Blockkedjor och deras användningsområden

Matias Kytömäki
Kandidatavhandling
Datateknik
Fakulteten för naturvetenskaper och teknik
Åbo Akademi
Handledare: Mikhail Barash

Referat

Att representera pengar och andra sorter av tillgångar digitalt har länge varit ett problem. Det krävs en tredje part, som oftast representeras av en bank, som har en översikt över hur tillgångarna används för att försäkra att ingen missbrukning av tillgångarna förekommer. Det här systemet är tidskrävande, dyrt och kräver att alla litar fullständigt på den tredje parten. Blockkedjan kan vara lösningen till hur man kan representera tillgångar på ett säkert sätt utan att ha ett behov för en tredje part. Blockkedjan kan också vara en lösning inom andra områden än ekonomi, till exempel kan den användas för röstning, inom hälsovård och andra statliga sektorer.

Denna avhandling kommer att behandla blockkedjans struktur, hur den används för att representera kryptovalutor och vilka andra användnings områden som blockkedjan kan användas till. Olika säkerhetsaspekter och problem som finns med blockkedjan kommer också att i viss mån tas upp i avhandlingen.

Syftet med avhandlingen är att ge läsaren en överblick över hur blockkedjor är strukturerade och varför blockkedjan är en stark kandidat till att representera information nu och i framtiden.

Innehåll

1 Introduktion

//TODO

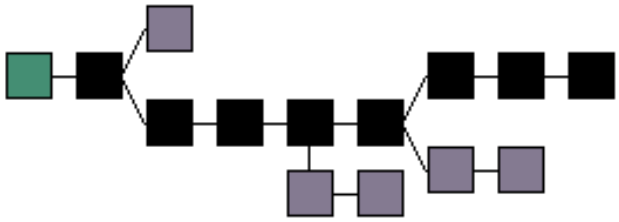
2 Blockkedja

En blockkedja representerar en lista av händelser eller transaktioner, beroende på användningsområdet, som sparas i block som är länkade till varandra och bildar en kedja. Blockkedjor är decentraliserade och distribuerade, varför det inte behövs en administrativ part som håller reda på händelserna, utan istället hanteras händelserna av användarna [8]. Strukturen hos en blockkedja gör att information som redan finns i den inte kan ändras utan man kan endast lägga till händelser [9]. Dessutom används öppna och hemliga nycklar för att kryptera informationen som finns i blockkedjan. Varje användare av en blockkedja har både en egen hemlig och en egen öppen nyckel. Den hemliga nyckel fungerar som ett lösenord och bör hållas hemlig från andra användare. Den öppna nyckeln är till för att delas med andra användare. Med hjälp av den öppna nyckeln kan en användare initialisera en transaktion. Den hemliga nyckeln i sin tur används för att verifiera transaktioner, när man vill överföra tillgångar till en annan användare [12]. Med hjälp av öppna och hemliga nycklar kan alla användare kontrollera hur mycket tillgångar en användare har, men endast ägaren av tillgångarna kan flytta på dem. Alla transaktioner som sker verifieras av andra användare innan de blir godkända [8]. Dessa egenskaper gör blockkedjor väldigt säkra och effektiva.

2.2 Struktur

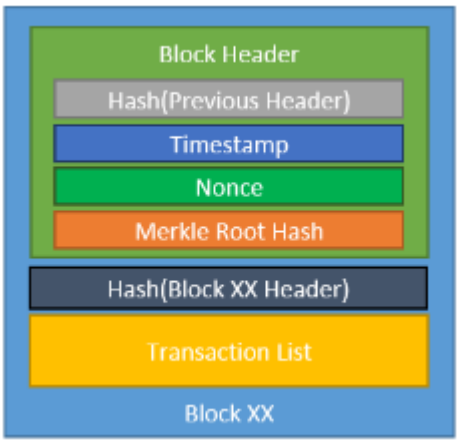
Varje blockkedja har ett start block som kallas för genesisblocket representeras av det gröna blocket i figur 1. Huvudkedjan är den kedja som har största antalet block och har sitt ursprung i genesisblocket, huvudkedjan består av det svarta blocken och det gröna blocket i figur 1. Block som finns utanför huvudkedjan kallas för föräldralösa block, dessa block är grå färgade i figur 1. Föräldralösa block förekommer när två block blir

skapade samtidigt [11]. När två block skapas samtidigt fördelas blockkedjan i två olika grenar (eng. forking), den grenen som stöds av majoriteten blir huvudkedjan [10].



