ARCADA

Blockkedjeteknik

Kim Andersson

Examensarbete

Informationsteknik

2017

EXAMENSARBETE	
Arcada	
Utbildningsprogram:	Informationsteknik
Identifikationsnummer:	5687
Författare:	Kim Andersson
Arbetets namn:	Blockkedjeteknik
Handledare (Arcada):	Göran Pulkkis
Uppdragsgivare:	Arcada

Sammandrag:

Blockkedjan, tekniken bakom Bitcoin och populariserad i dess introduktion, fungerar som en distribuerad databas och en publik huvudbok för transaktioner. Blockkedjetekniken har även andra implementeringar och användningsområden än endast Bitcoin. Syftet med arbetet är att beskriva blockkedjetekniken och några typiska blockkedjetil--lämpningar. I detta arbete presenteras blockkedjans struktur och säkerhet, publika, privata och tillståndsbelagda blockkedjor samt bevis på arbete, bevis på andel och andra konsensusmekanismer. Vidare beskrivs olika blockkedjor för kryptovalutor och andra implementeringar såsom smarta kontrakt, verifiering och medieadministration. Som källmaterial har använts artiklar och vitböcker publicerade på Internet. Programmering har utförts med Multichain för implementering av en privat blockkedja och samt med Blockcerts för digitala betyg. Blockkedjetekniken har redan många användningsområden samt nya förslag och idéer duggar tätt. Bitcoin riskerar dock att hamna i bakgrunden på grund av dess användares motvillighet att ta i bruk nyare, snabbare och mer funktionsrika blockkedjeimplementeringar.

Nyckelord:	Blockkedja. Kryptovaluta. Distribuerad databas. Publik huvudbok. Datautvinning. Smarta kontrakt.
Sidantal:	44
Språk:	Svenska
Datum för godkännande:	1.6.2017

DEGREE THESIS	
Arcada	
Degree Programme:	Information Technology
Identification number:	5687
Author:	Kim Andersson
Title:	Blockchain Technology
Supervisor (Arcada):	Göran Pulkkis
Commissioned by:	Arcada University of Applied Sciences

Abstract:

The blockchain, the technology behind Bitcoin and popularized in its introduction, functions as a distributed database and a public ledger for transactions. Blockchain technology has also other implementations and applications than Bitcoin. The purpose of this thesis work is to describe blockchain technology and some typical blockchain applications. In this thesis work is presented the structure and security of a blockchain, public, private, and permissioned blockchains as well as proof of work, proof of stake, and other consensus mechanisms. Different blockchains for crypto currency and other implementations such as smart contracts, verification, and media administration are also described. Literature sources are articles and white papers published on the Internet. Programming has been carried out with Multichain to implement a private blockchain and with Blockcerts for digital certificates. Blockchain technology has already many application areas and new suggestions and ideas are streaming in. Bitcoin itself risks falling behind due to its users' reluctance to deploy newer, faster and more feature rich blockchain implementations.

Keywords:	Blockchain. Crypto Currency. Distributed Database. Public Ledger. Data Mining. Smart Contracts.
Number of pages:	44
Language:	Swedish
Date of acceptance:	1.6.2017

INNEHÅLL

Figurer / Figures

Definitioner

Proof of Work – Bevis på arbete
Proof of Stake – Bevis på andel
Runtime Environment - Exekveringsmiljö
Data Miner – Datautvinnare
PKI – Public Key Infrastructure – Publika nyckelns infrastruktur
Cryptocurrency – Kryptovaluta
IoT – Internet of Things – Sakernas Internet
Nonce – Slumpmässigt värde
DDoS – Distributed Denial of Service – Fördelat nekande av tjänst (Överbelastningsat--tack)

1 INLEDNING

Blockkedjan, eller Blockchain, mest känd som tekniken bakom kryptovalutan Bitcoin, fungerar som en distribuerad huvudbok och databas. Blockkedjetekniken är dock inte bunden till endast kryptovalutor. Nätaktivister lyfter gärna fram den öppna källkoden, datasäkerheten, anonymiteten och svårigheten att spåra personer, dvs. egenskaper förknippade med blockkedjans decentraliserade struktur. Finansbranschen hoppas kunna göra stora inbesparningar genom att överge gamla system och tillämpningar. Statliga ämbeten och institutioner kan vinna mycket på att flytta kontrakt, bevis på ägande och verifiering till blockkedjan.

Då dagens värld i hög grad fungerar på tillit till en central auktoritet, såsom t.ex. en certifikatutfärdare eller bank, så fungerar blockkedjor i många fall i enlighet med distribuerad konsensus. Distribuerad konsensus betyder att användarna av nätverket gemensamt kommer överens om ett händelseförlopp. Detta händelseförlopp skrivs upp i en gemensam huvudbok där alla händelsetransaktioner inom en viss tidsram samlas ihop till ett block. Varje block refererar till det föregående blocket. På så sätt måste en illvillig användare manipulera över hälften av nätverket för att kunna ändra det registrerade händelseförloppet.

1.1 Syfte

Syftet för detta arbete är att beskriva blockkedjetekniken och några typiska blockkedjetillämpningar.

1.2 Avgränsningar

Arbetet beskriver inte alla varianter av blockkedjetekniken och beskrivningen av blockkedjetillämpningar är inte heltäckande.

2 RELATERADE ARBETEN

Crosby et al. (2015) presenterar blockkedjan och Bitcoin, dess teknik och tillämpningar inom och utanför finanssektorn.

3 GRUNDLÄGGANDE TEKNIK

Blockkedjan fungerar som en distribuerad databas och publik huvudbok som hela tiden uppdateras. Den är distribuerad så att alla noder har tillgång till hela databasen och alla följer den länken som har kommit längst och består av block som innehåller data, huvudsakligen om transaktioner. Varje gång en transaktion sker meddelar sändande part till alla noder i nätverket på en s.k. peer-to-peer basis. Då läggs transaktionen till i följande block. När blocket är skapat skickas det ut till hela nätverket, åter på en peer-to-peer basis, och valideras av alla andra noder innan det läggs till i kedjan. Blocket innehåller även det föregående blockets hash-summa som referens för att försvåra försök att manipulera eller ändra block. Ursprungsblocket, Genesis Block, som är det första blocket i en kedja och har ingen föregångare, är därmed det enda blocket som inte refererar till föregångaren. Det är nästan alltid hårdkodat i mjukvaran. Bitcoins ursprungsblock skapades den 3 januari 2009 klockan 20:15:05 (Blockexplorer.com).

Nodtyper

- **Datautvinnare**
  Datautvinnare (eng. Miner) skapar nya block.
- **Full nod**

Har tillgång till hela blockkedjan och medverkar i nätverket och dess P2P-funktion. Måste inte vara datautvinnare.

- **Lättviktsklient**

  Har endast laddat ner och verifierat delar av blockkedjan som är relevanta för dess funktioner och litar på att mer kraftfulla fulla noder filtrerar och tillhandahåller information som är relevant för dem i ett s.k. Simplified Payment Verification (SPV) -läge. Exempel är Bitcoin-klienter i mobila enheter.

3.1 Blockkedjans struktur

I ett block sparas information om alla händelser som har skett sedan det föregående blocket skapades (se Figur 1):

- **Tidsstämpel**

  Tiden då blocket skapades.

- **Föregående blocks hash-summa**

  Hash-summan av föregående blockhuvud. Hash-summan binder blocket till det föregående i kedjan.

- **Merkle Root**

  Alla transaktioner samlas ihop, kopieras och hash-summorna uträknas. Därefter uträknas hash-summorna av transaktioner i par tills endast en hash-summa återstår.

- **Nonce**

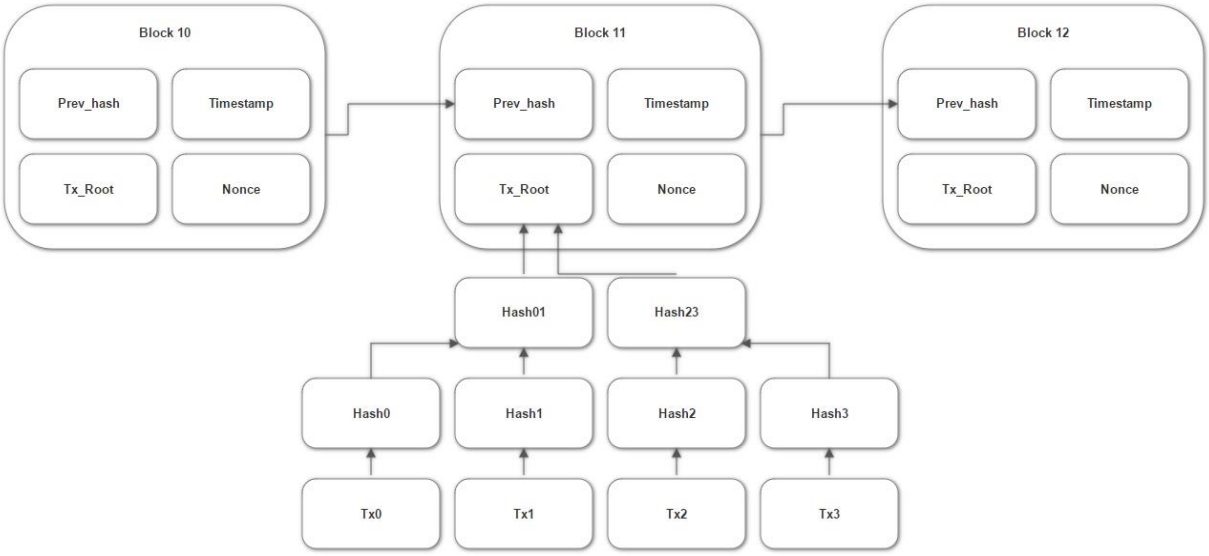
  Ett slumptal som läggs till blockhuvudet för att få fram en hash-summa med rätt svårighetsgrad.

- **Svårighetsgrad**

  Blockets svårighetsgrad används för att styra hur ofta ett nytt block kan skapas i ett nätverk som använder bevis på arbete (eng. proof of work) som konsensusmekanism.

I Bitcoin-nätverket justeras svårighetsgraden efter 2016 nya block varannan vecka beroende på beräkningskraften i nätverket för att bibehålla intervallen 10 minuter mellan nya block. Blockets svårighetsgrad, som kallas mål (eng. target), definieras av antalet nollbitar blockhuvudets hash-summa måste börja med. Blockhuvudets hash-summa skapas med två beräkningar. Först beräknas hash-summan på blockhuvudet, sedan beräknas den slutliga hash-summan av blockhuvudets hash-summa. För att skapa en behövlig

hash-summa testas ett nytt slumpmässigt värde (eng. nonce) i blockhuvudet tills ett tillfredsställande resultat har uppnåtts. Datautvinnaren meddelar nätverket när hen har uppnått målet varefter de andra noderna i nätverket lätt kan validera resultatet. Den uträknade hash-summan används sedan som referens i följande block. Ifall noll-bitarnas andel är *n* behövs i genomsnitt 2^n tester för att hitta en önskad hash-summa. I datautvinningen måste 2^n hash-summor således kunna beräknas under 10-minuters tid för att för att ett nytt block skall kunna skapas var 10 minut. Svårighetsgraden beräknas med $(10/60)\times(3600\times \ hashfrekvens)/2^{32}$. Antalet noll-bitar kan beräknas med $log_2(svårighetsgraden) + 32$. Hash-frekvensen (hash-summor per sekund) (eng. hash-rate) nätverket då måste prestera för att skapa ett nytt block var tionde minut beräknas med $2^n/600s$.



Figur 1: Bitcoin-block (Wander 2013)

Operationskoden (eng. Operation Code, OPCODE) OP_RETURN markerar data som inte utnyttjas av transaktioner och används därför för att spara meddelanden, data eller hash-summor som bevis på ägande. Bitcoin stöder för tillfället 80 byte långa OP_RETURN-meddelanden.

3.2 Blockkedjans säkerhet

Blockkedjan bygger på kommunikation mellan noder, de delar information om nya transaktioner, verifierade transaktioner och nya block. Beroende på vilken typ av block-

kedja, publik, privat eller tillståndsbelagd och typen av konsensusmekanism, bevis på arbete, bevis på andel osv. varierar förutsättningarna. En publik blockkedja med bevis på arbete som den som Bitcoin använder blir säkrare ju fler användare ansluter sig och deltar i kedjan. Problemet är att bevis på arbete kräver beräkningskraft som i sin tur kräver energi i form av elström. Detta leder till mera centralisering eftersom stora Bitcoinfarmer med för ändamålet specialutvecklad hårdvara har byggts upp och konkurrerat ut många små aktörer. I privata blockkedjor uppstår inte samma problem, men istället måste användarna lita mer på varandra.

