikation med patienter kan förklaring ges om hur övervakning och utvärdering sker så att patienten känner sig säker och för att säkerställa att datadelningen sker på ett etiskt och socialt sätt.

Tekniken som blockkedja är baserad på står i direkt konflikt med flera av bestämmelserna i GDPR, till exempel användarens rätt till radering eller ändring av information. Detta beror på att all data som är sparad på blockkedjan spelar en särskild roll i att bevara systemets kryptografiska egenskaper. Det är dock uppmärksammat att blockkedjor har flera fördelar för att uppfylla målen i GDPR som till exempel dess robusta kryptering och dess generella transparens. Blockkedjeindustrin utvecklas mycket snabbt, och det skapas ständigt nya produkter och lösningar som gör att regelverken kan ha svårt att hänga med. Det är därför viktigt att regelverken satsar på att utbilda sig om blockkedjor och skapar en bred uppfattning om industrin. Först då kan de skapa riktlinjer som både skyddar patienten men som även tillåter innovation och utveckling bland företagen. Generellt kan vi se att många av produkterna anpassar sig efter de lagar och regulationer som finns idag vilket är särskilt vanligt inom sjukvårdsindustrin som ofta har innovativa lösningar för att förhålla sig till GDPR.

Vidare kan blockkedjor vara ett sätt för patienter att få möjligheten att äga och kontrollera sin egen data till skillnad från dagens sjukvårdssystem där vårdgivare kontrollerar all data. När en blockkedja distribueras decentraliserat kan makten och ägandet av datan bäras kollektivt vilket kan vara stärkande för demokratin i ett samhälle. Huruvida blockkedjedatan bör ägas av vårdsystemen eller ägas kollektivt mellan patienter varierar beroende på vad man prioriterar som samhälle. Det viktiga är att vårdsystemen är fullständigt transparenta med hur datan lagras och delas för att garantera patientsäkerhet. Det här leder till en ökad tillit bland patienter till att datan hanteras säkert vilket återigen kan höja intresset bland patienter att dela med sig av sin hälsodata för bedrivande av kliniska studier och för att skapa en förbättrad sjukvård.

5.4 Framtida utveckling

Blockkedjeteknologin utvecklas ständigt men trots det finns det stora utrymmen för förbättring. Smarta kontrakt spelar en stor roll i effektiviseringen av framtidens sjukvårdsprocess eftersom det frigör administrativa arbeten som annars hade existerat. En viktig uppgift smarta kontrakt kan utföra i framtiden är att automatiskt larma till ambulanssjukvården när en sensor detekterar ett patientfall vid hemmonitorering. I framtiden skulle smarta kontrakt kunna automatisera flera processer på samma sätt men som sker manuellt i vårdkedjan idag. Till exempel kan smarta kontrakt uppdatera en patientjournal automatiskt efter att ett nytt labbsvar erhållits. Det administrativa arbetet bakom kliniska studier underlättas också av smarta kontrakt och blockkedjor. Detta beror på att en stor del av arbetet vanligtvis är att hitta rätt urval av patienter som uppfyller studiens krav. Med blockkedjor kan man smidigt sortera fram de patienter som uppfyller studiens krav utifrån till exempel ålder, sjukdom och kön. Sveriges befolkning visar dessutom en större tillit till sjukvården och villighet att dela hälsodata jämfört med andra EU-länder. Det betyder att implementeringen av blockkedjeteknologi i sjukvården och möjligheterna som följer med detta blir ännu fler i Sverige än i andra länder.

Blockkedja har goda framtidsprospekt då teknologin är ny och utvecklas snabbt. Problemet med datalagring off-chain kan minskas då teknologin för lagring på den förbättras. I framtiden kan system som IPFS inte behövas användas utan all medicinsk data lagras direkt på blockkedjan vilket minskar risken för attacker. Förbättrade konsensusmekanismer skulle också kunna utvecklas vilket skulle kunna direkt använda FHIR eller andra standarder för att uppdatera blockkedjan som nämns i 3.4.6. Något som vi inte kommer ta upp så mycket om är kvantdatorers påverkan på blockkedja då dessa i teorin skulle kunna lösa all kryptering som nuvarande blockkedjor använder. För att lösa detta skulle en kvantdatorsäker krypteringsmetod behövas.

