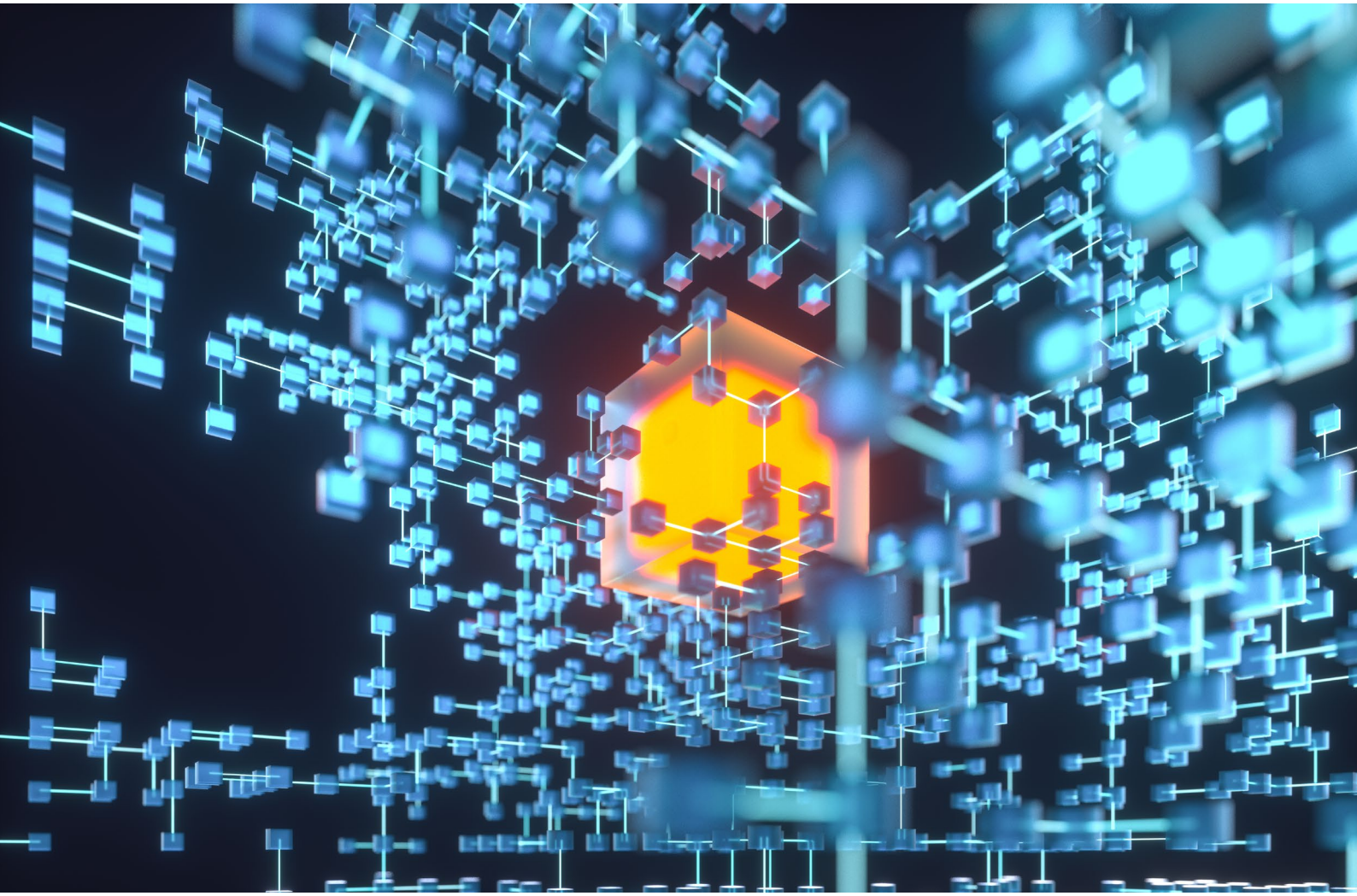
# Penningtvätt och finansiering av terrorism med kryptovalutor

Polisen

PMY Rapport

Polismyndigheten, Nationella operativa avdelningen, november 2022



Utgivare: Polismyndigheten, Nationella operativa avdelningen, Box 12256, 106 75 Stockholm
Dnr: A433.555/2022, Saknr: 423
Omslagsfoto: MostPhotos
Upplaga: Internet
Datum:2022-11-30

# Innehåll

# Sammanfattning

Marknaden med kryptovalutor utvecklas ständigt där alltfler använder nya och förfinade metoder att hantera sina tillgångar och transaktioner. Den globala räckvidden, snabbheten i internationella transaktioner och möjligheter att agera dolt gör att marknaden är särskilt attraktiv för den kriminella ekonomin. Kryptovalutor möjliggör metoder för att dölja, hantera och tvätta brottsvinster.

Antalet inkomna misstankerapporter till Finanspolisen som rör kryptovalutor har fortsatt öka de senaste åren i såväl antal rapporter som andelen av det totala antalet rapporter. Verksamhetsutövare inom kryptovalutor står för ungefär en fjärdedel av misstankerapporterna rörandes kryptovalutor under åren 2020-2021.

Vanliga anledningar till misstanke är att kunden har en avvikande omsättning eller att kunden antas agera åt någon annan. I misstankerapporter från banker är den enskilt mest förekommande misstanken att pengarna härrör från bedrägerier. Det är också vanligt med misstankar om kryptovaluta som medel för betalningar av illegala varor och tjänster.

Det finns ett tydligt samband mellan allvarlig och organiserad brottslighet och personer som rapporteras för transaktioner i kryptovaluta. Nära en tredjedel av personerna förekommer i andra underrättelser om allvarlig och organiserad brottslighet. Det handlar framförallt om narkotika, vapen och våld, penningtvätt, systematiska vinningsbrott, samt bedrägerier. I Sverige finns ett betydande antal personer som bedriver illegal växling av kryptovaluta och utgör möjliggörare för kriminella aktörer och nätverk. Det är troligt att penningtvätt och finansiering av brott t.ex. terrorism med hjälp av kryptovaluta kommer fortsätta att öka och följa den allmänna trenden inom området.

# Inledning

Användandet av kryptovalutor och kryptotillgångar ökar och marknaden är i ständig förändring. Intresset för kryptovalutor bland kriminella aktörer är stort, vilket medför att såväl myndigheter som verksamhetsutövare behöver ha en god kunskapsnivå och samverkan behövs för att kunna motverka penningtvätt och finansiering av terrorism som sker med kryptovalutor. Vidare är handeln med kryptovalutor internationell, vilket gör att ett gränsöverskridande samarbete blir en grundförutsättning.

Kryptoväxlare kan genom sitt medvetna, eller omedvetna, agerande främja möjligheten för någon annan att tillgodogöra sig brottsvinster. Individer ägnar sig åt växling i en omfattning som är näringsverksamhet och omfattas således av penningtvättsregelverket. Då flertalet av dessa växlare är oregistrerade trots att de bedriver registreringspliktig verksamhet kan de undgå penningtvättstillsyn. Denna typ av kryptoväxlare som agerar illegalt fungerar som möjliggörare av penningtvätt för kriminella aktörer och nätverk.

Denna rapport inleds med en beskrivning av utvalda aktuella trender. Nästa kapitel redogör för vilka bolag som är verksamma inom kryptohandel och hur lagstiftningen kring kryptovalutor för närvarande ser ut. Efterföljande tre kapitel ger en översikt kring omfattningen av brottslighet kopplat till kryptovalutor, en redogörelse kring tillvägagångssätt för penningtvätt och finansiering av terrorism med kryptovalutor samt presenterar statistik, analys och observationer från misstankerapporter som Finanspolisen mottagit. Avslutningsvis presenteras rapportens slutsatser.

## Syfte och metod

Denna rapport riktar sig till myndigheter och verksamhetsutövare som omfattas av penningtvättsregelverket.