Ett problem, främst för kryptovaluta, är att varje användare måste hålla reda på sin privata nyckel för att kunna signera transaktioner. En borttappad privat nyckel betyder att en användare inte kan använda valutan låst till sig och transaktioner med stulna nycklar ser inte annorlunda ut på blockkedjan. Detta är inte ett problem med blockkedjans säkerhet utan med användarnas privata säkerhet. Koden bakom DAOn och inte någon lucka i Ethereums säkerhet var orsaken till den stora läckan år 2016. Ethereumutvecklarnas beslut att ändå justera blockkedjan var därför kontroversiellt.

3.2.1 Säkerhetsstruktur

Säkerheten i en blockkedja uppstår av att varje block bygger på det föregående blocket. Om en nod försöker ändra på ett block i efterhand så ändras blockets hash-summa, vilket i sin tur ogiltigförklarar det och alla följande block. Då förkastas blocken av nätverket. Endast block som uppfyller kraven ställda av nätverket läggs till i kedjan. Som hash-algoritm används till exempel SHA-256 (Secure Hash Algorithm 2 med 256 bitar). Om en attackerare vill ändra på ett block i Bitcoins blockkedja i efterhand måste hen därför ha tillgång till minst hälften av nätverkets totala beräkningskraft för att hinna beräkna om alla block efter det hen ändrat och komma först i kedjan. Varje gång ett nytt block skapas ökar arbetskostnaden för att ändra på ett block. Om två block skapas samtidigt av olika noder lever de sida vid sida tills nästa block skapas. Det block som fungerar som förälder till följande block utses som vinnare och dess sida av kedjan fortsätter. (Nakamoto 2008)

3.2.2 Attackresistens

För att motstå och avskräcka attacker samt för att skapa förtroende för blockkedjan används olika former av ekonomiska bevis som kräver en mycket större insats för att skapa block än för att verifiera block. Bevis på arbete (eng. proof of work) används bland annat i Bitcoins blockkedja. Datautvinnare (eng. data miners) använder sin beräkningskraft för att lösa kryptografiska problem. Den vinnande lösningen används som bevis på rätten att skapa nya block med jämna mellanrum. Datautvinnarna beräknar hash-summan på blockets data förlängt med en s.k. nonce. Sedan beräknas hash-summan igen på den föregående hash-summan. Noncen ändras och allting beräknas på nytt tills en summa med rätt svårighetsgrad, t.ex. att summan måste vara tillräckligt liten, har uppnåtts. I Bitcoin skapas ett nytt block ungefär var tionde minut. För att hålla takten jämn justeras svårighetsgraden vart 2016 block beroende på hur mycket beräkningskraft som finns tillgängligt i nätverket. En attack blir olönsam på grund av den höga beräkningskraft som krävs. Attackeraren behöver ha tillgång till en majoritet av beräkningskraften i nätverket. Kostnaden för hårdvaran och elströmmen som behövs för att uppnå tillräcklig beräkningskraft ökar ju flera ärliga datautvinnare som finns i nätverket. Datautvinnaren som först lyckas lösa hash-summan för att skapa ett nytt block belönas med ett antal Bitcoins. Flera datautvinnare kan gå samman i en gemenskap (eng. mining pool) för att ha en större chans att vinna. Då delas belöningen upp mellan alla noder i gemenskapen.

I Ripple används RPCA (Ripple Protocol Consencus Algorithm) för att skapa ett nytt block med ett par sekunders mellanrum. Valideringsnoderna i nätverket kommunicerar med utvalda validerare (eng. Chosen Validators) på sina unika nodlistor (eng. Unique Node List, UNL) och uppdaterar sina förslag tills 80 % av noderna på listan håller med. Sedan beräknar valideringsnoderna hash-summan på sina kandidatblock. Ett block tas med i kedjan när tillräckligt många valideringsnoder har fått samma hash-summa för detta block. (Schwartz, Youngs, Britto 2014)

Andra sätt för att motstå attacker och skapa konsensus i blockkedjan är bl.a. bevis på andel (eng. proof of stake) och anförtrott bevis på andel (eng. delegated proof of stake). Istället för att ackumulera beräkningskraft för att skapa nya block används kryptovalu-

tan i sig själv. Ju större andel av kryptovalutan en enskild användare har desto större chans att skapa det nya blocket har hen. De största innehavarna av kryptovalutan har mest att förlora på en komprimerad blockkedja. En attackerare måste ha minst hälften av den totala kryptovalutan i blockkedjan för att kunna ändra på blockkedjan. När anförtrott bevis på andel används för att uppnå konsensus delegeras skapandet och verifierandet av nya block till vissa noder beroende på deras andel i kryptovalutan och deras historia i blockkedjan. Depositionsbaserat bevis på andel (eng. depostit-based proof of stake) är en vidareutveckling där användare måste deponera kryptovaluta till ett tidslåst konto innan de får delta i koncensusprocessen. Om de missköter sig konfiskeras den insatta valutan. (BitFury 2015)

3.2.3 Publika, privata och tillståndsbelagda blockkedjor

En publik blockkedja är öppen för alla som vill läsa, göra transaktioner och delta i koncensusprocessen för att administrera blockkedjan. En privat blockkedja kan vara låst till en eller flera organisationer. Den har förbestämda noder som måste validera och signera blocken för att de skall kunna läggas till i kedjan. Tillståndsbelagda blockkedjor har bestämda användare med tillstånd att skapa nya block eller utfärda nya kontrakt på blockkedjan. Tillståndsbeläggning försvårar spamutskick och ökar blockkedjans prestanda.

4 BLOCKKEDJOR FÖR KRYPTOVALUTA

1982 Introducerade David Chaum sin idé för en kryptovaluta med blinda RSA-signaturer (eng. Blind Signatures). I slutet av 80-talet flyttade han till Nederländerna där man hade börjat använda chipkort för att eliminera problem med nattliga räder mot bensinstationer, vilket ledde till utveckling av chipkort för direkt debitering från kundens bankkonto. Chaum grundade företaget DigiCash och produkten e-cash, men hamnade i strul med den nederländska centralbanken. Chaum blev erbjuden 180 miljoner dollar utav Microsoft men nekade. Företaget gick i konkurs 1998. Samma år hade Nick Szabo en idé om en decentraliserad digital valuta, Bit Gold, där användare lät datorer lösa kryptografiska pussel som registrerades i en huvudbok. Varje löst pussel blev en del av följande pussel, lika som blockkedjans bevis på arbete. Bit Gold blev aldrig populärt. Ett företag i Florida skapade en digital valuta nämnd e-gold. Användare kunde skicka in

värdemetaller och i gengäld få e-gold. Användare kunde göra direkta transaktioner med andra användare och kunde växla e-gold till dollar eller guld. År 2006 hade e-gold hand om transaktioner till ett värde över två miljarder dollar. E-gold hamnade i trubbel med myndigheterna eftersom tjänsten mer och mer blev använd för penningtvätt. Den 31 oktober 2008 introducerade
Sataoshi Nakamoto Bitcoin som sedan lanserades i början av år 2009. (Griffith 2014)

4.1 Bitcoin

Bitcoin populariserade blockkedjan genom att använda tekniken för en öppen huvudbok för transaktioner av Bitcoin. Noder som är med och använder sin beräkningskraft för att skapa block är belönade med ett visst antal Bitcoins varje gång ett nytt block skapas. Svårighetsgraden ändras varannan vecka för att hålla takten i kedjan så att ett nytt block skapas ungefär var tionde minut. Bitcoin använder hash-algoritmen SHA-256. För att använda Bitcoin krävs en Bitcoin-plånbok (eng. ”Bitcoin wallet”) med en unik adress, se Figur 2. I plånboken sparas adressens privata nyckel som kan användas för att signera transaktioner. För en standard transaktion mellan två parter krävs det att sändaren får tag i mottagarens publika nyckel, den skickas oftast hashad som en Bitcoin-adress. Sändaren kan nu skapa en output som tillåter ägaren av den privata nyckeln som hör ihop med mottagarens Bitcoin-adress att spendera summan. När outputen är skapad så meddelar sändaren nätverket om transaktionen och datautvinnarna validerar den och placerar den i ett block. Mottagarens plånbok visar nu att summan kan spenderas.

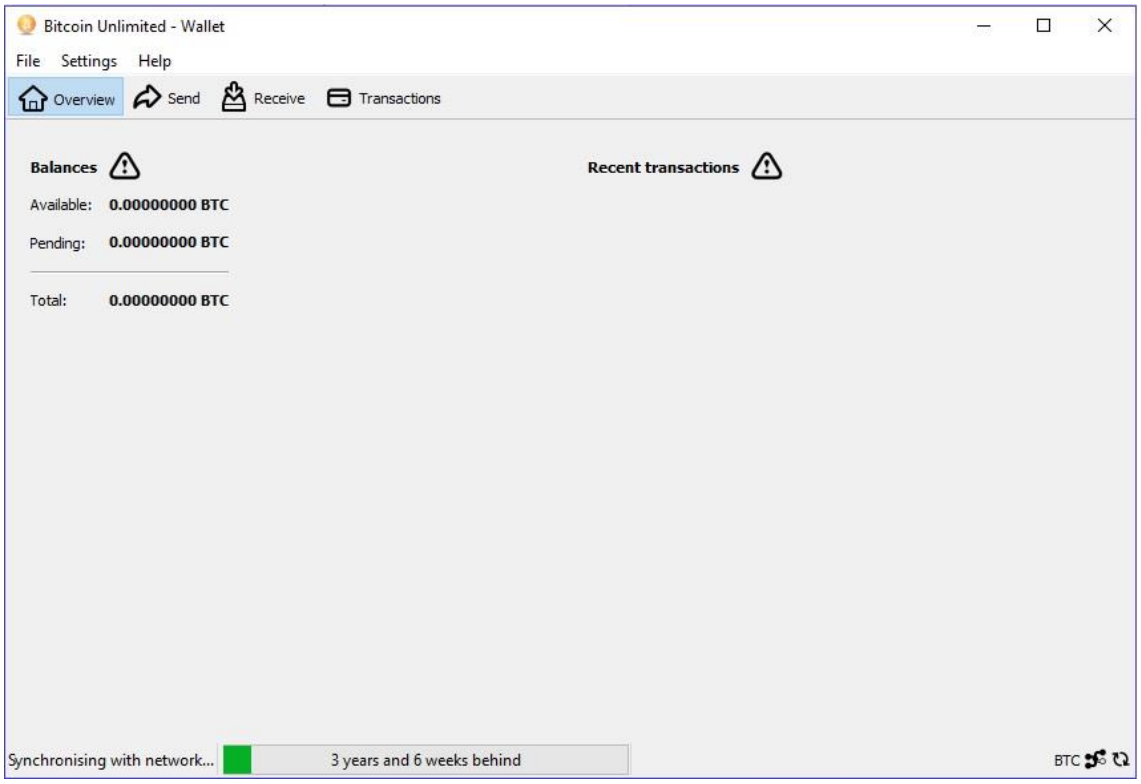
4.1.1 Plånböcker

Plånböcker måste klara minst en av funktionerna:

- Distribution av publik nyckel
- Signering av transaktion
- Ha tillgång till nätverket

De vanligaste plånböckerna är s.k. full-service plånböcker som klarar av alla funktioner, dvs. generera privata och publika nycklar, distribuera publika nycklar, övervaka nätverket för transaktioner, skapa och signera transaktioner som spenderar tillgänglig valuta samt meddela nätverket om signerade transaktioner. Den största nackdelen med full-

service plånböcker är att de sparar privata nycklar på en enhet ansluten till Internet t.ex. användarens dator eller smarttelefon. De flesta programmen krypterar plånboksfilerna som innehåller de privata nycklarna för ökad säkerhet. Det finns också online-plånböcker där användarens nyckelpar sparas på en server på Internet. Då användaren vill använda plånboken loggar hen in på online-tjänsten och har därmed tillgång till sina nycklar. Den största nackdelen är att användarens privata nyckel finns ansluten till Internet och om tjänsten hen använder inte finns tillgänglig eller går under så förlorar användaren också möjligheten att spendera sin valuta. Om tjänsten blir hackad eller missbrukad kan detta leda till att användarens privata nyckel hamnar i fel händer.



Figur 2: Bitcoin-plånbok synkroniserar med blockkedjan.

För ännu bättre säkerhet används skilda plånböcker för signering. I dessa fall körs de oftast på en enhet som inte är ansluten till Internet eller på dedikerad hårdvara. Då har användaren en skild nätverksansluten plånbok som distribuerar publika nycklar och övervakar nätverket för transaktioner. När användaren vill spendera valuta måste hen först skapa en transaktion, sedan flytta över den på bärbar media till enheten som inte är ansluten till Internet för signering av transaktionen med hens privata nyckel. Efter detta

måste användaren flytta tillbaka den signerade transaktionen till den Internet-anslutna enheten för att sända ut transaktionen över Bitcoin-nätverket. Säkerheten i dessa system är mycket högre än i full-service plånböcker men involverar flera steg och mera krångel för användaren då hen måste ha tillgång till en enhet som aldrig är ansluten till Internet för att kunna spendera valuta.

