KRYPTOSVINDELEN

Av Markus Johnsen Thonhaugen,
Hanne Wilhelms og Egil Ursin

Innledning

Kryptosvindelen er en featurereportasje som gir et sjeldent innblikk i hvordan svindelaktører på Internett opererer. Reportasjen viser hvordan «Anna», en utenlandsk svindelaktør, tar kontakt med et offer via appen «WhatsApp». Vi får være med når Anna bygger tillit over tid, og vi får innsikt i hva som skjer når et norsk offer lures til å investere betydelige beløp i en falsk børs for kryptovaluta. Gjennom detaljerte chatlogger, skjermdumper og verktøy for blokkjedeanalyse avdekkes det hvordan beløpet den norske mannen har betalt bare er småpenger i forhold til summene svindlerne håver inn fra ofre over hele verden. NRKs dekning ledet til slutt at politiet gjenåpnet etterforskningen av saken. Reportasjen resulterte også til en rekke konkrete tips som ga flere oppfølgingssaker.

Hvordan prosjektet ble til

Prosjektet ble utført av journalist Markus Johnsen Thonhaugen i NRK Nordland i samarbeid med Hanne Wilhelms i NRK Troms og Finnmark og grafiker Egil Ursin i NRK Nordland. Førstnevnte hadde fulgt saksfeltene «svindel» og «datasikkerhet» lenge, og fikk et tips om en interessant sak fra naboredaksjonen NRK Trøndelag. Tipset gikk ut på at en mann fra Tromsø holdt en samtale med en svindler «varm» på WhatsApp. I tipset leses: «*han holder svindleren varm mens han prøver å finne måter å få tilbake 200 000 kroner i bitcoin som han har blitt frastjålet i en sosial manipulerings-/kryptosvindel*». Tipset gikk videre ut på at han hadde hyret inn en privat detektiv fra England, og gjennom vedkommende klart å finne fram til en rekke interessante opplysninger om svindleren. «*Han kjemper for å få politiet (som har henlagt saken to ganger allerede) til å ta saken*», stod det i tipset. Mannen, som hadde blitt utsatt for svindelen, var en ressurssterk person og fremstod som troverdig.

Vedkommende mann ble kontaktet av førstnevnte journalist i NRK Nordland i begynnelsen av februar 2022, og han sa seg da villig til å fortelle sin historie. Etter dialog med redaktørene i NRK Nordland og NRK Troms og Finnmark, ble prosjektet etablert som et samarbeidsprosjekt mellom to redaksjoner i NRK (hhv. Nordland og Troms og Finnmark, der samarbeidet var mellom Markus Thonhaugen og Hanne Wilhelms som journalister på saken). Det ble besluttet at kilden skulle tilbys anonymitet med begrunnelse i følgende:

- Mulig organisert kriminalitet, og mulig beskyttelse av kilde mtp. reaksjoner.
- En sak med samfunnsmessig interesse der kilde vil advare andre, og der NRK gjennom sin journalistikk kan bidra til å sette fokus på et område som fremstår tabu.
- Kilden er selv i sin jobb avhengig av tillit, forståelig at han ikke ønsker stå fram.
- Kilde fremstår som habil.
- Saken må uansett dokumenteres grundig.

Innledende researchfase

Kilden ga fullt innsyn i all kommunikasjon vedkommende hadde hatt med svindleren, som omfattet hundrevis av chatmeldinger som utspant seg over en periode fra 20. november 2021 til slutten av februar 2022. Chatloggene ble eksportert ut fra WhatsApp som bildefiler, og så lest fra start til slutt. Viktige hendelser underveis, som mannens investeringsbeslutninger og opptakten til disse, ble markert og transkribert som tekst fortløpende – og dannet etter hvert hovedrammeverket og den røde tråden for reportasjen. Andre viktige opplysninger ble lagret i et eget dokument for senere analyse, og inkluderte blant annet Wallet-adresser mannen betalte inn til (*enkelt sagt «kontonummer» til krypto-lommebøker*), navn på kryptobørser mannen ble bedt om å overføre penger til samt WhatsApp-telefonnummeret det ble kommunisert med (altså svindlerens). Et lengre intervju med kilden ble utført i februar 2022, og bidro med mannens egne refleksjoner rundt det materialet vi hadde fått innsyn i.