Det primära syftet med rapporten är att ge en kunskapshöjande och uppdaterad lägesbild över penningtvätt och finansiering av terrorism via kryptovalutor genom att:

- Analysera och beskriva hur inrapporteringen till Finanspolisen ser ut.
- Genomföra en fördjupad analys kring illegala kryptoväxlare.
- Beskriva aktuella trender, brottslighet, penningtvätt och finansiering av terrorism kopplat till kryptovalutor
- Identifiera sårbarheter som utnyttjas av kriminella, så att verksamhetsutövare och myndigheter kan vidta åtgärder.

Analysen bygger i huvudsak på data ur penningtvättsregistret från perioden april 2020 till augusti 2021 i form av misstankerapporter som inkommit till Finanspolisen från svenska verksamhetsutövare. Totalt inkluderas ca 2 100 misstankerapporter och 6 100 personer.

Delar av observationerna bygger även på en genomläsning och kategorisering av ett urval av misstankerapporter i penningtvättsregistret med syftet att analysera möjliga illegala växlare och infrastrukturer.

Vidare har ett mindre underlag analyserats avseende utländska kryptobolags misstankerapporter. Analysen har även kompletterats med andra underrättelser, externa rapporter och undersökningar samt dialog med andra myndigheter.

# 1 Trender och betallösningar med kryptovalutor och kryptotillgångar

I kapitlet ges en kort beskrivning av begreppen DeFi och NFT då dessa är två aktuella trender i kryptovärlden som kan utnyttjas av kriminella. Avslutningsvis presenteras några av de möjligheter som finns för att utföra betalningar och transaktioner med kryptovalutor.

## 1.1 DeFi - Decentraliserad finansiering

DeFi är förkortning av Decentralized Finance och är en allmän term som beskriver finansiella applikationer som bygger på blockkedjor. DeFi-plattformar eller DeFi-appar (DApps) erbjuder finansiella tjänster med kryptovalutor så som sparkonto, lån/utlåning, valutaväxling, decentraliserade börser (DEX), försäkringar, och mycket mer. Förenklat består lösningarna av en samling smarta kontrakt[1], dvs kod som utför och beskriver vilka transaktioner som ska utföras. Tjänsterna i sig är inte reglerade och det finns således inget krav på att utföra kundkännedom eller att följa penningtvättslagen.

För brottsutredande myndigheter finns det utmaningar i att utreda de finansiella flödena kring dessa applikationer samt svårigheter med återtaganden av tillgångar. Exempelvis så finns det vanligtvis ingen verksamhetsutövare att ställa frågor till. Kunskap kring hur man tolkar smarta kontrakt och bra spårningsverktyg för att följa vad som skrivs på blockkedjan är några av förutsättningarna för att kunna motverka penningtvätt och terrorfinansiering genom DeFi-tjänster.

Bland kriminella är DeFi-tjänster intressanta av flera anledningar. Exempelvis för att utnyttja sårbarheter i tekniken och möjlighet att på en oreglerad marknad och avsaknad av mellanhänder undvika kundkännedom och kontroller mot penningtvätt och finansiering av terrorism. Det finns möjlighet att automatisera och utföra multipla och oåterkalleliga transaktioner. Tjänsterna medför flera möjligheter att skikta pengar från brott.

I en rapport från Chainalysis i oktober 2021 rankades 154 länders användande av DeFi tjänster. Sverige hamnade på plats 58, vilket kan jämföras med Norge på plats 29, Finland på plats 40 och Danmark på plats 67. [2] DeFi är också den kategori där penningtvätt via kryptovalutor ökade överlägset mest procentuellt med nästan 2 000 % mellan år 2020 och 2021. [3] I början

[1]”smarta kontrakt” är inte kontrakt i juridisk mening. Villkoren är skrivna i kod och fungerar som automatiska instruktioner som utför en uppgift när vissa givna villkor är uppfyllda.

[2]https://go.chainalysis.com/2021-geography-of-crypto.html

[3]https://blog.chainalysis.com/reports/2022-crypto-crime-report-introduction/

av augusti 2022 stod DeFi för 9% omsättningen av kryptohandeln enligt coinmarketcap.com. Marknadsvärdet beräknas samma dag till 51 miljarder dollar vilket var kring 5% av totala kryptomarknaden[4]. Hur stor andel av detta som är spekulation i DeFi tokens respektive användandet av mer finansiella tjänster är inte utrett.

## 1.2 NFT - Non-fungible token

NFT, Non-fungible token, kan associeras med en viss digital eller fysisk tillgång eller en licens som får ett unikt digitalt fingeravtryck. En NFT är en enhet av data som lagras på blockkedjan och som kan säljas och överlåtas. NFT fungerar således som ett ägandebevis till ett unikt objekt. NFT kan exempelvis användas för digital konst, bilder, samlarobjekt, musik eller videos men även för att representera materiella tillgångar så som äganderätter till fastigheter. För att skapa, sälja eller köpa NFT:er behövs en kryptoplånbok, då ägandet av NFT är kopplat till den publika nyckeln. Det finns sedan många marknadsplatser där man kan köpa, sälja och byta NFTs.

Marknaden för NFT har vuxit de senaste åren för att under år 2021 haft en explosiv tillväxt. Detta har också medfört att marknaden dragit till sig kriminalitet så som bedrägerier i form av falska marknadsplatser, projekt och erbjudanden. NFTs skapar möjligheter för de som är involverade i brottslighet att gömma tillgångar och tvätta pengar. Marknaden är ännu inte reglerad, således finns inget krav på marknadsplatserna att utföra kundkännedom eller följa penningtvättslagen i övrigt. För brottsutredande myndigheter är det svårt att kontrollera handeln samt identifiera personer bakom plånböcker kopplade till NFTs.

Följande är ett exempel på penningtvättsmodus där NFT används.
En person med ett behov att tvätta pengar skapar eller köper ett NFT-konstverk. Konstverket läggs sedan ut till försäljning på en marknadsplats och personen köper sedan NFT-konstverket dyrt från sig själv med pengar som härrör från brott. Personen använder vid köpet anonyma plånböcker. Pengarna integreras sedan som legitima medel från försäljningen av NFT-konstverket. Exempelvis kan pengarna föras över till en traditionell bank via växling och överföring hos en kryptoplattform. Personen kan då ha tillgång till dokumentation på just den försäljningen. Eftersom det saknas krav på kundkännedom behöver den påstådda köparen av NFT:en inte identifieras. Detta

[4]https://www.tradingview.com/markets/cryptocurrencies/global-charts/

handelsbaserade penningtvättsmodus är likt det man länge haft inom den traditionella konsthandeln.

Terroristorganisationer kan generera anonyma NFTs och sälja till sina givare. På så sätt kan de tjäna pengar på försäljningen av exempelvis en kollektion av konstverk och använda förtjänsten till terrorism-relaterade aktiviteter. Donationer kopplade till NFTs för välgörande ändamål är något som blivit vanligt på NFT-marknadsplatserna. En andel av betalningen för kommande försäljningar kan programmeras att gå till en organisation (dvs en plånbok). Möjligtvis skulle den typen av upplägg också kunna utnyttjas av terroristorganisationer. Även en upphovsman av verk skulle på liknande sätt kunna välja att en del av försäljningen går till en plånbok som kontrolleras av en terroristorganisation i syfte att stödja den. Terroristorganisationer kan även tjänar pengar med NFT genom att ägna sig åt den typ av brottslighet som tidigare nämns, dvs bedrägerier i olika former.

Hittills har det endast inkommit ett fåtal rapporter till Finanspolisen där NFT nämns. Rapporterna rör personer som i kundkännedomsprocessen uppgett att de handlar med NFTs. Sällan finns det med någon ytterligare information kring påstådd handel. I några fall har exempelvis inrapporterande bank efterfrågat information från kunden men inte fått svar. I en del av dessa rapporter kan Finanspolisen se ett mönster som inte alls tyder på någon NFT-handel, medans det i något fall ser ut att kunna stämma. Utifrån tillgänglig information är det svårt att dra slutsatser i vilken utsträckning svenska personer hanterar och förvarar brottsvinster i NFT:er eller nyttjar NFT:er i bedrägerier.