Hårdvaruplånböcker är dedikerade enheter för lagring av nycklar och signering med dessa. De kommer oftast i format som liknar USB-minnespinnar. När användaren vill spendera valuta så ansluter hen hårdvaruplånboken till sin dator. Hårdvaruplånboken kräver oftast en pinkod för användning. Den största nackdelen med hårdvaruplånböcker är den dedikerade hårdvaran som användaren måste inhandla för att kunna spendera sin valuta.

En annan form av plånböcker är pappersplånböcker, som är s.k. offline-plånböcker. Då sparas nycklarna, oftast i som QR-koder, utprintade på papper eller annan fysisk media. För att ta emot och spendera valuta matar användaren in sin publika och privata nyckel i någon lämplig mjukvara eller tjänst.

4.2 Litecoin

Litecoin är ett senare tillägg till världen kring kryptovaluta. Ett nytt block skapas med ungefär två och en halv minuts mellanrum och gör därmed Litecoin snabbare än Bitcoin. I motsats till Bitcoin som använder SHA-256 som hash-algoritm använder Litecoin istället Scrypt. Scrypt inkorporerar SHA-256 men är mera seriestrukturerad och föredrar stora mängder snabbt arbetsminne vid beräkningar. Detta skall enligt skaparna bakom Litecoin minska kapprustningen med applikationsspecifika integrerade kretsar (eng. Application Specific Integrated Circuit, ASIC) byggda speciellt för datautvinning. (Coindesk.com 2014)

4.3 Dogecoin

Dogecoin introducerades först som ett skämt i december 2013, men ett användarsamfund skapades snabbt runt kryptovalutan. År 2014 samlade Dogecoin-entusiaster ihop

25000 dollar för att skicka Jamaicas boblag till vinterolympiaden i Sotji. De samlade också pengar för den indiska rodelåkaren Shiva Keshavan. Doge4Water var ett projekt för att samla in 30000 dollar i donationer för att gräva en brunn i Kenya. Användarsamfundet lyckades t.o.m. samla ihop pengar för att sponsra NASCAR-föraren Josh Wise. Han körde en bil utsmyckad med Dogecoin-dekaler i loppet Aaron's 499 vid Talladega Superspeedway i maj 2014. (Hern 2014)

4.4 Monero

Monero är en kryptovaluta fokuserad på säkerhet, datasekretess, skalbarhet och decentralisering. Monero betyder mynt på språket Esperanto och lanserades 18.04.2014 som BitMonero. Fem dagar senare förkortades namnet till endast Monero. Den baserar sig inte på Bitcoin utan på protokollet CryptoNote för att ytterligare kunna fördunkla blockkedjan. För att uppnå anonymiserade transaktioner använder CryptoNote en modifierad version av algoritmen Diffie-Hellman där sändaren använder den ena av mottagarens två publika nycklar samt slumpmässig data för att skapa en delad hemlighet och den andra nyckeln tillsammans med den delade hemligheten för att beräkna en engångsdestinationsnyckel som utmatas av transaktionen på blockkedjan. Mottagaren går igenom alla transaktioner och kan beräkna engångsnycklarna till sina transaktioner med sina privata nycklar. Hen kan sedan signera transaktioner med dem för att spendera valutan i transaktionerna. För att ytterligare försvåra spårning av transaktioner använder CryptoNote ringsignaturer där flera användares publika nycklar används för att signera en transaktion. Sändaren kan bestämma, på bekostnad av ökade transaktionsavgifter, hur många signaturer ringen skall ha. Om n är antalet signaturer i ringen och $n = 2$ kan en observatör identifiera hen som sändare med 50 % sannolikhet, för $n = 100$ med 1% sannolikhet osv. CryptoNote använder en mera minneskrävande algoritm som bevis på arbete än Bitcoin för att minska fördelen för datautvinning med specialutvecklad hårdvara, s.k. ASIC (eng. Application Specific Integrated Circuit). (van Saberhagen 2013)

4.5 Dash

Kryptovalutan Dash skapades som XCoin den 18 januari 2014, bytte namn till Darkcoin den 28 februari 2014 och sedan igen till Dash den 25 mars 2015. Dash använder sig av

en kedjad hash-algoritm, X11, för beräkning av bevis på arbete. X11 är en serie av elva olika hash-algoritmer; blake, bmw, groestl, jh, keccak, skein, luffa, cubehash, shavite, simd och echo. X11 används för att hålla datautvinningen decentraliserad. Användare med vanliga datorer kan medverka i datautvinningen eftersom specialutvecklad hårdvara, s.k. ASIC (eng. Application Specific Integrated Circuit), är svår att utveckla för X11 samt eftersom X11 är en kedja utav flera hash-algoritmer så faller inte systemet ifall en utav dem skulle knäckas. Dash är den tredje mest handlade kryptovalutan i början av 2017 efter Bitcoin och Ethereum. (Duffield, Diaz)

4.6 Tether

Tether försöker införa traditionella valutors stabilitet på kryptovalutamarknaden. Användare kan deponera traditionell valuta, amerikanska dollar, euro eller yen, till företagets bankkonto och i gengäld få s.k. tethers i valörerna USDT, EURT eller JPYT. Tether fungerar på Bitcoins blockkedja och använder bevis på reserv (eng. Proof of Reserves) för att avvärja försök till fusk. I bevis på reserv måste antalet tether på blockkedjan alltid motsvaras av samma antal traditionell valuta i banksaldot. (Tether Limited 2017)

5 BLOCKCHAIN 2.0

Blockchain 2.0 är inte en egentlig produkt, utan en benämning på alla nyare blockkedjor som utökar funktionaliteten över det som Bitcoin erbjuder. Bitcoins blockkedja används som huvudbok över alla transaktioner i Bitcoin-nätverket. Blockkedjor som tillåter att man sparar mera än endast transaktionsdata i nätverket brukar ha namnet Blockchain 2.0 eller Bitcoin 2.0.

En del blockkedjor med mera funktionalitet än Bitcoin men ändå hänger ihop med Bitcoin kallas sidokedjor. De är egna kedjor som är sammanflätade med Bitcoin för att tillgängliggöra annan funktionalitet utan att användare och noder behöver vara oroliga över riskerna med en liten blockkedja och en liten kryptovaluta, en s.k. altcoin. På så sätt används Bitcoins storlek och säkerhet för att skapa ny funktionalitet och nya produkter.

5.1 Smarta kontrakt

En av de mest intressanta implementationerna av Blockchain 2.0 är s.k. smarta kontrakt. De är små program som fungerar på IF-THEN basis för att utföra någonting automatiskt. Enligt Nick Szabo som myntade termen Smart Contract så fungerar ett smart kontrakt i sin enklaste form som en varuautomat, men kan användas till nästan vad som helst för att utlösa en eller flera händelser utan behov av en tredje part. (Szabo 1997)

Ett hypotetiskt exempel är ett digitalt säkerhetssystem för bilar där bilens ägare har tillgång till rätta kryptografiska nycklar för användning av fordonet:

1. Ett lås för att släppa in ägaren och utesluta tredje part.
2. En bakdörr för att släppa in krediteraren.
3. A) Krediterarens bakdörr öppnas endast om ingen betalning har gjorts inom utsatt tid.
   B) Den sista avbetalningen stänger bakdörren permanent.

Om fordonet används som säkerhet för ett lån behövs för långivaren även en bakdörr som aktiveras och ger tillbaka kontrollen över fordonet om otillräckliga avbetalningar görs. När hela skulden är avbetalad stängs bakdörren för gott. Det behövs protokoll som räknar med användning och umbäranden, eftersom det vore grymt att frånta användarens rättigheter till fordonet mitt under färd på motorväg. (Szabo 1997)

5.2 Ethereum

Ethereum är en blockkedja helt fokuserad på smarta kontrakt där dess kryptovaluta, kallad Ether, fungerar som polletter. Inom Ethereum kallas ett smart kontrakt för DApp (Decentralized App) som kan köras på en server eller direkt på en Ethereum-nod. Ethereum Virtual Machine (EVM), är exekveringsmiljön för smarta kontrakt i Ethereum. När ett kontrakt körs krävs det betalning med kryptovaluta kallad Gas. En Gas är en bråkdel av en Ether och fungerar som betalning till noderna, som jobbar på att bygga vidare på blockkedjan. Antalet Gas ett kontrakt kostar att exekvera beror på hur mycket arbete noderna behöver utföra för att lägga till transaktionen i blockkedjan. (ethdocs.org 2016)

Smarta kontrakt i Ethereum kodas i ett av tre språk för att sedan kompileras till Ethereum Virtual Machine bytecode:

- Solidity
  Liknar JavaScript och är det mest använda.
- Serpent
  Liknar Python.
- LLL
  Liknar Assembly.

Läckan i Slock.it's DAO (Decentralized Autonomous Organization) som uppdagades den 17.06.2016 var inte ett fel i blockkedjan eller kryptovalutan Ethereum utan en bristfällighet i DAO-koden vilket gjorde det möjligt för attackeraren att anropa funktionen split och flytta över ett stort antal Ether till en barn-DAO. Två lösningar föreslogs. Den första (en s.k. soft fork) var att svartlista alla transaktioner från DAOn och dess avkommor. Den andra (en s.k. hard fork) var att göra ändringar i koden för att kunna återta bestulet kapital. I juli godkändes en hard fork av en majoritet av datautvinnarna, medan de som motsatte sig uppdateringen fortsatte på vad som nu kallas Ethereum Classic. Senare gjorde båda en hard fork igen för att åtgärda DDOS-problem. (Georgiev 2016)

Ethereum planerar att ersätta bevis på arbete med bevis på andel som koncensusprocess. (Back 2017)

5.3 Mikrobetalningskanaler

För att kunna göra betalningar som annars vore för små för att vara lönsamma kan parter öppna en kanal mellan sig i vilken den ena parten eller båda parter låser kryptovaluta i ett tidsbundet smart kontrakt. Öppnandet av kanalen registreras på blockkedjan. För att göra en transaktion krävs det att vardera parten signerar den med sin privata nyckel. Transaktioner kan utföras tills tiden på kontraktet tagit slut eller om en part eller båda parter har beslutat att stänga kanalen. När kanalen stängs publiceras slutsumman på blockkedjan. För att undvika väntetiderna i öppnandet av nya kanaler kan Lightning Network skapa ett nätverk av kanaler där användare kan utföra transaktioner med

varandra genom redan öppnade kanaler. Lightning Network opererar på Bitcoins blockkedja. (Stark 2016)

5.4 Counterparty

Counterparty inför extra data i OP_RETURN-delen av en Bitcoin-transaktion för att ge andra tjänster tillgång till Bitcoin-kedjans säkerhet och stabilitet. Användare exekverar vid sidan om Bitcoin också Counterpartys mjukvara som kodar in transaktioner i OP_RETURN. OP_RETURN tillåter 80 bytes av arbiträr data att skickas med en transaktion. Counterpartys mjukvara tolkar informationen och använder den för att spara information om andra händelser än rena Bitcoin-transaktioner (Dermody 2016). Counterparty implementerar också Solidity, Ethereums mest populära kodspråk för smarta kontrakt, för att tillgängliggöra smarta kontrakt på Bitcoins blockkedja.

5.5 Rootstock RSK

Rootstock är en sidokedja till Bitcoin som möjliggör smarta kontrakt samt snabbare transaktioner i större volymer. I Rootstocks sidokedja skapas ett nytt block var 30 sekund och 300 transaktioner avklaras per sekund (Lerner 2015), vilket är jämförbart med PayPals transaktionsfrekvens. Rootstock skall emellertid uppgraderas till 1000 transaktioner per sekund. Som jämförelse hanterar Visa Europe över 2000 transaktioner per sekund under julrushen (Visa Europe 2017).