6 Slutsats

I detta arbete har användningen av blockkedjeteknologin inom den prehospitala vården i Sverige undersökts. Vi har analyserat olika teknologier och regelverk som berör ämnet och diskuterat deras möjliga inverkan på hälso- och sjukvårdssektorn i Sverige.

Blockkedjeteknologin har potential att förändra den prehospitala vården på flera sätt, bland annat genom att förbättra hälsodatalagring, säkerhet, interoperabilitet, kommunikation och samarbete mellan vårdgivare. Genom att använda en decentraliserad och säker databas kan blockkedjtekniken bidra till att minska risken för dataintrång och förlust av känslig patientinformation.

En av dem mest lovande tillämpningarna av blockkedja inom den prehospitala vården är spårbarheten av patientjournaler. Genom att lagra journaler i en blockkedja kan vårdgivare snabbt och säkert dela information om patientens medicinska historia, vilket kan leda till en mer effektiv och säker vård.

Det finns dock utmaningar som måste övervinnas för att blockkedjeteknologin ska bli allmänt accepterad och implementerad i den prehospitala vården i Sverige. Dessa utmaningar inkluderar brist på standardisering, integritets- och säkerhetsfrågor samt juridiska och regulatoriska hinder. För att övervinna dessa utmaningar krävs samarbete mellan olika aktörer, såsom vårdgivare, teknikleverantörer, myndigheter och patienter.

Slutligen är det viktigt att notera att blockkedjeteknologin inte är en universallösning för alla problem inom den prehospitala vården, men den har potential att bidra till förbättringar inom vissa områden. För att säkerställa en framgångsrik implementering och utnyttjande av denna teknologi bör det finnas en ständig dialog och utvärdering mellan alla involverade parter. Framtida forskning bör fokusera på att identifiera de bästa sätten att integrera blockkedja i den nuvarande hälso- och sjukvårdsinfrastrukturen. Blockkedja inom hälso- och sjukvården är lovande, och en fortsatt utveckling och adoption av blockkedjebaserade lösningar kan man förvänta sig då teknologin utvecklas.

Referenser

[1] R. o. Regeringskansliet, "Sjukvård," May 2017. [Online]. Available: https://www.regeringen.se/regeringens-politik/sjukvard/

[2] Connecting for Health Personal Health Working Group, "The Personal Health Working Group: Final Report," Jun. 2003. [Online]. Available: https://www.policyarchive.org/handle/10207/15473

[3] H. Yang and B. Yang, "A Blockchain-based Approach to the Secure Sharing of Healthcare Data," 2017. [Online]. Available: https://www.semanticscholar.org/paper/A-Blockchain-based-Approach-to-the-Secure-Sharing-Yang-Yang/af404093a0fe066a43e5021b7d0f2a1c7b9105e6

[4] "An Overview of Cryptographic Hash Functions and Their Uses | SANS Institute." [Online]. Available: https://www.sans.org/white-papers/879/

[5] D. I. Dogaru and I. Dumitrache, "Cyber security in healthcare networks," in *2017 E-Health and Bioengineering Conference (EHB)*, Jun. 2017, pp. 414–417.

[6] K. S. Bhosale, M. Nenova, and G. Iliev, "A study of cyber attacks: In the healthcare sector," in *2021 Sixth Junior Conference on Lighting (Lighting)*, Sep. 2021, pp. 1–6.