Figur 1: En grafisk representation av en blockkedja [13].

Varje block har ett blockhuvud som består av en hash av föregående blocks blockhuvud, en tidsstämpel, en Merkle rot hash och ett randomiserat godtyckligt nummer (eng. nonce). Förutom blockhuvudet har blocket en lista på transaktioner samt en hash av sitt eget blockhuvud [10]. Ett exempel på ett block kan ses i figur 2. Varje del av blocket kommer att gås igenom mera i detalj inom detta kapitel.



Figur 2: En bild som åskådliggör uppbyggnaden av ett block i en blockkedja [10].

Blockkedjan struktur baserar sig på att varje block är länkad till föregående block med hjälp av deras respektive hash. Varje block i en blockkedja har en unik hash som skapas med hjälp av en hash-funktion. Med hjälp av hashfuntionen skapar man en relativt unik

identifierare på basis av den information som finns i det föregående blocket. Minsta ändring i informationen ändrar på hashen som skapas [14]. Ett exempel på hur hashen kan se ut finns i figur 3. Man kan genom att kontrollera hashen se ifall informationen har ändrats. Ifall man vill ändra på ett block som finns i blockkedjan måste man också ändra på alla blocken som följer det block man vill ändra på [10]. Detta system gör det i praktiken omöjligt att ändra på informationen som finns lagrad i en blockkedja.

Ett stort antal av de blockkedjor som finns i dagens läge använder sig av SHA-256 (eng. Secure Hash Algorithm) för att skapa en hash. Denna algoritm ger identifieraren en storlek på 256 bitar. Hash-algoritmerna fungerar endast ena vägen, det är i praktiken omöjligt att utgående från en hash skapa informationen som den representerar [10].

Input Text	SHA-256 Digest Value
1	0x6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01e52ddb7875b4b
2	0xd4735e3a265e16eee03f59718b9b5d03019c07d8b6c51f90da3a666eec13ab35
Hello, World!	0xdffd6021bb2bd5b0af676290809ec3a53191dd81c7f70a4b28688a362182986f

Figur 3: Till vänster i tabellen finns insättningsvärdet och till höger finns respektive hash resultat efter användning av SHA-256 [10].

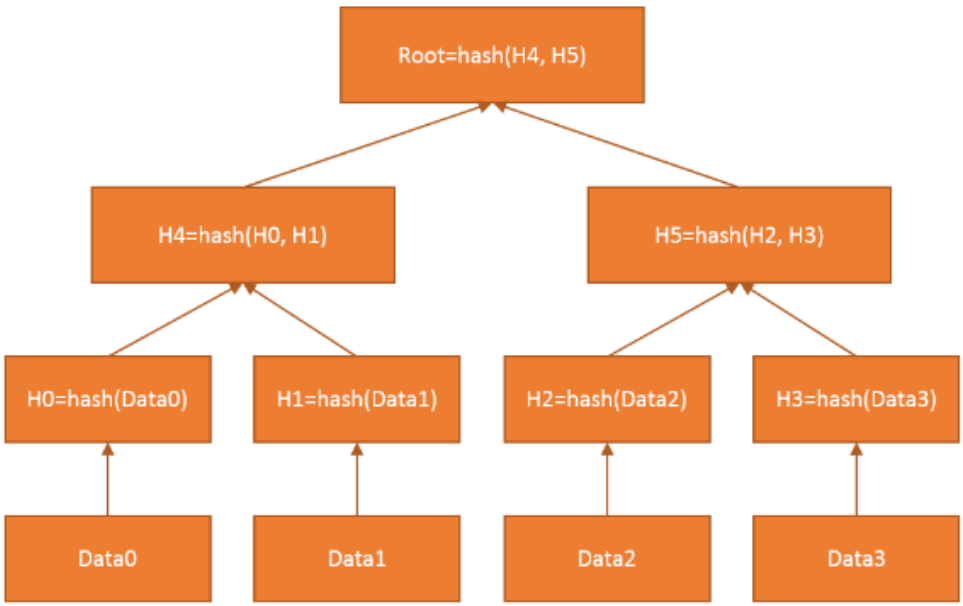
Blockkedjor har fördefinierade krav på hur en hash skall se ut, för att kunna kontrollera tiden det tar att lägga till nya block i blockkedjan. För att kunna ändra på hur hashen ser ut har varje block ett randomiserat eller pseudo-randomiserat godtyckligt nummer som manipuleras vid skapningen av blocket, för att uppfylla kraven på hashen [11].