## 1.3 Transaktioner och betallösningar

Kryptovalutor används av många främst som en spekulativ tillgång och inte som betalmedel. Att butiker vanligtvis inte erbjuder kryptovalutor som betalningsmedel kan bero på att det kan vara komplicerat att dokumentera försäljningen, att hantera den efterföljande värdeförändringen, att valutan är volatil eller som ett ställningstagande mot miljöpåverkan vid mining. Den främsta anledningen är dock möjligen att många kryptotransaktioner är långsamma. Exempelvis kan en bitcointransaktion ta mellan 10 minuter till 1 timme att slutföra. Dessutom kan transaktionsavgiften bli hög i förhållande till köpet. [5] Tiden att slutföra en transaktion är snabb sett till internationella överföringar men långsam i ett köpsammanhang.

[5] https://coinmarketcap.com/alexandria/article/how-long-does-a-bitcoin-transaction-take

Nedan presenteras några av de möjligheter som finns för att utföra betalningar med kryptovalutor samt vad som är aktuellt och vad som kan ändra förutsättningarna.

**Betalningar med betalkort**
En del neobanker (digitala banker) tillhandahåller plånböcker för kryptovalutor till sina kunder samt lösningar för överföringar mellan dessa. Kunder har således möjlighet att flytta kryptovalutor till och från externa plånböcker (egna eller andras). Ofta erbjuds numera också både virtuella och fysiska betalkort kopplade till kryptotillgångarna. Köp kan göras för fiatvaluta som finansieras genom automatisk eller manuell växling av kryptotillgångar. Utvecklingen av betalkort kopplade till kryptotillgångar är ett område som kortnätverk (exempelvis VISA och Mastercard) satsar på, bland annat med målet att tillhandahålla snabbare eller direkt inlösen av kryptotillgångar. [6]

**Betalning med kryptovalutor**
Flera betaltjänstleverantörer accepterar nätbetalningar med kryptovaluta på utvalda marknader, exempelvis Paypal och Square. Även här sker normalt ett mellansteg där kryptovalutan växlas till fiatvaluta. Ett relativt litet antal nätbutiker samt fysiska butiker erbjuder kryptovalutor som betalningsmedel och ofta sker även denna typ av betalning med hjälp av tredjepartslösning så som tex Bitpay eller Coinbase. [7]

Köp av egendom och varor för större summor erbjuds också. Exempelvis finns det i en del länder mäklare som accepterar kryptovalutor vid betalning för fastigheter.

**Betalningar på darknet**
Köp på darknet genomförs vanligen genom att köparen överför kryptovaluta till en marknadsplats där köparen registrerat sig som användare. På marknadsplatsen finner köparen en butik/säljare som tillhandahåller önskad tjänst/vara. Själva köptransaktionen hanteras och regleras sedan inom marknadsplatsen mellan köpare och säljare, varpå den blir svår att följa då transaktionen inte registreras i blockkedjan utan är en intern transaktion inom marknadsplatsen.

Marknadsplatser med ett fokus på droger är den vanligaste kategorin på darknet, följt av marknadsplatser för bedrägerier som tillhandahåller stulen data (t.ex. betalkortsuppgifter och användarkonton), skadlig programvara och tjänster för penningtvätt.

---

[6] En rapport om neobanker och deras risker relaterade till penningtvätt och finansiering av terrorism. Polismyndigheten 2022
[7] https://help.coinbase.com/en/commerce/getting-started/for-merchants

Under hösten 2021 upphörde den svenskbaserade marknadsplatsen Flugsvamp 3.0, som varit en betydande del av den svenska drogmarknaden på internet. Svenska säljare migrerade till internationella marknadsplatser, egna hemsidor eller tillhandahöll andra kontaktmöjligheter. En ny svenskbaserad marknadsplats med namnet Flugsvamp 4.0 lanserades kort efter.

På det öppna internet finns en mängd enkla steg-för-steg-instruktioner tillgängliga om hur personer bör agera för att handla kryptovaluta inför köp på darknet samt om hur kryptovaluta kan tvättas. Det finns även rekommendationer om olika handelsplatser för kryptovaluta, vilka växlare som bör undvikas samt tips som om att inte skicka pengar direkt till darknet från handelsplatser utan att istället skikta pengarna genom en privat plånbok. Förslag ges även på hur man kan växla pengar anonymt mellan olika kryptovalutor.

**Köp av digitala presentkort**
Ett antal verksamhetsutövare erbjuder försäljning av vanliga presentkort som betalas med kryptovaluta. Genom att i många fall endast uppge en e-postadress betalar köparen med olika typer av kryptovalutor och presentkortet levereras digitalt. Utbudet är ofta omfattande med presentkort för exempelvis flyg, hotell, kläder och mat och kopplat till välkända butiker så som Amazon, Apple, H&M, CDON och Hotels.com.

De digitala presentkorten har ett värde i fiatvaluta och då de oftast endast gäller inom ett begränsat nätverk, vanligtvis ett specifikt företag eller handelsplats, omfattas utgivningen av presentkorten inte av penningtvättsregelverket. Försäljningen av presentkorten betraktas också som varuhandel, och sådan är endast reglerad avseende penningtvätt när det sker mot kontanter över ett visst tröskelvärde. Det innebär att när presentkort betalas med kryptovaluta finns det ingen part som omfattas av penningtvättsregelverket.

Den omvända tjänsten, det vill säga att byta, växla eller att användaren säljer presentkort och erhåller kryptovaluta erbjuds också av ett antal aktörer.

**Transaktioner mellan personer och plånböcker**
Betalningar och överföringar mellan privatpersoner eller mellan privatpersoner och organisationer kan utföras genom en transaktion mellan två plånböcker.

**Layer 2**
Blockkedjor som Bitcoin och Ethereum beskrivs som layer 1-kedjor eftersom de löser varje transaktion på sitt nätverk. Layer 2 är ett lager som byggs ovanpå blockkedjan. Layer 2-lösningar används för att förbättra

skalbarheten[8] och effektiviteten på layer 1 genom att ta hand om en del av aktiviteten utanför huvudkedjan. Layer 2 kan således användas som ett betalningsprotokoll byggt ovanpå blockkedjan för att möjliggöra billigare och omedelbara kryptotransaktioner**.**

För Bitcoin är Lightning Network den mest kända layer 2-lösningen. Lighting Network användes exempelvis av betaltjänstleverantörer i El Salvador när landet införde bitcoin som en officiell valuta i juni 2021. För Ethereum finns ett stort antal layer 2-lösningar och varianter på hur data skrivs och valideras mot huvudblockkedjan. [9]

Då transaktioner utförs utanför huvudblockkedjan och ibland involverar flera parter finns utmaningar i hur finansiella flöden spåras och hur tjänsterna regleras samt vilken möjlighet till KYT (Know Your Transaction) och KYC (kundkännedom) leverantörerna har möjlighet till.

[8]Skalbarhet i betydelsen ett systems kapacitet att fortsätta prestera samtidigt som arbetsbelastningen ökar.

[9]https://ethereum.org/en/developers/docs/scaling/layer-2-rollups/

# 2 Bolag och lagstiftning

I följande kapitel redogörs kort om vilka verksamhetsutövare som finns registrerade och hur lagstiftningen kring kryptovalutor ser ut.

## 2.1 Registrerade bolag i Sverige

I Sverige finns det idag endast tio bolag registrerade[10] som finansiella institut där kryptovalutor är en del i verksamheten. En aktuell lista på dessa bolag kan tas fram genom att söka i Finansinspektionens företagsregister. De två största registrerade bolagen sett till omsättning är Safello och Goobit.

