Tillämpningar av blockkedjan

Gustaf Österberg, 38864

Kandidatavhandling i datateknik

Handledare: Kristian Nybom

Fakulteten för naturvetenskaper och teknik

2018

Innehållsförteckning

1. Inledning

1.1 Beskrivning av det vetenskapliga området

Konceptet blockkedja har existerat i flera årtionden, dock blev bitcoin den första som klarade av att penetrera marknaden med hjälp av den första blockkedjan. I avhandlingen gås det igenom historian bakom blockkedjan och hur blockkedjan grundades. Sedan gås det igenom de mera tekniska aspekterna för blockkedjan t.ex. nätverket, säkerhet och hur transaktioner utförs.

1.2 Vad är en blockkedja

Konceptet för blockkedjan har existerat redan sen 80-talet. Det fanns då ännu en del problem som bidrog till att blockkedjan inte lanserades före 2000-talet. Dock löste Satoshi Nakamoto problemet som de tidigare försöken på blockkedjor inte överkommit.

En blockkedja kan ses som en databas som innehåller transaktioner mellan noder i ett nätverk. Transaktionerna är indelade i block beroende på tiden för transaktionen. Blocken innehåller en referens till föregående block vilket gör blocken oföränderliga. Nätverket består av noder som alla har en kopia av databasen, vilket gör att nätverket är decentraliserat. Ett decentraliserat nätverk har ingen entitet som övervakar det utan övervakningen sker av alla användare i nätverket. Alla användare har tillgång till de tidigare transaktionerna i nätverket. Noder kan antingen passivt lagra databasen eller aktivt upprätthålla blockkedjan med hjälp av den så kallade ”mining” processen. Denna process går ut på att noder kontrollerar tidigare transaktioner för att verifiera om parterna i en transaktion är berättigade att utföra transaktionen. Block läggs till på kedjan genom att noderna som utför ”mining” löser ett matematiskt problem. Detta problem kräver en stor del av nätverkets datorkapacitet vilket gör illvilliga transaktioner osannolika då en ensam entitet inte realistiskt kan lösa problemet.

2. Historia samt ursprung för blockkedjan

2.1 Hur, när och varför kom blockkedjan till

Allting började år 2008 när Satoshi Nakamoto skickade ut ett epostmeddelande till en email lista med hundratals medlemmar. Dessa medlemmar var experter på kryptografi. Epostmeddelandet bestod av en idé som om några år kommer att revolutionera sättet man ser på pengar.

Digital valuta var dock inget nytt fenomen, flera av de experter som fick Nakamotos epostmeddelande hade själva försökt tillverka en digital valuta som var totalt decentraliserad. De hade alla misslyckats att få valutan att säkert förhindra så kallade dubbla transaktioner, vilket betyder att en person kan använda sin digitala valuta fler än en gång innan systemet hinner reagera. Nakamoto påstod dock att han löst problemet. Han visste att hans lösning innehöll två viktiga genombrott. En okränkbar databas som även kallas blockkedja. Mot denna blockkedja kunde vem som helst verifiera transaktioner vilket är en avgörande faktor för en decentraliserad digital valuta. Nakamotos lösning hade även monetärt incitament, vilket krävs för att locka användare som upprätthåller databasen. I januari 2009 satte Nakamoto igång sin algoritm och började generera de första bitcoinen. För att hela bitcoin nätverket skall fungera krävs det flera personer som använder nätverket. Nakamoto vände sig då igen en gång till kryptografiexperterna som han varit i kontakt med tidigare. Han möttes fortfarande med skeptiska tankar hos experterna och ingen verkade riktigt intresserad över vad han hade att säga. En del av experterna ansåg att det inte skulle vara lönsamt att bryta ut bitcoin då de ansåg att energikostnaderna överstiger valutans värde. Nakamoto var heller inte alls känd inom gemenskapen han försökte övertala, vilket ledde till att de inte tog honom seriöst.