[7] "Ransomware." [Online]. Available: https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/ransomware

[8] "The State of Ransomware 2022," Tech. Rep., Apr. 2022. [Online]. Available: https://www.sophos.com/en-us/content/state-of-ransomware

[9] "Metoder som används vid cyberangrepp." [Online]. Available: https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/cyberhot/metoder-som-anvands-vid-cyberangrepp/

[10] P. Aspden and Institute of Medicine (U.S.), Eds., *Patient safety: achieving a new standard for care*. Washington, D.C: National Academies Press, 2004.

[11] Riksdagsförvaltningen, "Hälso- och sjukvårdslag (1982:763) Svensk författningssamling 1982:1982:763 t.o.m. SFS 2016:1298 - Riksdagen." [Online]. Available: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/halso--och-sjukvardslag-1982763_sfs-1982-763

[12] ——, "Nationella riktlinjer för prehospital vård Motion 2014/15:1870 av Penilla Gunther (KD) - Riksdagen." [Online]. Available: https://www.riksdagen.se/sv/dokument-lagar/dokument/motion/nationella-riktlinjer-for-prehospital-vard_H2021870

[13] *Prehospitalt omhändertagande av patienter med misstänkt höftfraktur. Vårdprocess med transport direkt till röntgen eller akutmottagning.* Lund: Lund University, Faculty of Medicine, 2019, oCLC: 1097905622.

[14] "EENX16-2023-47.pdf: EENX16 Projektförslag Kandidatarbete E2 V23." [Online]. Available: https://chalmers.instructure.com/courses/21215/files/2388005?module_item_id=318569

[15] N. Davoody, S. Koch, I. Krakau, and M. Hägglund, "Accessing and sharing health information for post-discharge stroke care through a national health information exchange platform - a case study," *BMC Medical Informatics and Decision Making*, vol. 19, no. 1, p. 95, May 2019. [Online]. Available: https://doi.org/10.1186/s12911-019-0816-x

[16] S. Belfrage, G. Helgesson, and N. Lynøe, "Trust and digital privacy in healthcare: a cross-sectional descriptive study of trust and attitudes towards uses of electronic health data among the general public in Sweden," *BMC Medical Ethics*, vol. 23, no. 1, p. 19, Mar. 2022. [Online]. Available: https://doi.org/10.1186/s12910-022-00758-z

[17] S. Belfrage, N. Lynöe, and G. Helgesson, "Willingness to Share yet Maintain Influence: A Cross-Sectional Study on Attitudes in Sweden to the Use of Electronic Health Data," *Public Health Ethics*, vol. 14, no. 1, pp. 23–34, Apr. 2021.

[18] A. Skendzic, B. Kovacic, and E. Tijan, "General data protection regulation — Protection of personal data in an organisation," in *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO).* Opatija: IEEE, May 2018, pp. 1370–1375. [Online]. Available: https://ieeexplore.ieee.org/document/8400247/

[19] Directorate-General for Parliamentary Research Services (European Parliament) and M. Finck, *Blockchain and the general data protection regulation: can distributed ledgers be squared with European data protection law?* LU: Publications Office of the European Union, 2019. [Online]. Available: https://data.europa.eu/doi/10.2861/535

[20] Riksdagsförvaltningen, "Patientdatalag (2008:355) Svensk författningssamling 2008:2008:355 t.o.m. SFS 2022:915 - Riksdagen." [Online]. Available: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/patientdatalag-2008355_sfs-2008-355

[21] ——, "Lag (1998:543) om hälsodataregister Svensk författningssamling 1998:1998:543 t.o.m. SFS 2018:439 - Riksdagen." [Online]. Available: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-1998543-om-halsodataregister_sfs-1998-543

[22] I. Olaronke and O. Oluwaseun, "Big data in healthcare: Prospects, challenges and resolutions," in *2016 Future Technologies Conference (FTC)*, Dec. 2016, pp. 1152–1157.