## 2.2 Bolag utanför Sverige

Många bolag och tjänster som är tillgängliga för den svenska marknaden är utländska finansiella institut som är registrerade i en annan jurisdiktion. Långt ifrån samtliga bolag är dock registrerade och reglerade. Detta medför att inrapporteringen från bolagen samt kvalitén på tillsynen av bolagen är beroende av regelverket i det land där bolaget har sin registrering samt den tillhörande utländska tillsynsmyndighetens kapacitet.

## 2.3 Lagstiftning

I Sverige har vi två lagar som reglerar penningtvätt.

**Penningtvättsbrottslagen**, lag (2014:307) om straff för penningtvättsbrott, som kriminaliserar olika typer av penningtvätt. Den som begår sådana brott kan dömas för penningtvättsbrott eller näringspenningtvätt. Brotten kan bedömas som ringa, av normalgrad eller som ett grovt brott.

I den **administrativa penningtvättslagen**, **l**ag (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism, finns ett administrativt regelverk som är avsett att förhindra att det finansiella systemet utnyttjas för penningtvätt och finansiering av terrorism.

Förvaltning av eller handel med virtuell valuta är en verksamhet som ska registreras hos Finansinspektionen enligt lagen (1996:1006) om valutaväxling och annan finansiell verksamhet. [11] Verksamhet som omfattas av registreringsplikten är att betrakta som en verksamhetsutövare enligt lagen

[10] https://www.fi.se/sv/vara-register/foretagsregistret/tillstand-av-fi-eller-enbart-registrering/

[11] https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-19961006-om-valutavaxling-och-annan_sfs-1996-1006

(2017:630) om åtgärder mot penningtvätt och finansiering av terrorism, och verksamheten ska drivas i enlighet med denna lag. [12]

Privatpersoner som agerar kryptoväxlare åt andra kan göra sig skyldiga till penningtvätt eller näringspenningtvätt enligt penningtvättsbrottslagen. [13] En av skillnaderna mellan dessa två brottstyper är att i näringspenningtvätt är det inte avgörande att egendomen härrör från brott eller brottslig verksamhet, utan det räcker att gärningsmannen gör sig skyldig till ett klandervärt risktagande. Övriga brott som en kryptoväxlare kan göra sig skyldig till är exempelvis bokföringsbrott, skattebrott eller som delaktig i förbrottet till penningtvätt. Även registrerade kryptoväxlare kan naturligtvis bedriva illegal verksamhet, vilket något som både andra länder påvisar[14] och som framkommit i svensk domstol, eller genom bristande kontroller göra sig skyldiga till näringspenningtvätt. [15]

På EU-nivå förhandlas för närvarande nya åtgärder och lagförslag mot penningtvätt och finansiering av terrorism.[16] Transaktioner som involverar vissa kryptotillgångar samt vilken information som ska medfölja transaktioner kan komma att inkluderas i regelverket (2015/847). Åtgärderna ska medföra att det blir enklare att spåra samt få fram information om involverade parter i en transaktion samt att kunna ställa högre krav på verksamhetsutövarna vad gäller kundkännedom.

En reglering av handel med kryptotillgångar är under bearbetning. För närvarande saknas det ett bra konsumentskydd kring kryptovalutor. Europeiska kommissionen arbetar därför på en förordning om marknader för kryptovalutor, den så kallade MiCA-förordningen. MiCA står för Regulation of Markets in Crypto Assets och förordningen är tänkt att reglera utgivare och tillhandahållare av tjänster för vissa kryptovalutor (s.k. stablecoins och s.k. initial coin offering). [17]

---

[12] https://www.fi.se/sv/bank/sok-tillstand/valutavaxlare-och-annan-finansiell-verksamhet/

[13] https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2014307-om-straff-for-penningtvattsbrott_sfs-2014-307

[14] https://www.nsr-org.no/uploads/images/2020-10-29-Infoskriv-bruk-av-kryptovaluta-i-kriminell-virksomhet.pdf

[15] Svea Hovrätt 2021, mål nr B 11734-19, B 9244-19

[16] https://ec.europa.eu/info/publications/210720-anti-money-laundering-countering-financing-terrorism_en

[17] https://www.consilium.europa.eu/en/press/press-releases/2022/06/30/digital-finance-agreement-reached-on-european-crypto-assets-regulation-mica/

# 3 Omfattning av illegal användning

I följande kapitel berörs omfattningen av den illegala användningen av kryptovaluta genom att beskriva internationella uppskattningar, hur inrapporteringen till Finanspolisen statistiskt ser ut samt hur det förhåller sig med penningtvättsdomar rörandes kryptovalutor.

## 3.1 Internationella uppskattningar

Det finns olika internationella uppskattningar av hur stor andel av den totala kryptoekonomin som är relaterad till brottslighet, uppskattningarna varierar från mindre än en procent till närmare en fjärdedel.

Enligt analyser från Chainalysis är andelen transaktioner som är relaterade till brottslighet förhållandevis låg jämfört med traditionell ekonomi. I deras rapport utgjorde illegala aktiviteter 2,1 % av transaktionsvolymen för kryptovalutor år 2019. År 2020 sjönk den illegala andelen av all kryptovalutaaktivitet till 0,34 %, eller 10 miljarder USD i transaktionsvolym. En anledning, enligt Chainalysis var att den totala ekonomiska aktiviteten nästan tredubblades mellan år 2019 och 2020. Inför rapporten år 2022 har siffran för illegala aktiviteter under 2021 på 0,34% ökat till 0,62%. Siffrorna som de presenterar kan komma att redigeras när ny information uppkommer, som t.ex. att fler adresser identifieras ha en koppling till brottslighet.

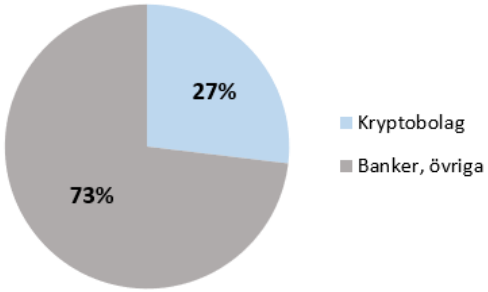
Det råder dock delade meningar om hur relevanta och tillförlitliga ovan siffror är, då kryptovaluta är något som många främst använder i spekulativt syfte och det går inte alltid att avgöra om syftet med en transaktion är att tvätta pengar, undandra sig skatt eller om överföringen sker mellan kriminella. Det finns stora utmaningar i hur man ska tolka syftet med olika transaktioner i krypto vilket påverkar statistiken markant. T.ex. som att kunna identifiera och koppla samman (klustra) adresser till specifika plånböcker eller tjänster (som t.ex. illegala marknadsplatser), samt huruvida enskilda transaktioner i kedjor med ursprung i brottslighet klassas. I en undersökning gjord vid universitetet i Sydney analyserades bitcoin-transaktioner utförda under åren 2009-2017 och det uppskattades att 23 % av transaktionerna hade en illegal koppling. [18]

Vad som är klart är att det totala illegala användandet av kryptovaluta fortsätter att öka samtidigt som andelen av totalen sjunker då användningen av kryptovaluta växer snabbare nu än någonsin tidigare.

[18] https://academic.oup.com/rfs/article/32/5/1798/5427781

## 3.2 Penningtvätt rapporterad i Sverige

Antalet inkomna misstankerapporter, som rör kryptovalutor, från svenska verksamhetsutövare under urvalsperioden är ungefär 5 % av totala antalet rapporter. Detta är en ökning i jämförelse med åren 2014-2016 då andelen var strax under 1 %. Verksamhetsutövare inom kryptovalutor står för ungefär en fjärdedel av rapporterna, resterande del kommer från banker samt ett fåtal övriga verksamhetsutövare.




**Figur 1 - Andel av inrapportering**

## 3.3 Penningtvätt rapporterad från utlandet

Inrapportering från kryptobolag i EU skickas till det FIU som finns i det land där kryptobolaget är registrerat, vidarerapportering av inrapporterade svenska invånare ska därefter ske till Sveriges FIU (Finanspolisen). Vidarerapporteringen från andra FIU:s avseende inkomna rapporter under urvalsperioden från kryptobolag i EU är till synes liten, speciellt med tanke på kryptomarknadens internationella karaktär. En del av dessa rapporter rör dessutom transaktioner till kryptoplattformar, det vill säga att de är inrapporterade av exempelvis en neobank. I slutet av 2021 och under 2022 ses dock en tydlig förändring där inrapporteringen och vidarerapporteringen från vissa verksamhetsutövare och länder ökar markant.

