Examensarbete

HÖGSKOLAN I SKÖVDE

NYCKELHANTERING FÖR BITCOIN

En studie om hur användare hanterar privata nycklar och hur säkerheten kan förbättras

KEY MANAGEMENT FOR BITCOIN

A study on how users manage private keys and how security can be improved

Examensarbete inom huvudområdet informationsteknologi med inriktning mot nätverks- och systemadministration
Grundnivå 22,5 Högskolepoäng
IT610G Vårtermin 2020

Gunnar Lindqvist
a17gunli@student.his.se
2020-06-15

Handledare: Dennis Modig
Examinator: Ali Padyab

Sammanfattning

Bitcoin har framträtt som den mest igenkännbara kryptovalutan sedan igångsättningen 2009 och har vid skrivande tillfälle ett börsvärde på 1,6 biljoner svenska kronor. Detta ihop med den ekonomiska friheten som Bitcoin erbjuder gör att användarantalet ständigt ökar. Likt all ny teknik så tar det tid innan teknologin är fullt utvecklad och anpassad för den bredda massan. I följd av detta kan säkerheten lida vilket kan resultera till ekonomiska förluster. Denna forskningsinsats undersöker vad för åtgärder och strategier som kan användas för att öka säkerheten via en litteraturstudie. Insatsen undersöker även med hjälp av en enkätundersökning ställd till ett Bitcoin-forum om hur användare av Bitcoin hanterar sina privata nycklar. Arbetet visar att det finns åtgärder som bidrar till ökad säkerhet såsom kryptering och multisignatur men att det hänger mycket på vad användarna själva väljer för typ av bäst strategi för deras användningsområde. Enkätundersökning redovisar att majoriteten av användarna gör säkerhetsmedvetna beslut för hur de använder Bitcoin men att en andel nyttjar mindre önskade tillvägagångssätt.

Nyckelord: Bitcoin, kryptovaluta, privata nycklar, Bitcoin-plånböcker, säkerhetskopiering

Abstract

Bitcoin has emerged as the most recognizable cryptocurrency since its inception in 2009 and, at the time of writing has a market capitalization of 165 billion dollars. This together with the financial freedom that Bitcoin offers means that the number of users is constantly increasing. Like all new technology, it takes time for the technology to be fully developed and adapted to the wider mass. As a result, security can suffer which can result in financial losses. This research effort explores what measures and strategies can be used to increase safety through a literature study. The effort also investigates with the help of a survey conducted at a Bitcoin forum on how users of Bitcoin manage their private keys. The work shows that there are measures that contribute to increased security such as encryption and multi-signature but that much depends on what the users themselves choose for the type of best strategy for their area of use. The survey shows that the majority of users make security-conscious decisions about how to use Bitcoin but that a proportion uses less desirable approaches.

Keywords: Bitcoin, cryptocurrency, private keys, Bitcoin wallets, backup

Förord

Ett stort tack till alla individer som bidragit till att arbetet har genomförts.

Stort tack till handledaren för mitt arbete, Dennis Modig. Dennis Modig har varit en go grabb som har gett användbar feedback som bidragit till att arbetet har ökat i kvalitet. Stort tack till examinatorn Ali Padyab som även gett givande feedback. Tack Dennis Modig och Ali Padyab som varit lättkontaktade och som har lett arbetet i rätt riktning.

Ett ytterligare tack till Daniel Jansson som under arbetets gång hjälpt till med den utförda enkätundersökningen. Även tack till alla som gav feedback från pilottestet och alla de som deltog i enkätundersökningen.

Även ett stort tack till vänner och familj för allt stöd under arbetets gång.

2020-06-15 Gunnar Lindqvist

Innehållsförteckning

1 Introduktion

Bitcoin introducerades 2008 under alias Satoshi Nakamoto där ett förslag för en digital valuta baserat på flertal koncept och teknologier presenterades i ett vitt papper. Denna digitala valuta baseras på offentlig nyckelkryptografi där alla transaktioner registreras på en öppen blockkedja. Bitcoin är den första digitala valutan som löser problematiken med dubbelspendering och gör det möjligt att skicka och ta emot valuta utan en tredjepart inblandad (Nakamoto, 2008). Med möjlighet för över en halv miljon transaktioner per dag och 48 miljoner användare sägs Bitcoin bli nästa stora uppfinning sen internet (Blockchain, 2020).

Detta tillåter individer att delta i ett peer-to-peer nätverk där transaktioner signeras och nås via privata nycklar. Dessa nycklar hanteras av Bitcoin-plånböcker som finns i flertalet olika typer. En Bitcoin-plånbok gör det möjligt att ta emot, skicka och se saldo över den Bitcoin som är tillgänglig. De olika plånböcker som finns erbjuder olika nivåer av användarvänlighet och säkerhet. Användarvänligheten är viktig för att underlätta användningen av Bitcoin medan säkerheten ser till att dem privata nycklarna är tillgängliga för rätt person. Då de flesta plånböckerna opereras av användaren själv. Detta gör att användaren är den som ansvarar för nycklarna vilket gör att säkerheten är viktig för att kontrollen av nycklarna ska bestå.

Problematiken med användningen av Bitcoin är att för att skicka och komma åt så krävs korrekt privat nyckel. Detta gör det viktigt att dem privata nycklarna hanteras med säkerhet i åtanke. Val av plånbok blir därför ett viktigt val där manövreringen inte ska hindra utövare. En annan del som gör detta viktigt är hur eller om säkerhetskopiering görs för att göra det möjligt för återställning från tappade privata nycklar. Även hur säkerhetskopiering sker är något som spelar roll. Dem privata nycklarna är essentiella och måste förbli hemliga då avslöjande av dessa för utomstående parter är motsvarande till att ge full kontroll över den Bitcoin som är säkrad med dem nycklarna. En förlorad nyckel resulterar till förlorad Bitcoin som aldrig kan återställas. Via användande av säkra plånböcker och säkerhetskopiering bidrar det till att färre antal Bitcoin går förlorade. En ökad säkerhet kan resultera till fler användare stannar och tillkommer. Vetskapen av hur säkerheten kan förbättras kan hjälpa vidare forskning att utveckla mer säkra plånböcker och säkerhetskopieringsmetoder för framtiden.

Tidigare forskning har fokuserat på plånböckerna utifrån en teknisk synvinkel där förbättringsförslag har angetts för att utveckla säkerheten för nyckelhantering (Liu, et al., 2017a). Motiveringen för arbetet är att utforska hur användare hanterar deras privata nycklar. Anledning till motivet är att tidigare forskning gällande användare endast har undersökt en snäv målgrupp i form av nybörjare där deras uppfattning om säkerhet och användning undersökts (Alshamsi & Andras, 2019). Forskningen ska bidra till att bemötande av outforskade områden inom Bitcoin besvaras.

Syftet med denna studie är att förstå vilka strategier Bitcoin-användare nyttjar för att säkerhetskopiera dem privata nycklarna och ge en överblick för vilka typer av plånböcker som används. Dessutom ska studien kasta mer ljus på vad för strategier och tekniker som kan vara till hjälp för framtida forskning och praxis för användare när det gäller användandet av Bitcoin. Studien ska besvara på vilka sätt Bitcoin-användare hanterar sina privata nycklar och hur hantering och säkerhetskopiering av nycklar kan förbättras.

Den enkätundersökning som genomförts visar att användare gör säkerhetsmedvetna val när det kommer till Bitcoin. Flertalet användare är villiga att investera i säkerhet och utför säkerhetskopieringar för möjligheten av återställning. Vidare visar den litteraturstudie som implementerats att flertalet åtgärder kan utföras för ökad säkerhet. Kryptering och multisignatur ökar skyddet mot förövare. Litteraturen visar att

användare måste reflektera själva över vad för användningsområde som Bitcoin ska fylla för dem och välja plånböcker efter det.

Rapporten är disponerad så att kapitel två ger den grundläggande informationen för att förstå vad Bitcoin är och hur Bitcoin fungerar för att sedan gå igenom mer centrala begrepp för just detta arbetet. Kapitel tre presenterar problemformulering där problematiken går igenom ihop med forskningsfrågorna. Även vad för mål motivering bakom arbetet förklaras. Fjärde kapitlet går igenom de metoder som ska användas där de validitetshot som finns förklaras ihop med hur de kan förhindras. Kapitel fem redovisar hur studien har genomförts där kapitel sex förklarar vad resultaten från genomförandena skapat. Det sjunde kapitlet analyserar resultaten och presenterar upptäckter som gjorts. Kapitel åtta diskuterar hela arbetet med olika aspekter och ger även ett frö för vad framtida arbeten kan utföra inom området. Kapitel nio förklarar den slutsats som gjorts över vad forskningen har resulterat till. Följt efter finns referenser och appendix för arbetet.

2 Bakgrund

Nedan förklaras först övergripande dem fundamentala bitarna om vad Bitcoin är för att sedan berätta vad för teknologier som Bitcoin är byggt på. Därefter finns en förklaring för vilka typer av plånböcker det finns. Kapitlet avslutas med relaterande arbeten för området.

2.1 Vad är Bitcoin?

Bitcoin är en digital valuta där enheten är Bitcoin. 100 000 bits är en Bitcoin där en bit kallas en Satoshi och är den minsta mängden en Bitcoin kan befinna sig i (Antonopoulos, 2017). Valutan använder sig av Bitcoin-protokollet över internet för att transportera värden. Bitcoin är gjord på en öppen källkod som kan köras på flertalet enheter, bärbara datorer och mobiltelefoner som exempel. Bitcoin fungerar likt en vanlig valuta där användare kan köpa och sälja varor men är helt virtuell (Liu, et al., 2017a). Detta gör att likt vanlig fiatvaluta såsom den svenska kronan så finns inte Bitcoin i mynt eller pappersformat.

Transaktioner sker via användning av nycklar där en privat nyckel kan bevisa ägande av Bitcoin för nätverket. Med nycklarna kan en signera transaktioner för att låsa upp värdet och spendera det via att föra över värdet till en ny användare (Liu, et al., 2017a). Nycklar är oftast förvarade i digitala plånböcker som kan finnas på mobiltelefoner eller datorer (Antonopoulos, 2017).

Bitcoin strävar efter att vara decentraliserat vilket gör att ingen individ har kontroll över Bitcoin. Ingen tredjepart är involverad i transaktionerna mellan användarna. Transaktionerna sker via peer-to-peer där båda parterna kan lita på varandra via säkerheten från nätverket. Det är inte som banksystemen där en bank verifierar varje transaktion, utan att Bitcoin-nätverket verifierar varje transaktion. Detta gör att ingen central server används. Decentraliseringen uppfylls via att varje block verifieras i form av en hashberäkning i ett distribuerat beräkningssystem. Om blocket ses som giltigt adderas det efter det tidigare godkända blocket där användare ”röstar” i form av datorkraft (Gervais, Karame, Capkun, & Capkun, 2014).

Nätverket är uppbyggt av noder och miners. Noderna lagrar den öppna huvudboken där nya block av transaktioner kommer från miners. Verifiering av nya transaktionerna görs av dem så kallade miners. Efter tio minuter sätts transaktionerna in i ett block som sänds ut till nätverket där varje nod för in det nya blocket i sin huvudbok. Varje transaktion tar då tio minuter att verifieras i snitt. Efter varje block får den miner som lyckades verifiera blocket en belöning i form av Bitcoin. Detta gör att ny Bitcoin kommer i rörelse. Denna belöning halveras i snitt var fjärde år för att motstå inflation. Totalt kommer 21 miljoner Bitcoin någonsin att skapas fram till år 2140 där ingen ny Bitcoin kommer att adderas i rörelse. Bitcoin kan ej likt vanlig fiatvaluta skrivas ut från tomma intet (Nakamoto, 2008).

Bitcoin är uppbyggt av regler som tillåter vem som helst att ha kontroll över Bitcoin och kan sända Bitcoin till vem som helst som har en adress. Censur är inget som existerar. Nätverket bryr sig inte om ens identitet eller uppsåt. Detta gör att Bitcoin kan opereras gränslöst hela världen då infrastrukturen är baserat på internet och ingen individ har totalt kontroll (Nakamoto, 2008).

2.1.1 Hur Bitcoin fungerar

En distribuerad öppen huvudbok per definition kallad blockkedja sparar alla skapade transaktioner för Bitcoin. En blockkedja är block som innehåller värden som är systematiskt uppradade i en linjär kedja (Hughes, Park, Kietzmann, & Archer-Brown, 2019). Blockkedjan delas av alla noder i nätverket. Varje block identifieras av ett unikt hashvärde som blockhuvud där varje block refererar till det tidigare block som finns i kedjan. Blockkedjan för Bitcoin använder algoritmen SHA256 för hashning. Ändras ett blocks hashvärde så

förändras dem block som ligger framför i kedjan. Ett block med flertalet block efter sig blir därför svårändrat. Detta gör att blockkedjan blir svårare att förändra desto längre historia ett block besitter. Den längsta kedjan av block är den som nätverket följer (Antonopoulos, 2017).

Blockkedjan är öppen och där varje block kan skådas enda bak till det första blocket i kedjan som skapades år 2009 då *Genesis Block* konfirmerades. Varje transaktion som någonsin registreras i huvudboken går därför att se. Hela databasen går att laddas ner för att beskådas. Att förändra kedjan är till stor del helt omöjligt då allt arbete som skapat blockkedjan måste göras om. Bara för att lyckas förändra dem nya block som skapas så krävs 51 procent av nätverkets datorkraft för att i längden vinna loppet mot resterande av nätverket. Brutala mängder datorkraft skulle krävas för att komma ikapp den längsta kedjan av block. Detta skapar säkerhet i blockkedjan där det går att lita på den (Antonopoulos, 2017).

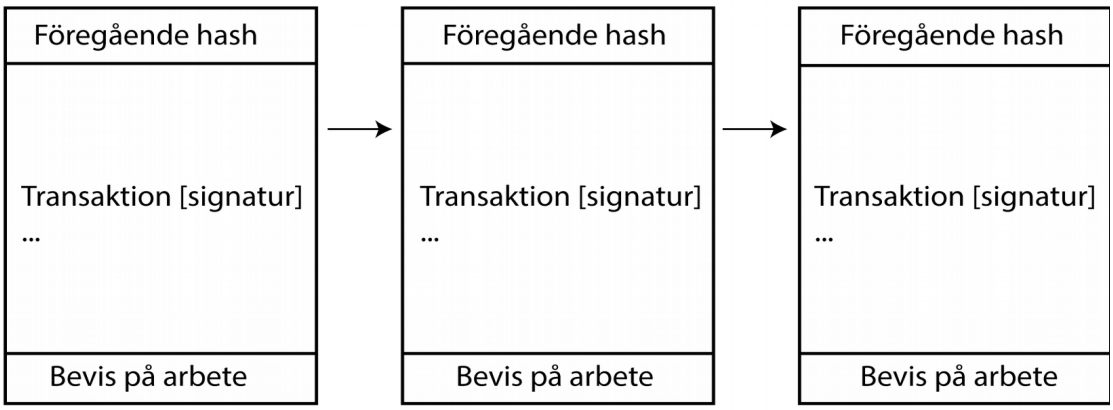


Illustration 1: Blockkedjan (författarens egna)

Bitcoin är pseudonym då varje transaktion på blockkedjan kan ses. Om en en adress länkas till personuppgifter så kan varje transaktion för adressen länkas till uppgifterna. För att vidhålla anonymitet kan en ny adress användas vid varje ny spenderad utmatning (Nagata, Kikuchi, & Fan, 2018)

Mining är det ord som beskriver skapandet av ny Bitcoin och det arbete som säkrar och möjliggör konsensus i nätverket. Mining bidrar även till decentralisering i nätverket, att ingen enhet eller individ ensamt styr nätverket (Antonopoulos, 2017).

Miners är dem enheter som kalkylerar ut hashvärden för de nya block som skapas var tionde minut. Nätverket kan opereras på inte så kraftfulla enheter såsom bärbara datorer och liknande. Men i följd av den belöning som ges ut vid ett validerat block så används ASIC's (application-specific integrated circuit) som är enheter endast skapade för ett visst mål och inget annat. I detta fall används ASIC's för att gissa ut rätt hash. Vid en korrekt gissning så publiceras blocket för hela nätverket och där det därefter valideras av alla miners. Om blocket var korrekt hamnar det i blockkedjan. Därefter görs samma process om igen tills någon miner lyckas beräkna ut korrekt hash för nästa block (Liu, Chen, Zhang, Tang, & Kang, 2017b).

En miner får två belöningar, en för att ha hittat korrekt hash för blocket och en för transaktionsavgifter. Belöningen för korrekt hash gör att ny Bitcoin skapas. Denna transaktion som minern får kallas coinbase-transaktion. Denna belöning halveras var fjärde år för att minska inflationen. Transaktionsavgiften är alla dem avgifter tillsammans från varje transaktion som även ges till minern. Det är vanligt att miners tillsammans gissar på block för att sedan dela på belöningen. Detta kallas mining pools (Liu, et al., 2017b).

2.2 Historia

År 2008 uppfanns Bitcoin då ett vitt papper publicerades av en grupp eller individ med pseudonymen Satoshi Nakamoto. Pappret gick under namnet “Bitcoin: A Peer-to-Peer Electronic Cash System,” och presenterade ett system där ingen central myndighet behövs för att validera eller avslå transaktioner. Detta via ett globalt decentraliserat nätverk som var tionde minut gör att globalt val. Ett distribuerat beräkningssystem kan göra att nätverket når konsensus om transaktionerna. Det som tidigare hindrat att sådant system att slå igenom är möjligheten för att spendera dubbelt. Förslaget av det distribuerade beräkningssystemet löste denna problematiken (Nakamoto, 2008).

Nätverket för Bitcoin startades 2009 där första blocket vid namn *Genesis Block* skapades av Satoshi Nakamoto som själv verifierade blocket. Detta block innehåller ett gömt meddelande som är följande ”The Times 03/Jan/2009 Chancellor on brink of second bailout for banks.” som refererar till en artikeln som tidningen *The Times* har publicerat. Artikeln är från samma datum som blocket skapades och ger en påminnelse om de svagheter dagens banksystem besitter (Antonopoulos, 2017).

Satoshi Nakamoto försvann från tomma intet 2011 och lät utvecklare fortsätta vidareutveckla källkoden. Det är än intill idag okänt vem eller vilka Satoshi Nakamoto var. Oavsett så kan inte Satoshi Nakamoto eller någon annan ha kontroll över Bitcoin (Antonopoulos, 2017).

2.3 Nycklar

Den privata nyckeln är den kontext som möjliggör spendering av Bitcoin. En privat nyckel består av 256 bitar som kan anges i hex- eller WIF-format (QR-kod). Detta gör att det totalt kan skapas 2^{256} nycklar. Privata nycklar är skapade helt slumpmässigt från siffror vilket plånböcker kan göra. Dem publika nycklarna skapas av en elliptisk kurva som är en asymmetrisk kryptografiteknik. Den publika nyckeln multipliceras med följande formel: $K = k * G$, där k är den privata nyckeln, G en konstant punkt och K är den publika nyckeln (Antonopoulos, 2017).

Den privata nyckeln används för signering där varje input är signerad självständigt. En digital signatur bevisar ägande av en privat nyckel där beviset är obestridligt. Signaturen bevisar även att en transaktion inte kan eller har ändrats (Antonopoulos, 2017).