[23] B. Marr, "What's The Difference Between Structured, Semi-Structured And Unstructured Data?" [Online]. Available: https://www.forbes.com/sites/bernardmarr/2019/10/18/whats-the-difference-between-structured-semi-structured-and-unstructured-data/

[24] T. Hulsen, "Sharing Is Caring—Data Sharing Initiatives in Healthcare," *International Journal of Environmental Research and Public Health*, vol. 17, no. 9, p. 3046, May 2020. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7246891/

[25] S. Sagiroglu and D. Sinanc, "Big data: A review," in *2013 International Conference on Collaboration Technologies and Systems (CTS)*, May 2013, pp. 42–47.

[26] E. M. Meslin, A. Blasimme, and A. Cambon-Thomsen, "Mapping the translational science policy 'valley of death'," *Clinical and Translational Medicine*, vol. 2, no. 1, p. 14, Jul. 2013. [Online]. Available: https://doi.org/10.1186/2001-1326-2-14

[27] Institute of Medicine (US), *Sharing Clinical Research Data: Workshop Summary*, ser. The National Academies Collection: Reports funded by National Institutes of Health. Washington (DC): National Academies Press (US), 2013. [Online]. Available: http://www.ncbi.nlm.nih.gov/books/NBK131772/

[28] G. E. Gross, "The Role of the Tumor Board In a Community Hospital," *CA: A Cancer Journal for Clinicians*, vol. 37, no. 2, pp. 88–92, Mar. 1987. [Online]. Available: http://doi.wiley.com/10.3322/canjclin.37.2.88

[29] J. W. London, "Cancer Research Data-Sharing Networks," *JCO Clinical Cancer Informatics*, no. 2, pp. 1–3, Dec. 2018. [Online]. Available: https://ascopubs.org/doi/10.1200/CCI.17.00145

[30] R. o. Regeringskansliet, "Nationell IT-strategi för vård och omsorg," Mar. 2006. [Online]. Available: https://www.regeringen.se/rattsliga-dokument/skrivelse/2006/03/skr.-200506139

[31] X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, "Integrating blockchain for data sharing and collaboration in mobile healthcare applications," in *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*. Montreal, QC: IEEE, Oct. 2017, pp. 1–5. [Online]. Available: http://ieeexplore.ieee.org/document/8292361/

[32] "Medical Identity Theft and Telemedicine Security," *Telemedicine and e-Health*, vol. 15, no. 10, pp. 928–932, Dec. 2009. [Online]. Available: https://www.liebertpub.com/doi/abs/10.1089/tmj.2009.9932

[33] A. Adjekum, A. Blasimme, and E. Vayena, "Elements of Trust in Digital Health Systems: Scoping Review," *Journal of Medical Internet Research*, vol. 20, no. 12, p. e11254, Dec. 2018. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6315261/

[34] J. Walker, E. Pan, D. Johnston, J. Adler-Milstein, D. W. Bates, and B. Middleton, "The Value Of Health Care Information Exchange And Interoperability: There is a business case to be made for spending money on a fully standardized nationwide system." *Health Affairs*, vol. 24, no. Suppl1, pp. W5–10–W5–18, Jan. 2005. [Online]. Available: http://www.healthaffairs.org/doi/10.1377/hlthaff.W5.10

[35] A. Tolk, "Interoperability, Composability, and Their Implications for Distributed Simulation: Towards Mathematical Foundations of Simulation Interoperability," in *2013 IEEE/ACM 17th International Symposium on Distributed Simulation and Real Time Applications*, Oct. 2013, pp. 3–9, iSSN: 1550-6525.