Tidsstämpel inkluderas också i blockhuvudet. Tidstämpeln är ett bevis på att händelserna som sparas i blocket har existerat vid skapningen av blocket. Stämpeln sätts inuti blockhuvudet för att den skall inkluderas i hashen som skapas, detta förstärker ytterligare blockkedjans struktur [5].

Informationen som sparas i blockkedjor är oftast transaktioner. En transaktion innehåller information om hur stor mängd av tillgångar som flyttas. Transaktionen har

också en lista på tillgångarna som flyttas, och varje tillgång har en unik identifierare. Även mottagarna och en identifikation finns i transaktionen. En mängd av transaktioner bildar ett block i blockkedjan. Efter att ett antal transaktioner har blivit skapade bildas ett block som innehåller dessa transaktioner. Varje transaktion blir digitalt signerad av den som överger tillgångar. Signeringen görs med en hemlig nyckel och kan verifieras av andra noder med hjälp av en öppen nyckel. Blocket bildas när transaktionerna har blivit verifierade och blocket läggs till i blockkedjan först när blocket har blivit verifierad av andra noder [5].

Alla transaktionerna sparas i sin helhet i blocket, men de inkluderas inte i blockhuvudet på grund av sin storlek. Trots detta måste transaktionerna sparas i någon form i blockhuvudet för att de skall inkluderas i blockhuvudets hash och på detta sätt förstärka blockkedjans struktur. För att lösa det här problemet används ett Merkle träd. Man börjar med att bilda en hash för varje enskild transaktion, efter detta kombinerar man hashen ända tills man når roten, ett exempel på Merkle trädet finns i figur 4. Roten som bildas av transaktionernas hash kallas för Merkle trädets rot hash och den kombinerar alla transaktionernas hash. Ifall någon försöker ändra på en transaktion i blocket kommer detta att synas, som det tidigare konstaterats, syns den minsta ändringen i informationen också i hashen [10].



Figur 4: Ett exempel på hur en Merkle rot hash skapas [10].

Användningen av Merkle trädets rot hash i blockhuvudet, ger friheten att radera själva transaktionerna. Bitcoin använder i sin blockkedja ett system som radera gamla transaktioner efter att samma Bitcoin har blivit flyttat ett godtyckligt antal gånger. Genom att radera gamla transaktioner kan man minska storleken på blockkedjan utan att förstöra kedjans struktur, eftersom Merkle rot hashen fortsättningsvis kommer att existera i blockhuvudet även om själva transaktionerna raderas [5].

Alla som använder sig av blockkedjan representeras av en nod. Noder kan indelas in i två huvudklasser, fulla noder och lättviktsnoder. Fulla noder har en egen lokal version av hela blockkedjan medan lättviktsnoder endast har en del av blockkedjan. Varje gång ett block skapas av en full nod måste blocket verifieras av andra fulla noder för att kunna läggas till i blockkedjan. Noderna verifierar att varje transaktion är signerad och att hashen både för transaktionerna och för själva blocket har blivit rätt uträknade.