Den publika nyckeln används som mottagaradress och kan säkert delas då en envägshash används för att kalkylera ut den (Kävrestad, 2018, s. 20). En privat nyckel kan omöjligen kalkyleras fram med endast vetskapen av en publik nyckel.

2.4 Transaktioner

De transaktioner som genomförs baseras på inmatning och utmatning av värden som sparas på blockkedjan. Vid en transaktion till en annan plånbok så används all den Bitcoin som finns tillgänglig där det skapas två utgångar, en för beloppet till den som tar emot och en för det beloppet som skall tillbaka. Detta fungerar likt den växel som ges när en kontant betalning sker (Antonopoulos, 2017).

Det saldo som finns tillgängligt för en användare kan bestå av flertalet nycklar som har kontroll över Bitcoin. Summan blir det totala värdet från alla nycklarna. Plånboken kalkylerar ut saldot via att skanna av hela blockkedjan och sätter ihop alla värden. Varje värde som kan spenderas och är tillgänglig kallas för UTXO som står för ”unspent transaction outputs” (Antonopoulos, 2017).

Varje transaktion har en liten avgift som har till nytta att säkra nätverket. Detta för nätverket inte ska svämmas över av transaktioner. Avgiften kompenserar även till dem miners som säkrar upp nätverket.

2.5 Plånböcker

En plånbok är den applikation som är det primära gränssnittet för en användare. En plånbok hanterar användares nycklar och adresser, spårar saldo, skapar och signerar transaktioner (Antonopoulos, 2017).

Det finns flertalet olika plånböcker där det går att kategorisera in dessa i fyra olika kategorier. Mjukvaruplånböcker, hårdvaruplånböcker, pappersplånböcker och webbplånböcker.

En mjukvaruplånbok är dem applikationer som kan köras på en dator eller mobil. Dem privata nycklarna är sparade lokalt på enheten. En mjukvaruplånbok kan med hjälp av den publika nyckeln derivera fram nya Bitcoin-adresser som tillhör den privata nyckeln. En mjukvaruplånbok kan även skapa den nya privata nyckeln för den växeladress som skapas vid genomförda transaktioner (Liu, et al., 2017a). En mjukvaruplånbok kan läsa av blockkedjan antingen via att ha en full kopia av blockkedjan lokalt. En sådan plånbok kallas för ”full node”. En mjukvaruplånbok kan även läsa av blockkedjan via att ansluta sig till en nod. Denna typen av plånbok kallas för ”SPV-wallet”. Om blockkedjan läses av från en specifik server så går plånboken under namnet ”API-wallet” (Antonopoulos, 2017).

Hårdvaruplånbok är när en separat enhet har dem privata nycklarna sparade i sig. Detta gör att plånboken är separerad från internet och kommunicerar endast med en dator eller mobil när den är auktoriserad (Liu, et al., 2017a). En hårdvaruplånbok har möjligheten att kalkylera och skapa nya nycklar utan att vara ansluten till internet likt en pappersplånbok. Plånbokens hårdvara är gjord för att matematiskt generera nycklar, både privata och publika (Khan, et al., 2019).

Privata nycklar utskrivna på ett papper kallas pappersplånbok. De har även ofta den publika nyckeln skriven men är inte helt nödvändigt då den publika nyckeln kan deriveras från den privata nyckeln. En pappersplånbok kan skapas offline. Pappersplånböcker kan enkelt skapas via JavaScript på webbsidor likt *bitaddress.org* (Antonopoulos, 2017). Det är även möjligt via att kasta ett mynt 256 gånger skapa en privat nyckel som skrivs ner på ett papper. Via att bestämma vilken sida av myntet som representerar en etta och vilken som är en nolla kan varje kast skrivas ner i turordning. Efter 256 kast kan resultatet omskrivas till hexadecimalt och representera en privat nyckel. Denna nyckeln kan då användas för att kalkylera ut en tillhörande publik nyckel som kan nyttjas som Bitcoin-adress.

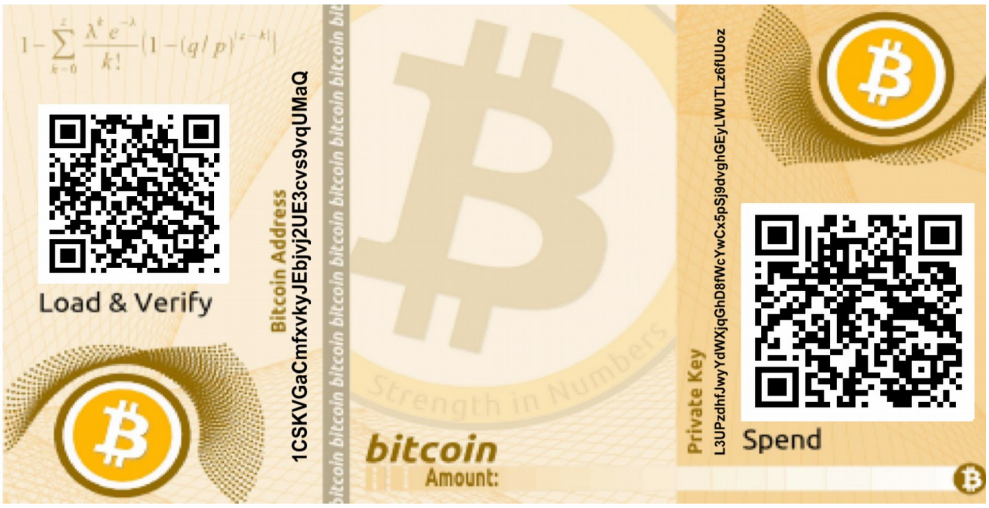


Illustration 2: Pappersplånbok skapad på bitaddress.org

Webbplånböcker är plånböcker som kan användas i webbläsare. Sidor där Bitcoin köps och växlas brukar erbjuda sådana plånböcker. Det finns även sidor som endast är skapade för att vara plånböcker. Här brukar den tredjepart som erbjuder tjänsten ha en egen databas över vem som har tillgång till vilken Bitcoin (Zollner, Choo, & Le-Khac, 2019).

2.6 Säkerhetskopiering

Den privata nyckeln det viktigaste som ska säkerhetskopieras för en återställning. Det går att kopiera den privata nyckeln och spara den på till exempel ett papper eller USB-minne. Standarden BIP-38 tillåter en att kryptera den privata nyckeln med en lösenordsfras vilket gör att en korrekt lösenordsfras behövs vid återställning. BIP-39 som är en nyare standard gör det möjligt att återställa en plånbok via en rad av engelska ord. En funktion som mjukvaruplånböcker kan besitta är möjligheten att exportera en säkerhetskopia i filformat till den enhet som är värd för plånboken (Antonopoulos, 2017).

2.7 Tidigare arbete

Tidigare forskning har fokuserat på ge förslag för olika implementeringar av hur plånböcker och säkerhetskopiering kan få ökad säkerhet. Dessa forskningar har även utvärderat och identifierat de säkerhetsbrister som finns.

Hileman och Rauchs (2017) har gjort liknande forskning inom området. Kartläggning via vad statistik i form av nedladdningar säger för vilka typer av plånböcker som används har genomförts. Studien försöker besvara aktiva användare och genomför jämförelse mellan andra valutor. Arbetet utför en bredd studie inom den globala marknaden för kryptovaluta.

Inom forskningsområdet så har Liu et al. (2017a) gett förslag för hur ett nyckelhanteringsschema kan användas för att signera transaktioner likt andra plånböcker. Detta via en lösenordsfras och personliga frågor som kan återställa en privat nyckel. Konceptet medför att den privata nyckeln ej lagras lokalt på en dator för en ökad säkerhet.

En annan studie för en säker plånbok är användandet av QR-koder. Förslaget ger ett extra lager av säkerhet där två mobiler används för autentisering. Ena som har den privata nyckeln och den andra som används som panel för utföra enklare funktioner såsom visa adresser. QR-koder används mellan mobilerna för att signera transaktioner (Khan, Zahid, Hussain, & Riaz, 2019)

Rezaeighaleh och Zou (2019a) fokuserar på ett enklare sätt att säkerhetskopiera en privat nyckel. Med hjälp av ett hårdvarukort som kan förvara säkerhetskopian slipper användare skriva ner den privata nyckeln. Förslaget använder NFC som överföringsmetod mellan plånbok och hårdvarukort för att överföra den privata nyckeln.

Många forskningsinsatser har gjorts rörande de säkerhetsbrister som finns för de olika typerna av plånböcker. Sai, Buckley och Gear (2019) redovisar de säkerhetsproblem som finns för mobila plånböcker där det även gjorts forskning rörande handelsplatser kring de risker som följer med där (Kim & Lee, 2018).

Nguyen och Zhou (2017) har genomfört en studie riktad mot dem hårdvaruplånböcker som finns på marknaden och genomgått de brister och attacker som finns. Inom samma område har Kaushal, Bagga, och Sobti (2017) genomfört en liknande studie riktad mot en mjukvaruplånbok för datorer, SPV-plånbock och handelsplatser för att redovisa de risker och säkerhetsproblem som finns.

När det gäller undersökningar kring Bitcoin-användare så har Alshamsi och Andras (2019) undersökt vad nybörjare tycker om säkerheten och användningen av Bitcoin. Undersökningen visar att Bitcoin som kryptovaluta är en stor utmaning för många användare, samt att Bitcoin fortfarande är i en ung fas där utveckling och kunskap bör förbättras.

Det som gör att detta arbetet skiljer sig från tidigare forskning är att arbetet ska redovisa vad för typer av plånböcker användare använder. En annan aspekt som urskiljer arbetet är att forskningen ska rikta in sig på de typer av plånböcker som finns tillgängliga och inte snöa in sig på en ensam lösning. Insatsen kommer att redovisa de brister som finns där rekommendering ska skapas för användare. Arbetet riktar in sig mot vanliga användare som ska få kunskap för att göra bra val utifrån säkerhet.

3 Problemformulering

Bitcoin har och förväntas nå mer användning hos företag och individer. Kryptovalutan gör varje användare till slutanvändare vilket i sig kan skapa problem. Då Bitcoin är ett relativt nytt ekosystem för att överföra värden så bör det ta tid för användare att använda tekniken på ett säkert sätt. Såsom andra tekniker där pengar är inblandade är säkerhet en viktigt faktor. Problematiken ligger i att användarna själva ansvarar för vem som har tillgång till en privat nyckel där ingen tredjepart kan återställa transaktioner (Wu, Luo, & Xu, 2019). Redan vid 2017 befarades det att runt 3,79 miljoner Bitcoin var förlorade för alltid. Detta är runt 18 procent av det totala antalet Bitcoin som någonsin kommer att skapas. Senare forskning från 2019 visar att mellan tre till sex miljoner Bitcoin befaras förlorade vilket är mellan 14,3 till 28,6 procent (Rakdej, Janpitak, Warasart, & Lilakiatsakun, 2019). Detta bevisar den problematik som finns med Bitcoin kring hur viktiga dem privata nycklarna är för att behålla den ägda Bitcoin som finns. Vidare finns det problematik kring att användare låtit handelsplatser administrera deras Bitcoin där flertalet handelsplatser stängts ner och användare har förlorat sin valuta (Moore, Christin, & Szurdi, 2018).

För att kunna dra slutsatser ska undersökningen granska hur användare hanterar sina privata nycklar. Detta via att se vad för applikationer de använder som hanterar deras nycklar. Undersökningen ska även se över ifall användare säkerhetskopierar dem privata nycklarna. Om de i sådana fall gör det så ska även hur de gör det undersökas. Arbetet kommer även att se över de olika typer av plånböcker säkerhetskopieringsmetoder som finns där säkerheten är fokuset. Slutsatser ska kunna dra utifrån litteratur om vad för metoder och strategier som kan rekommenderas.

Forskningen inom detta område fokuserar mycket på den teknik som används för att säkra dem privata nycklarna men saknar nyanser av hur privata nycklar hanteras av slutanvändarna. Forskning inom området har tidigare undersökt statistik för nedladdningar av plånböcker men brister i hur slutanvändarna faktiskt går tillväga (Hileman & Rauchs, 2017). Likt all ny teknik tar det tid innan den stora massan använder sig av den. När de väl gör det är det viktigt att rätt grund finns så att användarna stannar kvar. Ett viktigt steg här är att säker förvaring av privata nycklar används då dessa är vitala för tillgången till valutan.

3.1 Syfte och frågeformulering

Studien består av totalt tre syften och avsikter. Första syftet är att framställa metoder och strategier för hur användare kan använda Bitcoin för att minska sannolikheten av att förlorad Bitcoin sker. Forskningen ska undersöka de vanligaste metoderna som används för att hantera dem privata nycklarna där vilken applikation som hanterar nycklarna är av intresse. Arbetets syfte är även att se ifall säkerhetskopiering sker och i sådana fall hur. Det ska sedan studeras vad forskningen rekommenderar för typ av applikationer och tillvägagångssätt. Detta både för typ av plånbok och säkerhetskopiering. Avsikten är att skapa en rekommendation för vad för typ av plånbok som kan användas och hur en säkerhetskopiering kan ske med inriktning av säkerhet. Arbetet ska även göra ett försök med att utbilda och skapa medvetenhet för hur landskapet ser ut. Idén är att bidra med att arbetet gör att användare får mer förståelse och därefter ökar säkerheten. Följande forskningsfråga ska besvaras med syfte för arbetet:

På vilka sätt hanterar Bitcoin-användare sina privata nycklar för Bitcoin?

Denna typ av forskningsinsats är viktig för den utveckling och adoption som sker för Bitcoin. Syftet är att Bitcoin ska bli så säkert som möjligt för användare utefter deras användningsområde. Detta kan bidra till att fler användare vågar använda Bitcoin och att fler stannar kvar där de använder tekniken.

3.2 Forskningsmål

Målet med arbetet är att redovisa för hur användare kan öka säkerheten för hur de använder Bitcoin. Detta via att förklara vad för typ av tekniker som kan öka säkerheten men även föreslå för vad för typ av strategi de kan använda sig av. Forskningsmålet för studien är att bidra till att användare gör mer säkerhetsmedvetna val när det gäller val av plånböcker och hur de genomför säkerhetskopiering för återställning.

Forskningen ska även bidra till att utvecklare får en bättre bild av de nuvarande metoderna och teknikernas svagheter är för att skapa förståelse var förbättringar kan ske. Utvecklare ska även kunna identifiera vilka typer av plånböcker och säkerhetskopieringsmetoder som används för att ge vägvisa om vilka metoder som faktiskt används. Detta för att visa vilka typer av produkter som användare är intresserade av.

Arbetet satsar på att ta bort det gap som finns där svag forskning finns om hur användare faktiskt gör. Forskningen ska även se till att redogöra för hur de metoder och tekniker som redan finns kan öka sin säkerhet med redan utvecklade teknologier.

3.2 Avgränsning

Forskningen kommer att rikta in sig till den applikation för användaren som hanterar dem privata nycklarna med mest antal Bitcoin. Detsamma gäller säkerhetskopieringen. Anledning till detta är se över där majoritet av Bitcoin finns tillgänglig. Detta för att användare kan använda sig av flertalet av plånböcker med olika syften där varierande mängd Bitcoin finns åtkomlig.

Undersökningen avgränsas till kryptovalutan Bitcoin endast och kommer inte se över hur användare gör med andra valutor. Anledningen är för att Bitcoin är den valuta som nått ut till mest användare och är mest vanlig (Hileman & Rauchs, 2017). Utbud med plånböcker kan även skiljas mellan valutor vilket även kan vinkla undersökningen.

Rekommendationen kommer att ha inriktningen säkerhet där aspekter som design och användarupplevelse för olika metoder ej kommer användas som betydande faktorer.

Arbetet kommer inte att redogöra skillnader mellan genus och ålder. Detta för inte knyta personuppgifter till publika nycklar. Då Bitcoin är pseudonymt och en avsikt för användning av teknologin kan vara att erhålla en vis anonymitet så är detta inget som ska inkräktas. Forskningen kommer endast undersöka användare som använder Bitcoin av naturliga skäl då dessa endast kan ge valida svar.

4 Metod

Berndtsson, Hansson, Olsson och Lundell (2008) skriver att efter att en problemformulering är vald så är nästa steg att välja passande metod. För att nå projektets syfte rekommenderas det att forskningen delas in i mindre objektiv. Det kan därför behövas flera olika metoder ifall målet med arbetet har flera objektiv menar Berndtsson et al. (2008). Just att dela upp syftet i flera objektiv är något som kommer användas till detta arbete.

Wohlin et al. (2012) menar att alla metoder har sina för och nackdelar. Att välja den metod som kan ge bäst resultat bör därför användas för varje objektiv. Ett av objektiven är att kartlägga hur användare hanterar sina privata nycklar. För att uppnå detta mål bör användare utfrågas där de kan besvara hur de gör detta. För att enklast göra detta kommer en enkätundersökning att publiceras på internet.

En enkätundersökning passar bäst för målet då kvantitativ data ska samlas in med en önskan av stor datamängd. En enkätundersökning är det sättet som enklast når målgruppen. Detta för att en enkätundersökning publicerad på internet kan nå en stor mängd användare runtom världen utan interaktion och med låga resurser Fowler (2008). Det som ska utföras är att en enkätundersökning ska publiceras där användare av Bitcoin ska besvara frågor kring hur de hanterar sina privata nycklar. Robson (2002) beskriver att forskningsdesignen är en fast design. Detta då all data är av numeriska värden. Problematiken är att det kan vara svårt att se på individuella individer men att en generaliserad bild enkelt kan skapas.

Det andra forskningsmålet ska besvara hur lagring och säkerhetskopiering av privata nycklar kan förbättras för användare. En kvantitativ metod kommer att behövas då information ska tolkas för att avgöra vad för strategier som lämpar sig bäst. Forskningsmålet kommer även att ha som funktion med att utforska dem metoder som finns för att lagra och säkerhetskopiera privata nycklar. För att uppnå detta kommer en litteraturstudie att användas. En litteraturstudie lämpar sig bäst för målet då information lätt kan hittas för att därefter tolkas (Snyder, 2019). Litteraturstudien är även ett bra val då den även ger grund för den enkätundersökning som genomförs. Detta då det kan resultera till fler möjliga svarsalternativ och att alternativen backas av forskning.

Till anledning att litteraturstudien ger grund till enkätundersökning bör litteraturstudien först påbörjas för att ge kunskap inom området. Enkätundersökning kan genomföras då strategier och metoder för lagring och säkerhetskopiering sammanställts för att ge ett korrekt urval för dem alternativ som kommer att presenteras i enkätundersökningen. Detta gör att när dem forskningsartiklar som ska användas framställts så kan enkätundersökning påbörjas.

Strategin för hur forskningen ska utföras presenteras i *illustration 3* för arbetet nedan. Figuren visar i turordning för vad som sker i vilket steg.