## 3.4 Penningtvättsdomar

I en rapport från Brottsförebyggande rådet presenteras kryptovalutor som del i uppläggen i två procent av alla fällande och friande domar avseende penningtvätt eller näringspenningtvätt mellan åren 2015 och 2017. [19] I rapporten *Genomgång av penningtvättsdomar 2018-2019* från Samordningskansliet vid Polismyndigheten konstateras att kryptovalutor sällan omnämns som en tjänst eller verktyg vid penningtvättsåtgärder eller som del i skiktningsstadiet. [20]

[19] https://bra.se/download/18.7d27ebd916ea64de53077d3/1614334464128/2019_17_Penningtvatts-brott.pdf

[20] https://polisen.se/contentassets/a7aeda235652476b829488438e4aed8f/penningtvattsdomar-2018-2019.pdf

Utifrån genomgånget material finns få fällande domar avseende personer som agerat kryptoväxlare vad gäller penningtvätt och näringspenningtvätt. I vissa fall har växlarna uppmärksammats vid bedrägeribrott men inte åtalats. Vid några tillfällen har personer involverade i växling blivit fällda för bokföringsbrott.

# 4 Brott och tillvägagångsätt

I följande kapitel beskrivs några tillvägagångsätt för penningtvätt och finansiering av terrorism med kryptovalutor, hur brottsvinter hanteras med kryptovalutor samt vad de verksamhetsutövare som sänt misstankerapporter till Finanspolisen reagerat på.

## 4.1 Tillvägagångsätt - Penningtvätt med kryptovalutor

Brottsvinster från alla typer av kriminalitet kan tvättas med hjälp av kryptovalutor. Nya verktyg och metoder för att dölja spåren fortsätter dessutom att skapas och förfinas. Kriminella har samtidigt blivit mer bekväma i användningen av kryptovalutor och specialister på storskalig penningtvätt inkluderar numera penningtvätt via kryptovalutor i sina tjänster som säljs till kriminella, exempelvis genom att växla fiatvaluta till kryptovaluta.

**Växling mellan fiat och kryptovaluta**

Penningtvätten kan ske genom att fiatvaluta i digital form växlas mot kryptovaluta för att sedan skiktas, att kontanter växlas mot kryptovalutor eller att kryptovalutan kommer direkt från förbrottet (exempelvis som en betalning) för att sedan tvättas.

Växling via kryptovalutor lyfts fram som ett möjligt behov för kriminella miljöer som behöver växla valuta även i Finanspolisens rapport om *Penningtvätt via växlingskontor*[21]

Den största andelen kryptovalutor med koppling till brottslighet växlas från krypto till fiatvaluta, enligt Chainalysis, hos de större kryptoplattformarna följt av de som kategoriseras som riskfyllda tjänster. I kategorin inkluderas högriskväxlare, växlare i jurisdiktioner med hög risk, spelplattformar och mixers.

Bitcoin ATM:er, är bankomater som tillåter köp av bitcoin och annan kryptovaluta med betalkort eller genom insättning av kontanter. Användaren får efter insättning då antingen en pappersplånbok eller en överföring till en plånbok. Det finns även ATM:er där en person också kan sälja kryptovaluta och få ut kontanter. För närvarande finns det inga ATM:er i Sverige, men svenska medborgare har tillgång till över 1 000 ATM:er i Europa eller strax under 40 000 globalt. [22]

**Vanligt förekommande modus**

Ett vanligt penningtvättsupplägg är att den initiala skiktningen sker genom att fiatvaluta sänds via flera parter, exempelvis genom överföring mellan

[21] Penningtvätt via växlingskontor, Polismyndigheten 2021-11-17
[22] https://coinatmradar.com/

olika bankkonton, via målvakter eller via neobanker följt av transaktioner till en kryptoplattform. Integreringen kan ofta ske genom att kryptovalutor köps på en plattform, flyttas direkt eller via kryptoplånböcker för att samlas ihop och växlas till fiatvaluta hos ytterligare en plattform.

**Olika grader av penningtvätt**

Penningtvätt i sin ”enklare” form består ofta av överföringar mellan plånböcker och växling hos handelsplattformar, växling mellan privatpersoner direkt eller via handel på en P2P (peer-to-peer) marknadsplattform. Val av plattform för växling kan ske efter tips och guider och om möjligt hos oregistrerade växlare, för att undvika AML- och kundkännedoms processer. Den mer avancerade penningtvätten inkluderar steg som exempelvis växling mellan olika kryptovalutor, mixers, användandet av spelplattformar, köp av varor, NFT och DeFi.

**Verktyg för att dölja spåren**

Nedan presenteras kortfattat och förenklat några av övriga tjänster och verktyg som används i penningtvätt för att dölja spår.

| | |
|---|---|
| Mixer eller tumbler | Tjänster som går ut på att slå ihop och blanda kryptovaluta från flera användare i en plånbok för att sedan betala ut kryptovalutan minus en avgift till en eller flera andra adresser än den ursprungliga. Syftet är att dölja kopplingen mellan ingångs- och utgångsadresserna. |
| CoinJoin | I likhet med mixer är CoinJoin ett sätt att blanda kryptovalutor från flera avsändare i syfte att dölja kopplingen mellan ingångs- och utgångsadresserna, men det sker decentraliserat. CoinJoin kombinerar transaktioner av samma summa från flera deltagare till en plånbok. Genom ett protokoll där deltagarna signerat ett smart kontrakt. Den inbetalda summan, minus avgifterna, distribueras sedan tillbaka till deltagarna till andra adresser. |
| Peel chain | En större mängd kryptovaluta tvättas genom en lång rad transaktioner. Mindre belopp ”skalas” bort och sänds till en ny adress. Processen upprepas sedan flera gånger och är även möjlig att automatisera. Mindre summor kan sedan exempelvis överföras till kryptoplattformar och växlas till fiatvaluta. Genom att transaktionerna sker i ett stort antal steg skapas en distans till ursprunget. |
| Chain hopping | En typ av kryptovaluta konverteras/växlas till en annan kryptovaluta. En växlare tar då emot en typ av kryptovaluta och utbetalar en annan, och för penningtvättaren |

| | |
|---|---|
| | innebär det att värdet flyttas till en annan blockkedja. Vanligtvis är det endast växlaren som vet vilken ingående transaktion i den ena blockkedjan som är kopplad till den utgående transaktionen i den andra blockkedjan. |
| Cross-chain swaps | Cross-chain swap-funktionalitet byter två olika kryptovalutor på samma sätt som chain hopping men i likhet med CoinJoin sker det decentraliserat genom smarta kontrakt. Det innebär att det inte finns en växlare att inhämta information från för att följa transaktionen. |
| Privacy coins | Kryptovalutor som skapats för att tillhandahålla ökad anonymitet. De använder olika tekniker för att dölja insyn och försvåra analys av transaktionskedjan. Exempel på privacy coins är Monero, Zcash och Dash. |

## 4.2 Indikatorer som föranlett misstankerapporter

Vid inrapportering till Finanspolisen ska rapportören ange en eller flera indikatorer som föranlett misstanken. Indikatorerna kan ge en insikt i tillvägagångssätt för penningtvätt och terrorfinansiering.

Enligt de misstankerapporter som undersöktes inom ramarna för denna rapport ser fördelningen i kategorierna ”produkter och tjänster” samt ”kundkännedom” ut enligt nedan.