2.2 Olika typer av blockkedjor

Som redan tidigare konstaterats var den första blockkedjan byggstenen för bitcoin och nutidens kryptovalutor. Ordet blockkedja förknippas ofta med kryptovalutor och framförallt kryptovalutan bitcoin. Under de senaste åren har blockkedjan förknippats med kryptovalutor vilka även i nuläge är den mest centrala användningen för blockkedjan. Kryptovalutor som t.ex. bitcoin, Etherium och Litecoin baserar sig alla på olika blockkedjor med olika egenskaper. Det finns dock andra användningsområden för blockkedjor än bara kryptovaluta. Dessa blockkedjor kallas även för ”Blockchain 2.0”. De centrala begreppen inom ”Blockchain 2.0” är mikrotransaktioner, smarta kontrakt, smart egendom, Dapps, DAOs och DACs.

2.2.1 Mikrotransaktioner

Mikrotransaktioner kan ses som väldigt små enstaka samt digitala betalningar. Det är fråga om betalningar som är för små för att kunna bearbetas kostnadseffektivt med hjälp av konventionella betalningssätt.

2.2.2 Smarta kontrakt

Smart kontrakt är mer avancerade transaktioner inom blockkedjan jämfört med valutatransaktioner och de har oftast mer utförliga instruktioner inbyggda i dem. Ett smart kontrakt är per definition liknande som ett normalt pappers kontrakt, dock finns inte risken att ena parten inte utför sin andel av kontraktet. Ett smart kontrakt har alla villkor i koden och koden utför automatiskt villkoren efter att de uppfyllts. Smart kontrakt har tre egenskaper som gör dem unika, de är autonoma, självständiga och decentraliserade. Den autonoma egenskapen bidrar till att då ett smart kontrakt väl har körts, så behöver inte parterna mera vara i kontakt, kontraktet sköter allting självständigt. Smarta kontrakt är självständiga då de kan samla in resurser genom tjänster, varefter kontrakten kan spendera resurserna på rörliga kostnader som t.ex. el och lagring. Den decentraliserade egenskapen bidrar till att kontrakten inte finns på en skild server eller specifikt fysiskt utrymme utan kontrakten finns fördelade över nätverkets noder.

2.2.3 Smart egendom

Blockkedjan kan användas för registrering av vilken som helst tillgång, inom finans, ekonomi, pengar. Man kan även registrera fysiska och icke fysiska tillgångar som t.ex. röster, idéer, hälsodata och information. Det är därmed möjligt att registrera vilken tillgång som helst i blockkedjan och dess ägare kan lätt verifieras enligt vem som har tillgångens privatnyckel. Man kan sälja sin tillgång till en annan part genom att ge privatnyckeln till parten.

2.2.4 Dapps

Förkortningen ”Dapps” står för ”decentralized applications”, vilket på svenska kan översättas till decentraliserade program. Definitionen för ”Dapps” variera en aning beroende på vem man frågar. I grund och botten är det ett program som körs på ett distribuerat sätt och vars användarinformation är skyddat.

2.2.5 DAO och DAC

Om Dapps är decentraliserade program så är DAO(”distributed autonomous organization”) och DAC(”distributed autonomous corporation”) decentraliserade organisationer och decentraliserade bolag. Både DAO och DAC är mer avancerade former av Dapps, man kan se dem som organisationer som består av flera Dapps. Artificiell intelligens är nyckelordet för att förverkliga dessa organisationer. En decentraliserad organisation kan bestå av nätverk av autonoma smart kontrakt som körs utan human insats, enligt förutbestämda regler.

3. Tekniken bakom blockkedjan

3.1 Uppbyggnad

Som tidigare konstaterats består blockkedjan av block och varje block innehåller en referens till det föregående blocket. Dock innehåller blocken en del annan information. Block huvudet innehåller metadata, som beskriver blocket. I metadata ingår föregående blockkedjas hash, blockets eget hash som innehåller en tidsstämpel, nonce värdet samt brytningens svårighetsgrad (behandlas i kapitel 3.3). Merkle träd roten är den sista delen av metadata och är en datastruktur som innehåller en summering på transaktionerna inom blocket.

