Blockkedjor

Är blockkedjor en användbar teknik för militärt bruk?

AMUND GUDMUNDSON HUNSTAD, LARS WESTERDAHL

FOI-R--4679--SE
ISSN 1650-1942 December 2018

Amund Gudmundson Hunstad, Lars Westerdahl

Blockkedjor

Är blockkedjor en användbar teknik för militärt bruk?

Bild/Cover: Pixabay

Titel	Blockkedjor – Är blockkedjor en användbar teknik för militärt bruk?
Title	Blockchains – Are blockchains an applicable technology for military usage?
Rapportnr/Report no	FOI-R--4679--SE
Månad/Month	December
Utgivningsår/Year	2018
Antal sidor/Pages	44
ISSN	1650-1942
Kund/Customer	Försvarsmakten
Forskningsområde	4. Informationssäkerhet och kommunikation
FoT-område	Cyber
Projektnr/Project no	E72727
Godkänd av/Approved by	Christian Jönsson
Ansvarig avdelning	Ledningssystem
Exportkontroll	Innehållet är granskat och omfattar ingen information som är underställd exportkontrollagstiftningen.

Sammanfattning

Blockkedjor är digitala och distribuerade motsvarigheter till huvudbok eller liggare för att föra löpande anteckningar, i en miljö utan central lagring och central styrning. Användning av blockkedjor möjliggör att spårbart och tillförlitligt bokföra transaktioner av olika varianter.

Denna omvärldsstudie beskriver övergripande hur blockkedjor är uppbyggda och fungerar. Aktuella tillämpningar av blockkedjor och utvecklingsmöjligheter dessa ger redovisas och diskuteras.

Huruvida blockkedjor kan ha adekvata och relevanta tillämpningar inom Försvarsmakten diskuteras. Slutsatsen är att användning av blockkedjor kräver att Försvarsmakten resonerar kring sina behov av distribuerade system, spårbarhet, sekretess och hög systemprestanda.

Nyckelord: Blockkedjor, konsensusmodeller, distribuerade system, spårbarhet, oföränderlighet, tilltro, transaktion

Summary

Blockchains are digital and distributed ledgers for ongoing registrations, in an environment lacking central storage and central management. This facilitates traceability and reliability related to the bookkeeping of different types of transactions.

This report provides an overview of the design of blockchains and how they work. Current applications of blockchains and their potential development are presented and discussed.

Whether blockchains may have adequate and relevant applications within the Swedish Armed Forces is discussed. This report concludes that the use of blockchains requires that the Swedish Armed Forces considers to what degree they are in need of distributed systems, traceability, confidentiality and high system performance.

Keywords: Blockchains, consensus model, distributed system, traceability, immutability, trust, transaction

Innehållsförteckning

1 Inledning

Civil teknikutveckling har potential att möjliggöra förbättrad funktionalitet i olika tekniska system och tjänster inom Försvarsmakten. Likaså kan civil teknikutveckling möjliggöra nya tjänster och system som möter existerande såväl som nya behov av tjänster med tillhörande tekniska system. Det är därför av stor vikt för Försvarsmakten att via omvärldsstudier bevaka den allmänna teknikutvecklingen.

Blockkedjor har blivit allmänt kända som de distribuerade verifieringssystem som dokumenterar utförda transaktioner för kryptovalutor. Särskild uppmärksamhet har Bitcoin och dess blockkedja rönt, sedan den skapades 2009. De senaste åren har blockkedjeteknikens potential att användas för distribuerad verifiering och dokumentation av utförda transaktioner i andra sammanhang än för kryptovalutor fått en ökad uppmärksamhet. Bland annat testas blockkedjeteknikens användbarhet i samband med fastighetsköp, aktiehandel, arkivförvaltning och förvaltning av försörjningskedjor. Förväntningarna är hos många aktörer stora, kanske rent av upphaussade. Företag, organisationer och myndigheter satsar på och markerar intresse för blockkedjeutvecklingens potential. En bland många storstilade satsningar är Dubais blockkedjestrategi med sikte på att bli ”the first city fully powered by Blockchain by 2020” och som resultat av detta ”make Dubai the happiest city on earth” (Smart Dubai u.å.). För att nå detta mål avser Dubai med öppna målformuleringar satsa på effektivisering och besparingar inom myndighetsförvaltning, industriella satsningar och internationellt ledarskap.

Försvarsmaktens behöver väl utformade säkerhetsmekanismer och -tjänster , vilket är utgångspunkten för att granska huruvida blockkedjetekniken kan bidra till detta. I detta ingår att bedöma potentialen hos blockkedjetekniken och under vilka generella förutsättningar den kan bedömas vara användbar.

Denna omvärldsstudie är gjord inom Försvarsmaktens samlingsbeställning Operationer i cyberdomänen med beställningsnummer AF.9221516. Studiens målsättning är att beskriva förutsättningar för tillämpning av blockkedjeteknik och riktar sig därmed till de som väljer tekniska lösningar, exempelvis FM PROD. Uppdragets frågeställning och inriktning är avstämt med FoT-gruppen.

1.1 Genomförande

För att få en första uppfattning av omfattningen på vetenskapligt arbete på området genomfördes tre sökningar i Scopus. Två sökningar var med enbart teknikfokus (med och utan kryptovalutanyckelord) och en med fokus på teknik och militärt. Den första sökningen var generisk där endast sökorden ”blockchain” och ”block chain” användes. Båda stavningsvariationerna förekommer. I den

andra sökningen uteslöts nyckelord som anspelar på Bitcoin, kryptovaluta och andra valutaliknande associationer. En mer specifik avgränsning mot militära inriktningar gav endast en sökträff.

Googlesökning efter blockkedjor med militär tillämpning gav ett fåtal träffar. Dessa handlar dock främst om uppslag och idéer och inte så mycket om resultat. Även DARPA har finansierat ett par projekt men dessa är inte avslutade ännu.

Avseende tillämpningar har explorativa sökningar gjorts i svenska och amerikanska dagstidningar för att få en bild av hur allmänna medier berättar om det nyare teknikområde blockkedjor utgör. Explorativa sökningar har också gjorts via olika nättidningar och bloggar med fokus på tillämpning av nydanande teknik.

1.2 Avgränsningar

Redovisningen av blockkedjors tekniska uppbyggnad är avgränsat till att ge en allmän bild av hur blockkedjor fungerar, vilka grundläggande tekniklösningar de baserar sig på samt principiella val att göra inför design av en arkitektur för system med blockkedjor.

Endast ett relativt litet urval av blockkedjetillämpningar presenteras. Valda tillämpningar avser ge ett intryck av bredden av verksamheter och sammanhang där blockkedjetekniken testas. Samtidigt är inte avsikten att ge någon form av heltäckande redovisning av aktuella tillämpningar. En betydande, om inte rent av dominerande, andel av aktuella blockkedjetillämpningar utgörs av experiment och testverksamhet snarare än fullt operativa system. Detta medför att rapporten ger en fragmenterad bild av det dagsaktuella läget, ty dagsläget består av olika ansatser som i hög grad antyder snarare än visar vad blockkedjor är och kan bli framöver.

1.3 Läsanvisningar

Kapitel 2 presenterar kortfattat, utan att gå in på teknisk uppbyggnad, vad blockkedjor principiellt kan göra och i vilka generella systemsammanhang de kan tänkas användas.

Kapitel 3 redovisar blockkedjors tekniska uppbyggnad, med beskrivning av olika tillämpningsmöjligheter och målgrupper, samt vilka behov som kan ligga bakom val av teknik. Fokus ligger på tillämpningsmiljöer utan ett centralt system och de utmaningar detta innebär.

Kapitel 4 redovisar en övergripande bild av aktuella tillämpningar och utvecklingsmöjligheter för blockkedjor. Kriterier för att bedöma huruvida blockkedjetekniken är adekvat och relevant i olika kontexter redovisas.

Teknikens potential och begränsningar redovisas utifrån de olika tillämpnings-kontexterna.

I kapitel 5 diskuteras blockkedjeteknikens möjligheter och begränsningar utifrån tekniska såväl som tillämpningsrelaterade avvägningar respektive tidigare identifierade kriterier. Diskussion utmynnar i en uppsättning övergripande observationer och slutsatser avseende blockkedjeteknikens begränsningar och möjligheter inom svenska Försvarsmakten.

2 Blockkedjor i korthet

I detta kapitel redovisas kortfattat, utan att gå in på teknisk uppbyggnad, vad blockkedjor principiellt kan göra och i vilka generella systemsammanhang de kan tänkas användas.

2.1 Vad är blockkedjor?

Nationalencyklopedin (2018) definierar blockkedja som ett

> *öppet (publikt) och distribuerat verifieringssystem för digitala transaktioner, bland annat för valutaenheten bitcoin. Data lagras permanent i så kallade block som bildar en kedja i nätverket, var och en med information om en utförd transaktion. Varje ny transaktion måste godkännas av ett antal datorer i blockkedjans nätverk innan den läggs som ett nytt block till blockkedjan. Alla transaktioner krypteras och blockkedjan lagras i krypterad form. En nackdel är att blockkedjan därmed kan bli mycket lång.*

Definitionen accentuerar vikten av två egenskaper: spårbarhet och oföränderlighet. Resonemang kring dessa två egenskaper återkommer i rapportens senare delar. Bland tillämpningar omnämner (Nationalencyklopedin 2018) verifiering av transaktioner och saldoberäkningar avseende Bitcoin. Utöver tillämpningar i direkt anknytning till kryptovalutor, omnämner (Nationalencyklopedin 2018) även sammanhang där parters identitet och relationer behöver säkras, som exempelvis vid fastighetsköp, aktiehandel eller för att säkerställa varors äkthet och ursprung.

Standardiseringsarbete inom blockkedjeområdet pågår inom projektet Corda sedan 2015 (Nationalencyklopedin 2018; Corda u.å.). Projektet Hyperledger driver utvecklingsarbete inom ett globalt och omfattande konsortium av aktörer inom industri, teknikutveckling, bank- och finansvärlden, Internet-of-Things, supply chain-verksamhet och akademiska aktörer (Hyperledger u.å.). Hyperledger fokuserar på att förbättra prestanda och tillförlitlighet hos blockkedjebaserade system.

Mångfalden i föreslagna tillämpningar av blockkedjetekniken, vilka diskuteras mera i kapitel 4, visar på kreativitet, entreprenörskap och intresse av att utforska potentialen hos en ny teknik. Tillämpningarna handlar bland annat om arkivhantering, att uppnå tilltro och transparens, supply-chain-management, övergång till elektroniska handlingar och militära tillämpningar. Gemensamt för alla tillämpningarna är olika typer av *transaktioner som behöver hanteras på ett spårbart och tillförlitligt sätt*.

2.2 Begreppet transaktion

Begreppet *transaktion* är centralt för vad blockkedjor tillhandahåller, vilket framgår av att begreppet används frekvent i blockkedjerelaterade artiklar, såväl i vetenskapliga som mera populärt orienterade artiklar, men med en varierande precision i begreppets användning. I och med att Bitcoin fortfarande har en dominant ställning i blockkedjediskursen, tenderar transaktioner i blockkedjor att associeras till finansiella transaktioner. Det bör påpekas att detta ger en sned bild av potentialen hos blockkedjetekniken. Transaktioner finns i en mångfald andra sammanhang också.

Begreppet har sina rötter tillbaka till det senlatinska ordet *transactio* och det latinska verbet *transigere* med innebörden att genomföra, förmedla eller att komma överens med (Nationalencyklopedin 2018). Det torde därmed vara rimligt att beskriva blockkedjetekniken som att den på ett spårbart och tillförlitligt sätt dokumenterar hur något har genomförts som kräver förmedlande eller förhandling.