[36] "Legal Interoperability | Joinup," May 2023. [Online]. Available: https://joinup.ec.europa.eu/collection/nifo-national-interoperability-framework-observatory/glossary/term/legal-interoperability

[37] Y. Zhou, J. S. Ancker, M. Upahdye, N. M. McGeorge, T. K. Guarrera, S. Hedge, P. W. Crane, R. J. Fairbanks, A. M. Bisantz, R. Kaushal, and L. Lin, "The impact of interoperability of electronic health records on ambulatory physician practices: a discrete-event simulation study," *Journal of Innovation in Health Informatics*, vol. 21, no. 1, pp. 21–29, Feb. 2014. [Online]. Available: http://access.portico.org/stable?au=phw1p05tphc

[38] S.-Y. Choi and A. B. Whinston, "Benefits and requirements for interoperability in the electronic marketplace," *Technology in Society*, vol. 22, no. 1, pp. 33–44, Jan. 2000. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0160791X99000342

[39] I. Olaronke, A. Soriyan, I. Gambo, and J. Olaleke, "Interoperability in healthcare: Benefits, challenges and resolutions," *International Journal of Innovation and Applied Studies*, vol. 3, pp. 2028–9324, 04 2013.

[40] "ISO/TR 20514:2005." [Online]. Available: https://www.iso.org/standard/39525.html

[41] F. Oemig and R. Snelick, *Healthcare Interoperability Standards Compliance Handbook*. Cham: Springer International Publishing, 2016. [Online]. Available: http://link.springer.com/10.1007/978-3-319-44839-8

[42] "HL7 Standards Product Brief - HL7 Version 2 Product Suite | HL7 International." [Online]. Available: https://www.hl7.org/implement/standards/product_brief.cfm?product_id=185

[43] "Extensible Markup Language (XML) 1.0 (Fifth Edition)." [Online]. Available: https://www.w3.org/TR/2008/REC-xml-20081126/

[44] "Patient-example - FHIR v5.0.0." [Online]. Available: https://www.hl7.org/fhir/patient-example.html

[45] openEHR architectural overview (rel 1.2.3). [Online]. Available: https://specifications.openehr.org/releases/BASE/latest/architecture_overview.html#_architecture_overview

[46] Y. Xie, J. Zhang, H. Wang, P. Liu, S. Liu, T. Huo, Y.-Y. Duan, Z. Dong, L. Lu, and Z. Ye, "Applications of Blockchain in the Medical Field: Narrative Review," *Journal of Medical Internet Research*, vol. 23, no. 10, p. e28613, Oct. 2021. [Online]. Available: https://www.jmir.org/2021/10/e28613

[47] M. Di Pierro, "What Is the Blockchain?" *Computing in Science & Engineering*, vol. 19, no. 5, pp. 92–95, 2017. [Online]. Available: https://ieeexplore.ieee.org/document/8024092/

[48] H. Natarajan, S. Krause, and H. Gradstein, *Distributed Ledger Technology and Blockchain*. World Bank, Washington, DC, 2017. [Online]. Available: http://hdl.handle.net/10986/29053

[49] S. M. H. Bamakan, A. Motavali, and A. Babaei Bondarti, "A survey of blockchain consensus algorithms performance evaluation criteria," *Expert Systems with Applications*, vol. 154, p. 113385, Sep. 2020. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0957417420302098

[50] F. A. Aponte-Novoa, A. L. S. Orozco, R. Villanueva-Polanco, and P. Wightman, "The 51% Attack on Blockchains: A Mining Behavior Study," *IEEE Access*, vol. 9, pp. 140 549–140 564, 2021.

[51] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System." [Online]. Available: https://bitcoin.org/en/bitcoin-paper

[52] V. Buterin, "Ethereum Whitepaper." [Online]. Available: https://ethereum.org

[53] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei, and C. Qijun, "A review on consensus algorithm of blockchain," in *2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*. Banff, AB: IEEE, Oct. 2017, pp. 2567–2572. [Online]. Available: http://ieeexplore.ieee.org/document/8123011/

[54] SRI International, L. Lamport, R. Shostak, SRI International, M. Pease, and SRI International, "The Byzantine generals problem," in *Concurrency: the Works of Leslie Lamport*, D. Malkhi, Ed. Association for Computing Machinery, Oct. 2019. [Online]. Available: https://dl.acm.org/citation.cfm?id=3335936

