

Virtuella valutor i penningtvättsrapporter

I syfte att undersöka i vilken omfattning och enligt vilka mönster kryptovalutor förekommer inom penningtvätt och finansiering av terrorism har finanspolisen granskat penningtvättsrapporter inkomna under 2014 – 2016. Denna rapport är en sammanfattning de delar av granskningen som inte är föremål för sekretess.

Granskningen tog sikte på samtliga slag av kryptovalutor men alla förekomster rörde bitcoin. Inga rapporter avseende andra kryptovalutor har alltså inkommit. Däremot har det även inkommit rapporter rörande onecoin. All tillgängliga data talar för att onecoin inte är en kryptovaluta utan ett pyramidspel. Onecoin marknadsförs dock som en kryptovaluta och ingick därför i granskning.

Merparten av verksamhetsutövarna kommer aldrig i direkt kontakt med bitcoins - vilket egentligen endast de som bedriver handel med kryptovalutor gör - utan har främst möjlighet att rapportera transaktioner som avser betalning för kryptovalutor. Det innebär att det endast är transaktioner i den rapporteringspliktiga delen av det finansiella systemet och de personer som utför dessa som varit föremål för granskningen.

Rapporterna har också granskats utifrån hur ett antal faktorer – t.ex. rapporteringsgrund, åtgärd vidtagen av finanspolisen, förekomst i polisiära register – samverkar genom att korsreferera dessa samt genom en nätverksanalys av de inblandade aktörerna. Syftet var att identifiera i vilka sammanhang kryptovalutor förekommer, vilka omständigheter och grunder som föranleder rapportering, vilka åtgärder finanspolisens vidtar, och i hur stor utsträckning de rapporterade personerna visar sig vara av intresse i andra polisiära sammanhang.

I granskningen har ett antal modus och trender identifierats, vilka finanspolisen vill uppmärksamma rapporteringspliktiga verksamhetsutövare på.

Identifierade modus

Växlingsverksamhet

De granskade penningtvättsrapporterna och den påföljande nätverksanalysen gav starka indikationer på att ett antal personer handlade i bitcoins i sådan omfattning att det måste betraktas som näringsverksamhet. Tydliga indikatorer på växling var en stor omsättning på konton med transaktioner - vanligtvis genom Swish – åt båda håll. Ofta fanns det hänvisningar till bitcoins i transaktionsmeddelanden. Verksamheten bedrivs vanligtvis på personkonton.

En sådan verksamhet är anmälningspliktig till finansinspektionen och medför därmed krav avseende beskattning och bokföring, krav som sällan uppfylls.

När växlaren köper bitcoins som erhållits som brottsutbyte – t.ex. som vinst från narkotikaförsäljning – är det ett led i säljarens penningtvätt, och växlaren kan därför göra sig skyldig till medhjälp till penningtvätt, alternativt näringspenningtvätt.

Vidare kan det antas att flertalet av de personer som vänder sig till dessa växlare för att köpa bitcoins har ett intresse av att undandra sig den kundkännedom som etablerade och rapporteringspliktiga bitcoinförmedlare utövar.

Illegal handel

Även illegal handel präglades av stor omsättning och många mindre transaktioner, ofta via Swish. Till skillnad från aktiviteten på växlarnas konton rörde det sig av naturliga skäl främst om insättningar. Transaktionsmeddelanden innehöll sällan referens till bitcoins utan oftast ett namn eller någon form av referensnummer för att identifiera avsändare.

De enskilda insättningarna kom ofta från många olika personer och blir därför sällan särskilt avvikande sett från avsändarkontot. De genererade dock en avsevärd aktivitet på mottagarkontot, vilket oftast var det verksamhetsutövarna reagerat på.

I sammanhanget var transaktioner som gick från mottagarkontot också av vikt. När större överföringar gick till bitcoinförmedlare eller växlare fanns det anledning att misstänka att personen sålde illegala preparat i vanlig valuta men använde bitcoins för att göra egna inköp, förmodligen då via darknet. Om pengarna istället togs ut kontant eller fördes vidare till andra personer fanns det anledning att misstänka att personen agerade målvakt. Detta gäller särskilt om aktiviteten på kontot börjat relativt plötsligt och pågår under en begränsad tid för att sedan upphöra.

Av särskilt intresse i sammanhanget är större transaktioner från kända bitcoinväxlare (enligt ovan modus) eller företag som handlar med bitcoins, särskilt då utländska som inte är rapporteringspliktiga i Sverige. När en person mottar denna typ av transaktion finns anledning att anta att de har inkomst i bitcoins, och saknas näringsverksamhet som förklarar sådan inkomst bör verksamhetsutövaren reagera. Detta är generellt mer svårtupptäckt eftersom det sällan sker på ett konto där det förekommer annan aktivitet som ger anledning till misstanke.