I modern tid används begreppet *transaktion* i olika sammanhang och med variation i innebörd kring vad som genomförs och kräver förmedlande eller förhandling:

- Samlingsbegrepp för påverkande händelse mellan parter. Parter kan vara fysisk person, juridisk person eller systemkomponenter. Exempel på transaktioner: Affärstransaktion, datatransaktion, kassatransaktion (Postordlistan 2012).
- Separat funktion utförd av en IT-tjänst, till exempel en överföring av pengar från en bank till en annan (ITIL 2011).
- Rörelse på konto, oftast insättning eller uttag (Konsumenternas bank- och finansbyrå 2010).
- Affär, affärshändelse, uppgörelse, avtal, åtgärd. Exempel: betalningstransaktion, bokslutstransaktion etcetera (Laurelli, Örtengren & Ångström 1990).
- En följd av databasoperationer som hör ihop som en enhet (Padron-McCarthy 2005).
- Uppgörelse, affärsavtal; affär (Svenska Akademien Ordlista (SAOL) 2015).
- Genom förhandling åstadkommen överenskommelse (Svenska Akademiens Ordbok (SAOB) 2007).
- Utbyte av budskap mellan människor i en kommunikativ handling (SAOB 2007).

Variationen i innebörd av begreppet transaktion speglas i de tillämpningar av blockkedjor som har växt fram och som diskuteras vidare i kapitel 4.

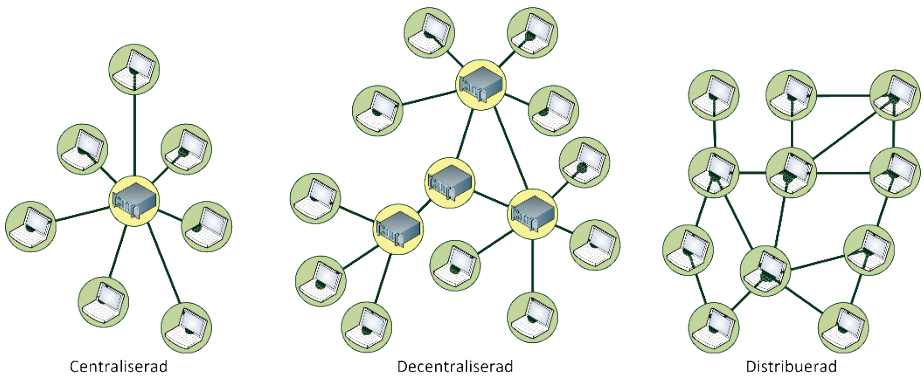
3 Blockkedjors tekniska uppbyggnad

Blockkedjor är en teknik för att skapa spårbarhet i en miljö där det inte finns eller man inte vill använda ett centralt system. Spårbarheten åstadkoms genom att händelser efter hand länkas ihop med varandra, för att på så sätt skapa en kedja av verifierbara händelser. Tekniken med blockkedjor har flera tillämpningsområden även om kryptovalutor, främst Bitcoin, är det område som för tillfället får störst uppmärksamhet.

I detta kapitel presenteras de bakomliggande tekniker som används för blockkedjor. Här beskrivs även olika tillämpningsmöjligheter och målgrupper samt vilka behov som kan ligga bakom val av teknik.

3.1 Centraliserade och distribuerade informationssystem

Information kan göras tillgänglig på flera olika sätt beroende på var informationen finns lagrad och var informationen kan påverkas. Tre principiella sätt att beskriva informationssystem är som centraliserade, decentraliserade, distribuerade arkitekturer. Dessa arkitekturer kan tillämpas i renodlad form eller kombineras efter behov. En illustration av arkitekturerna visas i Figur 1.



Figur 1. Principiella arkitekturer för nätverk. Gula noder motsvarar centraliserade funktioner som exempelvis servrar, medan gröna noder motsvarar klienter.

3.1.1 Centraliserat informationssystem

Centraliserade system byggde ursprungligen på att all information och beräkningskraft fanns i ett centralt datorsystem. Klienterna var enbart inmatningsplatser samt där resultat av beräkningar presenterades. Det finns fortfarande informationssystem som bygger på den ursprungliga principen, men då

kallas oftast klientnoderna för tunna klienter. I dagens informationssystem utgör servrar de centrala datorsystemen och klienterna är kraftfulla datorer men principen är den samma. Det är servern som lagrar information och det är på servern som den huvudsakliga databehandlingen sker. Ett typexempel på ett centraliserat informationssystem är en webbserver och en datorklient. En användare begär en webbsida ifrån en webbserver och webbservern levererar webbsidan. Om användaren vill ha mer information klickar denne på en länk vilket gör att en ny webbsida skickas från webbservern. Principen är densamma om tjänsten är internetbaserad, där användaren kommunicerar med en webb-server som hanteras av den organisation som användaren vill få tjänsten utförd av. En webbtjänst kan innehålla mer information och funktionalitet jämfört med en webbsida, som klienten interagerar med. En internetbank, exempelvis, hanterar all information och alla transaktioner och presenterar detta för klienten.

Styrkan i centrala datorsystem ligger bland annat i att de är lättare att underhålla och förvalta jämfört med programvara utspridda på flera datorer. Ägaren till den centrala delen av systemet, vare sig det är en privatperson eller en bank, kan hantera informationen och ansvarar för dess riktighet. Det är också upp till ägaren att informationen finns tillgänglig och inte förstörs vid händelse av ett avbrott. Ett centralt datorsystem har givetvis även svagheter. Då information hanteras centralt ökar risken för informationsförlust ifall det centrala systemet drabbas av haveri, avsiktligt eller inte. Den organisation som ansvarar för det centrala systemet är även påverkbar genom lagar, regelverk, med mera, vilket kan påverka informationens konfidentialitet, riktighet och tillgänglighet.

En annan fördel med en centraliserad lösning är att det är lättare att underhålla och förvalta system som bara finns på en plats. System- och policyförändringar får snabbt genomslag hos klienten.

En centraliserad arkitektur är sårbar i betydelsen att det endast krävs att en nod[1] (servern) angrips för att göra informationen eller tjänsten otillgänglig för klienterna. Även en olyckshändelse med ett datahaveri riskerar att få stora konsekvenser med risk för informationsbortfall. Den användare som efterfrågar information eller tjänster måste även känna tilltro till den organisation som äger och förvaltar tjänsten.

3.1.2 Decentraliserade datormiljöer

I en decentraliserad miljö delas funktionaliteten i den centraliserade miljön upp i flera delar. Den omedelbara fördelen med detta är att hela systemet inte kan sättas ur funktion genom att en nod slås ut. Om en nod angrips i ett decentraliserat system kan förhoppningsvis kvarvarande decentraliserade noder

[1] Information och tjänster finns sällan enbart på ett ställe. En förberedd leverantör har även redundanta och backupsystem vilka mildrar konsekvensen av olyckor och angrepp.

göra att systemet fungerar, om än begränsat. En ytterligare fördel med decentraliserade system är att noderna kan specialiseras och därmed utvecklas oberoende av andra noder. Inom en organisation kan detta till exempel innebära att en forskningsavdelning, en produktionsavdelning och en ekonomiavdelning kan anpassa hårdvara, mjukvara och rutiner oberoende av varandra.

I ett decentraliserat system kan fortfarande centrala tjänster finnas, exempelvis e-post, interna styrdokument, med mera. Om dessa funktioner sätts ur funktion tappar även det decentraliserade systemet denna funktionalitet, men övrig funktionalitet förblir intakt.

3.1.3 Distribuerade system

Ett distribuerat system är ett platt system utan centrala noder. Funktionalitet i ett distribuerat system kontrolleras genom den mjukvara som kopplar samman noder i systemet. Detta innebär att det inte finns någon given hierarki och därmed inte ett givet mål att angripa för att slå ut systemet. Resultatet blir ett robust system där en utslagen nod medför marginell påverkan på övriga noder.

Avsaknad av hierarki gör att distribuerade system kräver andra lösningar för att fatta beslut och att skapa tilltro till information och andra användare. Ett exempel på ett distribuerat system är krypteringssystemet Pretty Good Privacy (PGP). Inom PGP finns inga centrala servrar som kan skapa eller verifiera kryptonycklar åt användare. En användare får själv generera sitt nyckelpar. För att andra ska kunna verifiera att en viss publik nyckel tillhör en viss användare, signeras denna av andra användare som känner eller litar på den publika nyckelns ägare. På så sätt blir längden på listan med signeringar ett mått på hur mycket tilltro som kan tillskrivas att nyckeln faktiskt tillhör den som påstår sig inneha den.

Distribuerade system används främst i situationer där man vill undvika en central funktion, antingen för att se till att någon del av systemet alltid finns tillgänglig eller för att en central auktoritet inte är önskvärd. Det är i flera fall dock vanligt med hybridsystem, då det kan vara opraktiskt att söka efter information hos flera användare. Sådana hybrider kan då exempelvis vara uppslagsservrar vilka anger hos vilken nod eftersökt information finns, alternativt en filserver dit filer kan flyttas för att minska volymen i den ordinarie kommunikationen mellan alla noder. Blockkedjor är ett sätt att skapa spårbarhet för händelser i ett distribuerat system.

3.2 Blockkedjans byggstenar

En blockkedja består av sammanlänkade block, vilka innehåller ett antal verifierade transaktioner. Varje block i kedjan är också verifierbart, viket innebär att en blockkedja blir en historieskrivning av transaktioner som vem som helst kan verifiera äktheten i. Det är verifierbarheten som ger tilltro till systemet och

det är komponenter som hashfunktioner och digitala signaturer som skapar förutsättningar för detta.

3.2.1 Hashfunktion

En central funktion inom blockkedjor är kryptografiska hashfunktioner. I framställningen hädanefter används termen hashfunktion för enkelhets skull. En hashfunktion är en envägsfunktion vilken alltid ger ett resultat av fast längd. Att en funktion är en envägsfunktion innebär att det är lätt (för en dator) att ta fram ett resultat av funktionen för ett givet ingångsvärde, men att det är mycket svårt att utifrån resultatet av funktionen räkna ut vilket ingångsvärdet var. Svaret på funktionen kallas ofta hashsumma på svenska alternativt message digest eller bara digest på engelska. Det ingångsvärdet, vilket exempelvis kan vara en fil eller en sträng med tecken, kallas på engelska message.

Resultatet av en hashfunktion har en fast längd. Vilken längden är beror på funktionen, exempelvis så ger SHA-256 en 256-bitars hashsumma, men längder på upp till 512 bitar förekommer hos andra funktioner. Fördelen med att generera ett resultat med fast längd är att stora filer blir snabbare sökbara och att det blir enklare att spåra förändringar. En liten förändring i ingångsvärdet ger en tydlig skillnad i den resulterande hashsumman.

3.2.2 Digitala signaturer

Digitala signaturer är datorvärldens motsvarighet till en handskriven underskrift på papper. Samtidigt är en digital signatur mer specifik, då den ändrar sig beroende på det innehåll som signaturen ska fastställa. En handskriven signatur är den samma oavsett om den är till för att godkänna ett kontrakt, ett kvitto eller deklaration.[2] På så sätt är en handskriven signatur mer mottaglig för förfalskning genom att den inte ändras beroende på innehållet.[3] En digital signatur är en matematisk signatur baserat på det innehåll som ska signeras och den nyckel som tillhör den som signerar. Det innebär att om innehållet som signeras ändras så ändras också utseenden på signaturen men nyckeln som används för att signera meddelandet ändras inte.

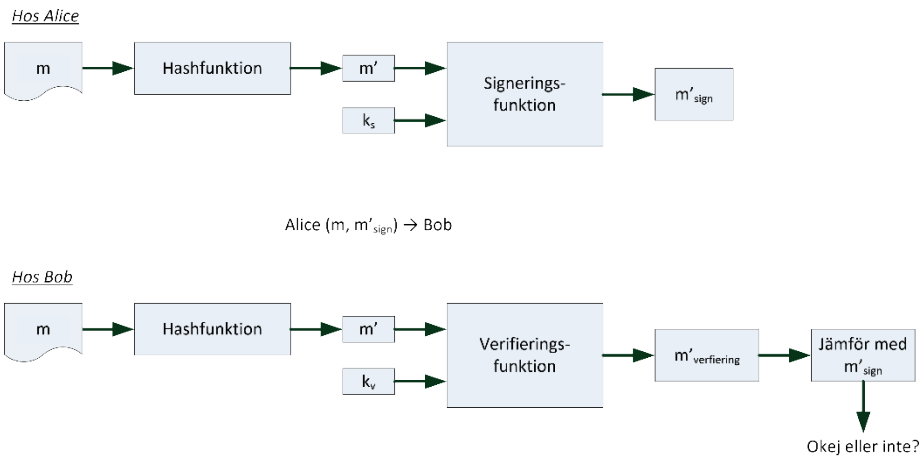
Digitala signaturer skapas genom användandet av asymmetrisk kryptering. I asymmetriska krypteringsfunktioner har en användare ett nyckelpar där nycklarna är olika, men kompletterar varandra. Det innebär att en nyckel kan kryptera ett meddelande och den andra nyckeln i paret kan dekryptera meddelandet och tvärt om. Båda nycklarna behövs dock för att ett meddelande både

[2] Handskrivna signaturer varierar visserligen *i detaljer* mellan olika signeringstillfällen, exempelvis på grund av stress, varierande temperatur, typ av penna – men inte på grund av dokumentinnehåll.
[3] Detta innebär dock inte att handskrivna signaturer är enkla att förfalska.

ska kunna krypteras och dekrypteras. Det blir därför viktigt att ägaren till nyckelparet håller den ena nyckeln (k_h) hemlig. På så sätt kan den andra nyckeln (k_p) spridas fritt då den endast kan kryptera ett meddelande, medan innehavaren av den hemliga nyckeln (k_h) kan dekryptera meddelandet.