3.2 Koden

Det är ganska lätt att implementera en simpel blockkedja i t.ex. Python eller Java. Python har en modul kallad hashlib för att hantera hash funktioner. Man kan lägga in vilken sträng som helst in i hashlib funktionen och den ger sedan en hexadecimal representation av strängen som output.

```
>>>print hashlib.sha1('Test').hexdigest()
```

Kodsnutten ovan ger följande hash: 640ab2bae07bedc4c163f679a746f7ab7fb5d1fa

För att komma vidare med implementation av en blockkedja behöver man definiera en klass som definierar vilka attribut blocken kommer att ha. Därefter definierar man en hash funktion som tar attributen och lägger ihop dem till samma sträng. Därefter hashas strängen. I Python när man definierar en funktion ger man in värden som attribut enligt vilka funktionen sedan exekverar när den körs. I detta exempel behöver man en tidsstämpel, transaktionens data och den föregående hashen. Tidstämpeln är viktig eftersom den ger blocket en unik parameter som inte går att replikera senare. Data är den information som transaktionen innehåller och tidigare hash är den föregående hashen i kedjan och gör så att det nya blocket refererar till det föregående och kan därmed inte ändras efteråt. Börjar med att konstruera en class i Python som beskriver blockets egenskaper.

```
import hashlib
class Block:
        def __init__(self, timestamp, data, tidigare_hash):
                self.timestamp = timestamp
                self.data = data
                self.tidigare_hash = tidigare_hash
                self.hash = self.blockhash()
```

Därefter definierar man en hash funktion som lägger ihop attributen till en sträng och hashar den.

```
def blockhash (self)
        blockhash = hashlib.sha1()
        blockhash.update (
                str(self.timestamp) +
                str(self.details) +
                str(self.tidigare_hash) )
        return blockhash.hexdigest()
```

3.3 Matematiken

För att förstå matematiken bakom blockkedjan är det viktigt att förstå benämningen ”proof-of-work”. Proof-of-work system kräver användare att utföra ett arbete för att delta i systemet. Det är essentiellt att arbetet är svårt för användaren men lätt att verifiera för serven. Hashcash är ett av de mest kändaste proof-of-work system och det används även i bitcoin. För att förklara vad Hashcash gör är det viktigt att förstå vad en hash är. Ett hash kan anses som en krypterad version av en sträng data. Varje sträng data har en unik hash och varje hash refererar till endast en sträng data. Om data ändras då ändras även hashen. Ett hash produceras matematiskt sätt av en hash funktion, det är viktigt att inputstorleken och outputstorleken är väldigt stora så att inte kollisioner sker, alltså två inputs som ger samma output. Hash funktioner används mest för att lagra lösenord i databaser. Då en användare registrerar ett lösenord så ändras det till en hash och lagras i databasen. Då användaren loggar in på nytt ändras lösenordet igen till ett hash och om det stämmer överens med hashet i databasen så kan användaren logga in. Det finns en del olika hash funktioner t.ex. ”Secure Hash Function” (SHA1, SHA256, SHA512, etc.). Hashcash går då alltså ut på att man går igenom olika hash, i detta fall SHA256, tills man hittar det efterfrågade hash värdet. Den efterfrågade hashen börjar med ett antal nollor, beroende på den önskade svårighetsgraden, desto flera nollor i början av hashen desto svårare är den att lösa.

```
"Hello, world!0" => 1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64
"Hello, world!1" => e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8
"Hello, world!2" => ae37343a357a8297591625e7134cbea22f5928be8ca2a32aa475cf05fd4266b7
...
"Hello, world!4248" => 6e110d98b388e77e9c6f042ac6b497cec46660deef75a55ebc7cfdf65cc0b965
"Hello, world!4249" => c004190b822f1669cac8dc37e761cb73652e7832fb814565702245cf26ebb9e6
"Hello, world!4250" => 0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9
```

3.4 Säkerheten

Då en blockkedja använder ”proof of work” medför det ett ganska stort problem med tanke på säkerheten för nätverket. Ett exempel på en säkerhetsrisk är ”The Majority Attack”. Attacken går ut på att en entitet, det kan vara en nod i nätverket eller en grupp noder (även kallade ”mining pools”) som innehar över 51% av nätverkets datorkapacitet. När detta sker så kan entiteten i fråga hitta lösningen på det matematiska problemet snabbare än de andra och har därmed makten att bestämma vilket block som accepteras till blockkedjan. Om man då löser flera block i rad så är det möjligt att kontrollera vilka transaktioner som accepteras och man kan även modifiera blocken. Denna sort av attack var tidigare mer aktuell då storleken på nätverket var mindre och det var lättare att uppnå en större andel av nätverkets datorkapacitet. Nuförtiden är en sådan attack praktiskt taget omöjlig. Om företaget Google år 2015 skulle ha lagt all sin datorkapacitet på att försöka ta över bitcoin:s nätverk så skulle Google endast uppnått 1% av den totala datakapaciteten av nätverket. Då hade bitcoin:s nätverk en hashrate på 350 000 terahash/sekund. Nuförtiden har nätverket en kapacitet på ca 26 000 000 terahash/sekund (14.04.2018).