För att skapa ett block krävs det att en dator utför en mängd beräkningar. Detta betyder att någon måste offra processortid för att skapa ett nytt block till blockkedjan. För att få användare att skapa nya block, fungerar de flesta blockkedjor med den principen att de ger en viss mängd tillgångar åt den som skapar ett block. Man vill heller inte att blockkedjan ska växa alldeles för snabbt, och därför kräver de flesta blockkedjorna att användaren utför ett antal väldigt tunga beräkningar för att bevisa att de har offrat tid och resurser på att skapa det nya blocket. Beräkningarna som utförs är gjorda så att det är väldigt tidskrävande för en dator att lösa de matematiska problemen men att verifiera svaret är väldigt enkelt. Problemen som ska lösas har ofta att göra med hur hashen ska se ut eftersom beräkningen av hashen är väldigt tidskrävande. [5]

3 Kryptovaluta

Den första kryptovalutan Bitcoin, skapades av en person eller grupp som använder sig av ett pseudonym, Satoshi Nakamoto. Grundidén för Bitcoin var att skapa en valuta som inte är beroende av en tredje part. Iden är baserat på det faktum att internetet skall vara tillgängligt åt alla och alla skall hanteras lika. Andra motiveringar till skapningen av Bitcoin var att man ville skapa en valuta som är kostnadsfri att använda. Bitcoin är baserat på kryptografiskt bevis istället för tillit för en tredje part [5]. Alla transaktioner gjorda med Bitcoin är irreversibla och enda möjligheten att ändra på en kryptovalutas egenskaper, som till exempel nya koncept eller implementationer, är att majoriteten av användarna röstar för en ändring, det här kallas för ”forking” [10], som kommer att diskuteras mera i detalj inom detta kapitel. Kapitel tre kommer också att behandla kryptovalutor i allmänhet och hur skapningen eller egentligen brytningen av kryptovalutor sker.

En kryptovaluta, som till exempel Bitcoin, kan enligt Melanie Swans bok [1] delas in i tre olika lager, själva kryptovalutan, protokoll och klient samt blockkedjan. Blockkedjan beskrivs i Swans bok som den underliggande tekniken för en kryptovaluta. Blockkedjan är synlig för alla, den uppdateras av brytare och ägs inte av någon. Protokoll och klient lagret är mjukvaran som möjliggör utförandet av transaktioner och det sista lagret är den egentliga valutan [1].

Krypterade blockkedjor används för att representera transaktioner av kryptovalutor. En kryptovaluta kan använda sig av egen blockkedja eller spara sina transaktioner i en annan kryptovalutas blockkedja [2]. Blockkedjor fungerar med hjälp av P2P-nätverk, ett icke-hierarkiskt nätverk, samma princip används också i olika fildelnings-program så som Bittorrent [3]. När en nod vill lägga till information i blockkedjan, i de flesta fall transaktioner, skickar noden ut informationen till dess närliggande noder, vars uppgift är att verifiera transaktionens giltighet [4]. Ifall transaktionen är giltig sätts den till i en kö med andra transaktioner som väntar på att bli en del av blockkedjan. Det finns ett antal fall där transaktioner inte godkänns av närliggande noder, en lista över de mest allmänna fallen finns i figur 4. Som det redan tidigare nämnts är blockkedjan

synlig för alla, detta innebär att varje nod har en egen kopia av blockkedjan, som är den nyaste versionen som noden känner till.

Type	Description
Repeated	The transaction has already been relayed recently.
Old	The transaction is already in the main block chain.
Double-Spend	The transaction attempts to claim an output already claimed by a previous transaction.
Bad Signature	The input signature(s) cannot be verified (e.g. attempting to spend someone else's coins).
Orphan	One or more of the outputs claimed by the inputs cannot be found.

Figur 4: En lista på de mest allmänna orsakerna till att en transaktion inte blir godkänd [4].

En kryptovaluta baserar sig på blockkedjans struktur och har alltså samma egenskaper som en blockkedja. Det här faktumet innebär att det flesta kryptovalutor har liknande egenskaper sinsemellan. Alla kryptovalutor har ett definierat antal start mynt som finns i genesisblocket av blockkedjan.

Brytning av Bitcoin

Att bryta Bitcoin betyder att man skapar nya block till blockkedjan. Brytningen utförs av fulla noder eller så kallade brytande noder. Brytning är ett av det viktigaste koncepten inom kryptovalutor. Brytning skapar inte enbart nya block, utan det är också ett sätt att introducera nya pengar till kryptovalutan [7].