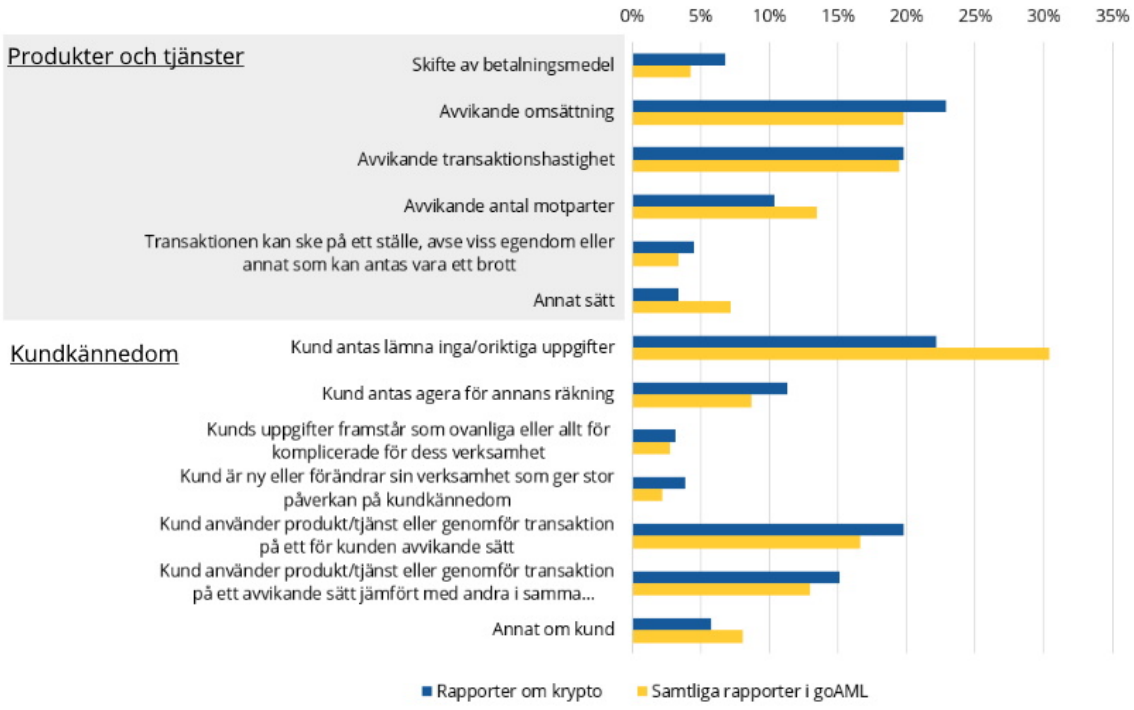



**Diagram 5** **Riskindikationer från verksamhetsutövare**

I kategorin ”produkter och tjänster” utmärker sig indikatorerna avseende *betalningsmedel, avvikande omsättning* och *transaktionen kan ske på ett ställe, avse viss egendom eller annat som kan vara kopplat till ett brott* i jämförelse med samtliga misstankerapporter.

I kategorin” kundkännedom” utmärker sig tre indikatorer. Här har rapportörerna i högre grad reagerat på att kunden är ny eller har förändrat sin verksamhet samt att kunden antas agera åt någon annan. Rapportörerna har även i lägre grad reagerat på att kunden lämnat oriktiga underlag eller inga underlag alls.

I en stor del av rapporteringen beskriver verksamhetsutövarna att deras kund har avvikande transaktioner eller att medels ursprung är oklart. Förfrågan har i vissa fall ställts till kunden. I en del fall anger kunden handel eller förtjänst från kryptohandel som anledning. I inrapporteringen är det i dessa fall sällan med ytterligare information kring påstådd handel. De flesta seriösa plattformarna tillhandahåller möjlighet att ta fram transaktionshistorik och det finns även verktyg för kunden att samla in data från olika plattformar, exempelvis inför skattedeklaration. En ökad kännedom och hantering kring kunders transaktioner efterfrågas således. Exempelvis om en kund som mottagit flera eller en större insättning från kryptoplattformar svarar att det är från tidigare kryptohandel som tex handel med NFT så bör kunden kunna ta fram kontrollerbar data kring sina kontouppgifter, publika kryptoadresser och när och hur köpen finansierats.

## 4.3 Brottsvinster som hanteras med kryptovalutor

Den kriminella användningen av kryptovaluta är inte begränsad till cyberkriminalitet, utan är kopplad till alla typer av brott som kräver betalning för illegala varor och tjänster eller överföring av kryptovaluta för att tvätta brottsvinster. Illegala tjänster accepterar ibland flertalet betalningsmöjligheter. För exempelvis illegal IPTV är PayPal, kreditkort och kryptovaluta de tre vanligaste betalmetoderna.[23] Penningtvätt är den huvudsakliga kriminella aktiviteten i samband med illegal användning av kryptovalutor, enligt såväl Chainalysis samt Europols rapport ”Tracing the evolution of criminal finances: cryptocurrencies”[24] De två största brottskategorierna globalt enligt Chainalysis Crypto Crime report[25] är bedrägerier följt av handel på darknet-

[23] https://www.ncprotection.com/wp-content/uploads/2020/02/NCP-annual-report-2020-final.pdf

[24] https://www.europol.europa.eu/publications-events/publications/cryptocurrencies-tracing-evolution-of-criminal-finances

[25] https://go.chainalysis.com/2021-Crypto-Crime-Report.html

marknader. Chainalysis har inte inkluderat penningtvätt som en egen kategori i analysen av brottskategorier.

**Bedrägerier**
Bedrägerier är de enskilt mest förekommande misstankarna bakom penningtvättsbrottet vid inrapporteringen till Finanspolisen rörande kryptovalutor.

Många rapporter rör personer som blivit vilseleda att föra över pengar eller lämna ifrån sig kortuppgifter i tron att överföringen avser en placering i bitcoin, finansiella instrument eller liknande. Bankkunderna upptäcker att belopp dragits från deras konton eller att de själva godkänt transaktioner utan att få något i gengäld och att pengarna gått till konton och plånböcker som kontrolleras av någon annan. Det förekommer även att bankkunder blir kontaktade angående bitcoin som de uppges investerat i för en längre tid sedan och blir informerade att dessa nu stigit i värde och erbjuds ”hjälp” att sälja loss dessa. Det är ofta oklart hur bedragarna känner till att kunden sedan tidigare har investerat i bitcoin, möjligen var det ett bedrägligt upplägg från första början. Troligt är också att bankkunden ibland inte ens tidigare gjort investeringar i bitcoin. Ett tredje förekommande sätt är att bankkunden blivit bedragen varpå någon som utger sig att vara rådgivare kontaktar vederbörande och erbjuder hjälp att återfå pengarna som gått förlorade mot att kund uppger konto/kortuppgifter etc. Detta drabbar oftast äldre personer.

Det är återkommande att den som verkar vara utsatt för bedrägeri nekar sina investeringar till banken, inte vill förklara avvikande transaktioner, eller ansöker om utlandsköp utan att vilja uppge anledning etc. Det kan därför ibland vara svårt att avgöra om den utsatte faktiskt är utsatt eller i det verkliga fallet är med på upplägget, antingen genom att vara målvakt eller liknande där syftet kan vara penningtvätt eller annan finansiell kriminalitet.

I en rapport från Finanspolisen år 2017[26] diskuterades Oncecoin som snarare är att se som ett pyramidspel än en kryptovaluta. Andelen misstankerapporter inkomna till Finanspolisen avseende rena pyramidspel med kryptovalutor är liten på senare år i jämförelse med år 2016. Andelen rapporter år 2016 rörandes Onecoin var 20-25 % av totala antalet misstankerapporter rörandes krypto. De misstankerapporter som nu berör ämnet handlar exempelvis om plattformar som Jubilee Ace och Crowd1 Network, vilka bägge finns med på Finansinspektionens varningslista.[27] Det är även troligt att information kring personer som förlorat pengar på kursmanipulerade eller falska kryptotillgångar inte når Finanspolisen.