En annan säkerhetsrisk sker då nätverket uppdateras med en ny mjukvaruuppdatering. Då en ny uppdatering lanseras är det möjligt att alla noder på nätverket inte installerar uppdateringen samtidigt. Då förgrenar sig kedjan och de som använder den gamla versionen fortsätter att bygga på den gamla kedjan och noderna som installerat uppdateringen grenar sig och fortsätter bygga kedjan på en parallell kedja (hard fork). Det finns två olika typer av förgreningar (fork), mjuka förgreningar (soft fork) och hårda förgreningar (hard fork). Då en hård förgrening sker accepterar den gamla kedjan inte den nya kedjans block.

http://ieeexplore.ieee.org/xpls/icp.jsp?arnumber=7796940

4. Blockkedjans användningsområden

4.1 Blockkedja inom leveranskedjan

Leveranskedjan är ett nätverk som innehåller processer för att leverera material och produkter från säljaren till köparen. Den består av leverantörer som bidrar med råmaterial, producenter som förädlar råmaterialet till produkter, distributörer som levererar produkterna till återförsäljare som sedan säljer produkterna till den slutliga användaren.

Enligt Europaparlamentet ingår leveranskedjan i en 16 biljoner dollar stor leveranskedjesektor. Det finns då ett stort intresse för att utveckla denna sektor för att få bort mellanhänder och få ner priserna. Leveranskedjan innehåller komplexa processer för att hantera logistik, betalningar, kontrakt, motverkning av förfalskning och bedrägeri. Ett problem med leveranskedjan är att det är en dyr process och priserna reflekterar ofta inte produktens verkliga värde. Det är väldigt svårt för konsumenten att veta hur produkten producerats, med vad för material och med vilka potentiella skador för arbetarna och miljön. Som konsument måste man helt enkelt lita på processen och alla komponenter inom den.

Med hjälp av blockkedjan kan man ta bort en stor del av komponenterna inom leveranskedjan och därmed få ner priserna. Man kan öka transparensen inom leveranskedjan via en distribuerad blockkedja som alla parter inom leveranskedjan har tillgång till. Via autonoma smart kontrakt kan man dra ner på priser och öka säkerheten inom leveranskedjan.

Ett stort problem leveranskedjan är förfalskande av produkter. Man skulle kanske inte tro att det är ett stort problem men förfalskade produkter skadar ekonomi och kan även producera hälso- och säkerhetsrisker för användarna. En lösning till problemet är BlockVerify. Ett användningsområde för BlockVerify är inom medicinindustrin, förfalskning av mediciner är ett stort problem och förorsakar stora mängder ekonomiska och humana förluster varje år. Med hjälp av BlockVerify kan man verifiera medicin lådor inom leveranskedjan och informationen finns allmänt tillgänglig på blockkedjan.

http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8024092

http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7948864

4.2 Blockkedja inom den finansiella sektorn

Den finansiella sektorn är en stor del av den globala ekonomin, ungefär 16,9% vilket ger sektorn ett värde på ungefär 13,1 biljoner. På grund av storleken på sektorn finns det mycket möjligheter till nedskärningar av transaktionskostnader och mellanhänder. Man kan helt eller till en viss del bli av med t.ex. valutaväxlare, investeringsbankirer, revisorer och advokater. Den europeiska banken Santander har räknat ut att en blockkedja kan spara 20 miljarder dollar för bankens kunder i transaktionsavgifter. Konsultföretaget Capgemini konstaterar också att deras kunder kan spara upp till 16 miljarder dollar med hjälp av blockkedjeteknologi.