Lokalt politi ble kontaktet og spurt om saken, som tidlig opplyste om at saken var oversendt Økokrim og at de ikke ville gjøre noe mer før en eventuell tilbakemelding fra dem forelå. Økokrim opplyste at de ikke kommenterer enkeltsaker. Etterlatt inntrykk for journalistene var at saken lå mer eller mindre død hos påtalemyndigheten. Samtale med politikilder avdekket videre at digitale bedragerier var et saksfelt i kraftig økning, men at så godt som alle saker ble (og blir) henlagt på grunn av mangel på ressurser og kompetanse.

Vi konkluderte med at vi måtte utføre våre egne undersøkelser for å se hva vi kunne finne ut om hvor pengene til mannen hadde tatt veien.

Hva vi kunne finne ut om «VP Markets»

Mannen ble, gjennom sosial manipulering, lurt til å overføre store beløp til en investeringsplattform for kryptovaluta som svindelaktøren omtalte som «VP Markets». Vi fant VP Markets registrert som et LTD hos Companies House (en troverdig kilde for selskaper registrert i UK). Firmaet ble nedlagt i desember 2021, men på samme adresse fant vi navnet på et annet nedlagt selskap: VP Markets Global LTD. Ut fra informasjonen i Companies House, så det ut til at svindlerne hadde operert siden 2019: VP Markets ble nemlig registrert i Storbritannia som et LTD 6. september dette året. Selskapet ble videre registrert med to direktører, men dette virket til å være falske navn, da personenes hjemadresser matchet kontoradressen til selskapet. NRK Research bistod i arbeidet.

Men det vi kunne se, var at det ene navnet kunne knyttes til 17 andre bedrifter innenfor ulike sektorer. Navnet var også knyttet til andre firmanavn som – gjennom Google søk, kunne linkes til lignende historier om svindel. Etter hvert kom vi også i kontakt med privatetterforskeren offeret hadde leid inn: Fred Harrison. En person med teknisk kompetanse som bor og jobber i London. Vedkommende er «svindeljeger» på fritida, og hjelper svindelofre med å avdekke og lete etter tekniske spor.

Harrison kunne fortelle at han kjente folk på innsiden av webhostingsleverandøren hvor domenene til «**VP Markets**» var registrert. Informasjonen han hadde fått ut var bl.a. de mailadressene domenene var registrert med. Dette var interessante opplysninger.

Hans påstand var at VP Markets-domenene var registrert med to mailadresser, og at disse mailadressene også hadde registrert en rekke andre domener: Faktisk hele 89 stykker. Vi tok stikkprøver av denne lista med domenenavn, og mens mange av domenene var inaktive kunne vi også finne at minst to av domenene kunne knyttes til tradingsider med et lignende teknisk oppsett som det til VP Markets. Noen av navnene etterlignet navnene på kjente kryptobørser, tilsynelatende i et forsøk på å utnytte tillitten til kjente børsnavn i markedet. Søk på navn og adresser i Companies House avdekket et spindelvev av ulike firmanavn som, gjennom Google-søk, også var omtalt på anti-svindelsider. Historiene vi leste om hadde mange fellestrekk: Brukere meldte om at de hadde blitt lurt til å først investere, og så (*gjennom manipulasjon av grafer på de falske kryptobørssidene*) trodd at investeringen hadde lønt seg – noe som hadde fått enkelte til å investere *mer*. Men at de så ikke kunne hente ut gevinsten når tiden var inne for å realisere denne (det ble til og med meldt om at man måtte betale et «uttaksgebyr» for å få pengene ut – de som betalte ble bedt om å betale *mer*).

Svindlerne brukte mange unnskyldninger på hvorfor det måtte investeres stadig mer for å kunne hente ut en gevinst. I vår konkrete sak hadde mannen faktisk fått ut noe penger, tilsynelatende for å bygge tillit fra svindlerens side, slik at det da også ble investert mer. Men han ble så møtt med nye pengekrav da tiden var inne for å hente noe av midlene ut.

Vi var senere i kontakt med eksperter som kunne fortelle at forhåndskonfigurerte administrasjonspaneler som de vi så i researchen av denne saken var lette å oppdrive, noe som gjorde svindel-nettsteder ekstremt lette å sette opp, og med minimale kostnader.