5.6 Ripple

Ripple fokuserar på banker och andra företag i finansbranschen för att erbjuda direkta lösningar utan mellanhänder. Kryptovalutan inom Ripple är XRP. En av XRPs funktioner är att fungera som mellanvaluta för växling. Ripple använder RPCA (Ripple Protocol Concensus Algorithm) då nya block skapas. (Ripple.com 2017)

5.7 Hyperledger

Hyperledger är Linux Foundations satsning tillsammans med andra intresserade företag i branschen, bl.a. IBM och Intel, för att skapa en allmän, öppen och decentraliserad lösning. (Hyperledger.com 2017)

Data från IBMs Watson IoT-plattform kan sparas i en blockkedja. Denna kombination skall enligt IBM ge fördelar inom bland annat leveranskedjor och regelefterlevnad. (Gutierrez, Khiznyak 2017)

Sawtooth Lake är Intels projekt för en modulär plattform för distribuerade huvudböcker. Bevis på förfluten tid (eng. Proof of Elapsed Time, PoET) är ett protokoll som använder en betrodd exekveringsmiljö (eng. Trusted Execution Environment, TEE) såsom Intels Software Guard Extension (SGX) för att validera nya block genom att anropa en betrodd timerfunktion garanterad av TEEn. Intels Software Guard Extension använder skyddade exekveringsenklaver för att motstå manipulering och kan köras på alla Intelprocessorer som stöder SGX. (Intel Corporation 2017)

5.8 Multichain

Multichain är en plattform för privata kedjor såsom t.ex. ersättning av vanliga decentraliserade databaser, flerpartsaggregation och journalföring mellan organisationer. Multichain finns tillgängligt för Linux, Microsoft Windows och Apple Mac servrar. (Greenspan 2015)

5.9 Microsoft Project Bletchley

I juni 2016 lanserade Microsoft sitt eget blockkedjeprojekt byggt på öppen källkod, Project Bletchley, för att skapa en egen standard för smarta kontrakt och transaktioner. Projektet är planerat att agera mellanvara mellan applikationer och olika blockkedjor, bl.a. Hyperledger och Ethereum. I projektet introducerades också Cryptlets, kod som är bunden till men inte körs på blockkedjan utan i molnet och kan ge utökad funktionalitet i smarta kontrakt. Utility Cryptlets tillhandahåller mera information såsom extern data

och autentisering. Contract Cryplets fungerar som surrogat till smarta kontrakt utanför kedjan och kan lätt uppgraderas för hög användning. (Gray 2016)

5.10 Corda

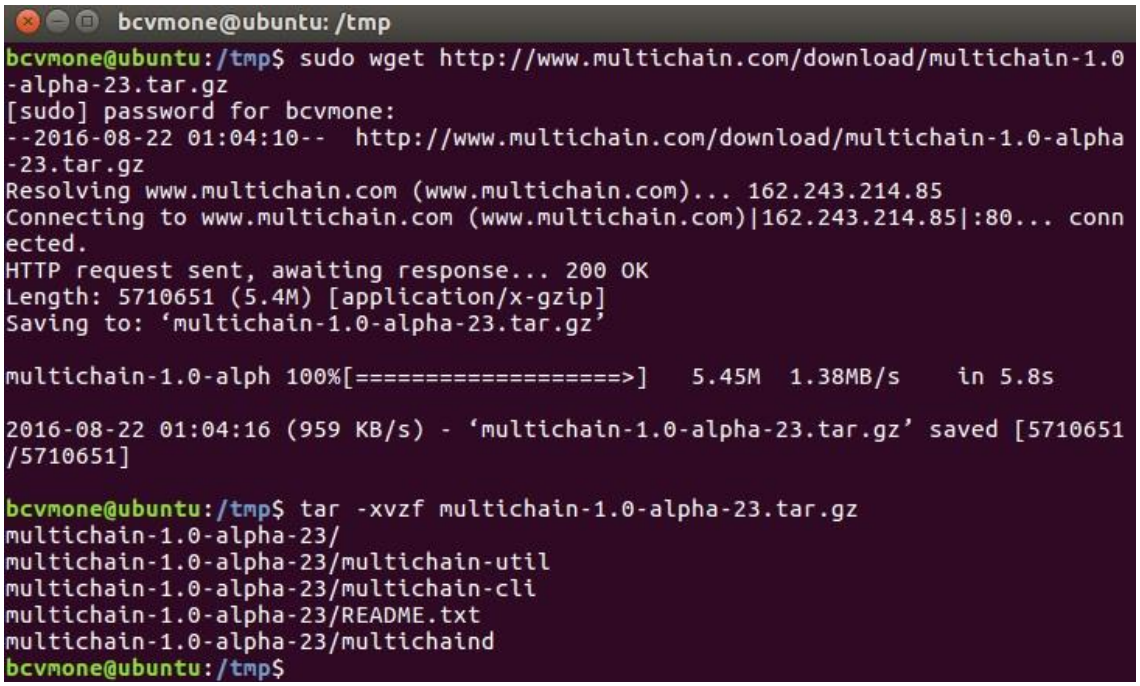
Corda är en blockkedja skapad av företaget R3 och dess konsortium bestående av ett 70-tal företag, bland dem stora banker och finansinstitutioner såsom Royal Bank of Scotland, UBS, HSBC, Deutsche Bank. Bland de nordiska aktörerna hittas bl.a. Nordea, Danske Bank, Skandinaviska Enskilda Banken och OP Financial Group. Blockkedjan är avsedd att användas som huvudbok för finansiella kontrakt och för att realisera företagslogik genom smarta kontrakt. (Gendal Brown, Carlyle, Grigg, Hearn 2016)

6 IMPLEMENTERING AV EN BLOCKKEDJA

Blockkedjeteknik kan ha många tänkbara applikationer, varav flera presenteras i detta arbete. Flera av världens ledande It-företag och finansiella institutioner jobbar på olika implementationer utav blockkedjeteknik.

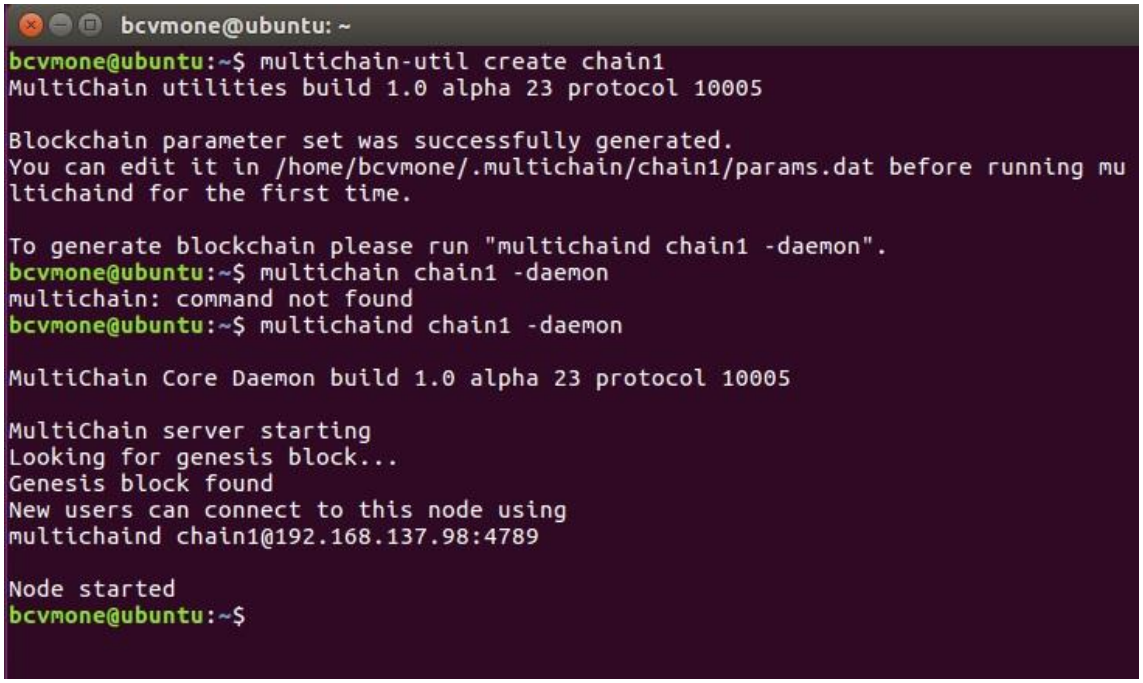
6.1 Implementering av en testkedja med Multichain

För att skapa en egen testkedja med Multichain behöver man först ladda ner och installera programmet på en s.k. frö-nod (eng. seed-node) och minst ytterligare en nod. Figur 3 visar nedladdning och installation av Multichain. Alternativt kan man köra programmet på virtuella maskiner i t.ex. Amazons molntjänst. Efter att ha laddat ner och instal--lerat Multichain på servern skapade jag en egen blockkedja med namnet chain1, se Figur 4.

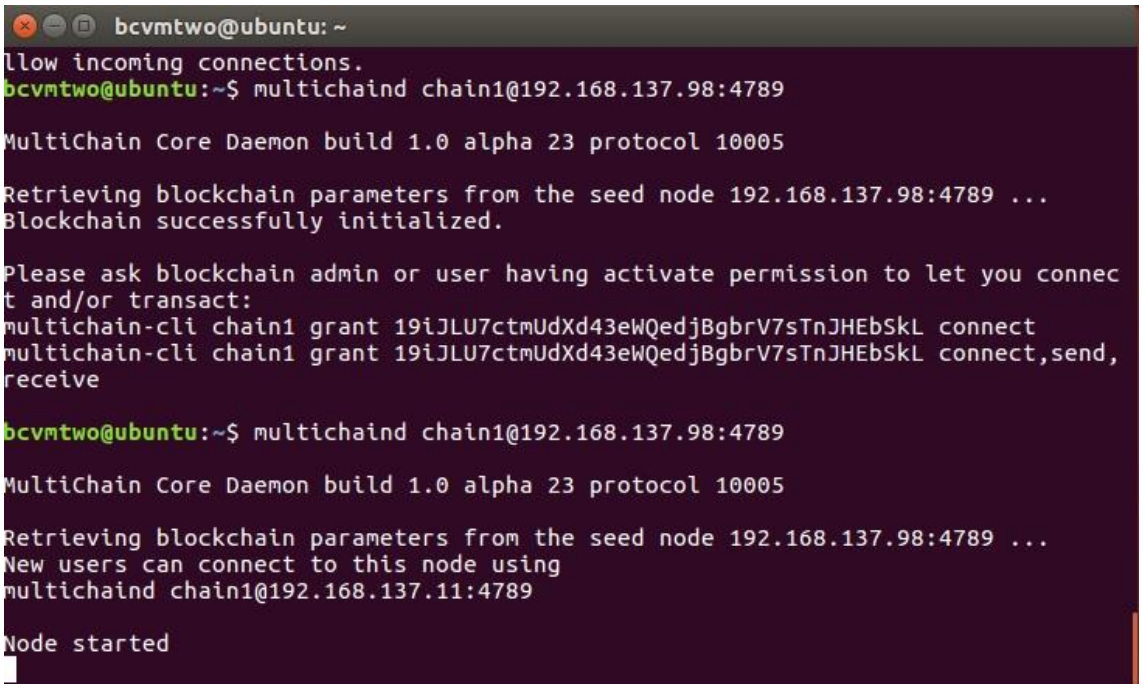


Figur 3: Nedladdning och installation av Multichain

Noder kan nu anslutas till blockkedjan på adressen 192.168.137.98:4789. När man försöker ansluta till den andra nodens adress får man nu veta att man måste bevilja rättigheter för nod nummer två (nod2). Noden identifieras med sin plånboksadress (eng. wallet address).