[55] P. W. Eklund, J. Spasovski, J. S. Sjøgaard, and L. Herskind, "Crash vs Byzantine fault tolerance at scale: the cost of distributing trust in a (trans)national invoicing system," 2021. [Online]. Available: http://rgdoi.net/10.13140/RG.2.2.29195.00802

[56] "Hyperledger architecture, volume 1: Introduction to hyperledger business blockchain design philosophy and consensus." [Online]. Available: https://www.hyperledger.org/learn/white-papers

[57] A. Jain and D. S. Jat, "A Review on Consensus Protocol of Blockchain Technology," in *Intelligent Sustainable Systems*, ser. Lecture Notes in Networks and Systems, A. K. Nagar, D. S. Jat, G. Marín-Raventós, and D. K. Mishra, Eds. Singapore: Springer Nature, 2022, pp. 813–829.

[58] N. A. Asad, M. T. Elahi, A. A. Hasan, and M. A. Yousuf, "Permission-Based Blockchain with Proof of Authority for Secured Healthcare Data Sharing," in *2020 2nd International Conference on Advanced Information and Communication Technology (ICAICT)*, Nov. 2020, pp. 35–40.

[59] K. Zheng, Y. Liu, C. Dai, Y. Duan, and X. Huang, "Model Checking PBFT Consensus Mechanism in Healthcare Blockchain Network," in *2018 9th International Conference on Information Technology in Medicine and Education (ITME)*, Oct. 2018, pp. 877–881, iSSN: 2474-3828.

[60] P. Prabha and K. Chatterjee, "Design and implementation of hybrid consensus mechanism for IoT based healthcare system security," *International Journal of Information Technology*, vol. 14, no. 3, pp. 1381–1396, May 2022. [Online]. Available: https://doi.org/10.1007/s41870-022-00880-6

[61] T. Hepp, M. Sharinghousen, P. Ehret, A. Schoenhals, and B. Gipp, "On-chain vs. off-chain storage for supply- and blockchain integration," *it - Information Technology*, vol. 60, no. 5-6, pp. 283–291, Dec. 2018. [Online]. Available: https://www.degruyter.com/document/doi/10.1515/itit-2018-0019/html?lang=en

[62] S. Kumar, A. K. Bharti, and R. Amin, "Decentralized secure storage of medical records using Blockchain and <span style=font-variant:small-caps;">IPFS : A comparative analysis with future directions," *Security and Privacy*, vol. 4, no. 5, Sep. 2021. [Online]. Available: https://onlinelibrary.wiley.com/doi/10.1002/spy2.162

[63] A. Kormiltsyn, C. Udokwu, K. Karu, K. Thangalimodzi, and A. Norta, "Improving Healthcare Processes with Smart Contracts," in *Business Information Systems*, ser. Lecture Notes in Business Information Processing, W. Abramowicz and R. Corchuelo, Eds. Cham: Springer International Publishing, 2019, pp. 500–513.

[64] K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson, and T. Hayajneh, "Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring," *Journal of Medical Systems*, vol. 42, no. 7, p. 130, Jun. 2018. [Online]. Available: https://doi.org/10.1007/s10916-018-0982-x

[65] "Proof-of-stake (PoS)." [Online]. Available: https://ethereum.org

[66] "An overview of hyperledger foundation." [Online]. Available: https://www.hyperledger.org/learn/white-papers

[67] P. Zhang, J. White, D. C. Schmidt, G. Lenz, and S. T. Rosenbloom, "FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data," *Computational and Structural Biotechnology Journal*, vol. 16, pp. 267–278, Jan. 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2001037018300370

[68] V. Mani, P. Manickam, Y. Alotaibi, S. Alghamdi, and O. I. Khalaf, "Hyperledger Healthchain: Patient-Centric IPFS-Based Storage of Health Records," *Electronics*, vol. 10, no. 23, p. 3003, Jan. 2021. [Online]. Available: https://www.mdpi.com/2079-9292/10/23/3003