Av tid- og ressurshensyn hadde vi ikke mulighet til å avdekke det fulle omfanget av operasjonen («*spindelvevet*»), men det som var tydelig var at det virket som en omfattende operasjon som involverte flere bakmenn. Harrison mente det måtte være minst fem personer som stod bak akkurat denne operasjonen. Akkurat dette klarte vi ikke bekrefte.

Konklusjon var dog: **Researchen avdekket «VP Markets» som stor svindeloperasjon**.

Kryptosporet

Kryptovaluta og blokkjedeteknologi fremstår som et komplisert område for uinnvidde, og den første tiden av arbeidet med reportasjen gikk derfor med på å få en grunnleggende forståelse av hvordan teknologien fungerer. YouTube viste seg her å være en fantastisk ressurs, med flere gode videoer som forklarte hvordan «krypto-pengeoverføringer» skjer. I denne saken skjedde handelen med bitcoin, og det vi raskt fant ut er at handel med bitcoin handler om overføring av digitale aktiva der alle har en kopi av (og dermed tilgang til) «regnskapsboken» - med oversikt over alle transaksjoner som er gjort. Krypto er det man på engelsk kaller «pseudonymous» som betyr at selv om dine faktiske detaljer ikke er åpne for alle (som navn eller e-postadresse), blir din offentlige nøkkel og unike identifikasjon bakt inn i blokkjeden ved utførelse av transaksjoner (blokkjede blir da teknologien som organiserer «regnskapsboken» som krypto bygger på). Alle har tilgang til «regnskapsboken», den er åpen – og det er dermed mulig å studere transaksjoner mellom wallets. Når man har fått denne forståelsen på plass, er det mulig å gjøre analyser med utgangspunkt i en mottakeradresse.

En slik mottaksadresse hadde vi tilgang på, nemlig adressen som svindlerne hadde oppgitt til offeret for å motta bitcoin-overføringer. Det vi ikke hadde tilgang på, var mer avanserte

verktøy for å gjøre analyser av denne adressen. Her kunne ikke de norske ekspertkildene vi kom i kontakt med hjelpe oss så langt på vei, men NRK Beta tipset om en amerikansk aktør som har gjort blokkjede-analyse til et levebrød: **CipherBlade**. En amerikansk cyberkrimorganisasjon som jobber spesielt med analyse av data i blokkjeden.

CihperBlades påsto tidlig at adressen ikke ledet til kryptobørsen «VP Markets», men isteden til en wallet (kryptolommebok) hos den legitime kryptobørsen FTX. FTX er en anerkjent børs i markedet, med relativt gode rutiner for å identifisere sine kunder.

Her må vi forklare at det finnes flere former for «kryptolommebøker» man kan benytte seg av for å sende og motta bitcoins. Man har grovt sett tre former: Programvarebaserte («hot wallets») samt maskinvarebaserte og papirbaserte («cold wallets»). Disse fungerer som en inngangsport som gir adgang til å kommunisere med blokkjeden hvor aktivaene (som bitcoin) ligger. Enklere sagt generer lommebøkene all informasjonen en trenger for å handle med krypto: Offentlige og private nøkler samt adresser man kan oppgi for å motta kryptoaktiva fra andre. Forskjellen på «hot wallets» og «cold wallets» er at førstnevnte er tilkoblet internett. Her er web-baserte hot-wallets blant de mest brukte. De er enkle å bruke og sette opp via kryptotjenester på nett, som håndterer alt av nøkler og slikt - sånn at du egentlig bare trenger å huske et passord. Samtidig er de langt mindre sikre enn «cold wallets» som benytter et fysisk medium for å lagre nøklene offline.

Hvorfor er dette interessant? Jo: Det at svindlerne valgte å bruke en hot-wallet hos FTX betyr at det i teorien er børsen som sitter med alle nøklene, og som eventuelt kan velge å kutte tilgangen for svindlerne (og dermed også returnere pengene til offeret).