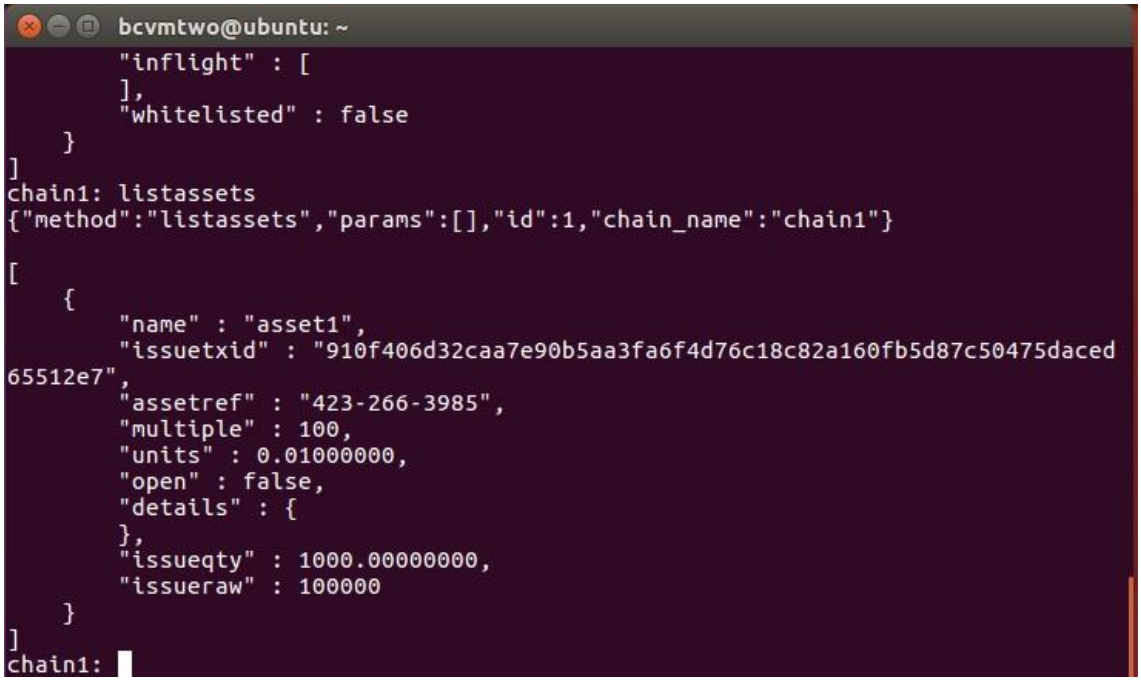


Figur 4: Skapande av blockkedjan chain1

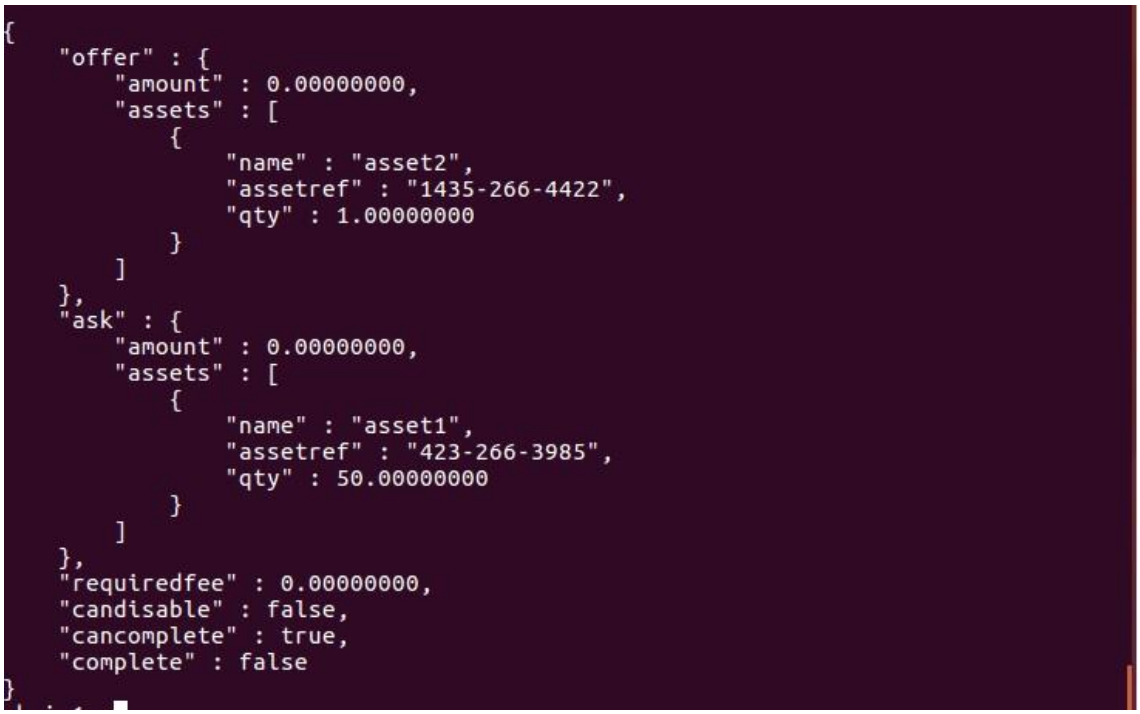


Figur 5: Anslutning av nod2 till kedjan

Jag lägger till anslutningsrättigheter för nod2 på frö-noden och kan nu ansluta nod2 till den, se Figur 5. Jag skapade en egen valuta nämnd asset1 med 1000 enheter. En enhet kan delas upp i 100 mindre delar, se Figur 6. Jag skickade 100 enheter till nod2.

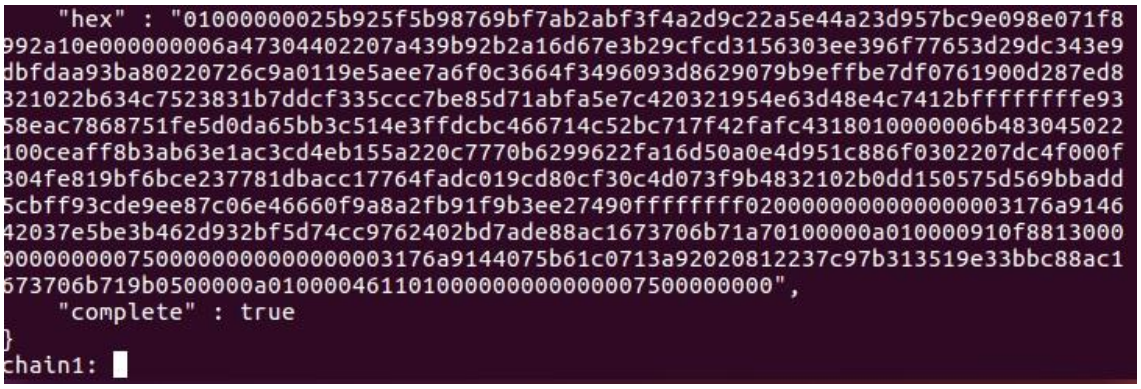


Figur 6: 1000 enheter av valutan asset1 har skapats



Figur 7: Erbjudandet att växla 1 enhet av asset2 för 50 enheter av asset1.

För att skicka med meta-data i transaktionen körde jag *sendwithmetadata (nod2) '{"asset1":125}' (önskad meta-data i hexadecimalt format).* Då skickades 125 enheter av asset1 till nod2 tillsammans med detta meta-data. Sedan skapade jag en till valuta, asset2, för att testa leverans mot betalning (eng. atomic exchange, delivery-versus-payment). För att växla 50 enheter av asset1 från nod2 för 1 enhet av asset2 skapade jag först en låst transaktion med *preparelockunspent '{"asset2":1}'*. Sedan specificerade jag med *createrawexchange* att nod1 ville ha 50 enheter av asset1 i utbyte. På nod2 körde jag *decoderawexchange* för att läsa erbjudandet, se Figur 7, innan jag låste 50 enheter av asset1. För att slutföra växlingen körde jag *appendrawexchange* vilket gav mig ett långt hexadecimalt tal som representerar den genomförda växlingen, se Figur 8. För att registrera händelsen på nätverket körde jag sedan *sendrawtransaction* med den slutförda växlingens hexadecimalvärde. För att även tillåta nod2 att agera datautvinnare körde jag *grant (nod2 adress) mine*. Ett nytt block skapas var femtonde sekund. För att få fram information om den nuvarande blockhöjden i kedjan körde jag *getinfo*, därefter tog jag fram hash-värdet för block 1664 med *getblockhash 1664* och kollade vilken nod som hade utvinnit den med *getblock*, i det här fallet var det nod2.



Figur 8: Hexadecimalt värde för genomförd transaktion.

7 BLOCKKEDJEEXEMPEL

Förutom Bitcoin och en myriad av altcoins finns det blockkedjeimplementeringar av en rad andra applikationer såsom t.ex.:

- Bitcoin-baserade plattformer för meta-data
  Nya tjänster och funktioner skapas genom att placera data i Bitcoins OP_RETURN. Detta ger dem Bitcoins säkerhet och tillgänglighet, t.ex. Counterparty.
- FinTech
  Blockkedjetillämpningar för den finansiella marknaden såsom direkta betalningar mellan banker och växling. T.ex. Ripple.
- Plattformer för smarta kontrakt.
  Möjliggör exekverandet av smarta kontrakt på en blockkedja. T.ex. Ethereum.
- Företagsplattformer.
  Privata blockkedjor för företag eller andra enheter. T.ex. Multichain.
- Sidokedjor och ankrade kedjor

Sidokedjor tillåter användning av annan valuta t.ex. Bitcoin på sidokedjan. Tar bort behovet att inneha flera plånböcker och valutor. Ankrade kedjor tillåter helt nya blockkedjor och applikationer för dessa, men sparar sina hashade blockhuvuden i en större kedja t.ex. Bitcoin för ökad säkerhet. (Baliga 2016)

7.1 Verifieringstjänster

Block Verify använder Bitcoins blockkedja för att spåra och verifiera produkter på blockkedjan och en sammanlänkad privat blockkedja för att spara annan samhörande

information för att försvåra förfalskning av produkter. Bland implementationerna finns verifiering av farmaceutiska produkter, elektronik, diamanter och lyxprodukter. (Traderman 2015)

Blockais mål är att verifiera upphovsrätt på Bitcoins blockkedja. (Ha 2016) Användare kan ladda upp sina skapade verk varvid detta registreras på blockkedjan och i en användarprofil. Blockai söker sedan igenom nätet efter kopior av dessa verk. Användaren kan utnyttja tidsstämplingen av verken på blockkedjan för att skicka ut upphovsrättsanmälningar.

Kouvola Innovation använder IBMs Watson IoT för att spåra t.ex. containrar och paket med en blockkedja för förbättrad logistik. (Kouvolan Sanomat 2016)

7.2 Bitnation

Bitnation är en decentraliserad organisation som erbjuder tjänster benämnda Governance 2.0. Ursprungligen utnyttjades blockkedjan Counterparty, men blockkedjan byttes till
Ethereum i februari 2016. Bland tjänsterna ingår:

- Världsmedborgaridentifiering.
- Nödutryckning i flyktingkriser.
- Bitnation-ambassadörer.

Via samarbete med tredje part erbjuds:

- Personligt skydd.
- Utbildning.
- Bitcoin-betalkort.

Bitnation har lanserat en vision om en decentraliserad rymdstyrelse tillsammans med SpaceChain. Bitnation Space Agency har som mål att bl.a. utveckla mjukvara med öppen källkod och hårdvara samt miljövänligt raketbränsle. I dess femårsplan för rymduppdrag ingår bl.a. placering av en strövare (eng. Rover) på månen, gruvdrift på månen, placering av satelliter i omloppsbana runt jorden samt en bemannad rymdstation. (Miribioki 2015)

7.3 Augur

Augur är en plattform byggd på Ethereums blockkedja där användare kan skapa egna smarta kontrakt för marknadsprognoser och spekulationer. För att hålla nätverket hederligt och motarbeta manipulering kan användare köpa s.k. Reputation-polletter ($REP). Det finns totalt 11 miljoner polletter. År 2015 såldes 80 % av polletterna till intresserade användare för sammanlagt 5,3 miljoner dollar. Innehavare av $REP rapporterar resultat om händelser som användare spekulerar på. De som rapporterar felaktigt eller försöker manipulera utgången fråntas sina polletter som omfördelas bland de pålitliga innehavarna. Som belöning för korrekt rapportering av händelser får pollettinnehavarna dela på hälften av marknadsavgifterna upptagna i nätverket. (Kysar 2016)

7.4 Växlingsplattformer

Coinbase är en plattform som tillhandahåller online-plånböcker samt växlar Bitcoin och Ethereum. I november 2016 krävde den amerikanska skattmasen IRS (Internal Revenue Service) att Coinbase överlämnar all egen användardata från de senaste tre åren i jakten på skattesmitare. (Techdirt 2016)

Poloniex tillhandahåller kryptovalutaväxling och lån. Användare kan växla över 360 olika kryptovalutapar. Poloniex har hand om en majoritet av växling med kryptovalutorna Dash och Monero. (Coingecko 2017)

Växlingsplattformen Kraken tillåter växling med över 50 olika valutapar. Kraken växlar även mellan kryptovaluta och traditionell valuta såsom euro, amerikanska dollar, kanadensiska dollar, brittiska pund och japanska yen. Kraken har den största växlingsvolymen av valutaparet Bitcoin – Euro. (Coinmarketcap.com 2017)

7.5 Blockkedja i media

Zlick är en estnisk tjänst för mikrobetalningar, främst för media. Denna betalningstjänst samarbetar med mobiloperatörer för att ta betalt för innehåll, t.ex. en artikel på en tid-

nings hemsida. Alla mikrobetalningar sparas på blockkedjan och betalas av kunden på hens telefonräkning. (Arvutimaailm 2016)

Steemit är en social medieplattform där användare kan tjäna Steem-polletter genom att skriva och dela inlägg och rösta på de inläggen de gillar. Ju tidigare en användare röstar på ett inlägg som blir populärt desto mera Steem Power tjänar hen. Steem fungerar som kryptovaluta och går att handla med, mera Steem skapas med varje nytt block. Steem Power fungerar som anseende-pollett, Steem Dollar är bunden till den amerikanska dollarn. Användare med mera Steem Power har större vikt vid röstning. Steem kan konverteras till Steem Power eller Steem Dollar och vice versa. Det tar dock tid, 104 veckor, att konvertera all sin Steem Power tillbaka till Steem och 7 dagar för att konvertera Steem Dollar till Steem. Steem Dollars kan endast bytas direkt till Steem på den interna marknadsplatsen. Användare får 10% ränta på sina Steam Dollars i sin plånbok. Steemit använder anförtrott bevis på andel som koncensusprocess. (Larimer, Scott, Zavgorodnev, Johnson, Calfee, Vandeberg 2016).