Samma teknik kan användas för att skapa digitala signaturer. En användare Alice har ett asymmetriskt nyckelpar för att digitalt kunna signera data. I det här fallet benämns den hemliga nyckeln som signeringsnyckel (k_s) och den publika nyckeln som verifieringsnyckel (k_v). När Alice vill signera ett meddelande använder hon sin signeringsnyckel för att kryptera meddelandet och skickar därefter både meddelandet och signaturen till mottagaren Bob. Bob dekrypterar Alice signatur med Alice publika verifieringsnyckel (k_v) och jämför resultatet med det meddelande som Alice sände samtidigt. Om de båda överensstämmer med varandra kan Bob vara säker på att det är Alice privata nyckel som har använts för att kryptera meddelandet.

Det är ofta opraktiskt att signera meddelanden av godtycklig storlek. Därför är det vanligare att avsändaren utför en hashfunktion på de data som ska kunna verifieras. Därefter signeras hashsumman. Alice skickar då sitt meddelande och signaturen till Bob. Bob kan själv skapa motsvarande hashsumma med hjälp meddelandet och därefter verifiera att det är den hashsumma som har signerats med Alice privata nyckel (Figur 2) genom att använda Alice verifikationsnyckel.

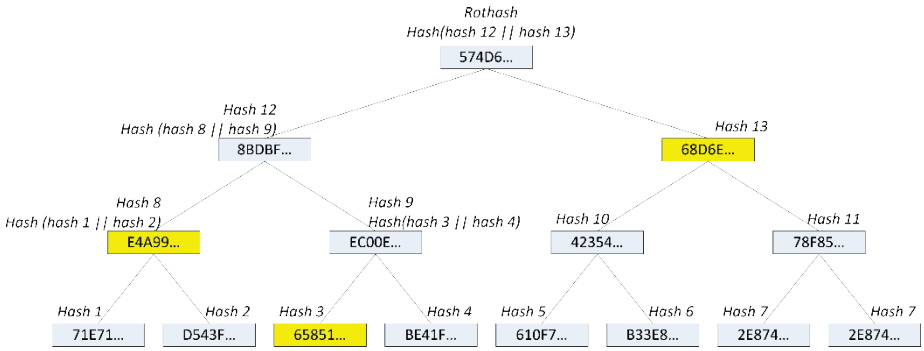


Figur 2. Digital signatur.

3.2.3 Merkleträd

Ett Merkleträd är en trädstruktur av hashsummor som används för att visa att alla hashsummor tillhör samma grupp. I Merkleträdet kopplas noder samman parvis, från botten (löven) till högsta nivån (roten). På så sätt blir varje överordnad nod

en hashsumma av de två underliggande noderna. Det innebär att roten i Merkleträdet är en hashsumma av hela trädet (Figur 3).



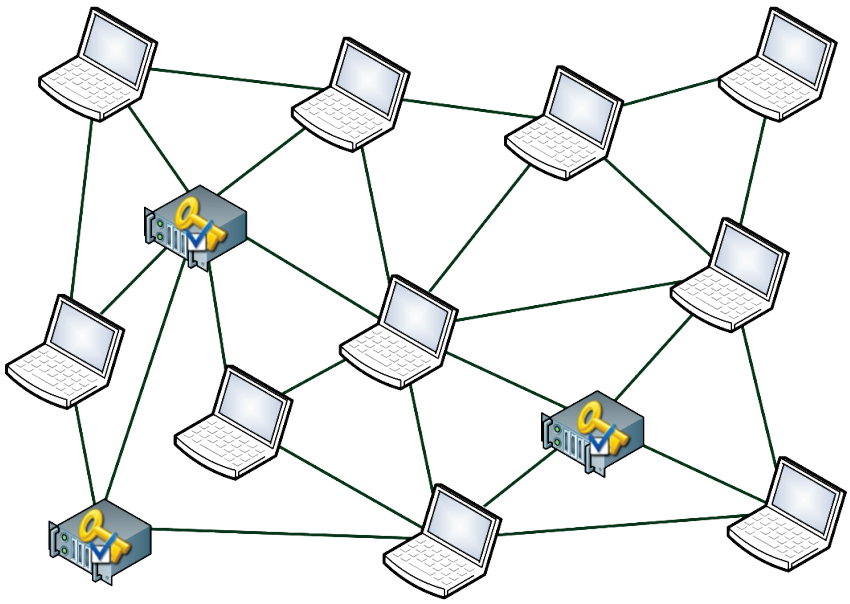
Figur 3 Merkleträd

En användare som har tillgång till alla löv i trädet har möjlighet att återskapa trädet och verifiera att löven tillhör trädet. Det är dock inte nödvändigt för användaren att ha tillgång till alla löv för att kunna återskapa trädet. En användare som känner till Hash 4 i Figur 3, behöver tillgång till Hash 3 för att själv kunna skapa Hash 9. Användaren behöver därefter tillgång till Hash 8 för att skapa Hash 12 och Hash 13 för att skapa hashroten. På så sätt kan användaren med ett fåtal noder verifiera riktigheten av godtyckliga löv i Merkleträdet. Denna egenskap är exempelvis värdefull i system där det finns en stor mängd data, men begränsad beräknings- eller kommunikationskapacitet.

3.3 Arkitektur

Blockkedjor används i en distribuerad miljö av datorer. I varje dator finns det en programvara som dels binder samman alla datorer i ett Peer-to-Peer-nätverk (P2P), dels som hanterar den trafik som relaterar till blockkedjan. Det innebär att en dator (en nod) delar information med andra datorer genom att sprida information till alla andra (eng. broadcast). I och med att det inte finns en central server i systemet blir alla noder ansvariga för att samla på sig den information som är nödvändig för att bidra till systemets syfte.

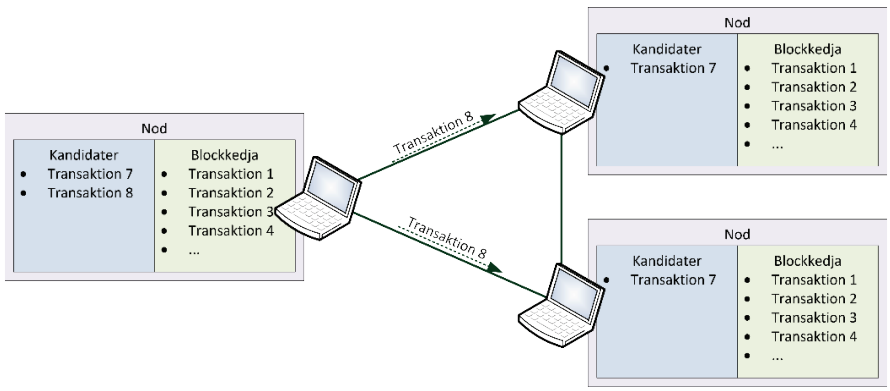
Utöver de vanliga användarna i systemet finns även särskilda noder vars uppgift det är att samla ihop den information som sprids i nätverket och paketera denna i block. Uppgiften att skapa block kallas ibland för mining eller minting, beroende på vilken blockkedjeplattform som används. De block som skapas bildar tillsammans med andra block en blockkedja och utgör det kollektiva minnet inom systemet (Figur 4).



Figur 4. Arkitektur för ett blockkedjesystem.

3.3.1 Transaktioner

Programvaran i varje nod hanterar bland annat användarens aktiviteter i P2P-nätverket, kommunikationen med andra noder, håller reda på de transaktioner som har distribuerats från andra noder samt uppdaterar blockkedjan då nya block blir tillgängliga (Figur 5). De transaktioner som skickas runt är kandidater till att tas upp i ett nytt block, och det är först när de kopplas till ett block som de blir en del av blockkedjan (se 3.3.2).



Figur 5. Enskilda transaktioner över nätverket.

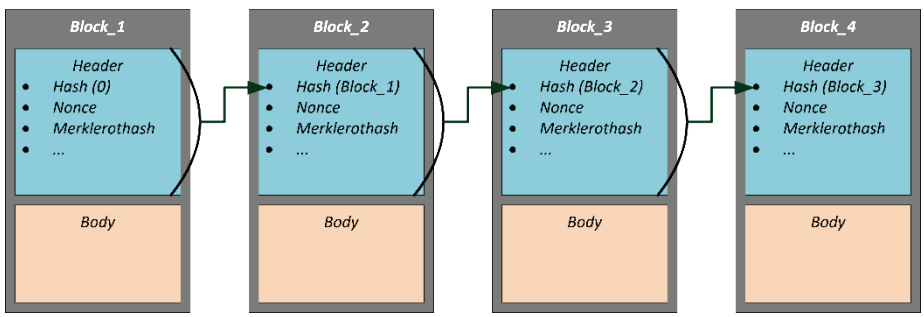
En transaktion är en förändring av tillståndet i nätverket. För ett nätverk för kryptovaluta kan en transaktion betyda att användare Alice för över 50 enheter till Bob. För att säkerhetsställa att det inte är Bob själv som hittat på denna transaktion signerar Alice transaktionen med sin signeringsnyckel, $Alice_{ks}$. I valutasammanhang så är inte Alice känd under sitt riktiga namn utan genom sin verifieringsnyckel, $Alice_{kv}$. Motsvarande gäller för Bob som också endast är känd genom sin verifieringsnyckel, Bob_{kv}. Alice dator sänder ut en transaktion över nätverket, innehållande sin egen verifieringsnyckel, Bobs verifierings-nyckel, ett belopp samt en signatur för transaktionen. Alla deltagare på nätverket kan verifiera att det är Alice som signerat transaktionen genom att applicera hennes verifieringsnyckel på signaturen:

Alice transaktion: $(Alice_{kv} \rightarrow Bob_{kv}, 50, Alice_{ks}(Alice_{kv} \rightarrow Bob_{kv}, 50))$

Verifikation: $(Alice_{kv}(Alice_{ks}(Alice_{kv} \rightarrow Bob_{kv}, 50)))$.

3.3.2 Block

De transaktioner som har skickats ut över nätverket är kandidater till de transaktioner som efter hand kommer att tas upp i ett block och därmed permanentas i blockkedjan. Blocken kan ha lite olika utformning beroende på vilket blockkedjesystem som blocket tillhör. På en högre abstraktionsnivå kan dock block beskrivas som innehållande en informationsdel om blocket (eng. header) och en lastdel (eng. body) där blockets huvudsakliga innehåll finns.



Figur 6. Generisk vy av en blockkedja.

Det är informationen i headern som skapar spårbarheten och som ser till att blocklistan förblir oföränderlig. I headern ingår bland annat en hashsumma av föregående blockheader, det nonce som användes för att klara utmaningen (se avsnitt 3.3.3) samt en hashsumma av den Merklerot som finns i blockets body. Genom att inkludera en hashsumma av föregående blocks header, knyts blocken ihop i en kedja av block (Figur 6). Det nya blocket skickas ut till alla användare i

systemet så att de, efter att ha verifierat blocket, kan lägga till blocket till sin blockkedja. Ett block blir inte fullt accepterat i en blockkedja förrän det tillkommit ytterligare block i blockkedjan.

3.3.3 Konsensusmodeller

Ett block skapas när en nod verifierar ett antal transaktioner och låser in dessa i ett block. Detta block signeras så att all information inom blocket kan verifieras utan att kunna ändras. Skyddet mot förändring stärks ytterligare när nya block skapas och det aktuella blocket blir en inre del av blockkedjan.