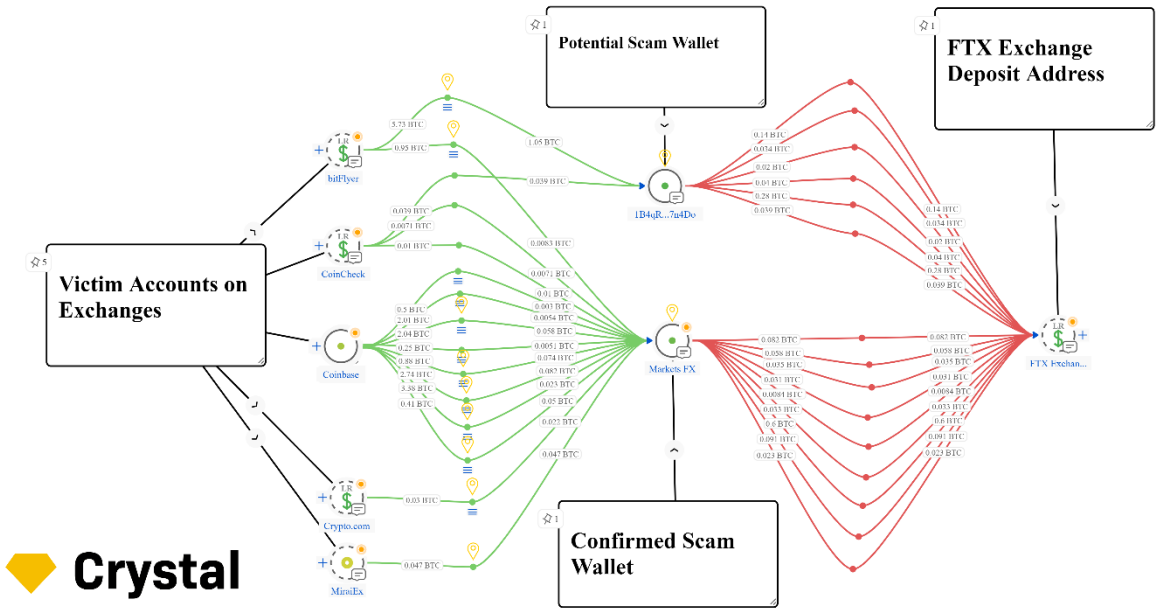
At svindlerne har valgt å bruke en legitim kryptobørs med godt rykte – som FTX er, øker også sjansene for at svindlerne på en eller annen måte har måttet identifisere seg for å få lov til å sette opp en konto gjennom en prosess kalt KYC (Know Your Customer). Dette var så interessant, at dette ble behandlet i en egen oppfølgingssak: ***Kryptoekspert sjokkert over hvor slurvete svindlerne har vært***, som senere resulterte i at politiet faktisk gjenåpnet etterforskningen: ***Gjenåpner grov bitcoin-svindelsak etter NRK-avsløring***.

I alle fall: CipherBlade bidro med en oversikt over det de kalte «eksponeringer» for svindlerens wallet-adresse. Det vil si hvilke andre adresser FTX-mottaksadressen (nevnt over) har mottatt midler fra. Et lite utvalg eksponeringer ses under:

Asset	Counterparty Root Address	Counterparty Name	Counterparty Org N	Counterparty Category	Indirectly Received in USD
BTC	113SAPUp85a	Binance.us		exchange	134.79775
BTC	1JYjwkqHJsPY	Coin.z.com - GMO Coin		exchange	5011.92524
BTC	3Qf4e6MMSntx	Roobet.com		gambling	27.12648
BTC	1Q57v5pnVxG			unnamed service	1.06385
BTC	1PUocbzxSL7b	BTC.top		mining pool	42.48126
BTC	1ApznPorjTmc	Coinsquare.com		exchange	15.62244
BTC	16FGRrU1a1TF			unnamed service	2.12771
BTC	14PJWCBytM4	LocalBitcoins.com		p2p exchange	1348.87176
BTC	39k8YhfbQhrb	LMAX Digital		exchange	13.41979
BTC	1128Ev6iMRQ2	Binance.com	Binance	exchange	100004.94619
BTC	387yftfhBm9i2	Celsius.network		other	19.99671
BTC	1Ba7moKduHp	EnvyCorporation.com		scam	9.33550
BTC	bc1q7cyrfmck2	Crypto.com		exchange	6544.77834
BTC	3SwTyBhuKgB	Blockchain.com		exchange	3581.51813
BTC	(coinbase)	Coin Generation		mining	2.97555
BTC	36EmADcNB2	BitBuy.ca		exchange	6.17203
BTC	13iPgr16eia2C	CoinPayments.net		merchant services	8.75203
BTC	1PchPNfqoryz	SendWyre.com		exchange	117.84835
BTC	15VyEAT4uf7y	Bittrex.com		exchange	19.05936
BTC	1HBZRbfjeM11	HitBtc.com		exchange	70.00974
BTC	35E8YJnDVHS9	WirexApp.com		exchange	3205.48578
BTC	16Di4Zcc3EkpP	SouthXchange.com		exchange	5.65769
BTC	3Mzi2xCvsbFq	PARiBU.com		exchange	4.94651
BTC	3DEi5HHAvCvj			unnamed service	13.41979
BTC	1BUVqay2X5pi	NiceHash.com		mining pool	9.91897
BTC	1rAiRiHSePVh	B2C2.com		exchange	1982.06060
BTC	17Urpq94H1TX	MiraiEx.com		exchange	23170.81056
BTC	157EDTdFDEyn	Kraken.com		exchange	12.25285