7.6 Storj

Storj är en plattform för distribuerad molnlagring där datautvinnare kan dela med sig av sitt lokala lagringsutrymme för andras bruk. En användare kan bestämma sig för att köpa lagringsutrymme i Storjs nätverk varefter data hen vill spara krypteras, delas upp i mindre bitar och laddas upp i nätverket till datautvinnare som delar med sig av sitt oanvända lokala lagringsutrymme och bandbredd (Wilkinson et al. 2016). I utbyte erhålls Storjcoin X. Storj använder Bitcoins blockkedja och Counterparty för transaktioner. Den 23 mars 2017 meddelade Storjs verkställande direktör att tjänsten kommer att flyttas från Bitcoin och Counterparty till Ethereum (Wilkinson 2017).

7.7 Digitala betyg

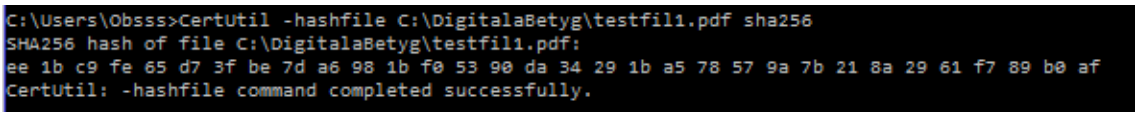
Holberton School i San Francisco, Förenta staterna, meddelade år 2015 att de skulle börja autentisera akademiska betyg och certifikat i Bitcoins blockkedja. De samarbetar med Bitproof och säkrar betygen med 256-bitars kryptering. (Eckert 2015)

Universitetet i Nicosia på Cypern har också tagit i bruk digitala betyg i Bitcoins blockkedja. De ville skapa ett system som inte använder andra tjänster än Bitcoins blockkedja, som går att verifiera utan att kontakta universitetet och som går att verifiera även om universitetet eller dess register inte längre är tillgängligt. För att uppnå målen så bestämde de sig för att tillämpa hash-algoritmen SHA-256 på betygens PDF-dokument och spara den skapade hash-summan i blockkedjan. För att minimera risken för mänskliga fel och minska antalet transaktioner på blockkedjan så valde de att skriva in alla hash-summor för betyg utfärdade inom en viss tidsram i ett dokument och sedan hasha det och publicera det på blockkedjan. För att uppnå en stor spridning av dokumentet för att försäkra om att det skall finnas tillgängligt även i framtiden så tilldelades varje student en kopia. För att verifiera ett betyg kan en intresserad part nu verifiera dokumentets hash-summa gentemot blockkedjan och sedan jämföra betygets egen hash-summa med dokumentets hash-summor. (University of Nicosia 2014)

Sony Global Education meddelade i februari att man håller på att utveckla egen teknik för digitala betyg och certifikat i en blockkedja. Denna teknik skall gå att använda för säker överföring av krypterad data mellan två parter. Sonys blockkedja skall även kunna användas för nya tjänster genom att utveckling av nya program som använder sig av Sonys infrastruktur och därmed locka till sig många användare. I framtiden skall Sonys blockkedja även kunna användas till andra applikationer. (Sony Global Education 2016)

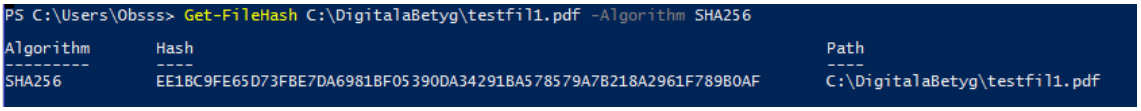
Vivacoin planerar att implementera ett system för meritöverföring i framtiden där studenten kan välja mellan kurser inom olika deltagande institutioner varefter prestationerna sparas på Vivas blockkedja för att sedan kunna användas vid ansökan om betyg. (Vivacoin.in 2017)

Verifiering av ett digitalt betyg på blockkedjan såsom vid Nicosia-universitetet på Cypern sker genom att beräkna hash-summor på dokument. I Microsoft Windows är kommandoradprogrammet CertUtil.exe och powershell-kommandot Get-FileHash förinstallerade. Med CertUtil beräknas hash-summan på en fil med kommandoraden *CertUtil -hashfile filväg [hash-algoritm]*, se Figur 9. Understödda hash-algoritmer är MD2, MD4, MD5, SHA1, SHA256, SHA384 och SHA512.



Figur 9: SHA256 beräknas på testfil1.pdf med CertUtil.exe.

Powershell-kommandot Get-FileHash är smidigare att använda och stöder SHA1, SHA256, SHA384, SHA512, MACTripleDES och RIPEMD160. En hash-summa på en fil beräknas med *Get-FileHash filväg -Algorithm [hash-algoritm]*, se Figur 10.

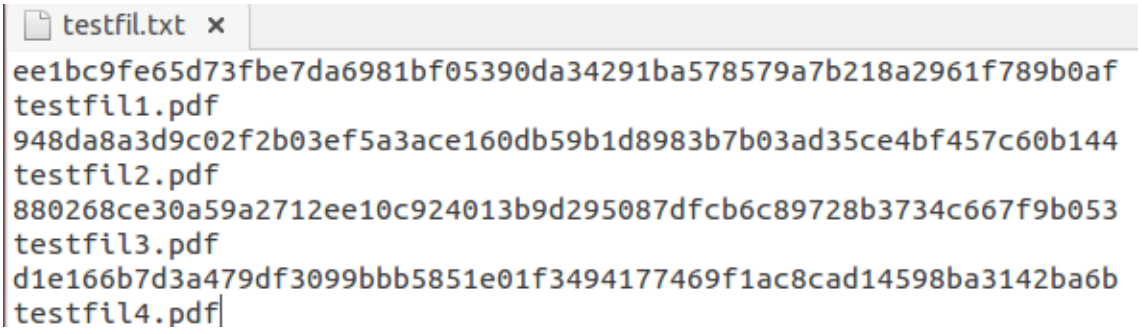


Figur 10: SHA256 beräknas på testfil1.pdf med Get-FileHash i powershell.

För att kunna beräkna hash-summorna på flera filer i serie och få samtliga hash-summor sparade i en fil kan man utföra kommandoraden *dir filväg | Get-FileHash -Algoritm SHA256 | Export-Clixml -Path filväg\fil.xml*. Härvid beräknas hash-summorna på alla filer i en mapp och resultaten sparas i en xml-fil, se Figur 11.

Figur 11: SHA256 hash-summor beräknade på 4 testfiler och sparade i en. xml-fil.

I Linux-distributioner såsom Ubuntu kan SHA256 hash-summor beräknas på alla filer i en mapp och sparas i en textfil med kommandoraden *filväg sha256sum * >fil.txt*, se Figur 12.



Figur 12: SHA256 hash-summor beräknade på 4 testfiler och sparade i en .txt-fil i Ubuntu.

För att följa Nicosia-universitetets exempel kan nu .xml-filens eller .txt-filens hash-summa beräknas och publiceras på blockkedjan. .xml-filen eller .txt-filen kan sedan publiceras på skolans hemsida. Så länge .xml-filens eller .txt-filens hash-summa kan verifieras är även alla betygs hash-summor korrekta. Användare som är intresserade av att verifiera betyg kan ladda ner .xml-filen eller .txt-filen och kontrollera de digitala betygens hash-summor mot hash-summorna i den nedladdade filen.

7.7.1 Blockcerts

Juliana Nazaré, Kim Hamilton och Philipp Schmidt vid Massachusetts Institute of Technology har skapat en första version av ett verktyg förutgivning, visning och verifiering av digitala betyg och referenser med Bitcoins blockkedja och Mozillas "Open Badges"-specifikationer. Betygsutfärdaren signerar ett digitalt certifikat med sin privata nyckel och sparar certifikatets hash-nummer i en blockkedjetransaktion. Transaktionens output tilldelas betygets mottagare. (Nazaré, Hamilton, och Schmidt 2016)

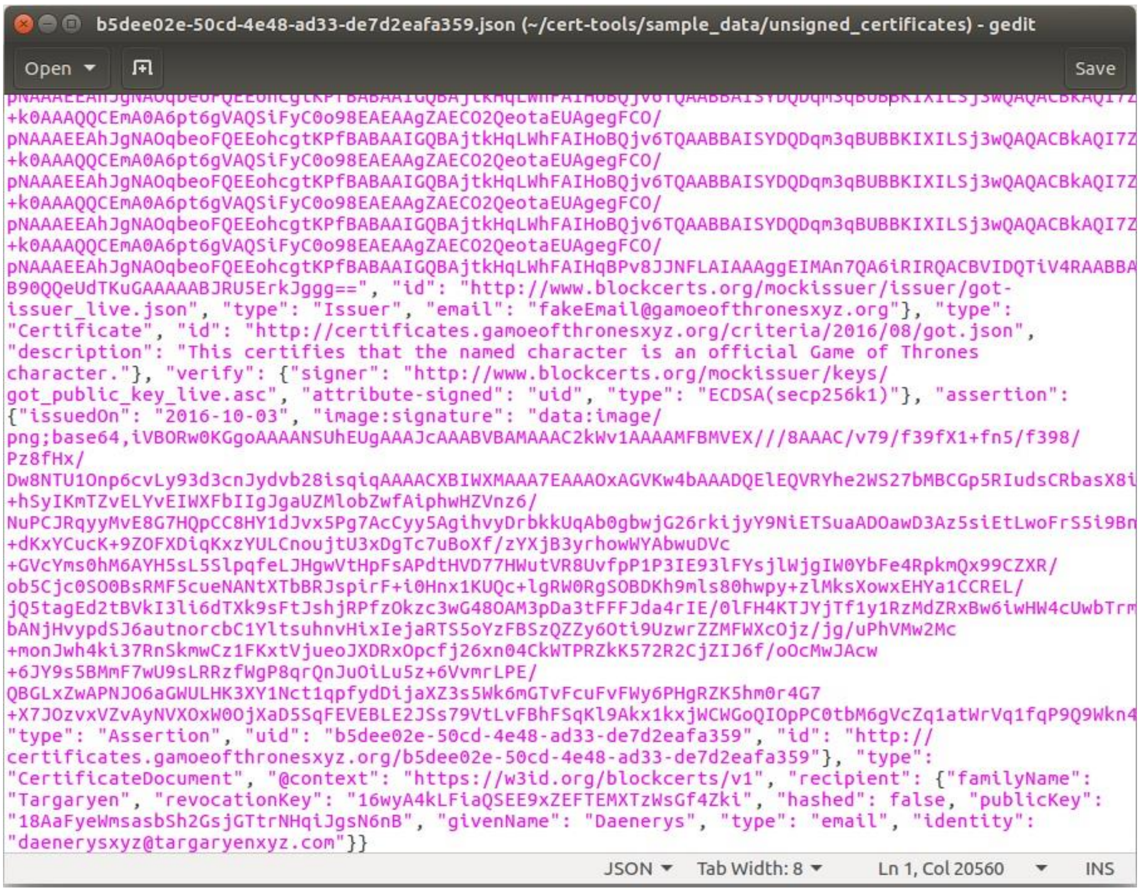
I oktober 2016 utgavs MIT-projektets första version omdöpt till Blockcerts i samarbete med startup-företaget Learning Machine tillsammans med en plånboks-app för Apples mobila operativsystem iOS. Learning Machine har som mål att börja testa en kommersiell version inom sommarmånaderna 2017 med utvalda partners, bland dem University of Melbourne där testerna börjar i juli och vidare i bruk tagning är planerad för år 2018. (Henderson 2017)

Malta var först i Europa med ett samarbete med Learning Machine, vilket presenterades den 24 januari 2017. (gov.mt 2017)

Blockcerts-verktyget finns också tillgängligt som öppen källkod på Github. Det består av 3 olika delar, cert-tools för att skapa osignerade betyg, cert-issuer för att utfärda betygen och cert-viewer för att visa och verifiera betygen. För att komma igång behövs virtualiseringsmjukvaran Docker som är tillgänglig på de flesta 64-bitars Linux-distributioner, även via molntjänster så som Amazon Web Services (AWS). Apple MacOS 10.10.3 eller nyare kan användas så länge kraven på minst 4GB arbetsminne och stöd för Intels MMU (Memory Management Unit) uppfylls. Även Microsoft Win-

dows 10 64-bit kan användas, dock endast versionerna; Pro, Enterprise och Education. För inkompatibla Apple MacOS och Microsoft Windows datorer finns ett verktyg kallat Docker Toolbox som kommer med en virtualiseringslösning från Oracle. Utöver Docker krävs en Bitcoin-core, en full nod på Bitcoins blockkedja, samt en Python-miljö.