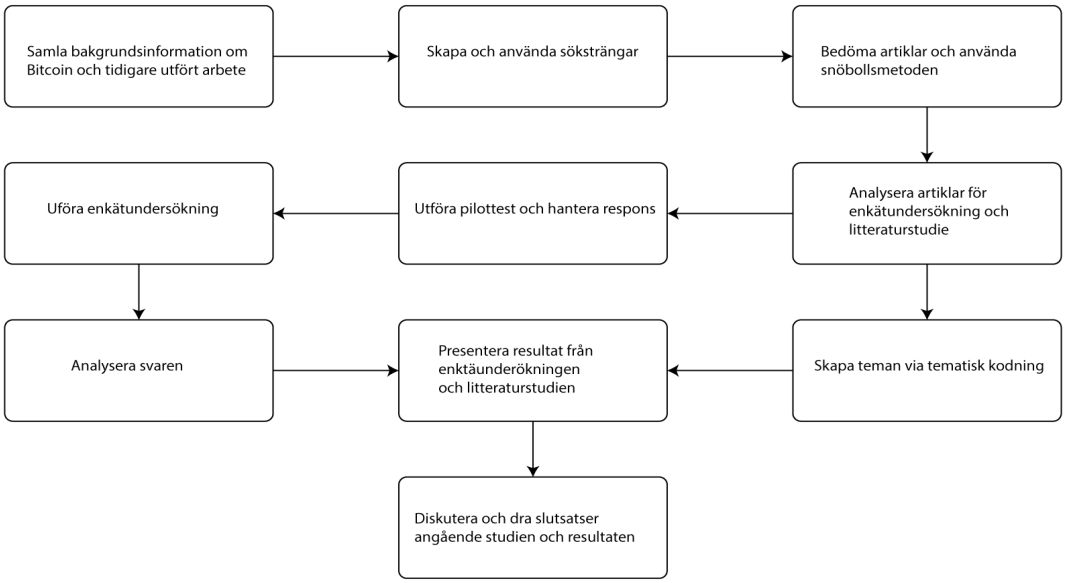


Illustration 3: Strategi (författarens egna)

4.1 Litteraturstudie

För att skapa en rekommendation för hur nycklar kan hanteras och lagras så kommer en litteraturstudie att användas. Berndtsson et al. (2008) beskriver att en systematisk undersökning är något som många projekt behöver. Utmaningen med en litteraturstudie är att det är en tidskrävande metod där ett problem är att avgöra när tillräckligt med material är insamlat. Litteraturstudien ska även bidra till en grund för dem svarsalternativ som ska finnas för enkätundersökning.

Vidare skriver Berndtsson et al. (2008) att det är svårt att avgöra för när läsare kan lita på resultatet. Med en medvetenhet om processen och strategin för att välja material ökar sannolikheten för att läsaren tror att materialet är tillräckligt.

Studien är av kvalitativ metod där litteratur kommer att analyseras för att ta fram en rekommendation för val av plånbok och säkerhetskopiering med säkerhet som aspekt.

4.1.1 Snöbollsmetod

För att använda mer litteratur kommer snöbollsmetoden att användas. Metoden går till så att efter att sökströngarna har identifierat litteratur så granskas referenserna för att inkludera mer litteratur i studien. Proceduren är uppdelad i två metoder för att få fram mer litteratur. Dessa två redovisas nedan (Wohlin, 2014).

- *Bolla bakåt* - Här används referenslistan för att identifiera ny litteratur som används till studien. Inkluderings och exkluderingskriterier används för att besluta vilka referenser som ska och ej ska vara med. Dem referenser som klarar kriterierna granskas sedan för att ingå i studien.
- *Bolla framåt* – Litteratur som citerar dem skrifter som undersöks granskas. Likt metod ovan så går dessa igenom kriterier för att bestämma vilka skrifter som används i litteraturstudien.

4.1.2 Tematisk kodning

Litteraturstudien kommer att använda sig av en tematisk kodning. Detta innebär att artiklar kommer att kategoriseras in i teman. Ett tema representerar viktig data med relation till forskningsfrågan. Data kategoriseras därför in i teman. Valet att använda en öppen metod är för att Braun och Clarke (2006) beskriver tematisk kodning som flexibel. Detta gör att teman kan skapas under projektets gång och anpassas efter vad all den insamlade data säger.

4.1.3 Urvalskriterier

För att besvara att artiklar är lämpade för forskningsfrågan används kriterier (Kitchenham, 2004). Detta för att exkludera dem artiklar som inte bidrar till forskningen. *Tabell 1* nedan visar dem kriterier som används.

Tabell 1: Inkludering och exkludering

Inkludering	IK1: Artikel är referentgranskad IK2: Publicerad mellan 2017-2020 IK3: Relevant med forskningsfrågan
Exkludering	EK1: Inte uppfyller kriterier för inkludering EK2: Betalning eller ytterligare inloggning krävs EK3: Ej skriven på engelska EK4: Är duplicerad

Anledning till val av bara referentgranskade skrifter är att de brukar bestå av högre kvalitet. Detta för att de går igenom utvärdering av andra parter som granskar rapporten. Enligt undersökning så anser 92 procent av utfrågade skribenter att referentgranskning ökar kvaliteten på forskningsartiklar (SENSE about SCIENCE, 2009). Därav finns kriterium *IK1* för att öka kvaliteten på dem artiklar som används.

Kriterium *IK2* anger årtal som artiklar är publicerade. Anledning av *IK2* för att Bitcoin är ett ständigt projekt som utvecklas och inga artiklar ska vara åldrade. Kriteriet används för att skapa relevans med det tillstånd Bitcoin befinner sig i. Exempel på detta är att HD-wallets introducerades i Bitcoin Core 0.13.0 år 2016 vilket gör att artiklar innan implementationen av HD-wallets kan vara utdaterade (Bitcoin Core, 2016). En annan anledning till kriteriet är att ha ett så stort artikelantal som möjligt för att täcka så många relevanta studier som möjligt.

För att eliminera artiklar som ej behandlar ämnet används kriterium *IK3*. Artiklar som anger plånböcker eller säkerhetskopiering behandlas ej i forskningen. Detta är artiklar som ej bidrar till forskningen.

Artiklar som ej uppfyller de angivna kriterierna kommer att exkluderas enligt kriterium *EK1*. Detta för en konsekvent inkludering.

EK2 finns då forskningen inte har ett ekonomiskt stöd men är även vald så att artiklarna finns tillgängliga för intressenter där inget konto måste skapas.

För att skapa mindre missförstånd och feltolkning används bara engelsk skrivna artiklar enligt kriterium *EK3*.

För att ej ha med flertalet av samma artiklar används exkluderingskriteriet *EK4*. Detta med anledning med att inte ta med samma artikel upprepade gånger vilket ej behövs.

4.1.4 Validitet

Berndtsson et al. (2008) berättar att för att litteraturstudie ska vara valid och trovärdig så är det viktigt att både processen och resultatet av analysen presenteras på ett korrekt sätt. Även att vilka källor som analysen byggs på presenteras är av stor vikt.

Maxwell (1992) redovisar tre huvudtyper som ses som hot mot validitet. Detta för en kvalitativ metod likt den litteraturstudie som utförs. Nedan adressera de två hot som är aktuella för studien:

- *Beskrivning* – Är huruvida en giltig beskrivning tillhandahålls, att det som lästs, hörts eller setts inte beskrivs felaktigt. Hotet för litteraturstudien kan ske vid granskning av litteratur där antingen misstolkning sker eller att en felaktig beskrivning görs utifrån litteraturen (Maxwell, 1992). Detta hot kan vara svårt att adressera för att försöka att motverka hotet så kan korrekturläsning vara en lösning. Studien kommer att bli referentgranskad av två studenter på Högskolan i Skövde som till viss grad förhoppningsvis kan ge input som motverkar hotet.
- *Tolkning* – Att kunna tillföra en giltig tolkning av litteraturen. Problematiken är att interferens från ord kan ske och därefter bli misstolkade. Även synvinklar för olika författare kan vara olika. Exempel på hur detta hot kan påverka litteraturstudien är huruvida något tolkas som säkert. Troligtvis är definition mellan människor olika skriver Maxwell (1992). För att minska hotet är referentgranskning till nytta för att se över de tolkningar som skett och se ifall de är rimliga. Snöbollsmetoden kan även öka validiteten via att se hur andra har tolkat litteraturen och hur de citerat den.

4.2 Enkätundersökning

En enkätundersökning passar bra för undersökningar där ett stort urval av respondenter finns där dessa besitter en viss kunskap om ämnet skriver Berndtsson et al. (2008). Den fördel som finns med att välja enkätundersökning är att med få medel nå ett stort antal som svarar på enkäten och därmed täcka mycket information för ett område. Alltså är det ett mer komplicerat ämne som vara svårt att besvara via en enkätundersökning. Det är därför viktigt att frågorna är lätta att besvara och inte är för många. Det kan vara vara problematiskt att bevara intresse från deltagarna då de kan tröttna. Undersökningen kommer att försöka att handskas via detta med att ha så få frågor som möjligt. Frågorna ska även vara tydliga där alternativ kommer att bestå av fördefinierade svar. Även för att öka deltagandet och intresset kommer en liten belöning i form av Bitcoin att skickas till deltagarna.

En enkätundersökning besitter problem med att deltagarna ej själva har interaktion med författaren vilket kan bidra till otydlighet. Dock kan detta leda till fördelen att deltagarna upplever att deras svar blir mer anonyma där de vågar svara mer öppet och ärligt. En enkätundersökning är även ett effektivt sätt att samla in data på kort tid (Robson, 2002).

Meningen med enkäten är att presentera beskrivande statistik för forskningsområdet. Detta leder till att stora mängder data kommer att samlas in. Därför passar en kvantitativ metod. Enkäten kommer att vara självutförande vilket innebär att deltagarna själva får svara på frågorna. Fördelen med en självutförande

metod är att de har lägre administrativ kostnad och möjligtvis kan enkelt distribueras geografiskt. Frågorna kommer att vara stängda frågor då stängda frågor är lättare att koda av (Robson, 2002).

Enkäten kommer att publiceras online då Fowler (2008) anser att det är en bra metod för att samla in många svar på kort tid. Bitcoin använder internet som infrastruktur vilket gör att de som använder tekniken har med mycket hög sannolikhet tillgång till en internetanslutning. Detta gör att de bör kunna besvara en enkät som publiceras på online. Flertalet olika verktyg finns för att skapa en elektronisk enkät, exempelvis Google formulär och LimeSurvey. Problematiken med Google formulär är att vid användning av deras tjänster så samlas uppgifter såsom IP-adress och GPS-koordinater. Detta gör att enkäten inte blir helt anonym vilket kan skapa problem med personuppgifter (Google, 2020). Därför kommer LimeSurvey som är baserat på en öppen källkod att användas. LimeSurvey går att administrera själv för hur dessa uppgifter ska behandlas (Schmitz, 2020). LimeSurvey kommer att installeras på en egen administrerad server vilket gör att enkäten går att genomföras anonymt för deltagarna.

Efter insamlade svar kommer en analys att ske där resultat presenteras i grafiska skalor. Stapel och cirkeldiagram kommer att användas för att visa det insamlade resultatet.

4.2.1 Pilottest

Ett pilottest är en miniversion av den enkät som sedan skickas ut innan den slutgiltiga enkäten begås. Ett pilottest hjälper till med att tekniken fungerar och att frågorna blir bra ställda för den slutgiltiga enkäten. Pilottestet kan hjälpa till får en förståelse ifall frågeformuläret är förståelig och otvetydig. Testet kan utveckla forskningsfrågorna och strategin (Robson, 2002).

Pilottestet ska bidra till följande:

- Att frågorna blir förståeliga.
- Att frågorna blir tydliga.
- Att svarsalternativen är rimliga.
- Att få en uppfattning om hur lång tid enkäten tar.

Pilottestet publicerades i den svenska Facebook-gruppen ”Bitcoin Sverige” 2020-04-15 klockan 15:03. Enkäten stängdes 2020-04-18 23:59. Gruppen har över 8,000 medlemmar och har ett brett spann kunskap. Anledning till val av publiceringsgrupp är att gruppen är relativt liten i jämförelse med det slutgiltiga urvalet men att responsen sker på svenska vilket kan minska feltolkningar.

4.2.2 Urval

Enkäten kommer att publiceras på det öppna forumet Reddit. Reddit är en webbsida där användare kan ladda upp material såsom textinlägg eller webblänkar. Reddit har flertalet olika kategorier av forum i stora variationer. Därav bör ett passande forum väljas. Det forum med flest deltagare rörande Bitcoin är /r/bitcoin som vid skrivande stund har över 1,300,000 användare.

Forumet och plattformen valdes då det rör sig om Bitcoin generellt där användare kommer från flera olika bakgrunder med varierande kunskap om Bitcoin.

4.2.3 Validitet

Fowler (2008) förklarar att validitet beskriver förhållandet mellan ett svar och ett visst mått mot verkligheten. Målet är att göra feltermen så liten som möjlig där svaren ska spegla verkligheten så bäst det går.

Robson (2002) förklarar orsaker som kan skapa förvirring och fel. Dessa orsaker kan skapa opålitlighet och påverka validiteten. Nedan redovisas de orsaker som kan påverka den beskrivande statistikstudien som ska utföras.

- *Pålitlighet* – Innebär att mätningarna är korrekta. En orsak till mätningarna är inkorrekta kan vara deltagarfel där det kan motverkas med att ha ett stort deltagande där avvikande försvinner i mängden. Partiska deltagare kan även vara en orsak för att en undersökning inte blir pålitlig (Robson, 2002).

  Detta försöks motverkas genom att ha ett brett urval med stor mångfald. Ett annat problem som kan uppstå är att samma deltagare svarar på enkäten flertalet gånger. Anledning till detta kan vara för att enkäten erbjuder en vis belöning vid deltagande. Användare kan då besvara enkäten flera gånger och derivera fram en ny publik nyckel som mottagaradress. Detta kan vara svårt att motverka, men mönster och granskning av publika nycklar kan motverka detta. Att deltagarna anger sin publika nyckel är dock en faktor som även generar validitet då det krävs en publik nyckel för att ta emot Bitcoin. Detta ger pålitlighet att de använder tekniken.

- *Observatörsfel* – Är hur den som skapat enkäten har gjort den. Exempel kan vara misstag som sker men även att observatören är partisk (Robson, 2002). För att motverka detta kommer deltagarna från pilottestet kunna ge respons för hur enkäten är. Responsen ska sedan hanteras för att förbättra enkäten.

- *Extern validitet* – Att resultatet går att generalisera från studien till andra situationer och grupper Robson (2002). Genom att avgränsa studien så att studien inte kan generaliseras mot andra grupper kan hotet minskas.

5 Genomförande

Följande kapitel kommer att redovisa tillvägagångssättet för hur litteraturstudien och enkätundersökning kommer att gå till.

5.1 Litteraturstudie

Flödesschemat baseras på den summerade granskningsmetod som Booth et al. (2016) beskriver för ett genomförande av en litteraturstudie. Granskningsmetoden inkluderar den tidigare förklarade snöbollsmetoden för insamling av artiklar. Genomförandet kommer även att följa den tematiska kodningens process. Tidsaspekten omfattar lite mer än fyra månader. Detta med en start i början av februari (godkänt ämnesförslag) och ett slutdatum 15 juni (slutinlämning).

Flödesschemat presenteras i *tabell 2* nedan som visar i vilka steg genomförandet utförs i och vad som utförs i varje steg.

Tabell 2: Genomförande litteraturstudie

Steg 1: Söka	1.1: Välja databaser 1.2: Testsökningar 1.3: Huvudsökningar
Steg 2: Bedöma	2.1: Inkludering 2.2: Exkludering 2.3: Snöbollsmetod 2.4: Kvalitetsbedömning
Steg 3: Analys och resultat	3.1: Kodning 3.2: Sammanställning
Steg 4: Slutsats	

5.1.1 Sökprocess

Den första startpunkten i sökprocessen är att välja vad för databaser som används för sökprocessen. Valet av databaser anpassades efter vad högskolebiblioteket i Skövde erbjuder. Databaserna baseras även på vad Brereton, Kitchenham, Budgen, Turner och Khalil, (2007) rekommenderar. Dem databaser som valdes efter dessa kriterier är följande:

- IEEExplore
- ACM Digital Library
- ScienceDirect

Den första sökströngen som användes för att få en uppfattning om hur mycket artiklar skrivits kring området var ”Bitcoin”. Detta gav följande resultat illustrerat i *tabell 3* nedan.

Tabell 3: Testsökning

Databas	Sökträffar
IEEExplore	1382
ACM Digital Library	1337
ScienceDirect	2053

För att precisera sökningen och minska antal artiklar rekommenderar Jesson et al. (2011) användningen av booleska värden. Exempel på detta är att använda OR and AND-värden. Detta hjälpte med att få fram mer relevanta artiklar. Då plånböcker och säkerhetskopiering är av intresse användes följande söksträng:

- Bitcoin AND (wallet OR backup)

Tabell 4 visar antal sökträffar med den nya sökströngen.

Tabell 4: Sökträffar med söksträng

Databas	Sökträffar
IEEExplore	64
ACM Digital Library	371
ScienceDirect	526

Sökströngen användes i samtliga databaser för att identifiera artiklar och resulterade till en minskning i 83 procent av antal artiklar.

5.1.2 Bedömningsprocess

Alla databassökningar genomfördes 2020-04-06 mot det tre valda databaserna. Den slutgiltiga sökströngen som redovisas i kapitlet ovan användes. Totalt är det 961 stycken artiklar som ska sållas ner via dem urvalskriterier som valts. Genomförandet av inkludering och exkludering genomfördes i följande steg som redovisas nedan:

- Steg 1 – Det första steget är att ta bort artiklar som ej matchar kriterium *IK1 (Artikel är referentgranskad)*. Samtliga artiklar hos IEEExplore går alltid igenom referentgranskning vid publicering vilket gör att inga artiklar väljs bort (IEEExplore, 2019). ScienceDirect plattform består också av referentgranskade artiklar likt IEEExplore vid sökning, dock bara vid tidskrifter (ScienceDirect). Likt ScienceDirect så är tidskrifterna som publiceras ACM Digital Library referentgranskade (ACM). I efterhand blev 379 artiklar kvar.

- Steg 2 – Via att applicera filter för årtal enligt kriterium *IK2 (IK2: Publicerad mellan 2017-2020)* så kunde kandidaterna minskas till totalt 323 artiklar

- Steg 3 – *IK3 (Relevant med forskningsfrågan)* innebär att samtliga artiklar ska granskas för att avgöra ifall de bidrar till forskningsfrågan. För att avgöra ifall en artikel är relevant med forskningsfrågan ska artikeln vara avgiftsfri enligt *EK2 (Betalning krävs)* vilket gjorde att sådana kandidater eliminerades i samband med *IK3*. En drastisk minskning av kandidater blev till, från 221 till 17. Anledning av detta är att flertalet artiklar rörande Bitcoin nämner i sin bakgrund hur plånböcker fungerar kort men inte handlar om det forskningsområde som finns i denna studie.

- Samtliga funna artiklar uppfyllde inkluderingskriterierna vilket gör att *EK1 (Inte uppfyller kriterier för inkludering)* ej exkluderar någon kandidat. Artiklarna var även skrivna på engelska vilket eliminerar exkluderingen *EK3 (Ej skriven på engelska)*. De 15 funna artiklarna behölls för att analyseras och gå igenom snöbollsmetoden.

5.1.3 Process för snöbollsmetoden

Som nämnt används snöbollsmetoden för att identifiera mer artiklar för litteraturstudien. Detta gör att dem referenser som de accepterade artiklarna har ska gås igenom. Det ska även identifieras ifall någon av artiklarna är citerade i någon annan skrift. Nedan redovisas de steg som görs för den bollning som sker bakåt där referenserna för de accepterade artiklarna ses över. Totalt är det 392 referenser som ska gå igenom dem kriterier som skapats för litteraturstudien.