Eksponeringene var interessante, og viste hvordan lommeboka mannen hadde betalt inn til hadde interagert med flere andre lommebøker.

Mannen hadde betalt midler til én «lommebok» (disponert av svindlerne) – og derfra har midlene gått videre til en lommebok nummer 2. Lommebok nr. 2 hadde mottatt betydelige beløp fra en rekke andre lommebøker (hele 11 stykker). CipherBlade hjalp med å lage en grafikk som viser hvordan ofres lommebøker (til venstre) betalte inn til svindel-lommebøker (i midten) som så raskt ble sendt videre til en lommebok hos FTX (til høyre):

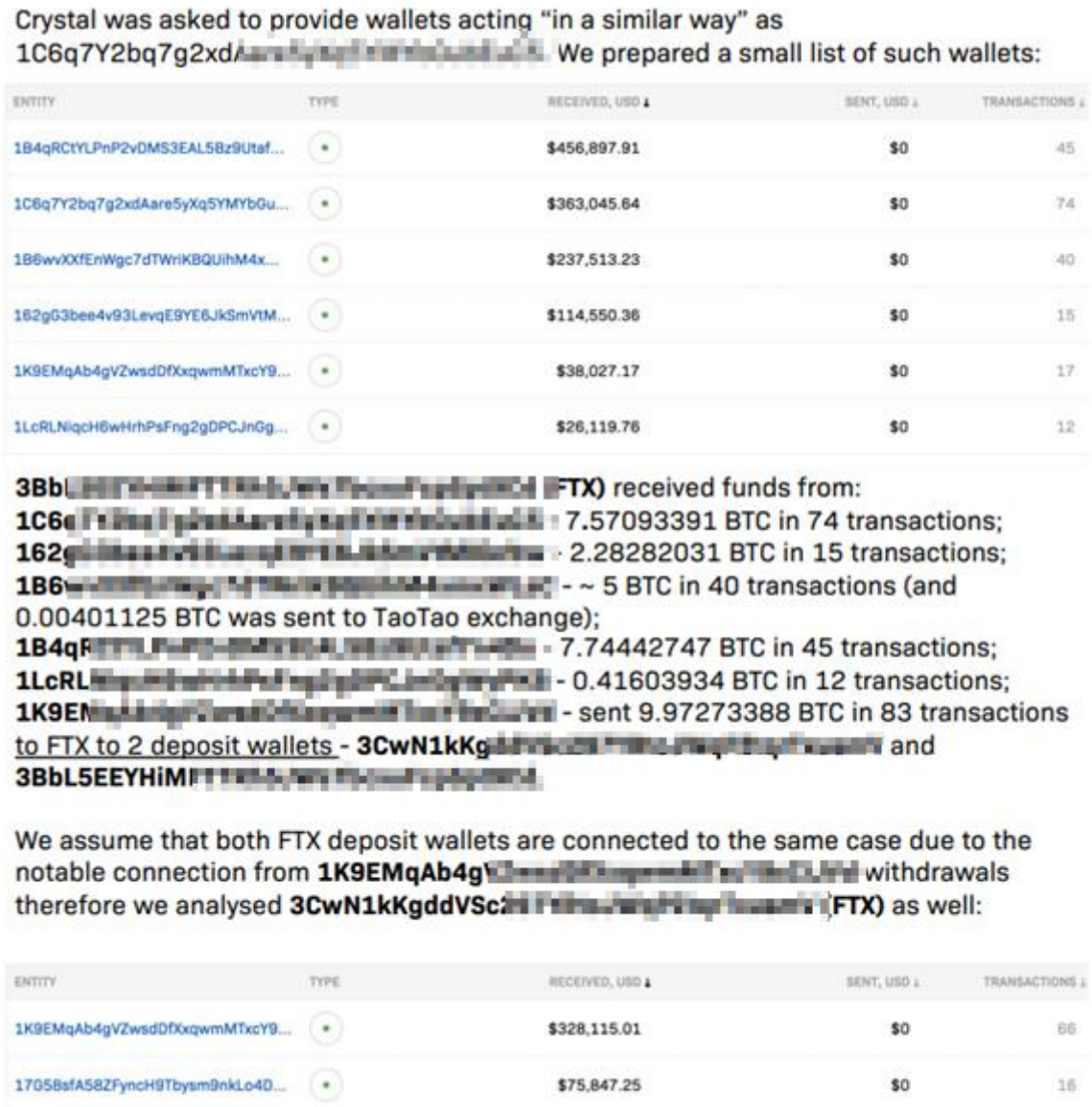


Den store lommeboka hos FTX til høyre – en slags «hovedlommebok», hadde mottatt midler fra i alt 11 unike wallet-adresser (midten) via 212 overføringer. Disse 11 hadde igjen mottatt