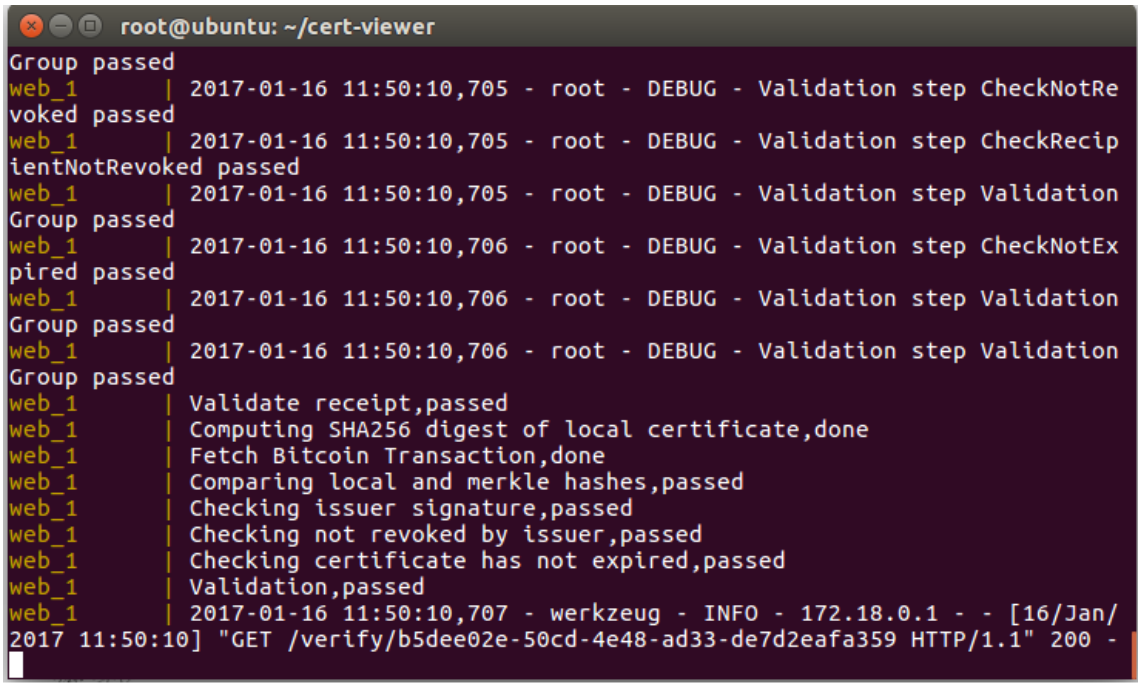
Med kommandoradsverktyget cert-tools skapas osignerade betyg. Utfärdaren kan konfigurera betygets utseende med sin egen logotyp och underskrift samt annan information om betyget. Betygsmottagarnas information redigeras enklast i t.ex. Excel. Information som måste finnas tillgänglig är förnamn, efternamn, epost-adress och Bitcoin-plånboksaddress. Även annan information går att lägga till. Utfärdaren kan även skapa annulleringsnycklar ifall denne eller mottagaren vill annullera betyget. Betyget sparas som en fil i JSON-format. Se Fig. 13.



Figur 13: Osignerat betyg i JSON-format.

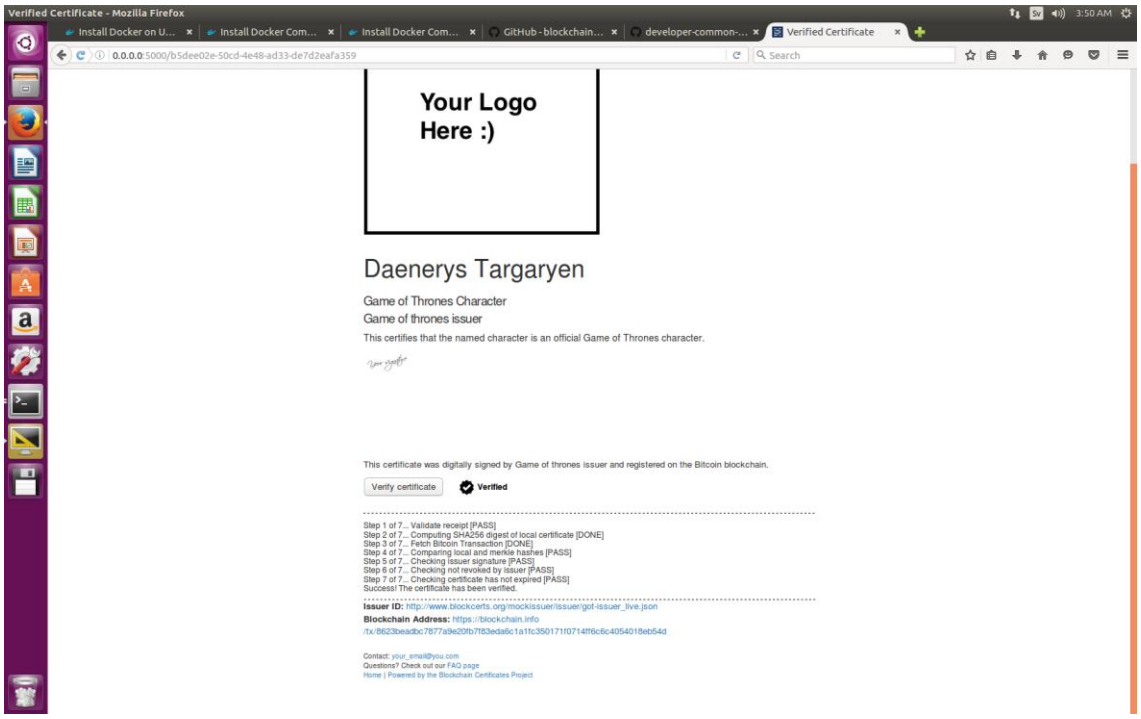
Med kommandoradsverktyget cert-issuer signeras betyg skapade med cert-tools. Då cert-issuer signerar ett betyg med sin privata nyckel skapas en transaktion till mottagarens adress. Utmatningen på blockkedjan är transaktioner med betygsinformationen hashad i OP_RETURN.

Cert-viewer används för att verifiera redan utfärdade betyg. Betygens hash-summor, utfärdare och eventuell annullering jämförs med informationen på blockkedjan. Se Fig. 14.



Figur 14: Cert-viewer.

Utfärdade betyg sparas i en databas, t.ex. MongoDB, och cert-viewer har också ett grafiskt gränssnitt som går att använda på en webbplats. Se Figur 15. Betygets mottagare kan skicka betyget t.ex. till en arbetsgivare som kan köra cert-viewer eller ännu smidigare, använda utfärdarens webb-applikation för verifiering.



Figur 15: Cert-viewer i webbläsare.

7.7.2 Digitala betyg i Arcada

En blockkedja skulle kunna användas för verifiering av digitala betyg från Arcada. Exemplen i avsnitt 7.7 har olika tillvägagångssätt. Holberton School använder sig av en tredje part för verifiering av betygen, Nicosia-universitetet sparar alla utförda prestationers hash-summor i dokument vilka sedan används för verifiering av betygen och projektet vid Massachusetts Institute of Technology har skapat mjukvara för realisering, verifiering och visning av digitala betyg. Alla använder vid skrivande stund Bitcoins blockkedja för att den är störst.

För Arcada skulle ett tillvägagångsätt likt det vid universitetet i Nicosia vara den smidigaste lösningen. Istället för att verifiera alla enskilda kursprestationer på blockkedjan så skulle man kunna spara endast slutbetyget. Årligen utexamineras runt 400 studenter från Arcada, ett tillräckligt litet antal för att det skall vara möjligt att verifiera varje betyg i en skild transaktion på blockkedjan. Då skulle skolan signera ett PDF-dokument av betyget med sin privata nyckel, sedan räkna ut hash-summan av dokumentet och införa den i en transaktion på t.ex. Bitcoins blockkedja. Transaktionen skulle inte nödvändigtvis gå till elevens privata plånbok utan skolan kunde ha två adresser, en adress som ut-

färdar betyg och skickar en transaktion till en annan adress som lagrar de mottagna transaktionerna. Den som vill verifiera ett digitalt betyg behöver nu bara jämföra betygets hash-summa med hash-summorna i transaktionerna. Om summorna stämmer så är betyget signerat av skolan och har inte manipulerats. Alternativt skulle skolan kunna använda sig av samma princip som Bitcoins pappersplånböcker för att också verifiera betyget i pappersform med blockkedjan och skapa ett unikt nyckelpar för betyget. Då skulle den publika nyckeln och betygets hash-summa kunna printas ut på pappersbetyget och alla intresserade skulle kunna spåra transaktionen från skolan till betygets publika nyckel och jämföra hash-summorna.

Blockcerts kan i framtiden vara ett bra alternativ, beroende på adoptering och utveckling. Dock är det för tillfället klumpigt för ändamålet att verifiera hela betyg på en blockkedja då Blockcerts enligt min mening är implementerad för verifiering av enskilda prestationer. Eftersom studerande sällan har exakt samma kurser även om de har gått samma utbildningsprogram krävs det mycket mer arbete för att skapa nya mallar där varje enskild prestation verifieras för varje betyg i verktyget cert-tools. I skrivande stund finns plånboksappen med inbyggd verifiering endast för Apples iOS. För större spridning behövs åtminstone också en Android-app, speciellt eftersom en av grundtankarna bakom Blockcerts är att underlätta verifiering av utbildningsprestationer och Android är världens mest använda operativsystem (Granroth 2017). Enklast skulle det vara med en webb-app som plånbok, men då måste användarna lita på någon tredje part för att spara nycklarna eller själva ha intresse av och kunskaper för att hantera egna nycklar i ett separat program eller manuellt. Detta är troligtvis inte det enklaste sättet med tanke på hur dåliga vi är att hålla reda på lösenord till olika tjänster idag.

Genom att verifiera betyg med blockkedjan behövs inte PKI-verifiering med en kommersiell certifieringsauktoritet såsom Symantec eller Verisign. PKI-verifiering har en begränsad giltighetstid och en av de största fördelarna med blockkedjan är att transaktionerna sparas för hela blockkedjans livslängd. Vid användning av PKI-verifiering måste verifieringen uppdateras innan giltighetstiden har tagit slut vilket skulle leda till en invecklad och sårbar betygshantering.

I framtiden kunde betygsverifieringen utvecklas att även innefatta verifiering av alla studieprestationer på blockkedjan. Då skulle myndigheter såsom Folkpensionsanstalten (FPA) kunna betala ut studiestöd för utförda prestationer registrerade på blockkedjan. Skolan kunde få sin finansiering genom att den statliga myndigheten kunde registrera alla utförda prestationer.

Ett enkelt betygsverifieringssystem på blockkedjan skulle lätt kunna implementeras internationellt och skulle underlätta vardagen för bl.a. utbytesstuderande och skolor som tar emot utbytesstuderande genom en snabb och enkel verifiering av utförda prestationer. Detta skulle minska arbetsmängden som krävs av skolorna och minimera risken för förfalskningar. Om efterfrågan blir tillräckligt stor kunde även flera skolor t.ex. inom Norden eller EU kunna skapa en privat blockkedja och en egen standard för digitala betyg. För att kunna verifiera ett betyg skulle skolorna kunna återvinna en liten summa av användaren. Summan kunde användas för upprätthållandet av blockkedjans hårdvara och infrastruktur.

8 DISKUSSION OCH SLUTSATSER

Blockkedjetekniken går framåt i rasande takt, nya idéer och förslag växer fram dagligen. Bitcoin riskerar att hamna i bakgrunden på grund av dess användares motvillighet att adoptera nyheter. Blockförstoringar som skulle minska på stockningen i Bitcoins blockkedja, såsom Segwit eller Bitcoin Unlimited, skulle behövas för att göra Bitcoin praktiskt i dagligt bruk men skulle även kräva en soft fork. Ett nätverk säkrat med bevis på arbete utsätts hela tiden för kapprustningen mellan datautvinnare. För att hinna med krävs hela tiden snabbare och mer energieffektiva lösningar. Miljöforskaren Sebastiaan Deetman förutspådde i en artikel i mars 2016 att strömförbrukningen vid Bitcoins datautvinning kunde ligga på samma nivå som i hela Danmark år 2020 om utvecklingen fortsätter i samma spår (Deetman 2016). Om konkurrensen bland datautvinnarna blir så stor att endast ett fåtal stora aktörer med tillgång till billig energi klarar av att överleva rubbas säkerheten i Bitcoins blockkedja. Ett annat potentiellt hot mot blockkedjor som använder bevis på arbete är kvantdatorn. Dess beräkningskraft kunde eventuellt helt annullera säkerheten i flera nu utnyttjade kryptografiska funktioner.

Vare sig Bitcoin överlever eller endast tilldelas en roll som föregångare eller startskott till en revolution återstår att se, men i min mening är blockkedjetekniken här för att stanna. Smarta kontrakt går att implementera för det mesta. I framtiden kunde en produkts hela livscykel kunna registreras på blockkedjan, dvs. allt ifrån registreringen av mineralerna och grundmaterialet då produkterna framställs, kvalitetsgranskas, packas och transporteras till varje punkt i leveranskedjan. Alla delar i den slutliga produkten kunde på så sätt spåras tillbaka till sitt ursprung. Smarta enheter i t.ex. husteknik kunde då själva kunna registrera tidpunkt för byte av filter eller dylikt, och varför inte automatiskt beställa underhåll baserat på sensordata och data om delars livslängd sparat på en blockkedja. Till slut kunde en produkt som en självstyrande bil kunna köpas in av ett taxiföretag. Bilen skulle själv bestämma vilka resor den skall göra för att maximera lönsamheten och själv bestämma när den skall tanka beroende på el- eller bränslepriset. När bilen märker att den är i behov av underhåll kan den själv beställa tid vid verkstaden med den kortaste kön eller det lägsta priset. När bilens teknik blir för gammal och inte längre kan konkurrera med nyare fordon eller underhållet skulle kosta för mycket kan bilen själv köra till ett återvinningsställe för att sälja delarna eller råmaterialet, vilket återigen skulle registreras på blockkedjan. Problemet med att alltid kunna spåra allt på en blockkedja uppstår förstås när människan blir inblandad. Den enskilda individens integritet måste respekteras, men om blockkedjetekniken utnyttjas på ett rätt sätt kan fördelarna klart överväga nackdelarna.