[26] Kryptovalutor - Kartläggning av kryptovalutor i penningtvättsregistret (Finanspolisen, 2017)

[27] https://www.fi.se/sv/vara-register/fis-varningslista/

**Finansiering av terrorism**

Enligt rapporten *Tracing the evolution of criminal finances: cryptocurrencies*[28] från Europol är användningen av kryptovalutor för finansiering av terrorism ett växande problem för myndigheter eftersom det är potentiellt attraktivt på grund av enkla och snabba gränsöverskridande transaktioner, även om det inte ansågs särskilt utbrett än.

Under 2020 avslöjade och lagförde statliga myndigheter runt om i världen fler terrorismfinansieringssystem som involverar kryptovaluta än någonsin tidigare. Exempelvis till insamlingar för al-Qaeda, ISIS och al-Qassam-brigaderna.[29]

Europol beskrev i IOCTA 2019 (Internet Organised Crime Threat Assessment)[30] att terroristgrupper ofta är tidiga användare av ny teknik och nyttjar framväxande plattformar för sina onlinekommunikations- och distributionsstrategier. Aktiva terroristgruppers missbruk av legitima tjänster inkluderar anonymiserade kryptovalutor.

Utöver extern finansiering förekommer att terroristorganisationer självfinansierats genom att begära betalning i kryptovaluta, exempelvis som lösensumma, utpressning och annan brottslighet.

I Sverige har såväl Nordiska Motståndsrörelsen (NMR) och Nordisk Styrka (NS) efterfrågat donationer i bitcoin via olika webbplatser efter att deras bankkonton blivit nedstängda av svenska banker. [31]

Enligt Finanspolisens årsrapport för 2021 visar samtliga våldsbejakande miljöer förmåga att använda kryptovalutor för insamlingsverksamhet från medlemmar eller från sympatisörer. I vissa fall sker dessa insamlingar under falsk förespegling att det handlar om donationer till välgörande ändamål. [32]

Misstankerapporter som inkommit rörande finansiering av terrorism står för 2 % av den totala inrapporteringen i urvalet kring kryptovalutor. Siffran ligger i nivå med den totala inrapporteringen från samtliga rapporter gällande finansiering av terrorism.

---

[28] Tracing the evolution of criminal finances: cryptocurrencies (Europol, 2022)

[29] https://go.chainalysis.com/2021-Crypto-Crime-Report.html

[30] https://www.europol.europa.eu/cms/sites/default/files/documents/iocta_2019.pdf

[31] https://www.europol.europa.eu/cms/sites/default/files/documents/tesat_2021_0.pdf

[32] Finanspolisen årsrapport 2021

# 5 Kriminella aktörer

I detta avsnitt presenteras statistik från misstankerapporter som Finanspolisen mottagit. Utifrån dessa ges en överblick över de inrapporterade personernas kön, ålder samt koppling till annan brottslig verksamhet. För att analysera den övergripande inrapporteringen och ta fram relevanta rapporter kring kryptovalutor har en kombination av sökord använts tillsammans med samtliga rapporter från verksamhetsutövare inom kryptovalutor. Underlaget omfattar totalt ca 2 100 misstankerapporter och 6 100 personer.

## 5.1 Misstankerapporterade

Det är viktigt att lyfta fram att på grund av hur data registreras i inrapporteringssystemet goAML har det inte varit möjligt att identifiera vilka personer som registrerats som misstänka och vilka som ingått i rapporten enbart för att de blivit utsatta på ett eller annat sätt.[33] Fördelningen av kön och ålder visar således en gemensam bild av kriminella aktörer och eventuella offer, medan kopplingen till annan brottslig verksamhet visar en statistisk bild av de personer som faktiskt förekommer i andra underrättelser kopplade till annan brottslig verksamhet.

**Personerna**

Av de 6 135 personer som ingått i misstankerapporter var 27% kvinnor och 73% män. Flest personer var födda under 1990-talet (34 %) följt av personer födda under 1980-talet (23 %), vilket tyder på en relativt ung bas. Diagrammet nedan visar fördelningen över de fem mest förekommande årtiondena.

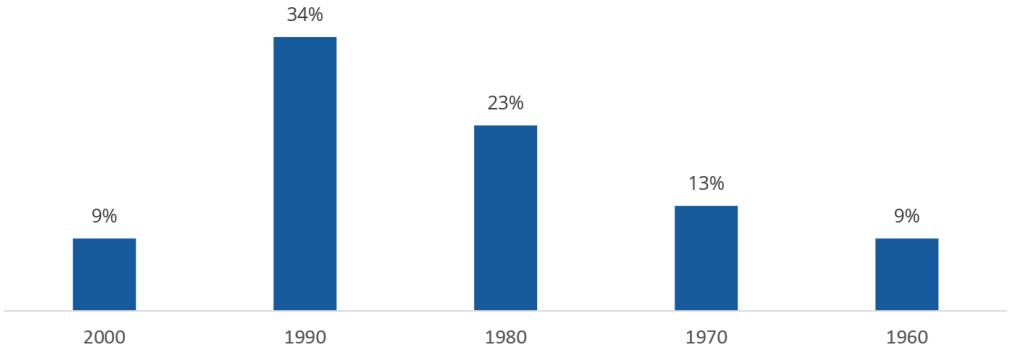



*Diagram 2 Inrapporterade personers fördelning efter födelseår*

Av de inrapporterade personerna som även förekommer i andra underrättelser är överrepresentationen av män större (85 %). Majoriteten av personerna är även här födda under 1990-talet (45 %), medelåldern var 33 år.

**Koppling till andra brottsområden**

Kopplingen till allvarlig och organiserad brottslighet för de inrapporterade

[33] Misstankerapporter som granskats är av typen STR (Suspicious Transaction Report).

personerna är förhållandevis stark. Närmare en tredjedel (32%) av personerna förekommer med minst en underrättelse om allvarlig och/eller systematisk brottslig verksamhet. I diagrammet nedan presenteras brottsområdena som det funnits starkast koppling till. Kopplingen är starkast till narkotika, vapen och våld, penningtvätt, systematiska vinningsbrott, samt bedrägerier. Kategorin penningtvätt innebär att brottsvinster kommer från annan brottslig verksamhet, men där det inte framgår vilken brottslighet som föregått penningtvätten. Andelen personer kopplade till underrättelser om sexualbrott mot barn är förhållandevis hög (4%), vilket kan ställas i jämförelse till Finanspolisens rapport om Neobanker där andelen var under 2%. Brottsområden med en koppling på under 2% är inte med i diagrammet. De kategorierna är exempelvis Miljöbrott, Korruption och IT-brott.

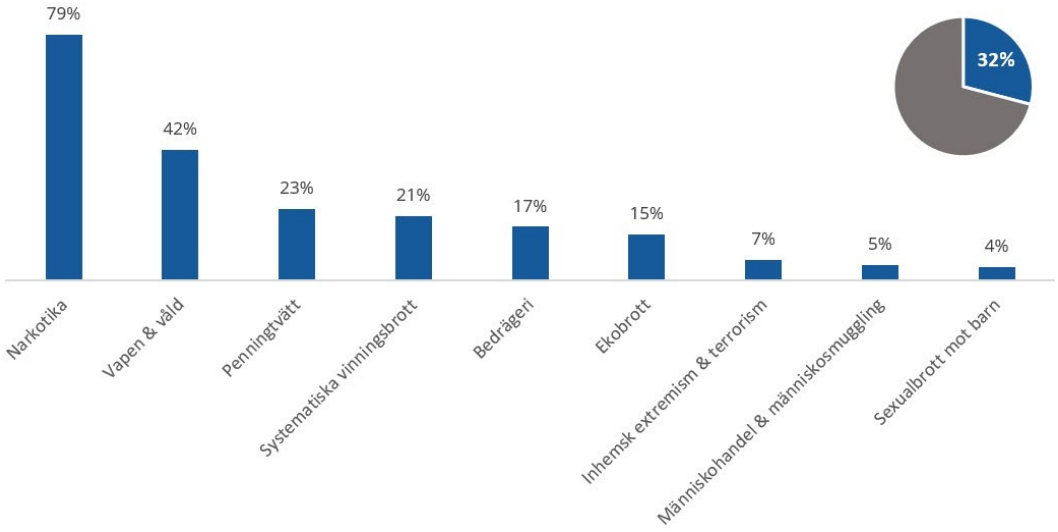



*Diagram 4 Andel av personerna med misstänkt koppling till andra brottsområden. En person kan vara kopplad till flera olika brottsområden vilket gör att antalet förekomster totalt för alla brottsområden fler än antalet personer som ligger till grund för underlaget.*