sine beløp fra en rekke andre, mindre lommebøker. Totalt kunne vi se at svindlerne hadde samlet inn et beløp tilsvarende 15 millioner kroner via to «hovedlommebøker».

Ekspertene vi snakket med mente videre at svindlerne trolig disponerer mange slike «hovedlommebøker» og at et konservativt anslag er at de har fått inn et tosifret millionbeløp (i dollar) via sin operasjon.

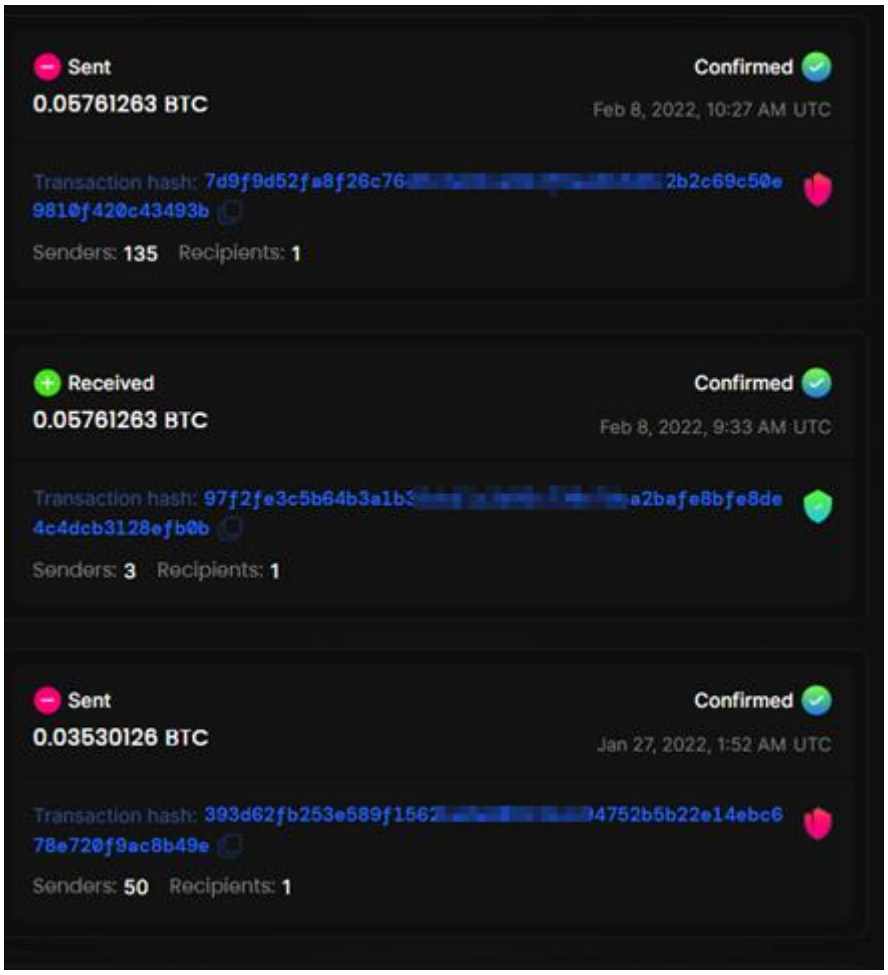
Analyseselskapet Crystal Blockchain utførte følgende analyse for oss, som illustrerer hvordan den lommeboka offeret betalte inn til knyttes til mange andre lommebøker. Skjermdumpen legges ved for å illustrerer hvorledes det er store beløp som er i sving, og som svindlerne klarer å få inn via sin operasjon:



Som nevnt er det et poeng at svindlerne har benyttet seg av FTX som innskuddsadresse for svindeloperasjonen. Det var derfor viktig for oss å ettergå opplysningene om at det faktisk

var en børs ved navn FTX som var mottaker av midlene til offeret. Vi så derfor etter det om kalles «sweeping transactions». Begrepet viser hvordan en børs rutinemessig vil flytte midler fra innskuddsadresser til sine «in house»-wallets, For å finne ut av dette studerte vi oppførselen til mottaksadressen i en block-explorer (*som gjør det mulig å se hvor krypto-aktiva har tatt veien*). Og det vi da så var at, jo; adressen sendte rutinemessig midlene videre kort tid etterpå, noe som ga støtte til påstanden om at det var en børs vi hadde med å gjøre.

Illustrert under:



Når det gjaldt å identifisere *hvilken* børs adressen befant seg på, var det et litt lengre lerret å bleke. Men det vi fant ut var at det finnes blokkjedeanalyseverktøy som merker adresser, og som dermed klarer å identifisere hvilke børser gitte adresser befinner seg på. Et slikt verktøy som er anerkjent, er det som utvikles av CrystalBlockchain.

Vi tok kontakt med etterforskningsleder Nicholas Smart i CrystalBlockchain, som ga oss en fire ukers prøveversjon av verktøyet. Her fikk vi ettergått påstanden om at ja; adressen viser til en konto på kryptobørsen FTX. Det var også via dette verktøyet vi fikk studert pengestrømmene inn i lommeboka mer inngående, og så hvordan store summer samles inn. Her ble det også tydelig for oss hvilket lukrativ business dette er for svindlerne: Mange av beløpene er relativt små (ned i noen få tusen kroner), og av den grunn er det også lite trolig at politiet vil bruke mye tid på en anmeldelse (mange vil helt sikkert ikke bry seg med å anmelde små beløp). Men på grunn av volumet av *alle småbeløp*, blir det også betydelige

summer til slutt. Dermed sitter svindlere i en situasjon der de kan håve inn store summer fra ofre over hele verden, uten i praksis løpe noen risiko for å bli tatt.

Som Rich Sanders i CipherBlade uttalte til oss:

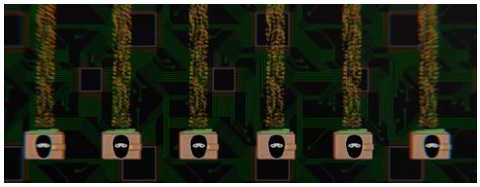
«*Vi ser ofte at det benyttes «kjedehopping» som består i å ha flere kontoer. Aktivaene overføres mellom kontoer og mellom ulike kryptovaluta der poenget er å forvirre etterforskere. En svindel som involverer kontoer på tre børser vil innebære at tre børser må stevnes for å få ut informasjon. Politiet er allerede overveldet, og mange av beløpene er for lave til at firmaet vårt kan ta det»*. Dermed løper svindlerne så godt som ingen risiko for å bli tatt.

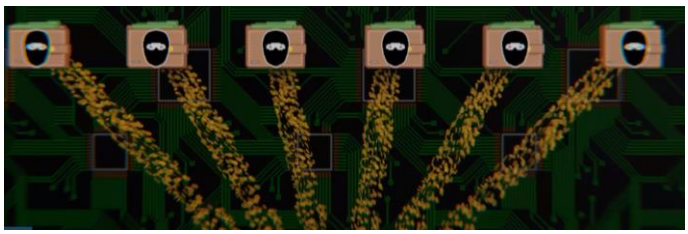
Til sist må det nevnes at det ikke er mulig å spore midlene etter at de er mottatt hos en krypto-innskuddsadresse hos en børs, som eksempelvis FTX. Det blir som å gjennomgå en banks transaksjoner (= en absurd mengde) etter å ha gjort et kriminelt innskudd i en mini-bank. Mao: Det er FTX som må utlevere opplysninger, og politiet som må kontakte dem (noe som igjen vil kreve ressurser og kompetanse hos det enkelte politidistrikt).