Alla noder inom blockkedjenätverket kan skapa nya block, men beroende på verifieringsmodell brukar vissa noder utmärka sig mer som renodlade block-skapande noder. I publika blockkedjesystem såsom Bitcoin och Ethereum används utmaningar som blockskapande noder måste lösa för att få skapa ett nytt block. Aktiviteten att lösa dessa utmaningar kallas vid olika namn, bland annat mining eller minting.

Syftet med mining är att reglera produktionstakten av nya block (Pham 2016). För kryptovalutor finns det oftast en ekonomisk vinning av att skapa nya block. I fallet Bitcoin exempelvis, erhåller den som skapar ett nytt block för tillfället 12,5 Bitcoin för varje block som skapas. Det innebär att blockskaparen skapar värde för sig själv samtidigt som denne ökar det totala värdet inom Bitcoinsfären. För att undvika att för många block skapas med enbart nya Bitcoin och att dessa därmed skulle falla i händerna på en eller ett fåtal personer, styrs svårigheten i den utmaning som presenteras. Regleringen av blocktillverkningen hanteras genom en konsensusmodell, vilket är en accepterad modell för hur nya block accepteras i en kedja. Saini (2018) presenterar en övergripande genomgång av konsensus-modeller men för den här rapportens syften presenteras här några utvalda konsensusmodeller som är kända eller relevanta för frågeställningarna inom denna rapport.

Proof of Work (PoW) är den vanligaste formen av konsensusmodell för blockkedjor, mest kanske för att den används inom Bitcoin men modellen används även av andra. Modellen bygger på att blockskaparen bevisar att denne har lyckats lösa ett svårt kryptografiskt problem, vanligtvis att räkna ut ett ingående värde till en envägsfunktion. Som nämndes i avsnitt 3.2.1 är det beräkningsmässigt lätt att ta fram en hashsumma för ett givet ingångsvärde, men mycket svårt att identifiera ingångsvärdet med stöd av hashsumman. I det här fallet utgörs det ingående värdet av två delar – ett känt värde i form av en sträng och ett nonce. Strängen kan vara godtycklig men räknas oftast fram. I fallet Bitcoin utgörs strängen av hashsumman av senast giltigast block headern. Blockskaparens uppgift är att hitta ett värde på noncet så hashsumman av noncet och den givan stängen blir lägre än ett bestämt målvärde. Målvärdet motsvarar en sträng med ett antal inledande nollor och därefter ettor. Strängens längd beror på

den hashmetod som används, vilket innebär att för SHA-256 så är strängen 256 bitar. Antalet nollor i början av målvärdet anger hur svårt det är att hitta ett värde som är lägre.

Det finns inget sätt att hitta ett lämpligt nonce annat än att testa alla möjliga kombinationer av värden, från noll upptill det som löser problemet. Detta är grunden till att metoden benämns PoW, då det är den som lagt ner mest arbete som också lyckas skapa det nya blocket.

Energiåtgången för blockskapningsprocessen är problematisk då den kan vara mycket energikrävande. I dagsläget uppgår energiförbrukningen för Bitcoin till mer än Islands energikonsumtion och redan år 2020 förväntas den överstiga Danmarks (Yaga, Mell, Roby & Scarfone 2018, s.28).

Proof of Stake (PoS) är ett mindre energikrävande system. Till skillnad från PoW där beräkningsförmågan styr vem som skapar block, så regleras här processen genom insatser. Terminologin är också lite annorlunda jämfört med PoW. Den som vill vara med och skapa nya block kallas för validerare (eng. validator) och väljs ut ur en grupp av validerare. Sannolikheten att bli vald validerare baseras på hur mycket som valideraren har investerat i systemet. Som exempel kan sägas att Alice satsar 1 000 enheter i systemet medan Bob endast satsar 100 enheter. I denna situation får Alice en tio gånger större chans att bli vald som validerare jämfört med Bob. Då Alice är vald behöver hon inte heller konkurrera med andra genom att lösa ett problem. Processen att ta fram nya block får därför ett annat namn än mining, nämligen minting.

Schemaläggning

Både PoW och PoS används i publika kryptovalutasystem. Det innebär att det måste finnas ett incitament för någon att lägga ner den ansträngningen eller de resurser som krävs för att skapa nya block. Drivkraften är ofta att den som skapar nya block tilldelas en belöning eller har rätt att ta ut en avgift för de transaktioner som blocket innehåller. Distribuerade nätverk och blockkedjeteknik används dock inte enbart för kryptovaluta utan kan även finna andra användningsområden.

I ett distribuerat system, där det inte finns något vinstintresse, måste block ändå skapas även om behovet av utmaningar för att få skapa blocken inte är aktuella. Ett sätt att lösa detta är att deltagarna i systemet turas om att samla in transaktioner och applicera dessa i block. Användarna kan fortfarande verifiera att det nya blocket är korrekt innan det ansluts till respektive blockkedja.

Avgränsade nätverk

Ett distribuerat nätverk behöver inte nödvändigtvis ha användare som är okända för varandra eller som kommer ifrån olika organisationer i övrigt. Valet av en distribuerad lösning kan göras av flera anledningar, vilket innebär att en organisation kan välja en distribuerad lösning för sitt interna nätverk. I ett sådant fall

finns det fortfarande en central organisation som äger nätverket och som kan påverka dess utformning. Det kan också finnas en permanent blockgenererande nod utses som bara har till uppgift att samla in transaktioner och skapa nya block efter en given storlek eller tidsperiod.

Tilltron till en fast blockgenereringsnod i ett centralstyrt distribuerad nätverk är densamma som för en databas eller en server i ett centraliserat system. Ägarskapet och därmed även kontrollen över vilka som bjuds in till systemet gör att behovet av konsensus inte uppstår och att systemägaren själv kan välja blockgenereringsmetod (Netis Group Blog 2018).

3.3.4 Underhåll av blockkedjan

Distribuerade system kommunicerar via en gemensam programvara som finns installerad på varje ingående dator i systemet. Denna programvara förvaltas av någon med intresse av att systemet ska leva vidare och utvecklas.

Uppdatering av programvaran kan få konsekvenser för den aktuella blockkedjan. Om det efter en uppdatering skapar ny funktionalitet eller på annat sätt påverkar strukturen i blocken, kommer block från den gamla programvaran inte att kunna verifieras i uppdaterade noder. Block från ouppdaterade noder kommer därför att förkastas och därmed inte kunna tillföras till blockkedjan. En sådan här uppdatering kräver att alla noder uppdateras för att blockkedjan ska bestå. Ett sådant skifte kallas för en *hard fork*, då blockkedjan får en ny gren, där transaktioner med den nya funktionen inte är verifierbar av noder med den gamla programvaran. Information om gamla transaktioner förs över till den nya förgreningen så ingen information går förlorad. Enklare uppdateringar av programvaran kräver inte att alla noder uppdaterar sin programvara direkt, utan kan fortsätta använda denna som innan och ändå skapa och verifiera block. Dessa enklare uppdateringar kallas för *mild fork* (NIST).

3.4 Smarta kontrakt

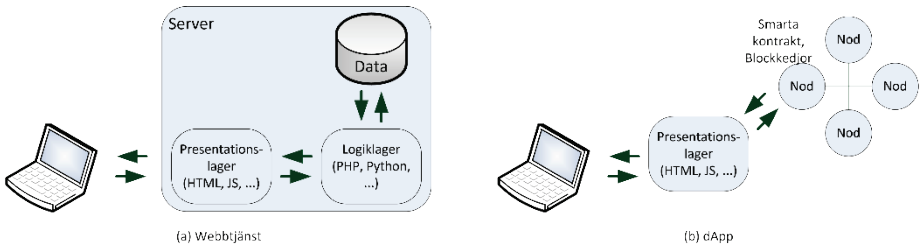
Smarta kontrakt är en utökning av blockkedjans funktionalitet genom att självexekverande kod lagras i ett block. Med programkod kan logiska argument tillföras, vilket medför att villkor kan ställas på mottagare innan transaktioner utförs. Ett exempel på ett sådant villkor skulle kunna vara att Lisa donerar 1 000 kronor till ett uppstartsföretag som har som mål att samla in 100 000 kronor till ett visst datum för att kunna förverkliga en idé. Om uppstartsföretaget når sitt mål får de tillgång till Lisas 1 000 kronor, men om målet inte nås återgår de till Lisa igen.

Ett system med smarta kontrakt behöver en pålitlig part som kan föra in aktuell information som kan användas för att avgöra uppfyllnad av villkor. En sådan part

kallas orakel (eng. oracle) och kan vara en person, men lika gärna en betrodd tjänst som förser blockkedjan med relevant information.

Smarta kontrakt är en viktig del av Ethereums plattform för blockkedjor. Det smarta kontraktet innehåller en virtuell maskin, vilken agerar på input från användare och orakel. Beräkningar av den logik som smarta kontrakt innehåller är dock kostsamma, vilket medför att ett smart kontrakt endast bör utföra enklare funktioner för att inte ge för stor belastning på nätverket (Kasireddy 2017).

En tillämpning av smarta kontrakt är som en del av distribuerade applikationer, dApp. Principiellt fungerar dApps som webbtjänster, men i dApps ersätter blockkedjan databasen och smarta kontrakt ersätter webbservern (McCubbin 2018), se Figur 7. All exekvering sker av kod sker lokalt i en nod.



Figur 7. Översiktbild av en webbtjänst och en dApp.

3.5 Säkerhet

Säkerhet för informationssystem beskrivs oftast utifrån konfidentialitet, riktighet och tillgänglighet.[4] Dessa egenskaper kan kompletteras med flera andra beroende på i vilken kontext som systemet i fråga ska verka. Robusthet och spårbarhet är ofta två viktiga egenskaper, men även personlig integritet, såsom anonymitet, är i många sammanhang en viktig egenskap.

3.5.1 Spårbarhet

Spårbarhet är en av blockkedjors främsta egenskaper. Tekniker med digitala signaturer är mycket robusta och accepterade, även i andra systemsammanhang än blockkedjebaserade. Blockkedjors främsta förmåga är dock att kunna skapa spårbarhet i en distribuerad miljö, det vill säga i en miljö utan en central auktoritet. Denna spårbarhet skapas genom blockens sammanlänkning i en kedja som gör att blocken kopplas till varandra och att kedjan inte obemärkt kan brytas.

[4] Från engelskans confidentiality, integrity, and availability.

Blockkedjor är en teknik för distribuerade miljöer. Om centrala system är möjliga, såsom centrala servrar och databaser, finns inget behov av blockkedjor.

3.5.2 Robusthet och skydd mot informationsförlust

Ett distribuerat system har en inneboende robusthet mot fysiska och till viss del även logiska angrepp. I ett distribuerat system där informationen är jämt fördelad inom systemet, orsakar en eller några bortfallna noder ingen större skada på systemet som helhet. Nya noder kan snabbt etableras och erhålla tillgänglig information.

Den distribuerade informationen medför också att risken för informationsförlust minskar. Ett välbyggt centraliserat eller decentraliserat informationssystem har en väl fungerande backup-funktion. Jämfört med ett distribuerat system är den dock bara utspridd på ett fåtal noder. Om all information ska gå förlorad i ett distribuerat system så måste alla noder slås ut.

3.5.3 Anonymitet och konfidentialitet

Syftet med en blockkedja är att skapa spårbarhet i en distribuerad miljö. Det medför att konfidentialitet och då främst sekretess inte är en prioriterad förmåga. I kryptovalutasystem har anonymitet och transparens prioriterats, vilket försvårar möjligheterna för konfidentialitet. För andra typer av publika blockkedjesystem eller avgränsade system kan det finnas behov av konfidentialitet. Tekniken i blockkedjor stödjer inte konfidentialitet, utan den förmågan får åstadkommas med annan teknik. Trafikskydd kan etableras inom det distribuerade nätverket genom att noderna krypterar trafiken mellan varandra, men det finns inget internt skydd inom nätverket som reglerar vem som har tillgång till blockkedjan. Ett trafikskydd innebär dock att noderna måste antingen lyda under samma auktoritet och dela en gemensam kryptonyckel, alternativt etablera kanaler mellan individuella noder. För att uppnå en skyddad kanal utan att dela en gemensam kryptonyckel krävs dock digitala certifikat. Både en delad nyckel och certifikat omöjliggör den anonymitet som finns i exempelvis Bitcoins öppna system. Smarta kontrakt som villkorar transaktioner kan i princip hantera anonyma sändare och avsändare så länge villkoren är enkla. Om de smarta kontrakten utvecklas kommer dock sannolikt det även krävas att parterna i transaktionen (kontraktet) är kända.