KÄLLOR

Arvutimaailm.ee 03.12.2016 *Tele2 tõi Eestisse ühe klikiga Zlick netimaksed* Hämtad: 04.05.2017 Tillgänglig: https://www.am.ee/Zlick

Back Anthony 08.03.2017 *Ethereum to swithc to "proof of stake" protocol despite skepticism* Hämtad: 11.05.2017 Tillgänglig: https://disruptive.asia/ethereum-proof-stake-protocol/

Baliga Arati 2016 *The Blockchain Landscape* Hämtad: 31.01.2017 Tillgänglig: https://www.persistent.com/wp-content/uploads/2016/03/The-Blockchain-Landscape-.pdf

BitFury Group 13.09.2015*Proof of Stake versus Proof of Work* Hämtad: 09.10.2016 Tillgänglig: http://bitfury.com/content/5-white-papers-research/pos-vs-pow-1.0.2.pdf

Blockexplorer.com *Block #0* Hämtad: 14.10.2016 Tillgänglig: https://blockexplorer.com/block/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f

Coindesk.com 02.04.2014 *What is the Difference Between Litecoin and Bitcoin?* Hämtad: 11.05.2017 Tillgänglig: http://www.coindesk.com/information/comparing-litecoin-bitcoin/

Coingecko 2017 *Dash Trading Exchanges* och *Monero Trading Exchanges* Hämtad: 27.03.2017 Tillgänglig: Dash: https://www.coingecko.com/en/coins/dash/trading_exchanges samt: Monero: https://www.coingecko.com/en/coins/monero/trading_exchanges

Coinmarketcap.com 2017 *CryptoCurrency Market Capitalizations* Hämtad 27.03.2017 Tillgänglig: https://coinmarketcap.com/exchanges/kraken/

Crosby Michael, Nachiappan, Pattanyak Pradhan, Verma Sanjeev, Kalyanaraman Vignesh, 16.10.2015 *BlockChain Technology*, *Beyond Bitcoin* Hämtad: 18.05.2017 Tillgänglig: http://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf

Deetman Sebastiaan 29.03.2016 *Bitcoin Could Consume as Much Electricity as Denmark by 2020* Hämtad: 18.05.2017 Tillgänglig: https://motherboard.vice.com/en_us/article/bitcoin-could-consume-as-much-electricity-as-denmark-by-2020

Dermody Robby 07.07.2016 *Frequently Asked Questions* Hämtad: 04.05.2017 Tillgänglig: https://github.com/CounterpartyXCP/Documentation/blob/master/Basics/FAQ.md

Duffield Evan, Diaz Daniel 2017 *Dash: A Privacy-Centric Crypto-Currency* Hämtad: 14.03.2017 Tillgänglig: https://www.dash.org/wp-content/uploads/2015/04/Dash-WhitepaperV1.pdf

Eckert Joe 21.10.2016 *Holberton School to Authenticate Its Academic Certificates With the Bitcoin Blockchain* Hämtad: 10.09.2016 Tillgänglig: http://www.marketwired.com/press-release/holberton-school-authenticate-its-academic-certificates-with-bitcoin-blockchain-2065768.htm

Ethdocs.org 2016 *Account Types, Gas, and Transactions* Hämtad: 24.05.2016 Tillgänglig: http://ethdocs.org/en/latest/contracts-and-transactions/account-types-gas-and-transactions.html

Gendal Brown Richard, Carlyle James, Grigg Ian, Hearn Mike 8.2016 *Corda: An Introduction* Hämtad: 15.02.2017 Tillgänglig: https://static1.squarespace.com/static/55f73743e4b051cfcc0b02cf/t/57bda2fdebbd1acc9c0309b2/1472045822585/corda-introductory-whitepaper-final.pdf

Georgiev Hristo 11.08.2016 *The hack that changed the blockchain prespective* Hämtad: 18.05.2017 Tillgänglig: https://labs.mwrinfosecurity.com/blog/the-hack-that-changed-the-blockchain-perspective/

Gov.mt 24.01.2017 *Press Release Issued by the Ministry for Education and Employment* Hämtad: 11.05.2017 Tillgänglig: https://www.gov.mt/en/Government/Press%20Releases/Pages/2017/January/24/PR170153.aspx

Granroth André 04.04.2017 *Android går om Windows som det mest använda operativsystemet* Hämtad: 19.05.2017 Tillgänglig: http://www.sweclockers.com/nyhet/23615-android-gar-om-windows-som-det-mest-anvanda-operativsystemet

Gray Marlay 15.06.2016 *Introducing Project "Bletchley"* Hämtad: 07.08.2016 Tillgänglig: https://github.com/Azure/azure-blockchain-projects/blob/master/bletchley/bletchley-whitepaper.md

Greenspan Gideon 07.2015 *MultiChain Private Blockchain – White Paper* Hämtad: 04.05.2017 Tillgänglig: http://www.multichain.com/download/MultiChain-White-Paper.pdf

Griffith Ken 16.04.2014 *A Quick History of Cryptocurrencies BBTC – Before Bitcoin* Hämtad: 25.04.2017 Tillgänglig: https://bitcoinmagazine.com/articles/quick-history-cryptocurrencies-bbtc-bitcoin-1397682630/

Gutierrez Carlo, Khiznyak Alex 12.05.2017 *IBM Aims to Improve Manufacturing and Supply Chain with IOT-Driven Blockchains* Hämtad: 15.05.2017 Tillgänglig: https://www.altoros.com/blog/ibm-aims-to-improve-manufacturing-and-supply-chain-by-coupling-iot-and-blockchain/

Ha Anthony 17.08.2016 *Blockai's new tool combines tweeting and claiming copyright* Hämtad: 07.12.2016 Tillgänglig: https://techcrunch.com/2016/08/17/blockai-twitter/

Henderson James 01.05.2017 *Aussie-first as University of Melbourne trials blockchain technology* Hämtad: 02.05.2017 Tillgänglig: https://www.arnnet.com.au/article/618446/university-melbourne-makes-aussie-first-blockchain-move/

Hern Alex 27.03.2014 *Dogecoin raises $55,000 to sponsor Nascar driver* Hämtad: 11.05.2017 Tillgänglig: https://www.theguardian.com/technology/2014/mar/27/nascar-dogecoin-sponsor-josh-wise-talladega-superspeedway

Hyperledger.com 2017 *Members* Hämtad: 15.05.2017 Tillgänglig: https://www.hyperledger.org/about/members

Intel Corporation 2017 *Sawtooth Lake Developer's Guide* Hämtad: 04.05.2017 Tillgänglig: http://intelledger.github.io/0.7/sawtooth_developers_guide/architecture_overview.html

Kouvolan Sanomat 15.02.2016 *Kouvola Innovation yhteistyöhön IBM:n kanssa – suunnitteilla muun muassa alykkäitä rahtikontteja, jotka järjestävät itse omat kuljetuksensa* Hämtad: 07.12.2016 Tillgänglig: http://www.kouvolansanomat.fi/Online/2016/02/15/Kouvola%20Innovation%20yhteistyy%C3%B6h%C3%B6n%20IBM%3An%20kanssa%20%E2%80%94%20suunnitteilla%20muun%20muassa%20%C3%A4lykk%C3%A4it%C3%A4%20rahtikontteja,%20jotka%20j%C3%A4rjest%C3%A4v%C3%A4t%20itse%20omat%20kuljetuksensa/20162203163349/4

Kysar Tom 20.12.2016 *Reputation 101 - A Guide to Augurs Rep* Hämtad: 18.05.2017 Tillgänglig: http://blog.augur.net/guide-to-augurs-rep/

Larimer Daniel, Scott Ned, Zavgorodnev Valentine, Johnson Nenjamin, Calfee James, Vandeberg Michael 03.2016 *Steem - An Incentivized, Blockchain-based Social Media Platform* Hämtad: 05.05.2017 Tillgänglig: https://steem.io/SteemWhitePaper.pdf

Lerner Sergio Demian 19.11.2015 *RSK Bitcoin Powered Smart Contracts* Hämtad: 24.02.2017 Tillgänglig: https://www.weusecoins.com/assets/pdf/library/Rootstock-WhitePaper-Overview.pdf

Miribioki Iman 2015 *Bitnation Space Agency* Hämtad: 15.02.2017 Tillgänglig: http://www.spacechain.org/documents/bitnation_space_agency.pdf

Nakamoto Satoshi *Bitcoin: A Peer-to-peer Electronic Cash System* Hämtad: 5.5.2016 Tillgänglig: https://bitcoin.org/bitcoin.pdf

Nazaré Juliana, Hamilton Duffy Kim, Schmidt J. Philipp *What we learned from designing an academic certificates system on the blockchain* Hämtad: 07.08.2016 Tillgänglig: https://medium.com/mit-media-lab/what-we-learned-from-designing-an-academic-certificates-system-on-the-blockchain-34ba5874f196#.rsjz6mkyo

Ripple.com 2017 *XRP Portal* Hämtad: 04.05.2017 Tillgänglig: https://ripple.com/xrp-portal/

Schwatz David, Youngs Noah, Britto Arthur 2014 *The Ripple Consensus Algorithm* Hämtad: 07.12.2016 Tillgänglig: https://ripple.com/files/ripple_consensus_whitepaper.pdf

Sony Global Education 22.02.2016 *Sony Global Education Develops Technology Using Blockchain for Open Sharing of Academic Proficiency and Progress Records* Hämtad 28.09.2016 Tillgänglig: http://www.sony.net/SonyInfo/News/Press/201602/16-0222E/index.html

Stark Elizabeth 15.09.2016 *What is the Lightning Network and how can it help Bitcoin scale?* Hämtad 15.03.2017 Tillgänglig: https://coincenter.org/entry/what-is-the-lightning-network

Szabo Nick 1997 *The Idea of Smart Contracts* Hämtad: 24.05.2016 Tillgänglig: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html

Techdirt.com 21.11.2016 *IRS Demands All Info On ALL Coinbase Customers* Hämtad: 07.12.2016 Tillgänglig: https://www.techdirt.com/articles/20161118/18090136088/irs-demands-all-info-all-coinbase-customers.shtml

Tether Limited 2017 *Tether: Fiat Currencies on the Bitcoin blockchain* Hämtad: 14.03.2017 Tillgänglig: https://bravenewcoin.com/assets/Whitepapers/Tether-White-Paper.pdf

Traderman 13.03.2015 *Block Verify: A Blockchain Based Counterfeit Solution* Hämtad: 07.12.2016 Tillgänglig: http://themerkle.com/block-verify-a-blockchain-based-counterfeit-solution/

University of Nicosia 2014 *Academic Certificates on the Blockchain* Hämtad: 21.09.2016 Tillgänglig: http://digitalcurrency.unic.ac.cy/free-introductory-mooc/academic-certificates-on-the-blockchain/

Van Saberhagen Nicolas 17.10.2013 *CryptoNote v 2.0* Hämtad: 29.03.2017 Tillgänglig: https://cryptonote.org/whitepaper.pdf

Visa Europe 2017 *Processing* Hämtad: 24.02.2017 Tillgänglig: https://www.visaeurope.com/enabling-payments/processing

Vivacoin.in 2017 *POETS* Hämtad: 28.04.2017 Tillgänglig: http://www.vivaco.in/

Wilkinson Shawn 23.03.2017 *Migration from Counterparty to Ethereum* Hämtad: 05.05.2017 Tillgänglig: http://blog.storj.io/post/158740607128/migration-from-counterparty-to-ethereum

Wilkinson Shawn, Boshevski Tome, Brandoff Josh, Prestwich James, Hall Gordon, Gerbes Patrick, Hutchins Philip, Pollard Chris 15.12.2016 *Storj – A Peer-to-Peer Cloud Storage Network* Hämtad: 05.05.2017 Tillgänglig: https://storj.io/storj.pdf

Young Joseph *BitProof: 17-Year-Old Entrepreneur Brings University Diplomas to the* Blockchain 21.09.2015 Hämtad: 27.11.2016 Tillgänglig: https://cointelegraph.com/news/bitproof-17-year-old-entrepreneur-brings-university-diplomas-to-the-blockchain