Hvordan vi tenkte presentasjon

Som denne rapporten bærer preg av, er det mye teknisk å forholde seg til. Hvordan klarer man å forklare dette enkelt for den jevne leser? Et hovedpoeng her er flyten av penger fra offerets lommebok, via en «mellomstasjon» til en «hovedlommebok». Vi identifiserte to «hovedlommebøker» hos FTX som svindlerne etter alle solemerker benytter for å samle inn beløpene fra sine ofre, men det er trolig flere som sagt. I alle fall bestod en viktig del i det journalistiske formidlingsarbeidet å gjøre pengestrømmene forståelige for folk. Til dette benyttet vi metaforer folk kunne kjenne igjen, hhv. lommebøker, mynter og pengehvelv.

Resultatet ses i reportasjen, der folk «scroller» mellom de ulike stegene i svindelen.



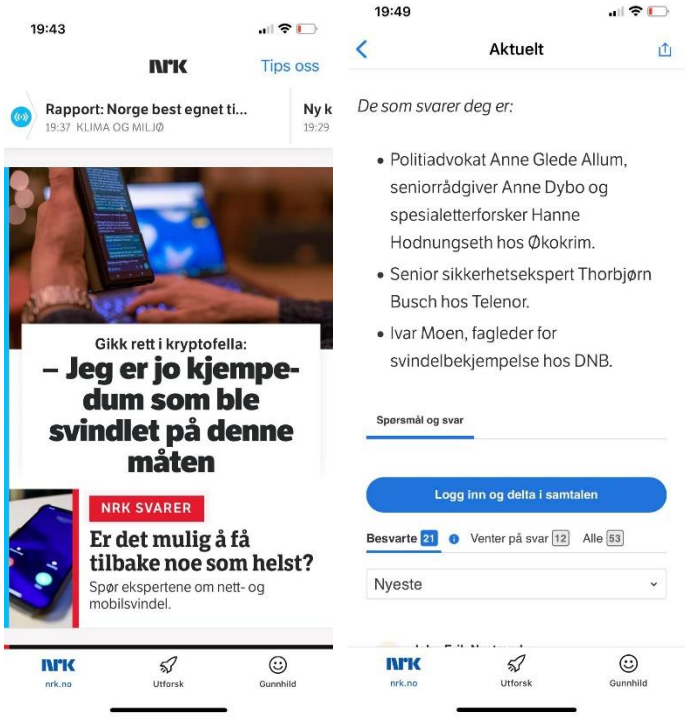


Utover dette jobbet vi mye med lesbarhet og visuelle grep vha. chatbobler, bilder og lignende.

Dette fremkommer av det ferdige produktet, og ikke noe vi vil gå inngående på her.

Oppfølgingssaker

Saken gikk ut som et oppslag på NRK.no sammen med en «NRK Svarer»-rigg, det vil en egen artikkel hvor publikum kunne komme med sine spørsmål rundt svindel. Et ekspertpanel svarte fortløpende, noe som ga en helt egen dimensjon til saken.



Folk var overraskende åpne om egne historier, og vi tok tak i flere av spørsmålene journalistisk i etterkant. Det ble produsert en rekke oppfølgingssaker i etterkant.

- **Hovedsak**: Kryptosvindelen.
- Politileder om kryptosak: – Ligner på «Tinder-svindleren»
- Kryptoekspert sjokkert over hvor slurvete svindlerne har vært: – Merkelig
- Gjenåpner grov bitcoin-svindelsak etter NRK-avsløring
- Svindeloffer kan få frådrag på skatten
- Tapte over 7 millioner i svindel, politiet henla på dagen: – Drøyt og jævlig
- Hør svindlerne i aksjon: Ble svindlet for 600 000 kroner
- Minstepensjonist Torhild fikk tilbake pengene sine etter svindelforsøk
- Bekymret for «deepfake»: Lurer deg til å tro at det er et familiemedlem som ringer
- Her aksjonerer politiet mot svindlerne: Beslagla luksusbiler og millionbeløp
- Quiz: Kunne du latt deg lure av svindlere?

Bodø, 2. september 2022