https://www.investopedia.com/ask/answers/030515/what-percentage-global-economy-comprised-financial-services-sector.asp

https://www.bedicon.org/wp-content/uploads/2018/01/finance_topic2_source2.pdf

Det finns redan olika teknologier som med hjälp av blockkedjan kan dra ner på transaktionskostnader inom den finansiella sektorn. Ett bra exempel är Ripple Labs som med hjälp av deras betalnings nätverk kan ge banker möjligheten att överföra tillgångar till andra banker utan utomstående mellanhänder. Ripple har även en kryptovaluta som är den tredje största kryptovalutan med ett marknadsvärde på 26,5 miljarder dollar (13.4.2018). Ripples fördel är möjligheten att leverera väldigt många transaktioner väldigt snabbt, enligt deras hemsida klarar dom 50000 transaktioner per sekund, vilket är dubbelt mer än vad kreditföretaget Visa klarar. Som jämförelse klarar bitcoin av 3-6 transaktioner per sekund. Många banker har visat intresse för Ripple och har även testat Ripple teknologi.

https://oracletimes.com/xrp-ripple-surpasses-visa-transaction-speed/

4.3 Implementationer av blockkedjor

Det finns en massa exempel på blockkedjor och användningsområden för dem är enorma. I detta delkapitel vill jag ta fram de största och centralaste exemplen på hur blockkedjan har implementerats.

4.3.1 Hyperledger

I december 2015 grundade The Linux Foundation ett initiativ som kallas Hyperledger. Det är ett samarbete för att öka utvecklingen av blockkedjor inom olika branscher. Hyperledger grundar sig på öppen källkod som då allmänheten har tillgång till och som får användas till egna projekt. Plattformen ger möjligheten för utvecklare att utveckla egna blockkedjor, med anpassade inställningar. Företaget IBM har fungerat som en stor investerare i Hyperledger och använder det för sin egen blockkedja men även för att utbilda omvärlden över konceptet blockkedjor. IBM använder blockkedjan för att spåra varor med högt värde inom leveranskedjan. Everledger är annat initiativ som baserar sig på IBM:s blockkedja och är med också med och stöder Hyperledger. Blockkedjan Everledger används huvudsakligen för att spåra diamanter inom leveranskedjan och för att monitorerna överensstämmelser över etiska standarder i Afrika. Man kan även använda Everledger för att verifiera legitimiteten för vinflaskor och konst.

4.3.2 Ethereum

Projektet Ethereum är den näst största blockkedjan och en av de snabbast växande blockkedjorna. Projektet är en decentraliserad plattform för dapps och har en egen kryptovaluta kallad Ether och plattformen stöder utvecklandet av projekt inom blockkedjor. På kryptovalutamarknaden har Ethereum ett marknadsvärde på 52.7 miljarder dollar (19.04.2018) vilket är en andel på 15% av den totala kryptovalutamarknaden.

Filosofin bakom Ethereum protokollet kan indelas i fem olika kategorier. **Enkelhet** (simplicity) är viktigt eftersom grundprincipen bakom Ethereum är att även en medelmåttig programmerare skall kunna använda Ethereums blockkedja. Man är även villig att ge upp en del prestanda inom datalagring och tidsineffektivitet för att uppnå enkelheten. Ethereums **mångsidighet** (universality) betyder att det inte finns

extra funktioner utan varje användare kan själv programmera sina smarta kontrakt. Till skillnad från bitcoin kan man inom Ethereum programmera turing fullständiga scripts, vilket betyder att man kan programmera allting som är matematiskt definierbart. **Modulariteten** inom Ethereum ger möjligheten att implementera eller modifiera små delar av protokollet utan att det påverkar andra delar. Funktioner och verktyg för Ethereum bör implementeras som skilda bibliotek så att de kan användas inom vissa Ethereum projekt men inte behöver användas i andra. **Smidigheten** inom blockkedjan möjliggör förändringar av protokollet. Gemenskapen är dock väldigt noga med att göra korrekta förändringar och vem som helst har inte rätten att ändra på större delar av blockkedjan. Vid stora förändringar håller man röstningar inom gemenskapen för att bestämma om en förändring skall ske. Ett exempel på detta är ”The DAO hack” då en hacker tog mer än 3.6 miljoner ether, vilket i dagen läge är värt ca 2.16 miljarder dollar. Ethereums gemenskap röstade för att utföra en uppdatering som återkallade transaktionerna som hackern utförde och därmed returnerades pengarna.

http://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=8927100&fileOId=8927102

Referenser

1. 2.1 - The Age of Cryptocurrency: How Bitcoin and the Blockchain Are Challenging the Global Economic Order
2. 2.2 - Melanie Swan
3. 3.2 - https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8024092&tag=1
4. 4.1 - https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7948864
5.