- Steg 1 – *IK2 (IK2: Publicerad mellan 2017-2020)* är det kriterium som referenserna först går igenom. Detta görs via att kolla i referenslistan och se när artikeln är publicerad. Totalt möter 119 referenser detta kriterium vilket gör att en minskning av 273 kandidater sker. Enligt exkluderingskriteriet *EK4 (Inga dupliceringar)* så exkluderas åtta artiklar då dessa var dupliceringar i artiklarna referenslistor.

- Steg 2 – I det andra steget används Ulrichsweb som är ett hjälpverktyg för att identifiera ifall referenserna genomgått referentgranskning som kriterium *IK1 (Artikel är referentgranskad)* anger. Ulrichsweb är en databas innehåller en stor mängd referentgranskade skrifter och artiklar. Högskolebiblioteket ger tillgång till denna databas. Vid skrifter som ej hittas på Ulrichsweb så används en manuell sökning. I dessa fall används hemsidan där artikeln är publicerad. 28 referenser mötte detta kriterium.

- Steg 3 - *IK3 (Relevant med forskningsfrågan)* resulterade till att fem artiklar blev behållna.

- Steg 4 – Artiklarna blev ej exkluderade enligt exkluderingskriterierna *EK1 (Inte uppfyller kriterier för inkludering), EK2 (Betalning eller ytterligare inloggning krävs)* och *EK3 (Ej skriven på engelska)* så blev samtliga kandidater kvar. Dock faller en artikel för exkluderingskriteriet *EK4 (Inga dupliceringar)* då den är redan identifierad från den tidigare databassökningen. Totalt blev det fyra artiklar adderade.

Nedan redovisas de steg som genomfördes för att se ifall nya kandidater kunde identifieras via att se över de valda artiklarna från databassökningarna. De valda databaserna redovisar ifall en artikel har blivit citerad vilket förenklar arbetet. Totalt kunde 16 artiklar hittas. Stegen för att granska artiklarna redovisas nedan.

- Steg 1 - Då artiklarna citerar artiklar från 2017 till 2020 så möter kandidaterna per automatik kriterium *IK2 (IK2: Publicerad mellan 2017-2020)*. För att att identifiera ifall referentgranskning

skett enligt *IK1 (Artikel är referentgranskad)* så används samma tillvägagångssätt som ovan. Alla kandidater har genomgått referentgranskning vilket gör att samma antal kandidater behålls.

- Steg 2 – *IK3 (Relevant med forskningsfrågan)* är det sista inkluderingskriteriet som appliceras. Totalt möte sju kandidater detta kriterium. För exkluderingskriterierna *EK1 (Inte uppfyller kriterier för inkludering), EK2 (Betalning eller ytterligare inloggning krävs)* och *EK3 (Ej skriven på engelska)* så blev samtliga kandidater kvar.

- Steg 3 – Kandidaterna jämfördes mot de redan valda artiklarna för att se ifall de redan identifierats. Detta enligt kriterium *EK4 (Inga dupliceringar)*. Resultatet blev att en artikel blev inkluderad i litteraturstudien.

5.1.4 Kodningsprocess

Kodningsprocessen sker i början av sökprocessen. Kodningen genomförs enligt Braun och Clarkes (2006) sex faser. Kodningen ger grund för det resultat som ska presenteras. Detta via att kategorisera de upptäckter som görs för att besvara den forskningsfråga som litteraturstudien ska bemötta. Nedan presenteras de steg som kodningsprocessen gick igenom för att extrahera den information som sedan presenteras i kapitel *6 Resultat*.

- *Bekanta sig med all data* – Började vid sökprocessens start via fördjupning i innehållets bredd och djup. Anteckningar och markerade idéer genomfördes. Alltså en lätt start med kodningsprocessen.

- *Generera initiala koder* – Denna fas började efter att en första lista med idéer hade skapats. Produktionen av initiala koder startades där kodningen påverkades beroende på om teman är datadrivna eller teoridrivna.

- *Söka efter teman* – Fas tre började när all data hade kodats och sorterats där en lång lista över koderna var skapad. Analysen omfokuserades till att sortera koderna in i möjliga teman. Överväganden kring hur koderna kan grupperas in i övergripande teman utfördes.

- *Granska teman* – Fas fyra startades efter att en uppsättning av kandidatteman var genererade. I denna fasen förfinades alla teman. Fasen resulterade till att visa kandidatteman faktiskt inte var teman.

- *Definiera och namnge teman* – Efter att en tillfredsställd temakarta var gjord så började fas fem. Här definierades och finslipades varje tema. Processen skapade en uppfattning om vad alla olika teman är och hur all data faktiskt ser ut och vad den tillgodoser med. Vad som är intressant och varför det är intressant definierades för varje tema. En analys skrevs för varje tema.

- *Producera rapporten* – När alla teman var uppsatta och helt utarbetade startades fas sex. Här berättas historian om all data för varje tema. En analytisk berättelse presenteras även med argumentation i relation med forskningsfrågan.

5.2 Enkätundersökning

För att kunna genomföra enkätundersökningen så installerades LimeSurvey enligt Appendix A.

5.2.1 Pilottest

Enkäten skapades på LimeSurvey hos den maskin som var installerad. Ett pilottest var den första undersökning som skedde. Pilottestet ska bidra med att skapa en uppfattning kring hur enkäten uppfattas

och även hjälpa till att göra den bättre via respons från deltagarna. Pilottestet publicerades på den svenska Facebookgruppen ”Bitcoin Sverige” 2020-04-15 där gruppen vid publicering bestod av 8348 medlemmar.

Enkäten bestod av flertalet fördefinierade svarsalternativ som användes för att kunna dra slutsatser. Svarsalternativen bestod av *ja* eller *nej* där ett par flervalsfrågor ställdes även. Den första delen av enkäten var den första versionen av den slutgiltiga enkäten skriven på engelska. Andra delen bestod av *ja* eller *nej* frågor där möjligheten för kommentar fanns möjlig. Detta för att få respons ifall en deltagare hade synpunkter på enkäten. Alla enkätfrågor för pilottestet går att se i Appendix A.

Följande tre frågor ställdes för att motta respons *Var frågorna förståeliga? Om nej, varför?*, *Saknades det svarsalternativ för någon av frågorna? Om ja, vilken och vad saknades?*, *Hur lång tid tog enkäten att göra? Endast för dem frågor på engelska. Svar är i minuter*.

De två första frågorna bestod av *ja* eller *nej* med möjlighet av en kommentar. Den sista frågan angående tid bestod av en rullgardinslista med heltal som representerade minuter.

Resultat från pilottestet var att enkäten besvarades av åtta deltagare där de angav att enkäten i snitt tog två minuter att genomföra. Detta är i linje av vad som var väntat då enkäten var utformad att vara snabbesvarad via få frågor med tydliga svarsalternativ. Vidare resulterade pilottestet till bättre förtydligande av enkäten. Detta via att specificera ett svarsalternativ mer. Addering av möjlighet till ett egenskrivet svar lades till för det frågor som behövde det. Respons om att lägga till en fråga huruvida multisignatur används applicerades. Möjligheten att ej ange publik nyckel för adress skapades för att pilottestet visade att deltagare ej var intresserade av belöningen. Detta gör att deltagare som är intresserade av belöning fortfarande utför enkäten medan deltagare som ej vill ange publik nyckel fortfarande kan genomföra enkäten. Det övergripande resultatet var att enkäten var tydlig att förstå och snabbgenomförd vilket är linje med dem mål som var angivna för enkäten.

Under tiden som pilottestet var ute genomfördes resultatdelen av litteraturstudien.

5.2.2 Enkätutformning

Enkäten består totalt av sex frågor där fem av frågorna bidrar till forskningen. Enkäten är skriven på engelska vilket gör att så många som möjligt förstår den. Enkäten inleds med en välkomstsida som förklarar i vilket syfte enkäten utförs. Vidare förklaras det vad all data kommer att användas till och hur personlig data hanteras. Enkäten är helt anonym där ingen personlig data såsom IP-adress, e-post eller geografisk plats samlas in. LimeSurvey erbjuder en inställning för att göra enkätundersökning anonym, vilket aktiverades. Alla enkätfrågor går att se i Appendix B.

Den första frågan i enkäten frågar om vilken plånbok som används för att lagra majoriteten av deltagarens Bitcoin. För att förtydliga att det är majoriteten av Bitcoin som är av intresse så är det ordet i fetstil. Anledningen till val av majoriteten av Bitcoin är att användare kan ha flera olika typer av plånböcker av olika anledningar. Därför är det av intresse att se vad för plånbok som används för att hantera högst antal Bitcoin för att det finns mest att förlora där. Frågan besvaras via en lista av svarsalternativ där endast ett svar kan anges. Svarsalternativen är följande sju:

- Software wallet on mobile
- Software wallet on computer
- Hosted web wallet (exchange)

- Non-hosted web wallet
- Paper wallet
- Hardware wallet
- Other:

Samtliga fördefinierade svar är vad Guri (2018) beskriver i sin tidskrift där det sista svarsalternativet är till för att ge möjlighet för svar som ej finns med. Även ett alternativ för fritext är möjlig ifall inget av alternativen är valida för deltagaren.

Fråga nummer två blev skapad efter den respons som pilottestet angav och tar reda på ifall multisignatur används för den specifika plånboken. Frågan besvaras via att ange *ja* eller *nej* via kryssalternativ. En förklaring av vad multisignatur finns även med för förtydligande. Anledning för ett förtydligande är att deltagare kanske inte vet vad multisignatur är.

Anledning till frågan är att multisignatur bidrar till en ökad säkerhet då mer än en nyckel behövs för att signera transaktioner. Multisignatur kan även ge en viss säkerhet av säkerhetskopiering beroende på relationen för hur många nycklar som krävs för signering. En 2-3 relation gör det möjligt att fortfarande signera transaktioner med två av tre nycklar tillgängligt. Detta gör att åtkomsten av Bitcoin fortfarande kan vara möjlig trots tappad nyckel (Sahmim, Gharsellaoui, & Bouamama, 2019).

Den tredje berör huruvida användare gör säkerhetskopiering på sin privata nyckel för plånboken. Frågan består av *ja* eller *nej* med kryssalternativ. Frågan därefter är om de gör det, på vilket eller vilka sett det utförs på. Frågan är utformad som en flervalsfråga med kryssalternativ. Det finns även ett alternativ för att ge möjlighet att svara för alternativ som ej finns i listan via fritext. Svarsalternativen är följande:

- On a piece of paper or something else that is physically writable
- On an external drive
- On an internal drive
- On a cloud service (Dropbox, Google Drive)
- On an email (Gmail, Hotmail, Outlook)
- Stored in brain memory
- Other:

Frågan är inte obligatorisk då alla användare kanske inte utför säkerhetskopiering.

Frågan därefter är kryssfråga i form av en *ja* eller *nej* fråga som frågar ifall ens säkerhetskopiering är krypterad. Frågan är inte obligatorisk av samma anledning som frågan ovan.

Till sist erbjuds det en belöning i form av Bitcoin. Detta via att ange en publik nyckel för en av användarens plånböcker i base58-format. Det uppmanas att derivering av en ny Bitcoin-adress ska användas av anonyma skäl. Frågan är i form av fritext där svaret kontrolleras av ett reguljärt uttryck. Uttrycket kontrollerar att det angivna alternativet är i base58-format och redovisas nedan:

/^[123mn][1-9A-HJ-NP-Za-km-z]{26,35}/

Det är inte obligatorisk att mottaga en belöning då pilottestet visade att alla inte hade intresse att ta emot Bitcoin. Men frågan uppfyller målet med att öka deltagandet och det bidrar även till en högre grad av validering.

Innan publicering av enkäten kontaktades administratörerna för ”/r/Bitcoin” för att klargöra att att var okej att publicera enkäten på forumet. Detta för att få det godkänt att lägga upp enkäten så att inlägget ej blir raderat.

Enkäten publicerades på ”/r/Bitcoin/” 23-04-2020 klockan 12:00 där den stängdes 27-04-2020 klockan 23:59. Enkäten laddas upp på en torsdag där den avslutades på en måndag. Val av tid och dag baseras på vad Delay for Reddit (2020) rekommenderar för bästa tid att lägga upp en post för det valda forumet. Posten lades upp som en länkpost med följande rubrik:

I'm writing my bachelor's degree on how users manage their keys, answer this 2 minute survey and receive some Bitcoin

Rubrikens mening är att ange vad enkäten handlar om och även locka deltagare med enkätens korta genomföringstid ihop med den belöning som delas ut.

Efter avklarad enkät exporterades svaren i form av grafer från enkätverktyget. Svar som angav ”Other” tolkades och gjordes till egna grafer. Alla deltagarna fick även dela på totalt 0.0336 Bitcoin.

6 Resultat

Kapitlet redovisar inledningsvis vad den tematiska kodningen resulterade för teman ihop med beskrivning av den data som identifierades i litteraturstudien. Därefter redovisas det resultat som enkätundersökning gav. Data i form av grafer kommer att presenteras.

6.1 Litteraturstudie

Sökprocessen resulterade till att totalt 20 artiklar inkluderades till litteraturstudien. Kodningsprocessen skapade åtta stycken teman för för att redovisa hantering av privata nycklar. I underkapitlen nedan presenteras dessa åtta stycken teman där genomgång av vad för upptäckter som gjorts.

6.1.1 Mjukvaruplånböcker för mobiler

Mobilapplikationer utnyttjar operativsystemresurser för att tillhandahålla tjänster. En inkorrekt konfiguration för resurserna kan leda till hot mot sekretess medan felaktig konfiguration av källkoden kan leda till säkerhetsbrister. Plånböcker för mobiler tenderar i att ha högre säkerhetssårbarhet jämfört med mobila bankapplikationer. Den säkerhetsbrist som var vanligast är att kryptografin är otillräcklig där detta kan motverkas via att välja en applikation med en modern kryptografi. SHA2 är ett exempel på en säker krypteringsalgoritm (Sai, Buckley, & Gear, 2019). Ett annat exempel för att öka säkerheten för en mjukvaruplånbok på en mobil är användningen av biometri. Moderna mobiler har en fingeravtryckssensor för autentisering vilket en del mjukvaruplånböcker utnyttjar. Sedan går det att istället utnyttja en mobil för tvåfaktorsautentisering för att autentisering för en plånbok (Orme, 2019).

Anledning till varför mobila plånböcker kan vara ett populärt val är att de är enkla att installera och att använda. Conti, Kumar, Lal och Ruj (2018) redovisar från sin undersökning att användare föredrar enkla användargränssnitt och simpel installation före säkerhet. De rapporterar att 22.5% i undersökningen förlorat Bitcoin på grund brist av kunskap för säkerhet. Risken med att använda en mjukvaruplånbok på en mobil är att applikationen oftast behöver flertalet rättigheter som är farliga där potentiell möjlighet till läckage är möjlig. Detta är ett hot mot sekretess men framförallt mot dem privata nycklarna (Biryukov & Tikhomirov, 2019).

6.1.2 Mjukvaruplånböcker för datorer

Mjukvaruplånböcker som körs på datorer kan resultera till att data lagras i RAM-minnet. Information såsom publika nycklar, privata nycklar och transaktionsdetaljer kan vara lagrat i arbetsminnet. Horst, Choo, och Le-Khac (2017) visar att den privata nyckeln kan identifieras i binärt format i RAM-minnet när kryptering ej sker. Vidare presenteras det att ifall en säkerhetskopiering som finns på datorn lokalt så kan filen identifieras i minnet. Volety, Saini, Mcghin, Liu, och Choo (2019) visar hur en sådan säkerhetskopia kan knäckas på kort tid. Detta specifikt för mnemoniska ord där endast 12 ord används.

Plånböcker som är fullständiga noder har mindre attacker som kan utfärdas jämfört med SPV-plånböcker. Anledning till detta är att en fullständig plånbok har en fullständig kopia av blockkedjan vilket gör att den självständigt verifierar transaktioner. En SPV-plånbok ansluter sig till noder för att få information om blockkedjan. Detta gör att flertalet attacker såsom ”bait and switch” , kedjekapning och förnekning av transaktioner kan ske (Kaushal, Bagga, & Sobti, 2017). Åtkomst till en dator kan resultera till en hackad plånbok där kontrollen av nycklarna tappas (Kaushik, Choudhary, Ektare, Thomas, & Akram, 2017).

Denna typen av plånbok har fördelen att nyckelfördelningen är simpel där åtkomsten är simpel. Detta i sig har nackdelarna att systemet inte är säkert för onlineattacker där skadlig programvara eller fysisk åtkomst kan skapa skada. Ett steg för att förbättra säkerheten är användning av kryptering och lösenord. Men denna lösning är som bevisat ovan sårbar mot lösenordsknäckning och tangenttryckningsattacker (Pal, Alam, Thakur, & Singh, 2019).

6.1.3 Handelsplatser

En handelsplats är enkelt sätt för att köpa och ”lagra” Bitcoin. Detta är likt hur en kommersiell bank fungerar. Att köpa och sälja en valuta till en annan. Användarna får en elektronisk plånbok kopplat till sina konton där lösenord sparas i ett hashvärde. Problematiken är att användare ej har full kontroll över den Bitcoin de äger. Detta för att deras saldo lagras på en databasserver tillhörande det företag som äger handelsplatsen (Kim & Lee, 2018). Detta sättet leder till lägre omkostnader för en klient men resulterar till försämrad säkerhet (Kaushal, Bagga, & Sobti, 2017). Det mest kända fallet som visar vad förödande konsekvenser som kan ske av att lagra Bitcoin på en handelsplats är Mt. Gox där över 450 miljoner dollar gick förlorade (Hu, Zhang, & Guo, 2019). Flertalet andra handelsplatser har gått i konkurs på grund av intern eller extern stöld eller på grund av tekniska misstag. Dessa sårbarheter ärvs för alla handelsplatser och kan inte helt undvikas (Conti, et al., 2018).

Handelsplatser har likt vanliga webbplatser samma sårbarheter. Exempel på sårbarheter är DDoS, bait-and-switch, man-in-the-middle, direktstöld och DNS-poisoning. Då dessa typer av webbplatser möjligtvis besitter värdebelopp är det ett väldigt attraktivt mål för attacker. Problematiken vid en lyckad attack är att det är svårt att återställa skadan. Detta för att Bitcoin baseras på blockkedja där transaktioner ej kan återställas. Tvåfaktorsautentisering är en metod från klientsidan som kan öka säkerheten, men annars baseras säkerheten mycket på handelsplatsen (Kim & Lee, 2018).

6.1.4 Webbplånböcker

Webbplånböcker där folk har kontrollen över dem privata nycklarna kan ses som ett mer säkert alternativ jämfört med användning av handelsplatser. Största skillnaden som nämnt är att lagring av nycklar sker på egen hand där de laddas upp till webbsidan vid upplåsning av saldo. Dessa webbplånböcker har liknande sårbarheter som handelsplatser med den största skillnaden att stöld av all ägd Bitcoin är svårare då webbplatsen ej har tillgång till dem privata nycklarna (Zollner, Choo, & Le-Khac, 2019).

Då webbsida används för att hantera dem privata nycklarna så finns risken för DNS-kapning där ett känt fall med MyEtherWallet år 2018 resulterade till att 160.000 dollar av kryptovaluta blev bestulet (Liu, Fu, & Chen, 2020).