3.5.4 Publika blockkedjor

Publika blockkedjesystem, såsom Bitcoin, saknar (medvetet) en central auktoritet. I viss mån är det inte helt korrekt, då någon måste underhålla den programvara som används för att skapa P2P-nätverket, men för verksamheten saknas en auktoritet. Detta löses genom en form av acceptans för ett antal givna

förutsättningar, såsom att den blockkedja som finns är giltig, att den längsta blockkedjan är giltig i händelse av konflikt mellan två konkurrerande blockförgreningar, med mera.

Avsaknad av auktoritet, framför allt när det gäller system där ekonomisk vinning är möjlig, medför behov av ett konkurrenssystem för att få skapa nya block. En fara med en till synes okontrollerad blockgenerering är att en stark genererare kan ta kontroll över blockkedjan, om denne har mer än 51 procent av blocktillverkningen. Med en majoritet av kapaciteten kan blockskaparen skapa godtyckliga block med transaktioner som är felaktiga. För att motverka denna situation används i PoW en så pass svår utmaning att ingen kan bli så stark (beräkningskraftig) att denna är bättre än alla andra flera gånger i rad. För PoS-system som har en annan uppbyggnad, kan en blockbyggare straffas om felaktiga block skapas. Programvaran i varje nod som verifierar block upptäcker om ett nytt block är felaktigt och kan därefter blockera nya block från aktuell blockskapare. Beroende på protokoll minskas samtidigt blockskaparens insats genom en straffavgift, alternativt tas den bort helt. På så sätt minskas inflytandet för den antagonistiska noden.

4 Tillämpningar och utvecklings-möjligheter: Tro och vetande vid slutet av 2018

Detta kapitel redovisar en övergripande ögonblicksbild över vilka tillämpningar och utvecklingsmöjligheter för blockkedjor som är aktuella vid slutet av 2018. Begränsningar i mötet mellan teknisk lösning och verksamhetsbehov tas också upp till diskussion. I och med att blockkedjetekniken har rönt betydande uppmärksamhet, bland annat i medierapportering, försöker detta kapitel att skilja orealistiska och rent av felaktiga förväntningar från de mer realistiska. Kriterier, potential och begränsningar för scenarion och kontexter, där det kan vara adekvat och relevant att välja blockkedjor som teknik, presenteras och diskuteras.

4.1 Är blockkedjor ändamålsenliga?

Idéer och förslag till tillämpning av blockkedjor är rikligt förekommande i de mest skilda sammanhang. Flertalet av dessa förslag torde inte vara realistiska på sikt, då blockkedjetekniken fortfarande brister i mognad och har inte med självklarhet ännu hittat sammanhang där den fungerar bäst. Därför är det förnuftigt att förhålla sig med kritiskt sinnelag även till de verktyg och kriterier som för närvarande existerar.

En inventering av olika uppsättningar ur forskningslitteratur och mera allmän litteratur av villkor för när blockkedjor kan vara adekvata och relevanta lösningar dokumenteras av (Gunnarson & Hamber 2018, ss.32). Villkorsuppsättningarna är av varierande utformning, men ändå med tydligt överlapp. Återkommande villkor handlar om

- multipla aktörer delar på data/databas
- multipla aktörer uppdaterar data/skriver i databasen
- förmedlande eller förhandlande mellanled kan potentiellt utgöra ej önskvärd extra kostnad och komplexitet
- beroenden mellan transaktioner skapade av olika aktörer.

Ytterligare villkor handlar om faktorer som bör beaktas avseende legala aspekter på blockkedjeteknik, affärsstrategier, anpassning mellan verksamheter och teknik etcetera.

Gunnarson & Hamber (2018) använder de olika villkorsuppsättningarna som en del av ett underlag för att designa ett ramverk. Ramverket är ett verktyg för att

identifiera blockkedjelösningar, prioritera bland dem och planera för deras implementering. Det större sammanhang som deras ramverk används inom är för att identifiera tänkbara blockkedjetillämpningar inom ett svenskt fjärrvärmeföretag. Gunnarson & Hamber (2018) poängterar det som viktigt att ramverket ska bidra till att värdera huruvida en blockkedjelösning är värdeskapande och om lösningen är användbar för att hantera ett identifierat problem.

Huruvida en blockkedjelösning är värdeskapande är ur en kommersiell verksamhets perspektiv till betydande grad en fråga om huruvida den genererar ekonomisk vinst. Ur Försvarsmaktens perspektiv är ekonomisk vinst inte en drivkraft, däremot är en drivkraft att en lösning bör bidra tydligt till att lösa en Försvarsmaktsrelevant arbetsuppgift eller uppdrag på ett effektivt och ändamålsenligt sätt.

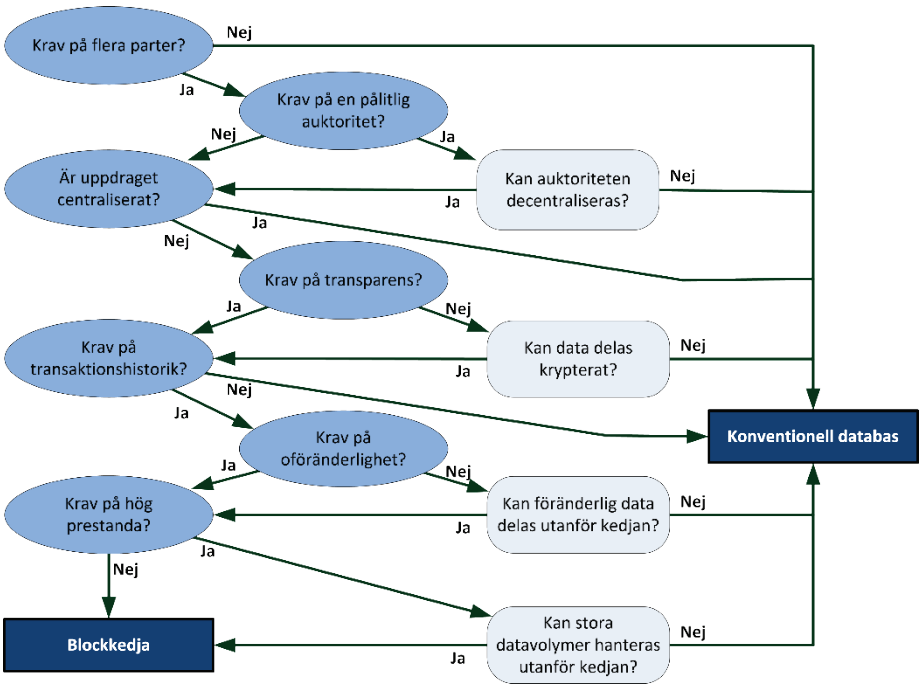
Avseende varför blockkedjor kan vara aktuella att använda och vilka problem de kan lösa, är det av vikt att fokusera på vad blockkedjor kan åstadkomma *bättre* än andra tekniska lösningar. Att blockkedjor kan lösa ett problem är inte tillräckligt för att motivera deras användning. Till exempel existerar det många konventionella databaslösningar med decennier av utveckling och erfarenheter inarbetade och som är effektiva lösningar för att lösa många problem. Som (Greenspan 2017) aningen provocerande formulerar det: “given a choice between two equally suitable technologies, why use the one that’s still in its diapers?”, till vilket det snabba svaret som ges är att det finns problem där just den nya tekniken är den adekvata, relevanta och bäst lämpade.

Med utgångspunkt i intervjuer med fjärrvärmeexpertis tar (Gunnarson & Hamber 2018) fram en uppsättning av 32 tänkbara blockkedjetillämpningar. Sju av dessa 32 tillämpningar prioriteras med hjälp av ramverket. Tillämpningar som prioriteras präglas bland annat av

- höggradig samverkan mellan aktörer för att nå synergieffekter
- marknadssituation med minskad centralisering
- infrastruktursystem med smarta förmågor inbyggda för att nå hållbarhetsmål
- flera fjärrvärmeproducenter och förstärkt kundposition innebär skarpare konkurrenssituation och krav på ständigt förbättrade affärsstrategier.

Lo, Xu, Chiam & Lu (2017) beskriver ett enkelt ramverk baserat på sju huvudfrågor (som är angivna i de två första kolumnerna i Figur 8) för att som ett första steg bedöma huruvida blockkedjelösningar är adekvata och relevanta relativt ett användningsfalls behov och krav. I tredje kolumnen i Figur 8 finns fyra underfrågor till vissa huvudfrågor. Huvudfrågorna är fokuserade på de kritiska teknikval dessa implicerar och huruvida valen resulterar i att blockkedjor kan vara adekvata och relevanta lösningssätt. De sju kritiska teknikvalen och avvägningar relaterade till dem är följande:

- *Krav på flera parter?* För att blockkedjor ska vara ändamålsenliga förutsätts att det finns flera parter (eller multipla aktörer). Där parter i dagens system ofta agerar via förmedlande eller förhandlande mellanled, möjliggör blockkedjor att kapa mellanleden, enligt (Lo et al. 2017). Vidare anser Lo et al. (2017) att konventionella system hos en enskild entitet (part) kan erbjuda motsvarande funktionalitet som blockkedjor till mindre kostnad. Huruvida detta fullt ut är korrekt bör bedömas närmare. Till exempel torde Försvarsmakten i sig vara en organisation av sådan omfattning att dess olika delar och agerande i vissa väl identifierade situationer kan bedömas vara en uppsättning parter. Försvarsmakten kan i koalitioner också anses vara en bland flera parter.



Figur 8. Ramverk för bedömning av blockkedjors lämplighet.

- *Krav på en pålitlig auktoritet?* Blockkedjor bryter beroendet av enskilda och centraliserade betrodda parter (som till exempel banker och myndigheter) och förlägger istället tilltron till den distribuerade liggaren som blockkedjan utgör.
- *Är uppdraget centraliserat?* För att blockkedjor ska vara ändamålsenliga förutsätts att drift och förvaltning av systemet inte är centraliserad. Lo et

al. (2017) jämför drift och förvaltning av blockkedjebaserade system med diplomati. Vidare påpekar Lo et al. (2017) att smarta kontrakt är svårare att implementera i blockkedjebaserade system än i konventionella distribuerade system. Argument för detta redovisas dock ej.

- *Krav på transparens?* Karakteristiska fördelar som återkommande lyfts fram avseende blockkedjor är möjligheter att kunna erbjuda distribuerad tilltro. Tilltro bygger typiskt på transparens. Sekretess minskar transparens. Härav följer att det finns en avvägning att göra mellan dessa egenskaper.
- *Krav på transaktionshistorik?* En central egenskap hos blockkedjor är att verifiera att data inte otillbörligt har ändrats, det vill säga att tillvarata riktighet eller integritet hos data. Lo et al. (2017) påpekar dock att kostnaden för att uppnå dataintegritet med hjälp av blockkedjor är relativt hög. Argument för detta redovisas dock ej.
- *Krav på oföränderlighet?* Beroende av inte alltid tillförlitliga tredjepartsaktörer är en situation som blockkedjesystem kan bidra till att lösa i och med att långa kedjor tillhandahåller ett mått av oföränderlighet och oavvislighet[5]. Huruvida detta hela vägen är den önskade egenskapen behöver beaktas vid systemdesignen.
- *Krav på hög prestanda?* Snabba beräkningar av stora datavolymer är inte lämpliga för blockkedjor. Publika blockkedjor blir lättare prestandamässigt krävande. För icke-publika blockkedjor är förutsättningarna annorlunda och kommande års utveckling kan ändra förutsättningarna ytterligare.

4.2 Blockkedjeteknikens potential: Ett axplock av tillämpningsmöjligheter

För närvarande är blockkedjetekniken primärt en teknik under utveckling, en teknik som kan vara en möjliggörare. En betydande, om inte rent av dominerande, andel av aktuella blockkedjetillämpningar utgörs av experiment och testverksamhet snarare än fullt operativa system. Därför finns det betydande osäkerheter i avvägningen mellan fördelar, nackdelar och kostnader. Om annan teknik kan lösa aktuellt problem, existerar det då några skäl att satsa på blockkedjor?