Bedrägeri

Det vanligast bedrägerimoduset kopplat till bitcoin har varit varianter av s.k. Blocket- eller Traderabedrägerier. Bedragaren har satt ut en annons på en vara som brottsoffret betalat för, ofta via Swish. Bedragaren har dock inte angett sitt eget telefonnummer eller kontonummer för betalning utan angett numret till en växlare, hos vilken bedragaren lagt en beställning på bitcoins för samma summa. När växlaren mottagit betalning från brottsoffret har denne överfört bitcoins till den virtuella plånbok bedragaren uppgett i beställningen.

Först när brottsoffret inte får varan och inte kan nå bedragaren via den e-post eller det telefonnummer de haft kontakt via uppstår misstanke. När brottsoffret då använder numret som betalningen gått till uppdagas det att växlaren har fått betalt för bitcoins och saknar vetskap om den vara som brottsoffret trott sig köpa. Då transaktioner med bitcoins är irreversibla och det inte finns en förteckning över vem som innehar en specifik plånbok blir det mycket svårt att spåra eller återta brottsutbytet.

Ett flertal växlare har varit utsatta för bedrägerier av detta slag. De förefaller ha vidtagit åtgärder för att skydda sig, bl.a. genom att bekräfta köp via sms innan överföring görs för att säkerställa att köparen faktiskt vill köpa bitcoins. I annat fall har de återbetalt pengarna istället för att överföra bitcoins till den plånbok som beställningen angett.

Även bedrägerier som vänder sig mot etablerade bitcoinmäklare har identifierats. Dessa har varit av sådant slag att man försökt att registrera konto och utföra köp, bl.a. med stulna kortuppgifter eller med liknande tillvägagångssätt som ovan. Samtliga sådana fall i granskningen har dock stoppats i kundkännedomsprocessen.

Pyramidspel

De personer som handlat med onecoin har uteslutande varit köpare, och det får antas att personerna ser inköpet som en investering. Någon egentlig handel har inte kunnat påvisas, och det förefaller heller inte användas som betalmedel.

Till skillnad från övriga kryptovalutor så har onecoin t.ex. inte en publik blockkedja som kan granskas och där användare verifierar transaktioner. Antalet onecoins, som från början påstods vara oföränderligt, har tiodubblats i antal sedan efterfrågan visat sig vara stor. Lotteriinspektionen har polisanmält företaget bakom onecoin för brott mot kedjespelslagen. Även finansinspektionen har varnat för riskerna med onecoin. De verksamhetsutövare som kommer i kontakt med kunder som har eller avser att investera i onecoin bör upplysa dessa om riskerna.

Rapportens generella slutsatser

Nätverksanalysen visade att de personer som bedrev växlingsverksamhet utgjorde naven i ett tydligt kluster av sammanlänkade rapporterade personer. Personerna var många gånger rapporterade vid ett flertal tillfällen och var starkt överrepresenterade vad gäller förekomst i polisiära register. De personer som handlade med onecoin hade däremot inga synliga kopplingar till andra personer. Detsamma gäller de personer som använde sig av etablerade och rapporteringspliktiga bitcoinförmedlare. De allra flesta var endast rapporterade vid ett tillfälle och var heller inte överrepresenterade vad gäller förekomst i polisiära register.

Det var mer än sex gånger vanligare att de rapporter som rörde bitcoin gav upphov till en brottsanmälan, jämfört med samtliga rapporter som inkommer till finanspolisen. Det var också nästan tre gånger vanligare att rapporten utgjorde grund för underrättelser till övriga polisen eller andra rättsvårdande myndigheter. Detta visar att rapporteringen avseende virtuella valutor håller god kvalitet och korrekt identifierar misstänkta transaktioner.

Merparten av överrepresentationen var koncentrerad till personer i det kluster som fanns runt bitcoinväxlarna. Undantaget var bedrägerier, vilket var lika vanligt förekommande hos samtliga som handlat med bitcoins, oavsett om de tillhörde klustret runt växlarna eller inte. De som handlat med onecoin var dock underrepresenterade, och avseende penningtvätt och finansiering av terrorism är onecoin för närvarande inte av stort intresse.

Finanspolisen vill understryka att personer som bedriver växlingsverksamhet i virtuella valutor i privat regi bör betraktas som högriskskunder. Om mönstret identifieras bör det föranleda ytterligare kundkännedomåtgärder. Kan kunden inte på ett tillfredställande sätt förklara transaktionerna bör verksamhetsutövaren vidta åtgärder, t.ex. att upphöra att tillhandahålla de tjänster som möjliggör den misstänkta verksamheten.