Säkerheten grundar sig huruvida den privata nyckeln hanteras. För webbplånböcker spelar det stor roll för hur och vilket format som nyckeln sänds. Kryptering av nyckel och SSL är teknologier som kan vara till stor nytta för att till exempel motstå man-in-the-middle attacker (Pal, et al., 2019). Vidare för att öka säkerheten kan lösenordsautentisering tillsammans med biometri bidra till en ökad säkerhet. Detta via tvåfaktorsautentisering som tidigare rekommenderat (Malathi, Pavithra, Preakshanashree, Kumar, & Tamilarashan, 2019).

6.1.5 Hårdvaruplånbok

Hårdvaruplånböcker har fördelen att de generar dem privata nycklarna i ett offline-läge vilket gör att de ej är utsatta för internet. Detta gäller även för när transaktioner signeras (Khan, et al., 2019). Signaturen skapas på enheten och sänds sedan över till enheten som har själva gränssnittet. Det är även vanligt att

autentisering sker via pinkod för att låsa upp hårdvaruplånboken. Den säkerhetsbrist som denna typ av plånbok kan besitta är att kanalen mellan plånbok och enhet inte är helt säker. Detta gör att man-in-the-middle attacker är möjliga där transaktionsattacker kan ske (Nguyen & Zhou, 2017).

Denna typ av plånbok ses som ett säkert alternativ men kan undvikas då den kan vara otymplig för praktiskt användande (Rezaeighaleh & Zou, 2019b). Jämfört med andra alternativ som erbjuder ett gränssnitt så har hårdvaruplånböcker lägre risk för stöld vilket dock resulterat till lägre användbarhet. De flesta hårdvaruplånböcker opereras via en webbklient eller datorklient. Detta gör att mobilitet blir lägre då enheten kopplas via USB-sladd till en dator (Conti, et al., 2018). Vidare nämns det hur autentiseringssäkerheten kan förbättras via användning av biometri (Orme, 2019). Detta då en pinkod lättare kan utsättas för en brute-force attack.

6.1.6 Pappersplånbok

Korrekt skapade pappersplånböcker är ett säkert sätt att förvara Bitcoin. Detta för att en sådan plånbok går att skapa i ett läge där ingen uppkoppling till internet alls används. Nycklarna är skrivna på ett dokument och kan förvaras fysiskt (Conti, et al., 2018). Denna typen av plånbok undviker möjligheten av online-hackning av nycklar och stöld via skadlig programvara. Stöld kan endast ske via att plånboken stjäls fysiskt. Dem nackdelar som finns med denna typen av lagring är att tillgängligheten påverkas negativt (Pal, et al., 2019). Vidare finns risken att dessa plånböcker går förlorade. Dessutom kan användare råka ut för att Bitcoin förloras vid import av den privata nyckeln till en programvaruplånbok då en transaktion sker. Detta för att all växel hamnar på en ny adress (He, et al., 2018).

6.1.7 Multisignatur

Multisignatur är en strategi som ger ökad säkerhet där multisignatur är relaterat till dem teman för typer av plånböcker som ovan nämns. Anledningen är att användare kan nyttja multisignatur för sina Bitcoin-plånböcker. Anledningen till varför multisignatur är en metod som ökar säkerheten är för att multipla privata nycklar används för att signera transaktioner. Multisignaturtransaktioner kan genomföras med olika förhållanden i form av hur många nycklar som behöver delta i signeringen. Exmpel på detta är att två av tre nycklar krävs för att signera (Conti, et al., 2018). Denna lösning bidrar till att ifall en nyckel går förlorad så är inte all Bitcoin borttapad. Detta gör att en förövare måste stjäla flertalet nycklar. Nackdelen med multisignatur är att flertalet nycklar används vid transaktion vilket kan resultera till en nedgradering i användbarheten (Rezaeighaleh & Zou, 2019a).

Multisignatur är en åtgärd som kan öka säkerheten men bidrar dock till en mer komplex plånbok. Detta gör att det kan vara svårt för användare att använda sig av tekniken(Thota, Upadhyay, Kulkarni, Selvam, & Viswanathan, 2020).

6.1.8 Säkerhetskopiering

Förvaringen av en säkerhetskopiering är avgörande för vilken nivå av säkerhet som uppstår. Det finns flertalet olika sätt för var förvaringen kan ske. Pal et al. (2019) förklarar tre olika tillvägagångssätt för hur förvaring av säkerhetskopia kan ske.

- *Lokalt* – Här lagras nycklarna på en enhets lokala lagring. Detta på den enhet där programvaran som är plånbok finns installerad. Detta gör att en snabb och enkel åtkomst finns tillgänglig. Problematiken är att säkerhetskopian ej är säker från hackning via internet, skadlig programvara,

fysisk åtkomst och fysisk skada på enheten. Det resulterar även till att ifall enheten fallerar så är dem privata nycklarna förlorade.

- *Offline* – Innebär att säkerhetskopiering är lagrad på en plats utan åtkomst till internet. Detta eliminerar möjligheten för hackning via internet och att skadlig programvara kommer åt nycklarna. Lagringen kan ske via extern lagring såsom USB-minne men även skrivit fysiskt i form av en pappersplånbok. Det går även att lagra i sitt egna minne i hjärnan. Nackdelarna med denna typ av av lagring av säkerhetskopiering är att nycklarna ej är omedelbart tillgängliga och att lagringen kan tappas bort, fallera eller glömmas bort.

- *Tredjepart* – Här sker säkerhetskopiering antingen via att en webbserver lagrar dem privata nycklarna eller att ett företag fysiskt lagrar kopian på något av ovanstående sätt. Här baseras säkerheten på företaget eller servern. Detta i sin tur innebär att den totala kontrollen tappas över nycklarna. Dessa tjänster har flertalet risker, hackning via internet, skadlig programvara, fysisk åtkomst, fysisk skada och stöld.

Det finns flertalet olika format för säkerhetskopieringen även som påverkar säkerheten.

- *Klarskriven* - Ett sätt för säkerhetskopiering vilket innebär att nyckeln är skriven i klartext. Detta kan vara allt från till exempel hexadecimalt, binärt, bitkey och WIF-format. Att lagra nyckeln på det viset gör den sårbar för skadliga attacker såsom skadlig programvara ifall den är sparad lokalt eller via en tredjepart. Vid stöld är kopian är all Bitcoin direkt tillgänglig.

- *Lösenordsdriven* – Är när nyckeln antingen kan återställas via ett lösenord eller en lösenordsfras. Gör att en plånbok inte behöver ha nycklarna vid användning. BIP-39 erbjuder mellan 12 till 24 slumpvalda ord från en ordlista på 2048 ord. Orden är sammansatta och generar deterministiska nycklar. Detta resulterar till att angripare har betydligt svårare att återställa nyckeln. (Rakdej, Janpitak, Warasart, & Lilakiatsakun, 2019). Om lösenordet är svagt så kan det knäckas via en regnbågstabell attack (Pal, et al., 2019). Vidare är lösenordsfraser på 12 sårbara då de kan knäckas under ”resonabel” tid (Volety, et al., 2019).

Vidare kan säkerhet utökas i form av kryptering. Även om detta gäller allmänt så har även kryptering en påverkan på säkerhetskopieringen. Beroende på om återställningen är skyddad av kryptering minskar risken av förlust då det bidrar till extra lager av säkerhet. Säkerheten baseras på lösnordet och krypteringsmetod. Krytpering kan resultera till att fysiskt stöld av säkerhetskopieringen ej resulterar till förlorad Bitcoin. Enda sättet att kringå detta är brute-force för de som kommer över säkerhetskopian. Detsamma gäller ifall lösenordet glöms av (Zollner, Choo, & Le-Khac, 2019).

6.2 Enkätundersökning

Enkäten var tillgänglig 23/04 till 27/04 2020 och resulterade till att enkäten fick 553 besök där 339 fullständiga medverkande genomfördes. Enkäten fick 214 ofullständiga deltagare där alla obligatoriska frågor ej besvarades.

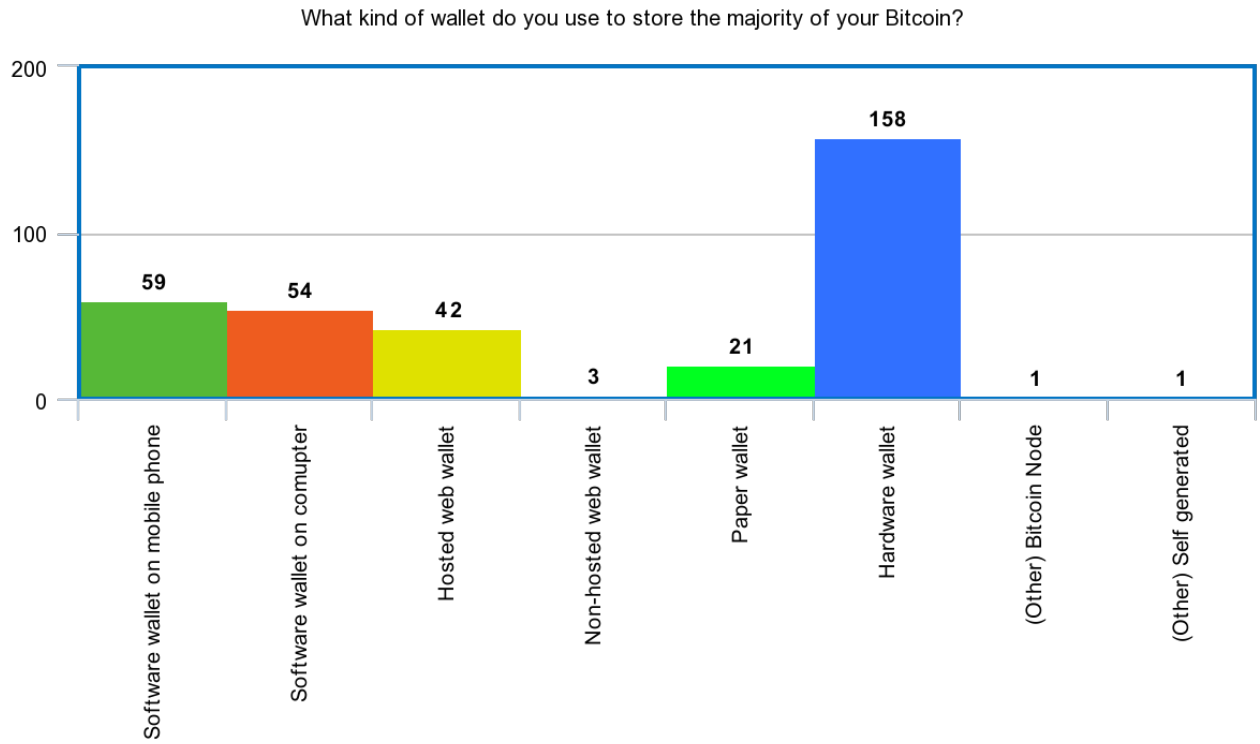


Illustration 4: Typ av plånbok

Första frågan ställdes för att ta reda på vilken typ av plånbok användarna hade för att hantera majoriteten av sin Bitcoin. Detta för att en användare troligtvis väljer den plånbok som den ser som säkrast för att det finns mest antal Bitcoin att förlora. Resultatet visar att 46.6 % använder sig av hårdvaruplånböcker vilket var det mest populära alternativet. Övriga svar var egenskapad plånbok och Bitcoin Node som var angivit en gång för vardera.

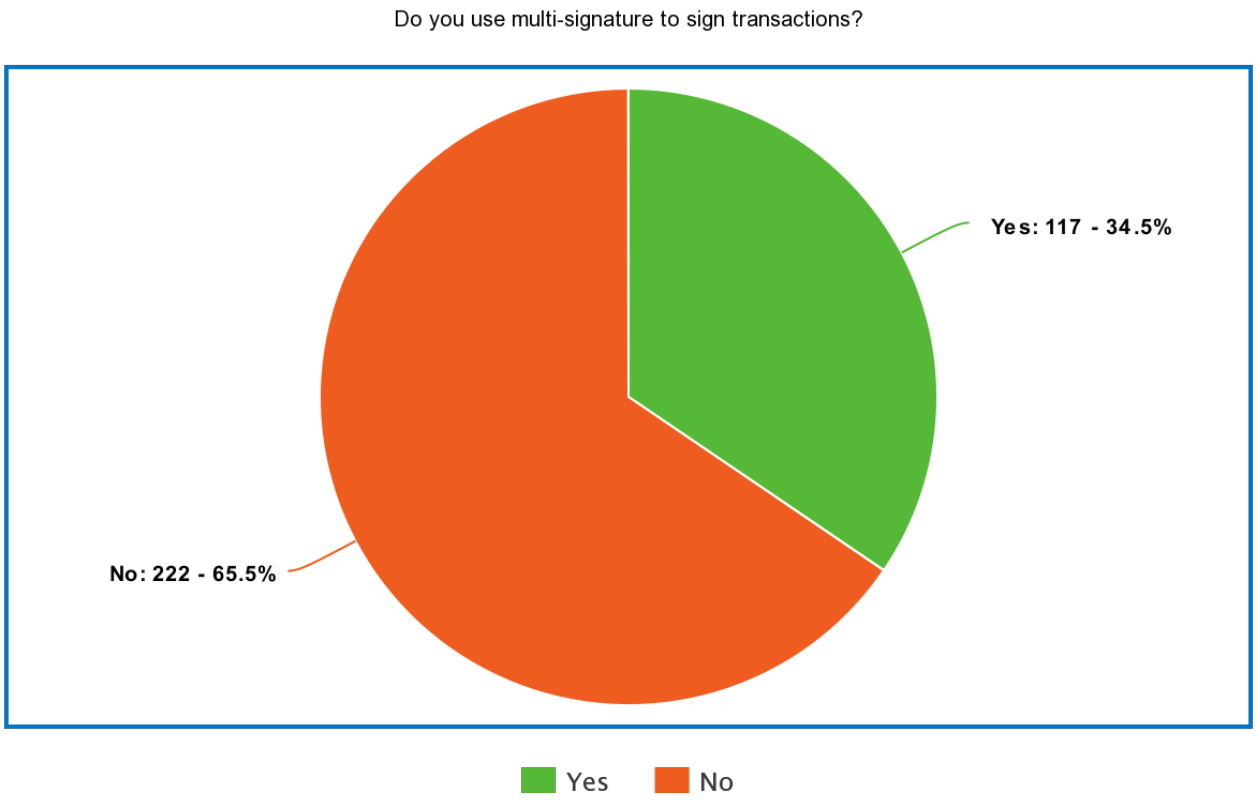


Illustration 5: Multisignatur

För att se ifall multisignatur är något som används ställdes en fråga ifall användarna gör det. Anledning till detta är att multisignatur bidrar till ökad säkerhet där det vill ses över ifall användare använder sig av multisignatur för att öka säkerheten. Resultatet visar att en mindre andel på 34.5 % gör detta.

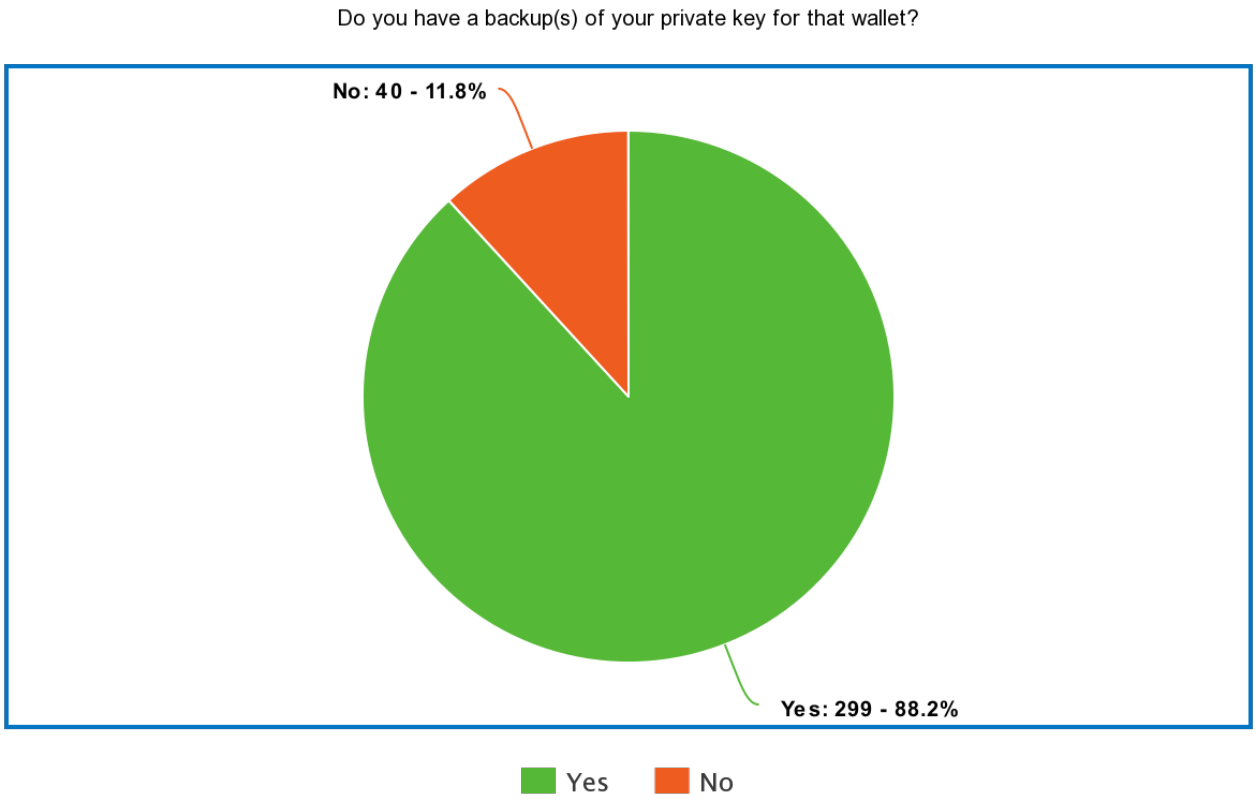


Illustration 6: Säkerhetskopiering

Fråga nummer tre frågar huruvida ifall användare gör säkerhetskopiering på den angivna plånboken. Anledning till frågan är att klargöra ifall användare själva gör säkerhetsåtgärder för att skydda sina privata nycklar ifall de går förlorade. Resultatet visar att 88.2 % gör detta.