Ett försök att indikativt besvara denna fråga görs här nedan i form av ett axplock av exempel på tillämpningar som är under planering, utveckling, testning eller rent av är operativa. De olika exemplen omnämns under delrubriker avseende

[5] Oavvislighet: Att en handling inte i efterhand ska kunna förnekas av utföraren.

övergripande behov eller potential de enligt denna rapports författare relaterar till. Vissa av dessa behov eller potential återfinns även bland de ovan listade sju kritiska teknikvalen enligt (Lo et al. 2017).

4.2.1 Spårbarhet och riktighet i distribuerade system

Grundkonstruktionen hos en blockkedja, med att transaktioner läggs till i ett block och godkänns av ett tillräckligt stort antal datorer i blockkedjans datornätverk, innebär att spårbarhet är en grundegenskap. Godkännandet innebär även att riktighet är en grundegenskap.

Spårbarhetsresonemang utgör en tyngdpunkt i olika förslag till tillämpningar och experiment med blockkedjor, även om inte nödvändigtvis begreppet spårbarhet används i beskrivningar. I Estland hanteras, enligt Törnvall (2017), en miljon medborgares vårdrelaterade journaler i en blockkedjelösning. Enligt tidningsartikeln är invånarnas ”medicinska journal sparad i blockkedjan”. Huruvida journaler i sin helhet är sparade i blockkedjor är oklart. Blockkedjor är, trots vad som åberopas i en del populärt orienterade artiklar, knappast att bedöma som fullvärdiga databaser med exempelvis nödvändig sökfunktionalitet. Ett sätt att realisera detta kan tänkas vara i form av en hybridlösning, där blockkedjan har en mera avgränsad funktionalitet av att vara primärt den distribuerade liggaren medan journalinformation i sin helhet finns i en konventionell databas med fullvärdig sökfunktionalitet.

I populärt orienterade artiklar, som exempelvis (Jeffries 2018), beskrivs utöver journaltillämpningar ett antal andra tillämpningar där spårbarhet och riktighet är av vikt. Det kan röra sig om olika handlingar och transaktioner som exempelvis relaterat till husköp, hantering av digitala arkiv, förteckningar och handlingar, välfärdsutbetalningar, rättsliga handlingar, ansökningar och testamenten.

4.2.2 Arkiveringssäkerhet

Blockkedjors förmåga att säkra spårbarhet och dokumentera riktighet medför även en potential att vara ett värdefullt verktyg i arkiveringssammanhang.

Storbritanniens National Archives är involverad i forskningsprojektet ARCHANGEL kring hur digitalt lagrad information över relativt få år kan ändras, till exempel på grund av formatändringar. Ur deras perspektiv är följande forskningsfrågor centrala:

- Hur kan det visas att den handling arkivet hanterar i dag är den samma som blev anförtrodd till arkivet för ett antal år sedan?
- Hur kan det bevisas att de enda ändringar som har inträffat med handlingen är legitima och att de inte har påverkat innehållet?

- Hur kan det säkerställas att invånare fortsätter beakta arkiv som legitima förvaltare av digitala publika handlingar?

Projektet ARCHANGEL har ett fokus på hur blockkedjor kan användas för att lösa de utmaningar som ligger i forskningsfrågorna ovan. Projektet arbetar på att skapa en blockkedjebaserad prototyp, där hashningar av handlingar sparas. Om legitima ändringar av handlingen har inträffat, sparas även hashningen av den kod som genomförde ändringen på blockkedjan. Därigenom skapas en verifieringskedja som i detalj dokumenterar ändringar ett dokument har genomgått. Genom att kopior av kedjan finns hos olika arkivinstanser är den bärande idéen i ARCHANGEL-projektet att en enskild arkivinstans hindras från att otillbörligt skriva om historien. För detta finns det styrkor med en distribuerad systemmodell (Jeffries 2018; Green 2018).

4.2.3 Tilltro och transparens

Blockkedjors förmåga att säkra spårbarhet och dokumentera riktighet medför även en potential att kunna bidra till att öka tilltro till information och de instanser som förvaltar informationen. Likaså kan sådan förmåga tänkas bidra till utökad transparens kring hur information förvaltas. (Jeffries 2018) lyfter frågan rörande vad blockkedjor kan bidra med för myndigheter. Åtminstone i teorin kan pengar sparas, fel minska och tydligt ansvar kunna dokumenteras och utkrävas genom att säkra publik dokumentation av myndigheters informationshantering. (Jeffries 2018) redovisar en Cornellprofessors bedömning att blockkedjor kan ha en större positiv påverkan i länder där människor har lågt förtroende för myndigheter.

Av vikt för att uppnå en sådan grad av tilltro och transparens är det faktum att blockkedjor är distribuerade. Därigenom finns det inte endast en kritisk punkt man är beroende av. Istället existerar det ett antal punkter som kan bidra till att kontrollera och övervaka, vilket försvårar missbruk och otillbörlig ändring av information. Samtidigt bör det observeras att tilltro har olika aspekter, bland annat avseende tilltron till tekniska lösningar relativt tilltron till helt manuella lösningar.

4.2.4 Supply chain management

Förvaltning av försörjningskedjor (supply chain management) är omfattande, arbetskrävande och icke minst involverar det fortfarande i stor grad pappersarbete. Transportföretaget A.P. Moller-Maersk och IBM arbetar med att ersätta pappershanteringen vid varutransporter mellan producenter och konsumenter med en blockkedjebaserad lösning. Exempelvis kräver i dagsläget en transport av ett parti avokado från Kenya till Nederländerna

- ursprungscertifikat på partiet

- ett dokument som verifierar att fruktpartiet har inspekterats
- fraktsedel
- packlista
- faktura.

Alla dessa dokument behöver godkännande från kenyanska myndigheter i form av signaturer. För att ordna detta transporteras de olika dokumenten typiskt via motorcykel mellan olika kenyanska instanser. Efter skeppstransport skickas dokumenten med bud till en mäklare i Rotterdam. Fyra till sex veckor krävs för godkännande av dokumenten, under vilken tid avokadopartiet för att fortfarande vara ätbara lämpligen bör nå fram till konsumenterna. Villkor inkluderande straffavgifter ställs innan avokadopartiet släpps ut på marknaden. En transport av ovan beskriven karaktär involverar typiskt 30 aktörer med totalt minst 100 individer och 200 dokumentutbyten (Shin 2018).

4.2.5 Övergång till elektroniska handlingar

Lantmäteriet har på ett regeringsuppdrag sedan 2016 tillsammans med Kairos Future[6], SBAB, Telia, Landshypotek bank och ChromaWay[7] drivit ett innovationsprojekt utifrån vad som benämns som principen *digitalt först*. Projektet har eftersträvat att på sikt kunna realisera en smartare samhällsbyggnadsprocess med bland annat minskad hantering av pappershandlingar och minskade handläggningstider för fastighetsbildning. I detta är blockkedjor bland de tekniker det finns tydliga förväntningar på. Målet har varit att verklighetstroget kunna demonstrera hur processen att köpa en fastighet och beviljas lagfart kan realiseras med blockkedjeteknik (Kairos Future 2018).

I juni 2018 demonstrerades ett första transaktionsärende avseende en fastighet på Gotland där köpare, säljare, berörda banker respektive mäklare steg för steg gick genom hela transaktionsprocessen. Respektive part fick information om de olika stegen till sina mobiler och signerade digitalt med hjälp av sina mobiler. Smidigheten och potentialen för besparingar i administrationen framhålls som centrala och betydande. Besparingar och värdeskapande för Sverige i en omfattning av tre till fem miljarder per år bedöms vara möjliga (Lindström 2018).

4.2.6 Militära tillämpningar

Inom militära kontexter kan det också noteras intresse för tillämpning av blockkedjetekniken. Även här är det i hög grad tal om experiment och testverksamhet

[6] Kairos Future är ett svenskt och internationellt konsult- och analysföretag som bland annat arbetar med trend- och omvärldsanalys, strategiarbete och omvärldsbevakning.
[7] ChromaWay är ett svenskt företag inom blockkedjebranschen, https://chromaway.com/

kring vad blockkedjor eventuellt kan åstadkomma och huruvida de kan göra det bättre än konventionella lösningar.

Amerikanska DARPA (Defense Advanced Research Projects Agency) studerar blockkedjeteknik i syfte att stärka skyddet runt kärnvapnen (Wong 2016). En annan tillämpning som DARPA är intresserade av är en robust och decentraliserad chattfunktion. Crypto-Chat är en produkt utvecklad av ITAMCO. Företaget har fått i uppdrag av DARPA att utveckla denna genom att tillföra blockkedjeteknik. Målet med utvecklingen är att skapa en mer robust chattfunktion (ITAMCO 2017). DARPA finansierar även ett uppdrag att verifiera Guardtimes blockkedjesystem (Kulshrestha 2016).

Lockheed Martin, som bland annat tillverkar det marina styrsystemet Aegis, samarbetar också med Guardtime för att implementera blockkedjefunktionalitet inom vad som omnämns som ”supply chain risk management and software development”. Intresset för blockkedjor i sammanhangen är, enligt företagen själva, baserade på att de ger säkerhet, robusthet och transparens i sammanhang av distribuerade system (Lockheed Martin 2018).

NATO Communication and Information Agency utlyste 2016 en tävling där bland annat militära tillämpningar av blockkedjeteknik ingick (NCI Agency 2016). Resultat från tävlingen verkar inte vara publika, även om vinnarna publiceras (Estonian Defence Industry Association 2016).

Blowers (2018) diskuterar potentialen för styrning av en uppsättning obemannade system (till exempel missilsvärm) med hjälp av blockkedjeteknik där smarta kontrakt ingår i systemet. Tänkt teknisk lösning avser förbättra säkerhetskontrollmekanismer, som såväl kan tillåta som hindra åtkomst till resurser utanför blockkedjan och att bygga upp kontraktsmodeller för denna kommunikation och interaktion fram till en definierad målsättning. I sammanhangen agerar uppsättningen av obemannade system med hjälp av smarta kontrakt och röstningsförfaranden som en distribuerad autonom organisation (DAO). Blowers (2018) diskuterar inte eventuella prestandabegränsningar avseende till exempel beräkningskapacitet i blockkedjan. Airbus arbetar också med arkitekturer för autonoma flygande farkoster (Toyota 2018).

4.3 Blockkedjeteknikens begränsningar

Än så länge brister det i teknikens mognad med problem relaterade till effektivitet och säkerhet. Utöver blockkedjeteknikens bristande mognad präglas även blockkedjebranschen i sig av bristande mognad, med aktörer som snabbt dyker upp och lika snabbt försvinner. Begränsningar och hinder existerar även i form av formella, politiska och byråkratiska begräsningar för att introducera ny teknik, som exempelvis i följande skeenden, (Jeffries 2018):

- Hong Kong Monetary Authority bedömer att digitala valutor i dagsläget allmänt inte utgör en tydlig förbättring från existerande betalningsinfrastrukturer och -tjänster, men att den internationella utvecklingen på området bör bevakas (Jeffries 2018; Chan 2018).
- Satsning på ett blockkedjebaserat fastighetsregister i Honduras stoppas på grund av kommunikationsproblem med myndighetsinstanser, växande insikt om den komplicerade naturen hos ärendetypen och att en teknisk lösning visar sig inte heller denna gång vara ett universalmedel (Jeffries 2018; Cadasta Foundation 2016).
- Pilotstudie avseende ett blockkedjebaserat fastighetsregister i Cook County, Illinois, USA, finns tillgängligt via en rudimentär webbsida, http://www.ccrecorder.org/. Arbetet gjordes på ideell basis av en konstellation av juridisk expertis, utvecklingsföretaget velox.RE, Cook Countys fastighetsregister och notarius publicus. (Jeffries 2018; Lifthrasir 2017). Pilotstudien visade att det är möjligt att realisera ett blockkedjebaserat fastighetsregister, dock krävs ytterligare digitalisering av fastighetsregister, standardiserade dataformat och ny lagstiftning. Utöver dessa aspekter har vid val i Illinois beslutats om hopslagning av nuvarande fastighetsregisteransvariga förvaltning med en annan förvaltning, vilket medför att beslut om ytterligare satsning på blockkedjebaserat fastighetsregister dröjer till 2020. Dessutom inspirerades nuvarande mjukvaruleverantör till att integrera blockkedjeliknande konstruktioner i sin mer konventionella lösning.
- I samband med presidentvalet i Sierra Leone i mars 2018 har rapportering förekommit om att det schweiziska företaget Agora ska ha bidragit till att valet genomfördes med blockkedjebaserad teknik. Sierra Leones valkommission bestrider detta. Agora hade status som internationell observatör på inbjudan av valkommissionen och fanns på plats i endast ett valdistrikt, där en demonstration av vad Agoras tekniska lösning kan göra genomfördes parallellt med valkommissionens manuella räkning. Valräkningen var hela tiden manuellt genomförd och under valkommissionens kontroll. Skillnaderna i vad som återberättas av olika aktörer kan konstateras vara betydande. Tilltro till en teknisk lösning är oerhört central i kontexten av ett lands val. Sannolikt har i dagsläget en ivrig marknadsföring från Agoras sida inte ökat tilltron till deras lösning. Samtidigt kan det noteras att det finns ett intresse för blockkedjors potential för valhantering, till exempel från Kenyas valkommission (Jeffries 2018; Pollock 2018; Kazeem 2018; Independent Electoral and Boundaries Commission 2018). Frågor kring tilltro och transparens som diskuteras i avsnitt 4.2.3 och särskilt avvägningen mellan tilltro till tekniska lösningar relativt helt manuella, ges en ytterligare tyngd av händelserna kring Sierra Leone-valet.