## Geografisk spridning

Det finns en viss överrepresentation av personer som bor i utsatta områden. Denna motsvarar dock överrepresentationen i penningtvättsregistret och andra penningtvättsupplägg som analyserats, och utmärker sig således inte. En analys utförd tillsammans med de fem storbankerna visar samtidigt att det generella användandet av kryptovalutor är något mindre vanligt i utsatta områden.[34]

[34] Pågående analys hos Finanspolisen i pilotprojekt inom SAMLIT

## 5.2 Kryptoväxlare och kryptospecialister – en kritisk kompetens

För att kriminella ska kunna tillgodogöra sig tillgångar utanför den kryptovalutabaserade ekonomin eller för att integrera brottsvinster från fiatvaluta finns behov av att växla mellan valutorna via legala eller illegala kryptoväxlare.

Vid växling sker den initiala kontakten mellan köpare och säljare ofta på P2P (peer-to-peer) plattformar utformade för handel främst mellan privatpersoner, men kontakten kan givetvis också både skapas och fortsätta via andra kanaler, appar och nätverk. Det finns ett antal P2P-plattformar som tillhandahåller handel mellan enskilda parter. Vissa P2P-plattformar har inga eller bristande kundkännedomsprocesser. Handel på P2P-plattformarna genomförs via ett brett utbud av transaktionsmöjligheter, vanligen genom överföringar via Swish, Paypal, Revolut eller annan neobank. Men även kontoöverföringar via traditionell bank, betalkortsöverföring via tredjepartslösningar och kontanta transaktioner förekommer.

Gemensamt för de individer som i rapportens fördjupade analys kategoriserats som möjliga kryptoväxlare är att de får en omfattande mängd Swish-inbetalningar på sitt konto, alternativt kontantinsättningar. I anslutning till dessa görs köp på vanligen etablerade större kryptoplattformar. Vissa av dessa individer uppger till banken att de handlar med kryptovaluta. De verkar inte alltid själva anse eller vara medvetna om att det de gör är olagligt. Banken avslutar ofta kundengagemanget. Vidare observation från materialet är att flera växlare på P2P-plattformar uppmanar köpare som betalar via exempelvis Swish att inte ange någon referens på handeln i meddelandet. Ibland uppmanas köpare även att skriva något helt annat för att få transaktionen att till synes handla om exempelvis köp av vara, köp av digitala skins till spel eller återbetalning av lån. Detta indikerar att säljaren är medveten om att handeln är illegal, eller i vart fall att banken inte accepterar att handeln bedrivs på kontot som de tillhandahåller.

**Kryptospecialister**

Utöver kryptoväxling så finns det bland kriminella grupperingar ett behov av stöd och administration kring hantering av kryptovalutor i brottsupplägg samt i den mer avancerade penningtvätten. Aktörer som besitter denna förmåga är sannolikt eftertraktade av kriminella aktörer och grupperingar.

Sammantaget framstår illegala kryptoväxlare och specialister inom kryptovalutor som en kritisk kompetens för kriminella aktörer för att de effektivt ska kunna dölja, hantera och tillgodogöra sig sina kriminella tillgångar. Intresset bland kriminella att använda kryptovalutor är växande varför betydelsen av denna kompetens troligen kommer att öka framgent.

# 6 Slutsatser och tänkbara åtgärder

- Kryptovalutor och kryptotillgångar utnyttjas för att hantera brottsvinster, tvätta pengar och finansiera terrorism. Det finns en koppling till miljöer inom organiserad brottslighet.
- Det är sannolikt att de verktyg och metoder som skapas och förfinas för att dölja finansiella spår inom krypto kommer att anammas av kriminella miljöer och därmed förväntas även kriminella upplägg att förändras.
- Det är *bekräftat* att det i Sverige finns ett betydande antal personer som bedriver illegal växling av kryptovaluta och utgör möjliggörare för kriminella aktörer och nätverk. Dessa är kritiska kompetenser för övriga kriminella miljöer. Efterfrågan på dessa aktörer väntas öka i takt med att specialiserad kompetens behövs.
- Det är *troligt* att penningtvätt och finansiering av terrorism med hjälp av kryptovaluta kommer fortsätta att öka och följa den allmänna trenden inom området.

Generellt finns ett behov av att öka kunskapen kring kryptovalutor hos myndigheter och verksamhetsutövare. För många verksamhetsutövare behövs en ökad förståelse kring sina kunders transaktioner, direkt eller indirekt relaterade till kryptovalutor. Identifierade hot, sårbarheter och risker i denna rapport bör analyseras utifrån respektive verksamhets uppdrag för att stärka arbetet inom området.

Finanspolisen ser utifrån ett aktörsperspektiv att ett brottsbekämpande arbete effektivt riktas mot de som underlättar för kriminellas brottsvinsthantering inom kryptoområdet. Där finns ett behov av att fortsätta att identifiera illegala kryptoväxlare och kryptospecialister som identifierats som möjliggörare i denna rapport. Dessutom finns behov av att fortsätta täppa till nuvarande och kommande sårbarheter genom ett fortsatt aktivt deltagande i framtagandet av lagstiftning samt förbättra det nationella och internationella informationsutbytet kring misstänkta personer och samverkan i kryptorelaterade frågor.

# Bilaga: Utbildning och kunskapshöjning

| |
|---|
| Två vägledningar finns upprättade, dels Skatteverkets vägledning[35] riktat till personer som kan stöta på kryptovalutor i samband med utredningar av penningtvätt, dels Åklagarmyndighetens rättsliga vägledning[36] om kryptovalutor. |
| Myndigheter och bolag anordnar regelbundet event där ämnet krypto presenteras och diskuteras |
| Flera av de större handelsplattformarna som Coinbase och Binance har tagit fram informativa guider.[37] |
| Bolag inom blockkedjeanalys erbjuder ofta såväl information som kurser inom kryptospårning. |
| På CEPOLs utbildningsplattform LEEd för brottsutredande myndigheter finns en mängd webinars rörandes krypto. CEPOL erbjuder även återkommande både grundläggande och avancerade ”på-plats-utbildningar”. |
| På polisens interna hemsida Intrapolis finns en informationssida[38] med material om hur man spårar virtuell valuta samt länkar till rättsfall och fördjupningsmaterial. På polisens lärplattform Ping Pong finns en interaktiv utbildning om kryptovalutor lanserad 2022.[39] |
| Europol har lanserat ett utbildningsspel för brottsutredande myndigheter, Cryptopol, som är en simulator med praktiska övningar i spårning av kryptovalutor från verklighetsbaserade situationer. [40] |

[35] https://www.skatteverket.se/download/18.1c68351d170ce5545274989/1588770809742/penningtvatt-och-kryptovalutor-20200502.pdf

[36] https://www.aklagare.se/globalassets/dokument/rattspromemorior-och-rattslig-vagledning/rav-202111-kryptovalutor.pdf

[37] https://www.coinbase.com/learn/crypto-basics , https://academy.binance.com/en/articles/what-is-cryptocurrency

[38] https://intrapolis.polisen.se/bekampa-brott/omraden-amnen/it-relaterad-brottslighet/spara-virtuella-valutor/

[39] E-kursen finns i Ping Pong under Aktiviteter - Katalog - ”It-brottslighet – Kryptovaluta grund – e-kurs”

[40] https://www.europol.europa.eu/media-press/newsroom/news/game-for-europol-and-centric