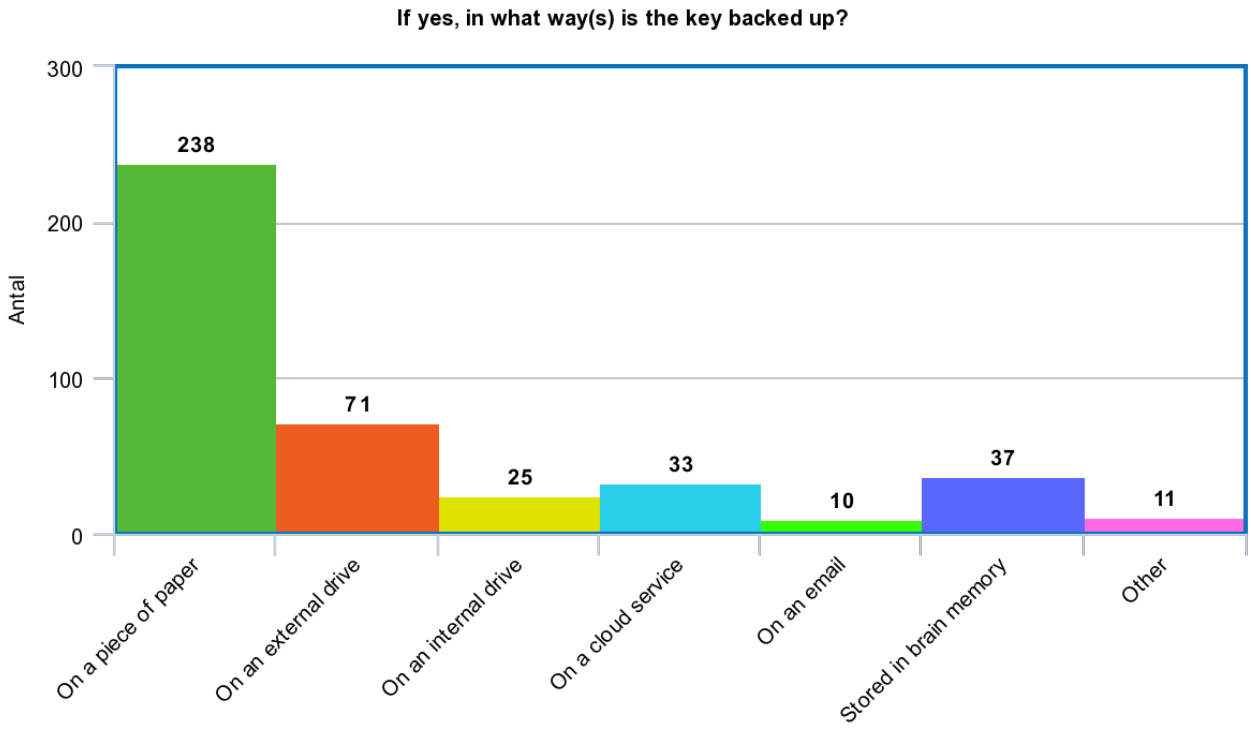


Illustration 7: Typ av säkerhetskopiering

Illustration 7 visar resultatet för vilka typer av säkerhetskopieringar som görs på den angivna plånboken. 70.21 % anger att de gör detta genom att skriva ner dem privata nycklarna. Frågan ställdes för att redovisa på vilka sätt användarna gör säkerhetskopiering och är av intresse för att se hur säkert det utförs.

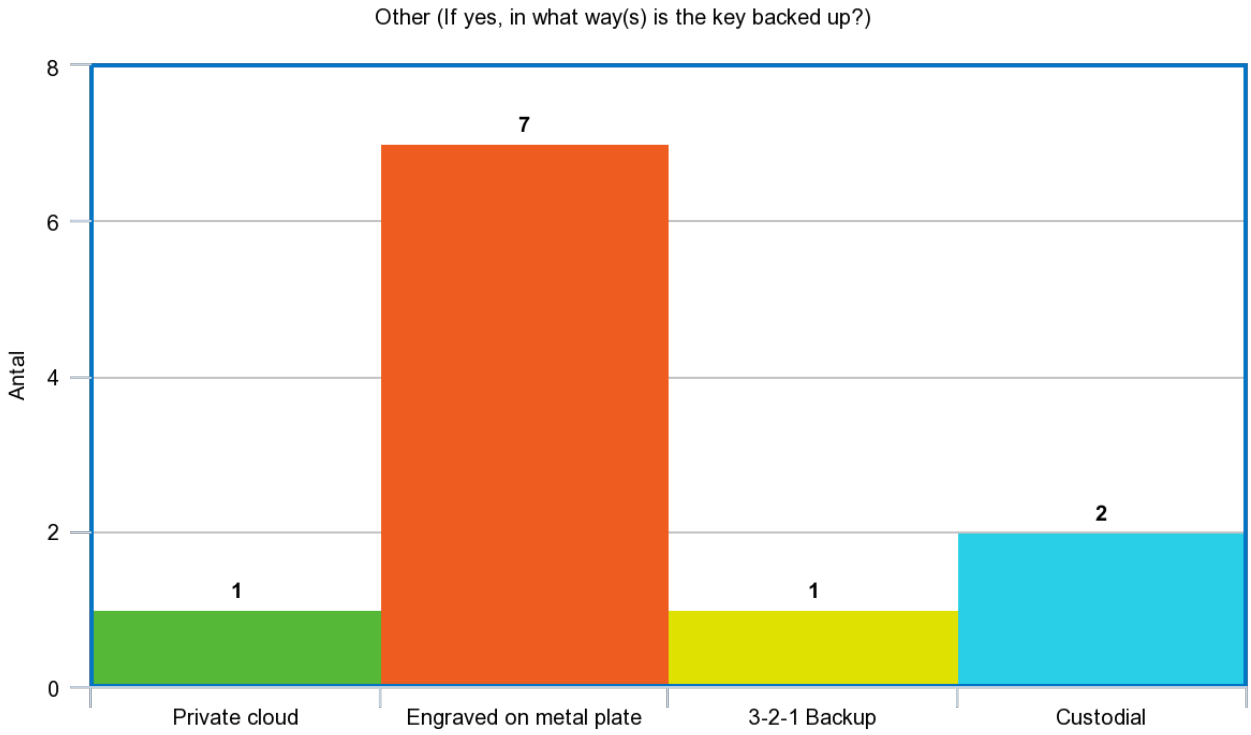


Illustration 8: Annat alternativ typ av säkerhetskopiering

De övriga svaren visar att ingravering på metall är ett populärt alternativ. Betald förvaring var även alternativ som angavs två gånger. Anledning till varför responsen är låg är för att grafen endast presenterar övriga svar för frågan nummer fyra.

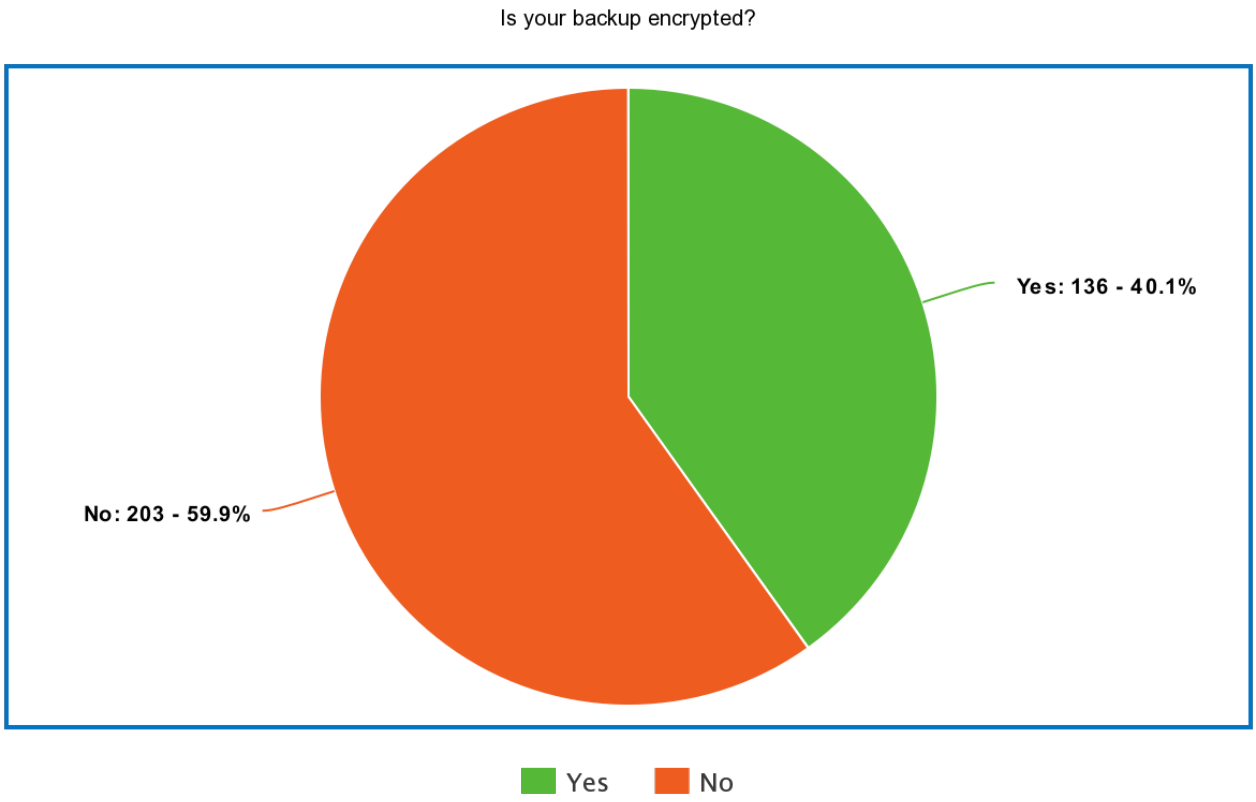


Illustration 9: Kryptering

Den sista frågan som ställdes undrade huruvida kryptering används på säkerhetskopieringen. Anledning till frågan är att kryptering bidrar till ökad säkerhet där det vill redovisas ifall användare använder sig av den säkerheten.

7 Analys

Följande två underkapitel analyserar det totala resultat från litteraturstudien om hur säkerheten av hantering av privata nycklar för Bitcoin kan ökas och svaren från enkätundersökningen. Analysen sker via granskning av olika teman från resultatet där en egen utvärdering sammanfattar resultatet för att ange riktlinjer för hantering och säkerhetskopiering av privata nycklar. Varje fråga från enkätundersökningen analyseras var för sig.

7.1 Litteraturstudie

Resultatet från litteraturstudien redovisar att flertalet säkerhetsåtgärder finns att utnyttja. Studien visar att kryptering går att applicera för alla typer av plånböcker och säkerhetskopieringar för en ökad säkerhet. Biometri är en åtgärd som kan bidra till förbättrad säkerhet på grund av unikheten som kan finnas. Dessutom kan användningen av biometri potentiellt förenkla användningen av skyddade nycklar. Anledningen är att användare nyttjar delar av sin kropp för att få tillgång till dem privata nycklarna. Resultatet indikerar att multisignatur kan vara en åtgärd som både skyddar mot stöld och förlust av privata nycklar.

Studien visar att säkerheten förändras beroende på vad för plånbok och säkerhetskopiering som används. Vidare finns det åtgärder som användarna själva kan göra för att öka säkerheten för vald metod.

7.2 Enkätundersökning

Följande underkapitel tolkar och analyserar dem svar som kom in för enkätundersökningen.

- *Fråga 1* – Resultatet visar att hårdvaruplånböcker är den mest använda typen av plånbok för förvaring av majoriteten av all Bitcoin. Anledning till varför är att användare kan finna en hårdvaruplånbok säker, användarvänlig och relativt tillgänglig. Anledning till detta är att flera olika företag säljer dessa typer av plånböcker där de vill sälja så lockande produkt som möjligt. Sedan är det en stor del av deltagarna som använder sig av mjukvaruplånböcker där fördelen är att dessa är gratis. De flesta hade nog helst ägt en hårdvaruplånbok men kanske inte anser det värt att investera i en sådan.

- *Fråga 2* – Ett förvånande resultat där det var förväntat att få skulle använda sig av multisignatur. Detta för att det kan vara tekniskt svårt och att alla plånböcker ej använder sig av tekniken. Sedan bidrar det till lägre tillgänglighet.

- *Fråga 3* – Visar att majoriteten gör säkerhetskopieringar på sina nycklar vilket är positivt. Något som är missvisande med resultatet är att två deltagare som angett handelsplats som plånbok svarar att de gör säkerhetskopiering på sina privata nycklar. Det som gör resultatet lite missvisande är att en handelsplats inte ger användare kontroll över dem privata nycklarna där saldot egentligen är från deras egna databas. Troligtvis har dessa deltagare trott att en säkerhetskopia på deras lösenord för autentisering är deras privata nyckel vilket är inkorrekt.

- *Fråga 4* – Upplyser att säkerhetskopiering på något fysiskt skrivbart är den mest populära metoden. Trolig anledning till detta är att denna typ av säkerhetskopiering kan vara billig att göra i form av papper och penna. Sedan kan den utföras säkert i form av att den är frånkopplad från internet. Något som var förvånande var att flera deltagare angav graverad metallplatta som

säkerhetskopiering vid annat svarsalternativ. Svaret visar att det går att utföra säkerhetskopiering som är mer hållbar jämfört med användning av papper.

- *Fråga 5* – Troligtvis skriver de flesta som använder sig av papper dem privata nycklarna eller lösenordsfrasen direkt i klartext där de sedan gömmer säkerhetskopian från tillgång. Kryptering kan ses som mer aktuellt för hårddiskar men framförallt e-post och och molntjänster då säkerhetskopiorna förvaras hos en tredjepart. Något som kan ha gjort frågan otydlig är huruvida kryptering kan ske på ett nedskrivet papper eller metallbit. Detta är något som helt klart är möjligt, detta via att kryptera kopian för att sedan anteckna den i krypterat format.

Enkäten indikerar på att Bitcoin-användare gör säkerhetsöverväganden när det gäller säkerheten. En stor anledning till detta kan vara är att det handlar om valuta som har ett riktigt värde. Skillnaden mot vanlig fiatvaluta är att säkerheten baseras på ens egna val. Med en bank så får en helt enkelt lite på att deras säkerhet är tillräcklig. Sedan så kan förlorad Bitcoin ej återställas vilket även kan vara en stor faktor till dem säkerhetsåtgärder som görs. Dessa anledningar gör att folk är beredda att betala för ökad säkerhet.

8 Diskussion

Följande kapitel kommer att diskutera de olika aspekterna för arbetet. Kapitlet inleder med en diskussion om den rekommendation som skulle framtas enligt ett av dem forskningsmål som angavs för arbetet. Efter rekommendation diskuteras dem metodval som gjordes och därefter reflektera över dem urval som gjorts. Etiska, vetenskapliga och samhälleliga aspekter kommer att gås igenom där en diskussion rörande vad för bidrag forskningen har skapat. Framtida arbete avslutar kapitlet.

8.1 Rekommendation

Resultatet klargör att det finns flertalet åtgärder som kan göras för att öka säkerheten vid lagring och hantering av nycklar för Bitcoin. I samtliga typer av plånböcker är kryptering en klar fördel att använda. Anledning till att säkerheten blir högre är att ifall en angripare kommer över dem privata nycklarna så är dessa skyddade i form av kryptering som är ett extra lager av skydd. Resultatet visar hur enkelt nycklar kan identifieras på datorer ifall kryptering inte används. Kryptering som dekrypteras i form av pinkod, lösenord eller biometri kan användas, där biometri kan ses som mest säker på grund av dess singularitet.

Multisignatur är även en faktor som ökar säkerheten då flertalet nycklar krävs för signering. En förövare måste därför komma över flertalet nycklar. Beroende på förhållande så kan även signering av alla nycklar ej krävas. Detta tillåter att ifall en nyckel går förlorad så är inte all Bitcoin förlorad. En bra strategi är att låta varje nyckels säkerhetskopia ej finnas på samma plats som dess nyckelpar.

Vidare är valet av plånbok viktig där den mest säkra bör väljas utefter användningsområde. Problematiken är att en plånbok inte passar alla ändamål. Nedan redovisas dem plånböcker som identifierades från litteraturstudien och huruvida om och när de ska användas.

- *Mjukvaruplånböcker för mobiler* – Till skillnad från de andra plånböckerna är att en mjukvaruplånbok på en mobil tillåter en att signera transaktioner ute på fot. Till exempelvis vid köp i affärer och liknande. Något som de andra plånböckerna lider av, mobilitet. Betalningar kan ske snabbt via NFC eller skanning av QR-koder. Denna typen av plånbok rekommenderas i situationer där tillgänglighet och mobilitet är av prioritering. Kan vara ett bra komplement till en mer säker plånbok.

- *Mjukvaruplånböcker för datorer* – Ifall en mobil inte finns tillgänglig så är detta ett alternativ. Denna typen av plånbok är av att ej föredra över en smarttelefon på grund av att datorer är mer utsatta för olika typer av skadliga program.

- *Handelsplatser* – Uppfyller endast ett användningsområde och det är vid utbyte av valuta. En handelsplats bör aldrig användas för att ”lagra” Bitcoin på. Detta för att ägandet av privata nycklar ej sker. Kontrollen av nycklarna har det företag som bedriver sidan där de är ett stort mål för hackare. Vid utbyte av valuta bör all Bitcoin genast överföras. Frågan är inte om en handelsplats Bitcoin blir stulna, utan när.

- *Webbplånböcker* – Bör ej användas med den enkla anledningen att en tredjepart mottar dem privata nycklarna via internet. Detta resulterar till flertalet säkerhetsproblem som gör att denna typ av plånbok ska undvikas.

- *Hårdvaruplånbok* – Besitter hög säkerhet då nycklarna aldrig lämnar enheten. Vid val av denna plånbok bör dock typ av kanal mellan dator och plånbok ses över, anledning är för att typen av

kanal kan vara en säkerhetsbrist. Är ett bra val ifall säkerhets prioriteras ihop där tillgängligheten är relativt hög. Den nackdel som bör ses över är att en hårdvaruplånbok kostar att köpa. Det bör därför reflekteras huruvida ett köp av en hårdvaruplånbok kan rättfärdigas.

- *Pappersplånbok* – Den plånbok som kan ses som mest säker vid hantering av privata nycklar. Anledningen till varför en pappersplånbok kan ses som mest säker är ifall plånboken är skapad under rätt omständigheter. Att skapandet sker utan anslutning till internet. Det som är den stora fördelen med en pappersplånbok jämfört med övriga plånböcker är att den privata nyckeln kan skapas helt isolerat från internet. Den kan sedan förvaras frånkopplad från internet även. Detta gör att dem hot som finns är fysisk stöld och brute-force attacker där att en sådan attack blir lyckad är av försumbar chans. Vidare kan säkerheten via att nyckeln är skriven i krypterat format förhindra att en stöld resulterat till förlorade Bitcoin. Att pappersplånboken är av ett hållbart material såsom metall minskar risken för att den blir fördärvad. Problematiken är att samma nyckel används där anonymitet kan minskas. Vid signering så måste all Bitcoin skickas då återstående medel hamnar på en så kallad växeladress. Detta gör att en pappersplånbok är den mest säkra plånboken fram tills signering sker. Användningsområdet är därför anpassat för endast förvaring.

En strategi att använda sig av är att kombinera dessa olika typer av plånböcker utefter användning. Exempel på detta är hur en mjukvaruplånbok för en mobil kan representera en fysisk plånbok med pengar i och ett sparkonto en hårdvaruplånbok eller en pappersplånbok, att liknande riskmedvetenhet används.

För att öka säkerheten för säkerhetskopiering kan användning av en HD-wallet vara till fördel. Detta för att en HD-wallet tillåter att endast en säkerhetskopia återställer alla nyckelpar i form av en lösenordsfras. En sådan säkerhetskopia representerar alla privata nycklar använda för plånboken. En lösenordsfras ökar tydligheten även då engelska ord används jämfört med privata nycklar skrivna i hexadecimal form. Annars hade varenda privat nyckel behövts säkerhetskopieras vilket ökar sannolikheten för misstag.