Brytningen av Bitcoin går ut på att, när det finns ett tillräckligt antal av nya transaktioner för att bilda ett block, behövs det en hash åt blocket. Det är brytarnas uppgift att skapa en hash. Det krävs processortid för att bilda den nya hashen och man kan reglera tiden det tar att bilda ett nytt block genom att ge krav på hur hashen skall se ut. Inom Bitcoin brytning krävs det att hashen börjar med ett antal noll bitar för att kunna accepteras [5]. Eftersom man inte kan veta på förhand hur en hash kommer att se ut, har varje skapning av en hash lika stor sannolikhet att vara giltigt. Det här leder till att desto snabbare en brytare kan skapa en hash desto större sannolikhet har brytaren att vara den första som skapar en giltig hash åt blocket. Brytaren som först skapar en

ny hash åt det nya blocket kommer att få en belöning i form av Bitcoin för sitt utförda arbete [7].

Brytning kan göras individuellt eller genom att ett antal noder samarbetar för att skapa en hash. Ifall brytningen utförs av en grupp kommer varje enskild nod att belönas procentuellt lika stor del som noden har kontribuerat till att skapa hashen.

Problemet med dubbel spendering

Ett av det största problemen med att virtuellt representera pengar är att man måste se till att pengar inte blir spenderade dubbelt. För att kunna undgå detta problem används en pålitlig tredje part som måste verifiera transaktionerna så att pengar inte används dubbelt. Problemet med denna lösning är att man måste fullt lita på den tredje parten och att den sköter sina uppgifter, hela valutan är beroende av denna part. Enligt Satoshi Nakamotos artikel [5] löser Bitcoin problemet med dubbel spenderings på ett sätt som inte kräver en tredje part. Lösningen till problemet var att spara alla transaktioner i en blockkedja som alla användare har tillgång till och varje transaktion verifieras med hjälp av bevis-på-arbete. Tekniken är dock inte fullständig. Det finns ett antal artiklar och forskningar som bevisar att Bitcoin inte har löst problemet fullständigt. Karame, Androulaki och Capkun skriver i sin artikel ”Double-spending fast payments in bitcoin”[6] att man kan missbruka systemet när det gäller snabba betalningar. Orsaken till att systemet kan missbrukas beror på att Bitcoin skapar nya block till blockkedjan med ungefär tio minuters mellanrum. En transaktion blir fullständigt verifierad först när den sätts till i blockkedjan, men i praktiken finns det inte alltid tid att vänta i tio minuter innan en betalning blir godkänd.

4 Applikationer

Blockkedjans egenskaper gör den till en väldigt stark kandidat att användas som ett sätt att lagra information. Problemen som finns i dagens läge, är koncentrerade på säkerhet,

kostnad och åtkomst. Blockkedjans struktur gör att den löser en stor del av dessa problem och det finns ett stort antal forskningar som studerar de olika möjligheterna som blockkedjan har att erbjuda på [9].

Kapitel fyra kommer att behandla ett antal olika användningsområden för blockkedjor. En del av texten kommer att referera till olika källor gällande texter om de olika användningsområden som finns, och den andra delen av texten kommer att bestå av diskussioner över respektive användningsområdena. Kapitel fyra är indelad i två olika huvudgrupper, smarta kontrakt samt samhälleliga användningsområden.

Smarta kontrakt

Ett användningsområde som redan finns tillgängligt för blockkedjor är smarta kontrakt. Ett konkret exempel på smarta kontrakt finns implementerad i till exempel Ethereums blockkedja. Smarta kontrakt kan fungera som ett tillägg till vanliga transaktioner eller så kan man använda sig endast av smarta kontrakt. Definitionen för smarta kontrakt är att den består av kod samt data som finns med i blockkedjans struktur. Smarta kontrakt kan utföra ett antal olika funktioner, beroende på hur kontrakten är definierade. Olika uppgifter som kan göras med hjälp av smarta kontrakt är till exempel datorberäkningar, bekräfta olika saker eller spara någon sort av information, annat än transaktioner [10].