- Dataskyddsförordningen, GDPR, kan enligt Gartners analytiker Daryl Plummer sätta stopp för hantering av personuppgifter i blockkedjor. Gartners prognos är att 75 % av alla publika blockkedjor 2021 kan vara olagliga enligt GDPR. Orsaken till detta är att information i blockkedjor, som till exempel personinformation, ligger där okrypterad (block-kedjetekniken fungerar i utgångspunkten så) och på grund av block-kedjornas grundkonstruktion ligger informationen kvar där för alltid (Lindström 2018).

4.4 Blockkedjeteknikens avarter

I och med att blockkedjetekniken i viss omfattning har präglats av upphaussade förväntningar och begränsad realism, redovisas i detta avsnitt några exempel på mer avvikande eller partiellt bisarra tillämpningar eller händelser från de senare åren. Exemplen kan ses som en dokumentation av kreativitet. Det bör noteras att dessa torde vara teknikområdets extremyttringar eller eventuellt humorinslag:

- Flera företag byter namn och affärsidé genom att satsa på kryptovalutor eller blockkedjeteknik. Isteproducenten Long Island Iced Tea Corp. ombildas till Long Blockchain Corp och hamnar på en börsbevaknings-lista. Andra företag som omprofilerar sin verksamhet på liknande sätt har innan arbetat inom e-cigarettbranschen, som farmaceutföretag, med träningskläder för kvinnor, som inkubator för internetföretag, som cigarrproducent, med finansiella tjänster eller med mineralprospektering (Popper 2017).
- Företaget Decentraland säljer virtuella fastigheter i sitt virtuella land. En 100 kvadratmeter virtuell fastighet har exempelvis sålts för $120 000. Under loppet av 30 sekunder lyckas Decentraland samla $26 miljoner från investerare (Sorkin 2018).
- Decenturion, världens första blockkedjestat bildas enligt (Kuznetsova 2018). Staten sägs vara lokaliserad i sin blockkedja, men förhandlingar pågår för att köpa öar nära Kuala Lumpur som fysisk lokalisering. Styrandet av landet avses ske med smarta kontrakt.
- Det franska företaget Qarnot marknadsför sin produkt Crypto-Heater som på samma tid värmer ett rum och utvinner kryptovaluta. Enligt marknadsföringen finns följande fördel: ”make heating a source of revenue, not an expense” (Redman 2018). Eventuellt kan produkten även betraktas som ett inlägg i debatten om omfattningen av energi som går åt för att utvinna vissa kryptovalutor som till exempel Bitcoin.
- Avi Aisenberg vid South Florida Distillers snabbar upp mognings-processen för företagets rom EthereRum genom att tillvarata värme som alstras av datorer som utvinner kryptovaluta (Connell 2017).

5 Diskussion och slutsatser

Blockkedjor är för närvarande ett stort diskussionsämne och det finns höga förväntningar på vad som går att åstadkomma med denna teknik. Avseende tillämpningar så är blockkedjor i sin barndom även om de komponenter som bygger upp blockkedjor kan spåras längre bak i den datalogiska och kryptologiska historien. Det är dock vanligt att nya tillämpningar får mycket uppmärksamhet och att dessa prövas på flera användningsområden. Hittills har kryptovalutor varit den tillämpning som fått mest uppmärksamhet och då särskilt Bitcoin. Detta är dock inte den enda implementationen eller tillämpningen av blockkedjor. Det finns plattformar som är stabila bland annat för kryptovalutahantering, men som även kan användas i andra sammanhang. Exempelvis har Ethereum omnämnts flera gånger i rapporten och deras plattform har stöd för smarta kontrakt. Smarta kontrakt har en intressant utvecklingspotential, men är än så länge bäst lämpade för enklare transaktioner. Tillämpning av blockkedjor inom *supply chain management* skulle kunna vara intresseväckande i Försvarsmaktssammanhang som ett sätt att säkra spårbarhet för ingående komponenter i system. Tillämpning inom området behöver dock mogna innan det kan anses vara en tillförlitlig lösning.

Frågan om blockkedjor ska användas som teknik för en tillämpning är dock inte den första som bör ställas inför ett tänkt utvecklingsarbete. Lo et al. (2017) beskriver ett flöde av frågor (Figur 8, sida 29) som bör ställas innan en blockkedjelösning väljs framför en mer traditionell databaslösning. En av de mest grundläggande frågor som en systemägare bör ta ställning till är hur man vill kommunicera inom systemet. De flesta systemlösningar är idag centraliserade eller decentraliserade, med ett antal centrala tjänster. En central lösning kan vara en förutsättning för en verksamhets affärsidé då det underlättar övervakning och debitering (Kandaswamy, Valdes, Furlonger & Chesini 2017). Även om det inte bedrivs en affärsmässig verksamhet så är ett centraliserat system exempelvis smidigare att underhålla. Svagheterna med centrala system är att de också blir mer sårbara genom att de har en eller ett fåtal noder som kan slås ut och därmed få hela systemet att haverera och med följdeffekter för verksamheten.

För en organisation som Försvarsmakten är robusthet ett viktigt kriterium, framför allt för de system som stödjer operativ verksamhet. Robusta tjänster och nätverk kan åstadkommas på flera sätt. Redundans och säkerhetskopiering är exempel på lösningar som stärker ett system och som gör det möjligt att snabbare återhämta sig från exempelvis en informationsförlust. Centraliserade tjänster har dock svagheten att de är lättare att slå ut jämfört med decentraliserade eller i än större grad distribuerade system. Långtifrån alla systemägare väljer dock distribuerade systemlösningar, varken för tjänster eller för kommunikationssystem, då de är mer krävande att underhålla. Försvarsmaktens verksamhet skiljer sig från andra, genom att deras system måste kunna hantera allvarliga fysiska och logiska hot som kan få stor påverkan på deras system. En distribuerad lösning kan vara

lämplig för en del av Försvarsmaktens verksamhet. På så sätt kan verksamhet fortgå även om en delmängd av noder i systemet sätts ur spel.

Motiven att skapa ett distribuerat system varierar, från en målsättning att skapa en platt beslutsstruktur där alla noder är jämlika, till en strategi för resiliens i en i övrigt hierarkisk organisation. Således kan nätverket vara distribuerat även om organisationen som använder systemen är hierarkisk och dess metoder är centraliserade.

Blockkedjor är en teknik för att samla historik och ge spårbarhet i ett distribuerat system. Detta är den uppgift som normalt en central server har i ett nätverk. Den spårbarhet som blockkedjor ger är dock mer långtgående än vad lösningar för centrala servrar normalt erbjuder eller behöver. Blockkedjan är hela historiken för en aktivitet och det är verifierbarheten av blockkedjan som skapar tilltro till denna historik. I fallet med en central server är det tilltron till den auktoritet som äger servern som skapar tilltro.

I flera fall beskrivs blockkedjor i en distribuerad miljö där man inte vill eller kan lita på en central auktoritet. För Försvarsmaktens system kommer det sannolikt alltid att finnas en central auktoritet i systemet, även om nätet i sig självt kan vara uppbyggt på ett distribuerat sätt. Det är möjligt att tänka sig en situation där Försvarsmakten delar resurser med exempelvis andra länder i en koalition, men även i denna bidrar sannolikt respektive nation med information och ibland system för en viss funktionalitet. En annan svårighet för blockkedjetekniken i koalitioner är att den inte är interoperabel (Furlonger & Valdes 2017). För att dela blockkedja i en koalition måste ingående parter använda samma programvara eller plattform. I dagsläget och en del år framåt torde denna information inte befinna sig i blockkedjor och systemen inte vara blockkedjebaserade.

Blockkedjor beskrivs ha en hög grad av säkerhet. Detta är korrekt avseende spårbarhet och riktighet. En blockkedja innehåller verifierbara uppgifter vars riktighet garanteras av en serie digitala signaturer. Signaturerna skyddar inte uppgifter från att ändras, men säkerhetsställer att en förändring upptäcks om en användare väljer att verifiera dem. Av de egenskaper som beskrivs i informationssäkerhetstriaden konfidentialitet, riktighet och tillgänglighet så står riktighet i centrum för blockkedjor. Tillgängligheten i en blockkedja är också mycket god i och med att alla uppgifter sprids till alla deltagare som ingår i blockkedjan. Det finns dock inte något direkt stöd för konfidentialitet i själva blockkedjan, då alla uppgifter ska vara verifierbara. Konfidentialitet kan uppnås i det underliggande distribuerade nätverket genom att alla noder krypterar kanalen mellan sig själva och de som de kommunicerar med, men uppgifterna i blockkedjan är tillgängliga för alla inom nätverket.

Energikostnader och beräkningskraft är något som för tillfället diskuteras mycket när det gäller blockkedjor. Denna diskussion kan i princip helt och hållet härledas till Bitcoin och hur nya block skapas där. Bitcoin är ett globalt system som

bygger på att inte någon nod litar på en annan nod, bara på vad som kan verifieras. Inom Bitcoin finns även en konsensusmodell som alla användare delar, vilken säger att den som skapar ett nytt block måste visa att den löst ett givet och beräkningstungt problem. Det är denna problemlösning, att hitta ett värde som resulterar i en hashsumma som är lägre än ett visst förutbestämt värde, som främst orsakar energikostnaderna. Det finns andra globala konsensussystem som inte är lika kostsamma. Beräkningsproblematiken är dock ett sätt att reglera produktionshastigheten för nya block. I ett blockkedjesystem som inte genererar valuta och därmed inte har liknande incitament att skapa nya block, kan blockskapandet exempelvis hanteras genom schemaläggning, vilket helt tar bort konkurrenssituationen. I en avgränsad blockkedja kan ytterligare ett steg tas genom att en eller flera noder helt enkelt pekas ut som blockskapare och därmed enbart lyssnar efter transaktioner och skapar nya block efter behov.

Det finns dock ett inbyggt problem med blockkedjor som kan uppträda efter hand. Blockkedjan växer kontinuerligt vilket gör att den kan bli mycket lång och därmed volymkrävande. Block distribueras ut över nätverket när det skapas, men en användare behöver kunna skapa hela blockkedjan lokalt för att kunna verifiera innehållet. Livslängder på blockkedjor har inte diskuterats direkt, även om vissa farhågor uppmärksammats kopplat till risken för några mycket starka noder som har möjlighet att hantera hela blockkedjan. Farhågorna är kanske mest kopplade till valutasystem, men storleksproblemet kan uppkomma i alla blockkedjesystem med en hög blockproduktionstakt.

Prestandan i distribuerade lösningar är lägre än i centraliserade lösningar med kraftfulla servrar. Även om en hashfunktion går snabbt att beräkna så ingår det många hashsummor i en blockkedja som behöver verifieras. Smarta kontrakt tillför funktionalitet till en blockkedja, men denna funktionalitet är begränsad jämfört med en vanlig webbtjänst.