För förvaring bör säkerhetskopian skapas och befinna sig frånkopplad från internet. En enkel metod är att skriva ner lösenordsfrasen på ett papper. Som enkätundersökningen visade så är även en bit av metall ett bra alternativ då metall är mer hållbart. Detsamma gäller externa hårddiskar där en metallbit kan vara mer hållbar. En säkerhetskopia bör även finnas på olika platser ifall en kopia går förlorad. Multisignatur är därför en bra idé vid säkerhetskopiering. Litteraturstudien visar dessutom att en krypterad säkerhetskopia ökar säkerheten mot stöld.

8.2 Metodval

För att kunna besvara hur forskningsfrågan huruvida Bitcoin-användare lagrar och säkerhetskopierar deras privata nycklar så användes en kvantitativ enkät. Enkäten var utformad på ett sådant vis att fördefinierade svarsalternativ fanns ihop med *ja* eller *nej* frågor. Det fanns även möjlighet att ange ett eget svar i form av fritext. Detta lede till att enkäten kunde utföras på kort tid för deltagarna.

Den problematik som uppkom för enkäten var valet över att endast tillåta base58-format för adresserna vilket resulterade till att en del deltagare hade problem med att ange en korrekt adress. Sedan hade *fråga 5* kunnat förtydligats specifikt för att förklara att nedskriva säkerhetskopior kan krypteras.

Enkäten påverkades även av att en del deltagare fann enkäten som ett möjligt hot då de skulle ange information som kan anses som konfidentiell. Trots att enkäten var anonym och att enkäten var installerad på en egen värd så ansåg ett litet antal enkäten som osäker. Detta kan ha resulterat till mindre tekniskt kunniga deltagare ej deltog.

För forskningsmålet om hur lagring och säkerhetskopiering kan förbättras användes en litteraturstudie för att besvara frågan. Valet av litteraturstudie bidrog till att resultatet hade vetenskaplig bakgrund där det dock finns risk för att subjektiva förklaringar kan ha skett. Metodvalet kan även resultera till att resultatet kan vara utdaterat då Bitcoin ständigt utvecklas där nya typer av tekniker och protokoll bidrar till ökad säkerhet. Även nya typer av plånböcker kan ha förbisetts. En alternativ metod för forskningsfrågan hade kunnat vara intervjuer av företag och personer med stor kunskap inom området. Anledning till intervjuer ej användas var att ett mer subjektivt resultat hade varit möjligt då personliga åsikter angetts och möjligtvis utan vetenskaplig grund.

8.3 Urval

Urvalet för enkätundersökningen bidrog till att ett relativt högt deltagande begicks med medverkande runt om världen. Problematiken med att välja ett forum som urval är att resultatet kan bli partiskt. Detta då medlemmar i ett forum har ett intresse av Bitcoin vilket kan göra att de besitter mer teknisk kunskap inom området jämfört medelanvändaren. Resultatet kan då bli missvisande där det inte riktigt representerar alla användare vilket i sig är omöjligt att skapa en bild då drygt 48 miljoner plånböcker finns där forumet bestod av 1.3 miljoner användare (Blockchain, 2020). Totalt svarade 339 på enkäten där möjlighet för att svara på enkäten flertalet gånger var möjligt.

För litteraturstudien så riskerar valet av databaser att vara ett subjektiv val. Urvalet av artiklar löper samma risk då egen granskning av vad för artiklar som är aktuella för forskningsarbetet. Även en ofullständig mängd data kan ha använts för forskningen. Även val av att ej inkludera företagsartiklar för typer av plånböcker och säkerhetskopiering kan ha resulterat till att flertalet typer av metoder uteblivit.

8.4 Etiska aspekter

De deltagare som varit med i enkäten fick information om vad studiens syfte varit i följd av den välkomstsida som skapades för enkäten. På välkomstsidan blev de informerade om meningen med enkäten och att enkäten är anonym där ingen personlig information samlas in. De blev även informerade med hur all insamlad data skulle användas och av vem. Även information om hur länge databasen kommer att finnas angavs.

Ett problemområde som enkäten kan resultera till är att angripare kan få en bättre bild av vad för typ av plånböcker som används. Illasinnade personer kan därav prioritera på vad för typ av plånböcker de vill identifiera säkerhetshål och möjliga attacker.

Då ett stort antal deltagare angav en Bitcoin-adress så finns det möjlighet till att använda dessa adresser till skadliga ändamål. Även om adresserna endast hanterades internt och ej presenterades så är dessa möjliga att identifiera på blockkedjan. Att endast veta om en av dem Bitcoin-adresser som angavs gör det möjligt att spåra resterande adresser med en blockkedja utforskare.

Litteraturstudien har utförts i syfte med att presentera för användare hur de kan förbättra tillvägagångssättet för hantering och säkerhetskopiering av privata nycklar. Även om arbetet erbjuder förbättring för användare så kan även förövare se över informationen och identifiera de brister som finns för olika metoder. Detta för att använda i eget syfte för att identifiera säkerhetsbrister som kan utnyttjas vid attacker.

8.5 Vetenskapliga aspekter

Studien granskar ett område där inte mycket tidigare gjorts. Det finns flera studier där specifika metoder av hantering och lagring av privata nycklar för Bitcoin granskas men bara någon enstaka där alla metoder jämförs. Arbetet har gett riktlinjer för nya och nuvarande användare för hur de kan använda Bitcoin på ett säkrare sätt. Forskningen bidrar även till att användare av andra kryptovalutor kan använda samma riktlinjer ifall tekniken tillåter det.

Enkäten ger en grund för vilka tekniker användare utnyttjar för att ge en bättre bild för hur landskapet ser ut. Ett större urval och deltagande skulle kunna genomföras. Detta med en mer djupare granskning med jämförelse mellan olika typer av plånbokstekniker och deras tillvägagångssätt för multisignatur och säkerhetskopiering. Detta för att identifiera korrelation mellan plånbok, multisignatur och tillvägagångssätt för säkerhetskopiering.

8.6 Samhälleliga aspekter

Baserat på ett nätverks- och systemadministration synsätt bidrar arbetet med förståelse för vilka åtgärder som kan göras för informationssäkerheten inom området. Arbetet bidrar till vilka säkerhetsåtgärder som kan genomföras för att uppnå en ökad informationssäkerhet.

Studien ger samhället riktlinjer för vilken typ av plånbok är lämpad för vilket användningsområde. Vidare kan individer ta del av hur av vilka säkerhetsåtgärder som kan göras för ökad säkerhet och hur en säkerhetskopia kan genomföras med säkerhet som mål. Studien kan vara nyttig för nya användare som besitter låga kunskaper om hur Bitcoin fungerar. Forskningen kan bidra till att en lägre mängd Bitcoin blir förlorad.

Vidare kan utvecklare ta del av studien för att se vilka plånböcker som är populära för att även identifiera vilka säkerhetsbrister som finns. Detta för att utveckla plånböcker som används där säkerheten är tillräcklig. Detta i sin tur bidrar till att samhället kan ta del av säkrare lösningar.

En indikation på att studien är relevant och intressant är att reportern Wright (2020) publicerade en artikel på nyhetssidan CoinTelegraph. Artikeln har i skrivande stund fått 7101 visningar med 170 delningar. Reportaget redovisar enkätundersökningen ihop med en intervju.

8.7 Bidrag

Arbetet bidrar till en bättre förståelse för Bitcoin-användares tillvägagångssätt när det gäller hantering av dem privata nycklarna. Studien har samlat in data via att direkt fråga användare istället för att se över statistik i form av vad företag och applikationsutvecklare anger. Forskningen har därför berört tillvägagångssätt som faktiskt nyttjas vid användning av Bitcoin och lagt grund för ny unik data inom området.

Forskning som genomförts innan har missat att ha användarna i fokus och endast berört de tekniska aspekterna inom området. Arbeten innan har endast behandlat en snäv målgrupp medan denna studie har nått en bred målgrupp utan geografiska gränser och obetydlig bakgrund. Det var tidigare ej utforskat för hur säkerhetskopiering av dem privata nycklarna sker eller huruvida multisignatur nyttjas. Arbetet bidrar med att det finns data för säkerhetskopiering och multisignatur inom området. Den kunskap som studien ger ut är data för vilka applikationer som används och de säkerhetsval som görs utav människor som använder Bitcoin.

Tidigare forskning har ej behandlat alla de olika typerna av plånböcker och säkerhetskopieringsmetoder utan istället granskat specifika metoder. Användare kan nyttja denna forskning via att identifiera vad för typ av metoder som kan användas för att få en förståelse för hur de kan gå tillväga. Studien bidrar förhoppningsvis till att mer säkerhetsmedvetna val utförs vilket har potential till en minskad förlust av privata nycklar.

Det bidrag som görs för framtida studier är att det finns data för vilka plånböcker som används vilket gör att forskning inom området får en tydligare bild inom vad som är av intresse. Studien bidrar även en grund för de säkerhetsåtgärder och brister som finns för olika typer av plånböcker och säkerhetskopieringsmetoder. Framtida forskning kan nyttja denna forskning med att utveckla teknologier, plånböcker och säkerhetskopieringsmetoder som handskas med dessa problem. Plånböcker med ökad säkerhet kan med hjälp av detta arbetet skapas ihop med förståelse för vilka typer av plånböcker som är av intresse för målgruppen.

8.8 Framtida arbete

När det gäller framtida arbeten inom området så finns det många möjligheter. Kryptovalutor är en ganska ung teknologi som med största sannolikhet kommer att utvecklas och få större antagande. Då kryptovalutor besitter ett slags värde är det alltid intressant att se över hur tillgångar skyddas. Arbeten för plånböcker är även möjligt då dessa kan vara ansiktet utåt för användare. Att skapa säkra och lättanvända lösningar är något som kan leda till att användarantalet ökar.

Liknande enkätundersökning kan ske i form av att se över korrelationerna av den data som samlas in. Även att se över i vilket format som säkerhetskopiering sker. Exempel på detta är huruvida säkerhetskopiering sker i form av lösenordsfraser eller privata nycklar. Korrelation mellan mängd Bitcoin och typ av hantering är även ett möjligt framtida arbete. Sedan kan forskning där jämförelse mellan olika kryptovalutor ske. Detta kan vara av intresse då olika valutor kan uppfylla olika sorters funktioner där antal plånböcker kan vara mindre utvecklat. Framtida arbete kan även täcka vad för relation multisignaturen utförs i.

Möjligheterna för framtida forskning är väldigt brett då tekniken är i en ung fas. Flertalet utmaningar för att förbättra tekniken i form av säkerhet, användarvänlighet, integritet och prestanda finns.

9 Slutsats

Denna forskningsinsats presenterar en enkätundersökning om hur 339 Bitcoin-användare agerar för att hantera dem privata nycklarna som är den tillgång av Bitcoin som är möjlig. Genom att publicera en enkät för Bitcoin-användare kan grafer i form av beskrivande statistik presenteras. Resultatet från enkäten visar att användare gör säkerhetsmedvetna val i form av att majoriteten nyttjar hårdvaruplånböcker där statistiken visar markant att säkerhetskopiering genomförs för möjlig återställning. Resultatet visar även att överraskande stort antal använder sig av multisignatur för att öka säkerheten.

Resultatet från litteraturstudien visar att kryptering är en säkerhetsåtgärd som kan bidra till ökad säkerhet för de olika typerna av plånböcker. Användning av multisignatur är även en åtgärd som bidrar till ökad säkerhet mot attacker och förlust att säkerhetskopior. Forskningen visar att säkerhetskopiering som sker isolerat från internet via en lösenordsfras är en metod som kan ge skydd och tydlighet för användare. Detta då HD-plånböcker generar lösenordsfraser av ord där 24 ord är av rekommendation för att motstå brute-force attacker. Dem deterministiska orden bidrar till alla nycklar kan återställas där orden skapar begriplighet.

Det finns inget klart svar över vilken typ av plånbok som bör användas. Detta för att plånböckerna för tillfället uppfyller olika användningsområden. Analysen visar att användare får göra medvetna val efter vad för tillämpning som ska uppfyllas. Kombination av plånböcker efter ändamål kan därför vara ett önskat val för användare för ökad säkerhet.

Bitcoin blir lika bra så som dem plånböcker som finns. Likt hur dagens webbläsare erbjuder användarvänligt gränssnitt med säkerhet underbyggd bör plånböckerna gå i samma riktning. Det viktigaste för hur säkerheten kan ökas för Bitcoin-användare är att säkerhet byggs in utan att användare självmant behöver göra säkerhetsmedvetna beslut. Dagens webbläsare för internet ska bli vad plånböcker är för Bitcoin.

Referenser

De referenser som är markerade med * (asterisk) tillhör granskningen.

ACM. (n.d.). About ACM Publications. Hämtad april 5, 2020, från https://www.acm.org/publications/about-publications

Antonopoulos, A. M. (2017). *Mastering Bitcoin 2nd Edition* (2nd ed.). O'Reilly Media, Inc.

Alshamsi, A., & Andras, P. P. (2019). User perception of Bitcoin usability and security across novice users. *International Journal of Human-Computer Studies*, *126*, 94–110. doi: 10.1016/j.ijhcs.2019.02.004

Berndtsson, M., Hansson, J., Olsson, B., & Lundell, B. (2008). Thesis Projects (2nd ed.). London: Springer-Verlag.

Bitcoin Core. (2016, August 23). Bitcoin Core version 0.13.0 released. Hämtad april 12, 2020, från https://bitcoin.org/en/release/v0.13.0#database-cache-memory-increased

* Biryukov, A., & Tikhomirov, S. (2019). Security and privacy of mobile wallet users in Bitcoin, Dash, Monero, and Zcash. *Security and Privacy of Mobile Wallet Users in Bitcoin, Dash, Monero, and Zcash*, *59*. doi: https://doi.org/10.1016/j.pmcj.2019.101030

Blockchain. (2020, May 6). Blockchain.com Wallets. Hämtad maj 6, 2020, från https://www.blockchain.com/charts/my-wallet-n-users

Booth, A., Sutton, A. & Papaioannou, D. (2016). Systematic approaches to a successful literature review. (2:a uppl.) Los Angeles: Sage.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77–101. doi: 10.1191/1478088706qp063oa

Brereton, P., Kitchenham, B. A., Budgen, D., Turner, M., & Khalil, M. (2007). Lessons from applying the systematic literature review process within the software engineering domain. *Journal of Systems and Software*, *80*(4), 571–583. doi: 10.1016/j.jss.2006.07.009

* Conti, M., Kumar, E. S., Lal, C., & Ruj, S. (2018). A Survey on Security and Privacy Issues of Bitcoin. *IEEE Communications Surveys & Tutorials*, *20*(4), 3416–3452. doi: 10.1109/comst.2018.2842460

Delay for Reddit. (2020). Subreddit Traffic Analysis. Hämtad april 23, 2020, från https://www.delayforreddit.com/analysis/subreddit/bitcoin

Fowler, F. J. (2014). *Survey research methods* (5th ed.). London: Sage Publication.

Gervais, A., Karame, G. O., Capkun, V., & Capkun, S. (2014). Is Bitcoin a Decentralized Currency? *IEEE Security & Privacy*, *12*(3), 54–60. doi: 10.1109/msp.2014.49

Google. (2020, March 31). Privacy Policy – Privacy & Terms. Hämtad april 12, 2020, från https://policies.google.com/privacy

Guri, M. (2018). BeatCoin: Leaking Private Keys from Air-Gapped Cryptocurrency Wallets. *2018 IEEE International Conference on Internet of Things (IThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*. doi: 10.1109/cybermatics_2018.2018.00227

* He, S., Wu, Q., Luo, X., Liang, Z., Li, D., Feng, H., … Li, Y. (2018). A Social-Network-Based Cryptocurrency Wallet-Management Scheme. *IEEE Access*, *6*, 7654–7663. doi: 10.1109/access.2018.2799385

Hileman, G., & Rauchs, M. (2017). 2017 Global Cryptocurrency Benchmarking Study. *SSRN Electronic Journal*. doi: 10.2139/ssrn.2965436

* Horst, L. V. D., Choo, K.-K. R., & Le-Khac, N.-A. (2017). Process Memory Investigation of the Bitcoin Clients Electrum and Bitcoin Core. *IEEE Access*, *5*, 22385–22398. doi: 10.1109/access.2017.2759766

* Hu, K., Zhang, Z., & Guo, K. (2019). Breaking the binding: Attacks on the Merkle approach to prove liabilities and its applications. *Computers & Security*, *87*, 101585. doi: 10.1016/j.cose.2019.101585

Hughes, A., Park, A., Kietzmann, J., & Archer-Brown, C. (2019). Beyond Bitcoin: What blockchain and distributed ledger technologies mean for firms. *Business Horizons*, *62*(3), 273–281. doi: 10.1016/j.bushor.2019.01.002

IEEEXplore. (2019). About the Peer Review Process. Hämtad från https://journals.ieeeauthorcenter.ieee.org/submit-your-article-for-peer-review/about-the-peer-review-process/.

Jesson, J., Matheson, L., & Lacey, F. M. (2011). Doing your literature review: Traditional and systematic techniques. Los Angeles, CA: Sage Publications

* Kaushal, P. K., Bagga, A., & Sobti, R. (2017). Evolution of bitcoin and security risk in bitcoin wallets. *2017 International Conference on Computer, Communications and Electronics (Comptelix)*. doi: 10.1109/comptelix.2017.8003959

* Kaushik, A., Choudhary, A., Ektare, C., Thomas, D., & Akram, S. (2017). Blockchain — Literature survey.*2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*. doi: 10.1109/rteict.2017.8256979

* Khan, A. G., Zahid, A. H., Hussain, M., & Riaz, U. (2019). Security Of Cryptocurrency Using Hardware Wallet And QR Code. *2019 International Conference on Innovative Computing (ICIC)*. doi: 10.1109/icic48496.2019.8966739

* Kim, C. Y., & Lee, K. (2018). Risk Management to Cryptocurrency Exchange and Investors Guidelines to Prevent Potential Threats. *2018 International Conference on Platform Technology and Service (PlatCon)*. doi: 10.1109/platcon.2018.8472760

Kitchenham, B. (2004). Procedures for performing systematic reviews. Keele, UK, Keele University, 33(2004), 1-26.