Smarta kontrakt är ett säkert sätt att utföra olika saker, eftersom koden för att utföra smarta kontrakt är inkluderat i blockkedjan och blockkedjans struktur är oföränderlig. En annan orsak som bidrar till säkerhetsaspekten är att smarta kontrakt ger en möjlighet att bekräfta händelser utan behov av en tredje part. Smarta kontrakt kan automatisk flytta på en del tillgångarna när en transaktion görs, den här händelsen motsvarar betalningen av skatt. En implementation kunde vara att när lönen betalas ut på blockkedjan dras skatten av automatiskt med hjälp av ett smart kontrakt inbyggt i blockkedjan.

Smarta kontrakt består som tidigare nämnts av kod och data. Koden som finns inbyggt i blockkedjan utförs av brytande noder. För att utföra beräkningarna som krävs för smarta kontrakt krävs det mera beräkningskapacitet än det krävs för att bekräfta vanliga

transaktioner. På grund av detta, är det oftast implementerat i blockkedjan att det krävs en betalning för att utföra det uppdraget som har blivit ställt på smarta kontraktet. Brytningen av transaktioner sker som vanligt, vilket innebär att brytaren får mynt i belöning, men för att utföra smarta kontrakt krävs det en betalning av den som gör en förfrågning på att utföra ett smart kontrakt. För att undvika DDOS attacker är smarta kontrakt begränsade till ett vist tidsintervall. Genom att definiera ett tidsintervall kan man se till att beräkningarna inte tar för länge att utföra, det här ser till att inte brytande noder blir utsatta för oändliga loopar, vilket skulle totalt frysa noden [10].

Samhälleliga applikationer

Allting som stater och andra liknande maktapparat kontrollerar, så som hälsovård, röstning, egendom samt många andra områden, kräver enorma mängder data. Av dessa data krävs det att de är tillgängliga hela tiden och att de bevaras på ett säkert sätt så att endast personer med behörighet har åtkomst till data.

Röstning

Elektronisk röstning är något som flera stater håller på att utreda för tillfället. Största problemet med elektronisk röstning är att bevara säkerheten. Man vill garantera alla röstare valhemlighet och man måste också kunna garantera att utomstående parter varken kan komma åt eller ändra informationen. Ett annat problem är att alla röster måste registreras och sparas för att valresultatet skall vara giltigt.

I Finland har det gjorts försök på fullständigt elektroniska röstningar, där personer endast röstar elektronisk och ingen pappersverifikation på röstningen finns. Försöket gjordes år 2008 inom kommunerna Högfors, Grankulla samt Vichtis och den elektroniska röstningen kunde endast göras via de apparater som fanns på röstningsställen [15].

Genom att använda blockkedjor kan man skapa ett system för elektronisk röstning som gör det möjligt att rösta varifrån som helst. Alla röstberättiga personer skulle bli registrerade som användare av blockkedjan och varje användare skulle bli tilldelad en röst. Användarna skulle ha åtkomst till sin röst via ett användargränssnitt som skulle vara åtkomlig via en elektronisk apparat med internet uppkoppling. Varje användare skulle ha ett eget lösenord som skulle ge åtkomst till den hemliga nyckeln, som används när rösten registreras. Alla röster skulle sparas i blockkedjan på samma sätt som transaktioner. Varje röst skulle verifieras av andra användare innan rösten blir giltig. Enligt samma princip som med kryptovalutor kan varje röst verifieras av andra användare via öppna nycklar[16].

Blockkedjans decentraliserade struktur har också bidragit till koncept som försöker göra demokrati effektivare. Till exempel Liquid Democracy, där alla användare har möjlighet att bli vald. System fungerar så att man tilldelar varje användare en röst och användaren kan rösta på vem som helst som finns i samma blockkedja. Rösterna kan också flyttas när som helst, där av namnet Liquid Democracy (flytande demokrati). Detta system för röstning kan användas på många olika områden utöver politiska val. Problem med systemet är bland annat stabiliteten [1].