Sammanfattningsvis och med utgångspunkt från (Lo et al. 2017) ramverk för bedömning av blockkedjors lämplighet, kan sägas att de frågor som Försvarsmakten bör ställa sig innan en blockkedjelösning beaktas är

- Finns det behov av ett distribuerat system?
- Finns det ett starkt behov av spårbarhet?
- Finns det sekretessbehov?
- Finns det höga prestandabehov?

En distribuerad miljö har flera fördelar, främst när det gäller förmågan att hantera bortfall av noder utan att systemet som helhet kollapsar. I en miljö där det inte finns eller man inte vill ha en central auktoritet kan distribuerade system vara lämpliga som lösning. Kostnaden för distributionen kommer traditionellt i form av lägre prestanda och minskad spårbarhet. Blockkedjor löser problemet med spårbarhet i en distribuerad miljö och har dessutom en hög tillförlitlighet.

Referenser

Blowers, M. (2018). Blockchain as a New Framework for Unmanned Systems. I Meeting Proceedings of Mission Assurance for Autonomous Unmanned Systems. Lissabon, Portugal 16–17 oktober 2018. https://www.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-IST-166/$MP-IST-166-KN2P.pdf

Cadasta Foundation (2016). Blockchain for Land Administration: Hype or Substance? [blogg] *Cadasta*, 25 augusti. https://cadasta.org/blockchain-for-land-administration-hype-or-substance/ [2018-11-23]

Chan, J. (2018). LCQ5: Issuance of cryptocurrency. *The Government of the Hong Kong Special Administrative Region*, 30 maj. https://www.info.gov.hk/gia/general/201805/30/P2018053000387.htm?fontSize=1 [2018-11-23]

Connell, J. (2017). Making 'EthereRum' Distilled by a Bitcoin Miner. *Bitcoin.com*, 21 januari. https://news.bitcoin.com/south-florida-distillers-bitcoin/

Corda (u.å.). https://www.corda.net/

Estonian Defence Industry Association (2016). *Rangeforce from Estonia among top 10 of NCI Agency winners of the inaugural defence innovation challenge*. https://defence.ee/2016/06/rangeforce-from-estonia-among-top-10-of-nci-agency-winners-of-the-inaugural-defence-innovation-challenge/ [2018-11-30]

Furlonger, D. & Valdes, R. (2017). *Practical Blockchain: A Gartner Trend Insight Report* [id: G00325933]. https://haas.campusgroups.com/htc/get_file?eid=139611897577441f06512fc062b0a63e [2018-11-22]

Green, A. (2018). Trustworthy technology: the future of digital archive [blogg]. *The National Archives*, 5 juni. https://blog.nationalarchives.gov.uk/blog/trustworthy-technology-future-digital-archives/ [2018-11-23]

Gunnarson, H. & Hamber, E.M. (2018). *The future of blockchain in district heating – An investigation of possible blockchain applications for a Swedish district heating company*. Magisteruppsats, Skolan för industriell teknik och management (ITM), Energiteknik. Stockholm: Kungliga Tekniska Högskolan. https://kth.diva-portal.org/smash/get/diva2:1235834/FULLTEXT01.pdf

Greenspan (2017), Do you really need a blockchain for that? *Coin Center*, 26 juli. https://coincenter.org/entry/do-you-really-need-a-blockchain-for-that

Hyperledger [hemsida]. https://www.hyperledger.org/ [2018-11-23]

Independent Electoral and Boundaries Commission (IEBC) (2018). *The Commission's update on activities and electoral reform agenda*. https://www.iebc.or.ke/uploads/resources/hetNmcFb7S.pdf

ITAMCO (2017). ITAMCO to Develop Blockchain-Based Secure Messaging App for U.S. Military (2017). *PR Newswire*, 25 maj. https://www.prnewswire.com/news-releases/itamco-to-develop-blockchain-based-secure-messaging-app-for-us-military-300464063.html

ITIL (2011). http://www.pmweb.co.uk/wp-content/uploads/2012/01/ITIL_2011_Swedish_Glossary_v1.0.pdf

Jeffries, A, (2018). Governments Explore Using Blockchains to Improve Service, *The New York Times*, 27 juni. https://www.nytimes.com/2018/06/27/business/dealbook/governments-blockchains-services.html

Kairos Future (2018). *Fastighetsköp och lagfart genom en blockkedja – governance och juridik*. https://www.lantmateriet.se/contentassets/8d2b5d7647634c02a329b01e46e61071/publikation-swe-fastighetskop-och-lagfart-genom-en-blockkedja--governance-och-juridik-2018.pdf

Kulshrestha, S. (2016). Military Applications of Blockchain Technology. *CLAWS*, 23 november. http://www.claws.in/1666/military-applications-of-blockchain-technology-sanatan-kulshrestha.html

Lindström, K. (2018). Lantmäteriet klarar examensprovet – går att göra husköp i blockkedjan. *ComputerSweden*, 13 juni. https://computersweden.idg.se/2.2683/1.703915/lantmateriet-hus-blockchain

Lindström, K. (2018). GDPR gör blockkedjor olagliga – här är Gartners 10 strategiska spådomar. *CIO Sweden from IDG*, 7 november. https://cio.idg.se/2.1782/1.709869/blockkedja-gdpr-gartner

Kandaswamy, R., Valdes, R., Furlonger, D. & Chesini, F. (2017). *Predicts 2018: Top Predictions in Blockchain Business* [id: G00342298]. Gartner. https://static1.squarespace.com/static/581ca875f5e2313c7cbad236/t/5a0ef7a6f9619ae2897011bd/1510930343698/Predicts+2018+Top+Predictions+in+Blockchain+Business.pdf

Kasireddy, P. (2017). How does Ethereum work, anyway? [blogg]. *Medium*, 27 september. https://medium.com/@preethikasireddy/how-does-ethereum-work-anyway-22d1df506369

Kazeem, Y. (2018). Sierra Leone's electoral commission is pushing back on reports that blockchain powered its election. *Quartz Africa*, 21 mars. https://qz.com/africa/1234268/sierra-leone-blockchain-election-election-commission-denies-use-of-blockchain/

Konsumenternas bank- och finansbyrå (2010). http://www.rikstermbanken.se/visaTermpost.html?id=176783 (2018-11-23)

Laurelli, R., Örtengren, J., Ångström, L-J. T. (1990). *Ordbok för affärsfolk*.

Lo, S.K., Xu, X., Chiam, Y.K. & Lu, Q. (2017). Evaluating Suitability of Applying Blockchain. I *ICECCS'17, Proceedings of the 22nd International Conference on Engineering of Complex Computer Systems*. Fukuoka, Japan 5–8 november, ss. 158–161. DOI: 10.1109/ICECCS.2017.26

Lockheed Martin (2018). *2017 Sustainability Report – The Science of Citizenship*. https://www.lockheedmartin.com/content/dam/lockheed-martin/eo/documents/sustainability/Lockheed_Martin_Sustainability_Report_Full_2017.pdf

McCubbin, G. (2018). How to Build Ethereum Dapp (Decentralized Application Development Tutorial) [video]. *Dapp University*, 25 januari. https://www.youtube.com/watch?v=3681ZYbDSSk [2018-11-21]

Nationalencyklopedin (2018). Blockkedja. https://www.ne.se/uppslagsverk/encyklopedi/lång/blockkedja [2018-11-22]

NCI Agency (2016). NCI Agency innovation challenge. *Industry Relations*, 25 april. https://www.ncia.nato.int/NewsRoom/Pages/160425_Innovation.aspx

Netis Group Blog (2018). The difference between permissionless and permissioned networks [blogg]. *Medium*, 30 maj. https://medium.com/netis-group-blog/the-difference-between-permissionless-and-permissioned-networks-5acd05578676

Padron-McCarthy, T. (2005). *En webbkurs om databaser*. http://www.databasteknik.se/webbkursen/ [2018-11-23]

Pham, J. (2016). Can you create a blockchain without miners? *Quora*, 23 augusti. https://www.quora.com/Can-you-create-a-blockchain-without-miners

Pollock, D. (2018). Who Created the Story of Sierra Leone's Blockchain Election? *Cointelegraph*, 29 mars. https://cointelegraph.com/news/sierra-leones-fake-blockchain-election-hasnt-damaged-the-technologys-reputation

Popper, N. (2017). The Can’t-Lose Way for Your Business to Pop: Add Bitcoin to Its Name. *The New York Times*, 21 december. https://www.nytimes.com/2017/12/21/technology/bitcoin-blockchain-stock-market.html

Postordlistan (2012). http://www.rikstermbanken.se/visaTermpost.html?id=202650 (2018-11-23)

Redman, J. (2018). The ‘Crypto-Heater’ Mines Digital Currency While Heating Your Home. *Bitcoin.com*, 9 maj. https://news.bitcoin.com/the-crypto-heater-mines-digital-currency-while-heating-your-home/

Saini, V. (2018). ConsensusPedia: An Encyclopedia of 30 Consensus Algorithms - A complete list of all consensus algorithms [blogg]. *Hackernoon*, 2 juli. https://hackernoon.com/consensuspedia-an-encyclopedia-of-29-consensus-algorithms-e9c4b4b7d08f [2018-11-22]

Shin, L. (2018). Industries, Looking for Efficiency, Turn to Blockchains, *The New York Times*, 27 juni. https://www.nytimes.com/2018/06/27/business/dealbook/industries-blockchains-efficiency.html

Smart Dubai (u.å.) https://smartdubai.ae/initiatives/blockchain (2018-11-23)

Svenska Akademiens ordbok (SAOB) (2007). https://svenska.se/saob/?id=T_2241-0077.eL3X&pz=7 (2018-11-23)

Svenska Akademiens ordlista (SAOL) (2015). https://svenska.se/saol/?id=3246745&pz=7 (2018-11-23)

Sorkin, A.R. (2018). Demystifying the Blockchain, *The New York Times*, 27 juni. https://www.nytimes.com/2018/06/27/business/dealbook/blockchain-technology.html

Toyota, M. (2018). Mutually verifiable proof and the maturity of the Blockchain technology for “permissioned” chain – Opportunities and challenges. *Blockchain Technologies applied to Defence – Workshop*, Bryssel, Belgien 6 juni 2018. https://ecp.eda.europa.eu/W/Blockchain_Technologies_applied_to_Defence__Worksh/_layouts/15/WopiFrame.aspx?sourcedoc=/W/Blockchain_Technologies_applied_to_Defence__Worksh/Documents/Blockchain%20Technologies%20workshop%2006.06.18/3_Blockchain%20technology%20for%20%E2%80%9Cpermissioned%E2%80%9D%20chain_AIRBUS_Toyota.pdf

Törnvall, M. (2017). Största hotet mot bitcoin – en bättre version, *Svenska Dagbladet – Näringsliv*, 21 december. https://www.svd.se/storsta-hotet-mot-bitcoin--battre-bitcoin

Wong, J.I. (2016). Even the US military is looking at blockchain technology—to secure nuclear weapons. *Quartz*, 10 oktober. https://qz.com/801640/darpa-blockchain-a-blockchain-from-guardtime-is-being-verified-by-galois-under-a-government-contract/

Yaga, D., Mell, P., Roby, N. & Scarfone, K. (2018). *Blockchain Technology Overview* (Draft NISTIR 8202). Gaithersburg: National Institute of Standards and Technology.

FOI är en huvudsakligen uppdragsfinansierad myndighet under Försvarsdepartementet. Kärnverksamheten är forskning, metod- och teknikutveckling till nytta för försvar och säkerhet. Organisationen har cirka 1000 anställda varav ungefär 800 är forskare. Detta gör organisationen till Sveriges största forskningsinstitut. FOI ger kunderna tillgång till ledande expertis inom ett stort antal tillämpningsområden såsom säkerhetspolitiska studier och analyser inom försvar och säkerhet, bedömning av olika typer av hot, system för ledning och hantering av kriser, skydd mot och hantering av farliga ämnen, IT-säkerhet och nya sensorers möjligheter.

FOI
Totalförsvarets forskningsinstitut
164 90 Stockholm

Tel: 08-55 50 30 00
Fax: 08-55 50 31 00

www.foi.se