Kävrestad, J. (2018). *Fundamentals Of Digital Forensics: theory, methods, and real-life applications*. S.l.: Springer, Cham. doi: https://doi.org/10.1007/978-3-319-96319-8

Liu, Y., Li, R., Liu, X., Wang, J., Zhang, L., Tang, C., & Kang, H. (2017a). An efficient method to enhance Bitcoin wallet security. *2017 11th IEEE International Conference on Anti-Counterfeiting, Security, and Identification (ASID)*. doi: 10.1109/icasid.2017.8285737

Liu, Y., Chen, X., Zhang, L., Tang, C., & Kang, H. (2017b). An Intelligent Strategy to Gain Profit for Bitcoin Mining Pools. *2017 10th International Symposium on Computational Intelligence and Design (ISCID)*. doi: 10.1109/iscid.2017.184

* Liu, X., Fu, J., & Chen, Y. (2020). Event evolution model for cybersecurity event mining in tweet streams. *Information Sciences*, *524*, 254–276. doi: 10.1016/j.ins.2020.03.048

* Malathi, M., Pavithra, S., Preakshanashree, S., Kumar, S. P., & Tamilarashan, N. (2019). Wield Blockchain TechnologyTo Fortify Smart Wallet. *2019 IEEE International Conference on System, Computation, Automation and Networking (ICSCAN)*. doi: 10.1109/icscan.2019.8878815

Maxwell, J. A. (1992). *Understanding and Validity in Qualitative Research*. Harvard Educational Review, 279-300

Moore, T., Christin, N., & Szurdi, J. (2018). Revisiting the Risks of Bitcoin Currency Exchange Closure. *ACM Transactions on Internet Technology*, *18*(4), 1–18. doi: 10.1145/3155808

Nagata, K., Kikuchi, H., & Fan, C.-I. (2018). Risk of Bitcoin Addresses to be Identified from Features of Output Addresses. *2018 IEEE Conference on Dependable and Secure Computing (DSC)*. doi: 10.1109/desec.2018.8625106

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Hämtad från https://bitcoin.org/bitcoin.pdf

* Nguyen, P. Q., & Zhou, J. (2017). Information Security. *Lecture Notes in Computer Science*. doi: 10.1007/978-3-319-69659-1

* Orme, D. (2019). Is biometrics the answer to crypto-currency crime? *Is Biometrics the Answer to Crypto-Currency Crime?*, *2019*(2), 8–10. doi: https://doi.org/10.1016/S0969-4765(19)30025-6
* Pal, O., Alam, B., Thakur, V., & Singh, S. (2019). Key management for blockchain technology. *ICT Express*. doi: 10.1016/j.icte.2019.08.002
* Rakdej, P., Janpitak, N., Warasart, M., & Lilakiatsakun, W. (2019). Coin Recovery from Inaccessible Cryptocurrency Wallet Using Unspent Transaction Output. *2019 4th International Conference on Information Technology (InCIT)*. doi: 10.1109/incit.2019.8911915
* Rezaeighaleh, H., & Zou, C. C. (2019a). New Secure Approach to Backup Cryptocurrency Wallets. *2019 IEEE Global Communications Conference (GLOBECOM)*. doi: 10.1109/globecom38437.2019.9014007
* Rezaeighaleh, H., & Zou, C. C. (2019b). Deterministic Sub-Wallet for Cryptocurrencies. *2019 IEEE International Conference on Blockchain (Blockchain)*. doi: 10.1109/blockchain.2019.00064
Sahmim, S., Gharsellaoui, H., & Bouamama, S. (2019). Edge Computing: Smart Identity Wallet Based Architecture and User Centric. *Procedia Computer Science*, *159*, 1246–1257. doi: 10.1016/j.procs.2019.09.294
* Sai, A. R., Buckley, J., & Gear, A. L. (2019). Privacy and Security analysis of cryptocurrency mobile applications. *Privacy and Security Analysis of Cryptocurrency Mobile Applications*. doi: 10.1109/MOBISECSERV.2019.8686583
Schmitz, C. (2020). Limesurvey - the most popular foss survey tool on the web. Hämtad april 12, 2020, från https://www.limesurvey.org/
ScienceDirect. (n.d.). ScienceDirect FAQs. Hämtad april 5, 2020, från https://learning.acm.org/faq/sciencedirect-faqs
SENSE about SCIENCE. (2009). Peer Review Survey 2009. Hämtad april 6, 2020, från http://senseaboutscience.org/activities/peer-review- survey-2009/.
Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal Of Business Research*, *104*, 333-339. doi: 10.1016/j.jbusres.2019.07.039
* Thota, A. R., Upadhyay, P., Kulkarni, S., Selvam, P., & Viswanathan, B. (2020). Software Wallet Based Secure Participation in Hyperledger Fabric Networks. *2020 International Conference on COMmunication Systems & NETworkS (COMSNETS)*. doi: 10.1109/comsnets48256.2020.9027445
* Volety, T., Saini, S., Mcghin, T., Liu, C. Z., & Choo, K.-K. R. (2019). Cracking Bitcoin wallets: I want what you have in the wallets. *Future Generation Computer Systems*, *91*, 136–143. doi: 10.1016/j.future.2018.08.029
Wohlin, C., Runeson, P., Höst, M., Ohlsson, M. C., Regnell, B. & Wesslén, A. (2012). Experimentation in software engineering. Springer Science & Business Media.
Wohlin, C. (2014). Guidelines for snowballing in systematic literature studies and a replication in software engineering. *Proceedings of the 18th International Conference on Evaluation and Assessment in Software Engineering - EASE 14*. doi: 10.1145/2601248.2601268
Wright, T. (2020). Survey Shows Many BTC Holders Use Hardware Wallet, Have Backup Keys. *Cointelegraph*. Retrieved from https://cointelegraph.com/news/survey-shows-many-btc-holders-use-hardware-wallet-have-backup-keys
Wu, Y., Luo, A., & Xu, D. (2019). Forensic Analysis of Bitcoin Transactions. *2019 IEEE International Conference on Intelligence and Security Informatics (ISI)*. doi: 10.1109/isi.2019.8823498
Zollner, S., Choo, K.-K. R., & Le-Khac, N.-A. (2019). An Automated Live Forensic and Postmortem Analysis Tool for Bitcoin on Windows Systems. *IEEE Access*, *7*, 158250–158263. doi: 10.1109/access.2019.2948774

Appendix A – LimeSurvey

LimeSurvey installerades på en Ubuntu 19.04 server med ESXi 6.5 som hypervisor. Den fysiska hårdvaran var följande:

- Dell R320
- Intel Xeon E5-1410
- 48 GB pc3-9500 RAM-minnen

Den virtuella maskinen fick följande konfiguration:

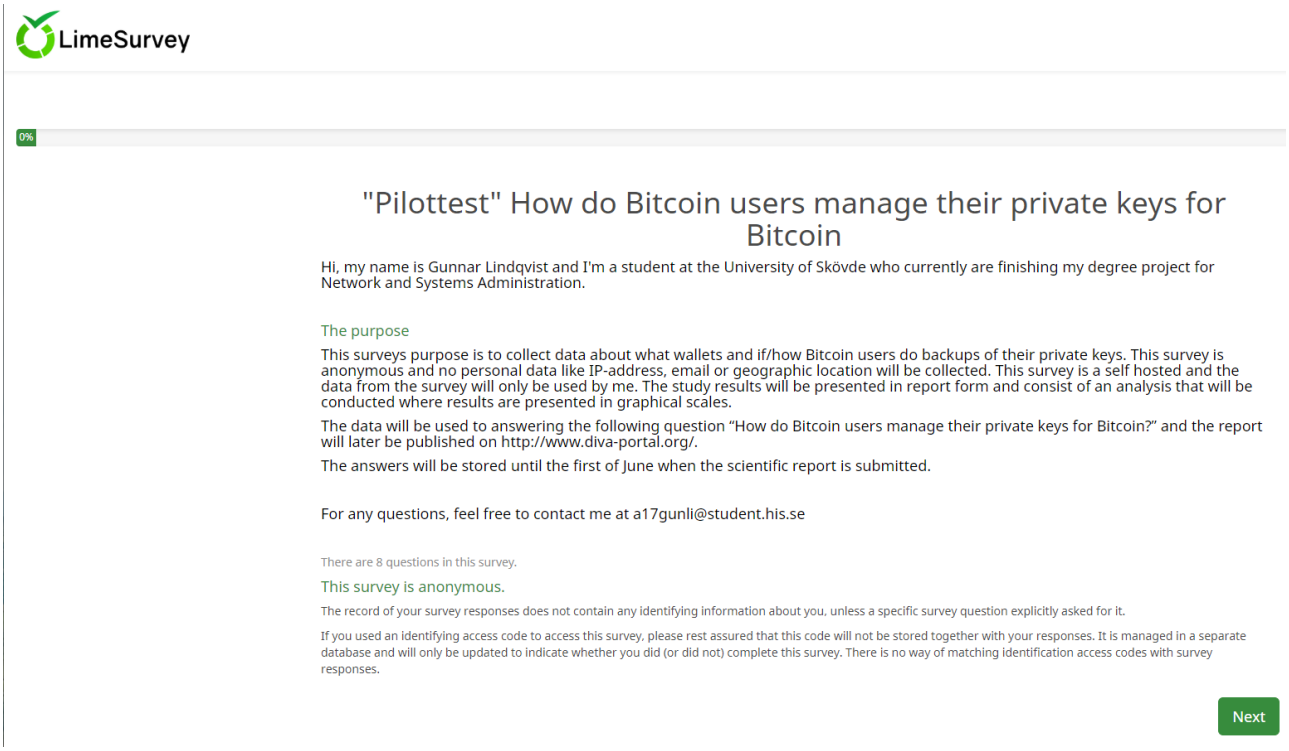
- 8192 MB RAM (8GB)
- 2 Virtuella processorer
- 30 GB HDD

I denna virtuella maskin installerades LimeSurvey 4.1.17 ihop med följande tjänster:

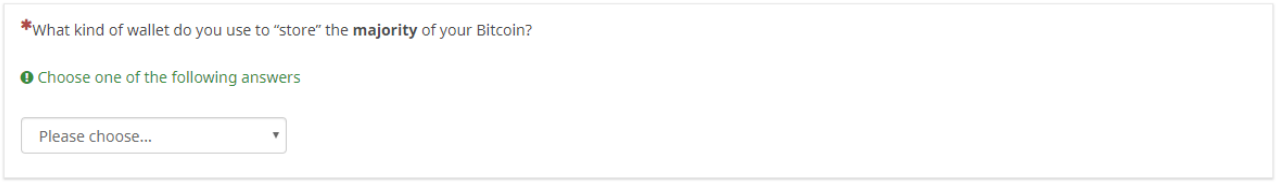
- MariaDB 10.4.12
- PHP 7.4
- Apache 2.4.41

Appendix B – Pilottest

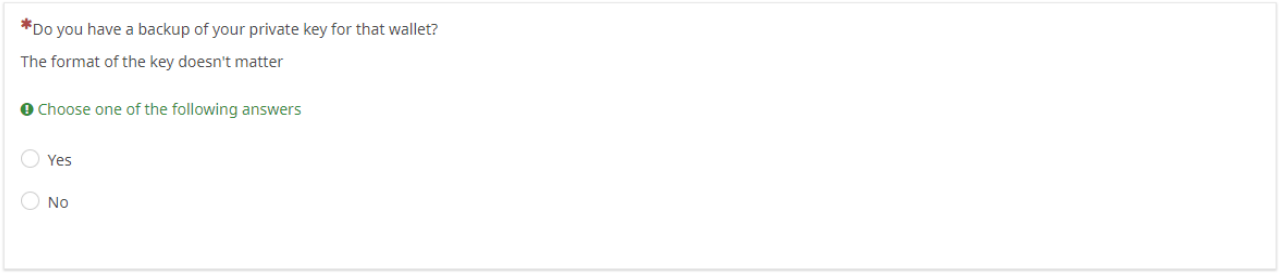
Välkomstskärm



Fråga 1.



Fråga 2.



Fråga 3.

If yes, in what ways is the key backed up? (Format of the key doesn't matter)

Check all that apply

- [ ] On a piece of paper
- [ ] On an external drive (USB, CD)
- [ ] On an internal drive (HDD, SSD)
- [ ] On a cloud service (Dropbox, Google Docs)
- [ ] On an email (Gmail, Hotmail)
- [ ] Stored in brain memory

Fråga 4.

Is your backup encrypted?

Choose one of the following answers

- ( ) Yes
- ( ) No

Fråga 5.

*Enter your public key in Base58 format for a reward! (If possible derivative a new key)

Base58 example: 1DSsgJdB2AnWaFNgSbv4MZC2m71116JafG

Please check the format of your answer.

Fråga 6.

*Var frågorna förståeliga? Om nej, varför?

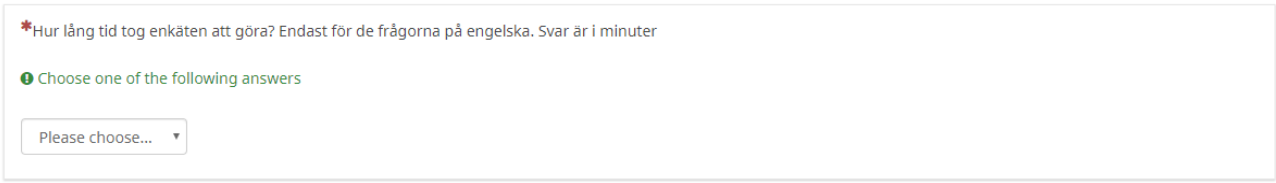
Choose one of the following answers

- ( ) Ja
- ( ) Nej

Please enter your comment here:

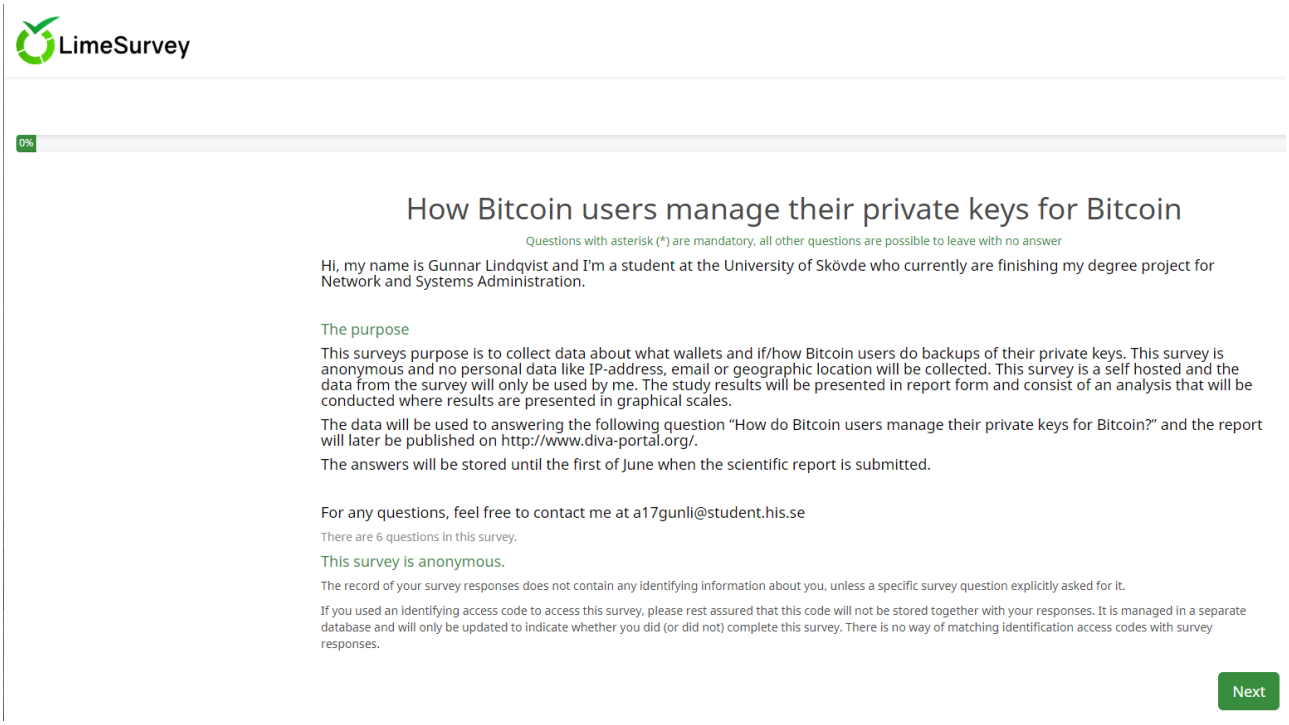
Fråga 7.

Fråga 8.

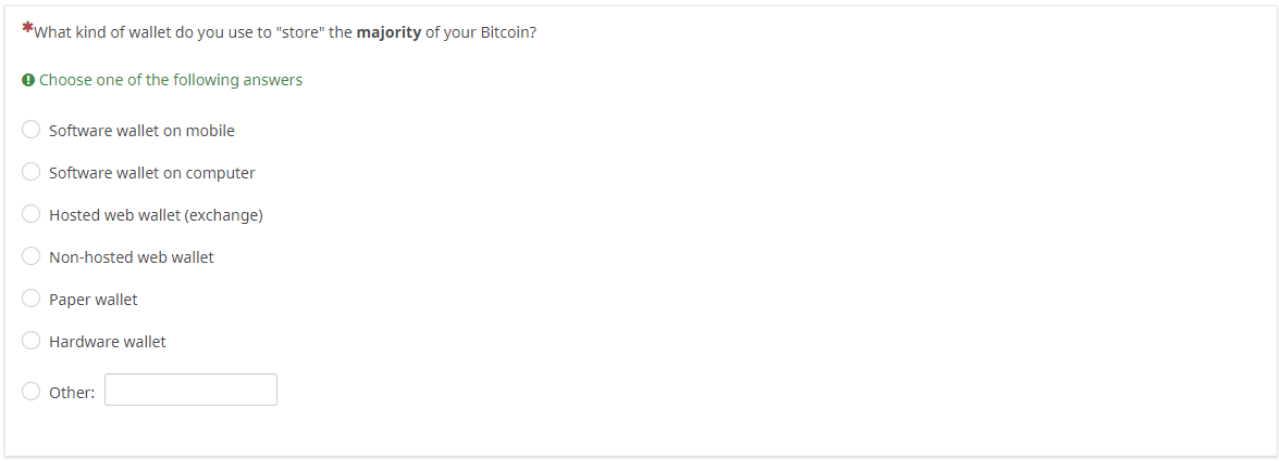


Appendix C – Enkätundersökning

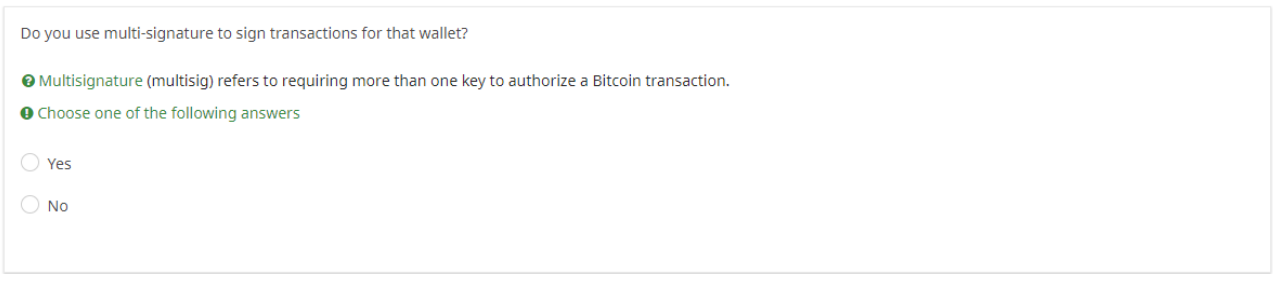
Välkomstskärm



Fråga 1.



Fråga 2.



Fråga 3.

*Do you have a backup(s) of your private key for that wallet?

The format of the key doesn't matter

Choose one of the following answers

- ○ Yes
- ○ No

Fråga 4.

If yes, in what ways is the key backed up? (Format of the key doesn't matter)

Check all that apply

- ☐ On a piece of paper or something else that is physically writable
- ☐ On an external drive
- ☐ On an internal drive
- ☐ On a cloud service (Dropbox, Google Drive)
- ☐ On an email (Gmail, Hotmail, Outlook)
- ☐ Stored in brain memory
- ☐ Other:

Fråga 5.

Is your backup encrypted?

Choose one of the following answers

- ○ Yes
- ○ No

Fråga 6.

Enter your Bitcoin address in Base58 format for a reward! (If possible derivative a new key)

Base58 example: 1DSsgJdB2AnWaFNgSbv4MZC2m71116JafG

It's possible to skip the reward

Please check the format of your answer.