Identifikation

För att identifiera personer på nätet används många olika medel beroende på hur säker man måste vara på en persons identifikation. Många sidor har den egenskapen att man logga in genom att använda sig av sociala medier som till exempel Facebook. Andra sidor använder sig av MAC-adresser, som är unika identifierare som finns i varje nätverkskort. Ett tredje alternativ är att använda bankernas identifikations system för att identifiera personer. Alla dessa alternativ har sina respektive problem. Sociala medier till exempel anses inte vara väldigt säkra och de kan skapas av vem som helst, dessa konton kan också ändras när som helst. Problemet med MAC-adresser är att de endast identifierar nätverkskortet, inte nödvändigtvis personen som äger kortet. MAC-adresser kan också ändras med hjälp av olika verktyg [17]. Bankverifikation anses vara

ett ganska säkert sätt att identifiera personer men de är invecklade och verifikationen tar en längre tid att utföra.

Det finns ett antal olika försök där man använder blockkedjor för att identifiera användare. Dessa implementationer fungerar på olika sätt och används för olika ändamål [18]. En del av tjänsterna som erbjuder identifikation använder sig av kryptovalutor för igenkänning av användare. Varje användare som har en virtuell plånbok för till exempel Bitcoin har en identifierare för sin plånbok. Denna identifierare, även så kallad plånboksadress, är personlig och kan därför användas som en identifierare för en användare.

OneName är ett exempel på en tjänst som erbjuder identifiering och som använder sig av Bitcoin blockkedjan. OneName ger användare möjlighet att själv skapa ett användarnamn som används istället för plånboksadressen. Användarnamnet är mycket lättare för människor att använda än det invecklade Bitcoin adressen. Användningen av OneName är lätt, snabbt och har relativt hög säkerhet. Säkerheten kommer från blockkedjans egenskaper och baserar sig på öppna och hemliga nycklar. Med öppna nyckeln kan man verifiera en användares identifikation utan att fråga efter personlig information. Eftersom användarnamnet är länkat till en Bitcoin plånbok kan användare enkelt göra betalningar med samma konto, på en webapplikation som stöder Bitcoin, utan att göra övriga identifieringar [1].

Hälsovård

//TODO

5 Referenser

[1] Swan Melanie, Blockchain Blueprint for a New Economy

[2] http://kevinriggen.com/files/sidechains.pdf

[3] http://pages.cpsc.ucalgary.ca/~carey/CPSC641/archive/Sept2004/notes/p2p/torrent.pdf

[4] https://www.ifca.ai/fc14/papers/fc14_submission_71.pdf

[5] https://bitcoin.org/bitcoin.pdf

[6] https://www.eecis.udel.edu/~ruizhang/CISC859/S17/Paper/p9.pdf

[7] https://arxiv.org/pdf/1112.4980.pdf

[8] http://design.inf.usi.ch/sites/default/files/biblio/2016_WICSA_BlockChainSoftwareConnector.pdf

[9] http://www.cs.unibo.it/~montesi/CBD/Articoli/2017Blockchain.pdf

[10] https://csrc.nist.gov/CSRC/media/Publications/nistir/8202/draft/documents/nistir8202-draft.pdf

[11] https://arxiv.org/pdf/1505.05343.pdf

[12] Olleros F. Xavier och Zhegu Majlinda, Research Handbook on Digital Transormations, 2016

[13] https://en.bitcoin.it/wiki/File:Blockchain.png

[14] http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8246573

[15] http://www.vaalit.fi/material/attachments/vaalit/vaalitietoa/kehittamishankkeet/6Ku3Plfex/Sahkoinen_aanestaminen_tekninen_toteutus_ja_tietoturva.pdf

[16] https://www.researchgate.net/profile/Georgios_Foroglou/publication/276304843_Further_applications_of_the_blockchain/links/5556f20608ae6fd2d8237a34/Further-applications-of-the-blockchain.pdf

[17] https://www.getsmarter.com/career-advice/wp-content/uploads/2017/07/mit_blockchain_and_infrastructure_report.pdf

[18] https://www.cs.bgu.ac.il/~frankel/TechnicalReports/2016/16-02.pdf