ØKOKRIM

Bruk av kryptovaluta i kriminell virksomhet

Hva er kryptovaluta?

Kryptovaluta er en digital valuta som bruker kryptografi for å sikre transaksjoner. Dette muliggjør overføring av store beløp på tvers av landegrenser, som regel med lave gebyrer.[1] I likhet med ordinær valuta (euro, dollar, kroner, m. fl.), benyttes kryptovaluta både som betalingsmiddel og investeringsobjekt. Transaksjonene skjer uten en tredjepart, slik som i en bank.

De fleste kryptovalutaer har full åpenhet om transaksjoner, adresser (tilsvarende bankkontoer) og inneståend beløp på de ulike adressene. Man vet imidlertid ikke hvem som eier de ulike adressene.

Identifisering av hvem som står bak transaksjoner i kryptovaluta krever kompetanse innen teknisk og taktisk etterforskning, digital sporsikring, datateknisk kompetanse og kompetanse i å spore, følge og analysere pengestrømmer. Fra myndighetenes ståsted, er dette en grunnleggende sårbarhet ved kryptovaluta.

De fleste som bedriver kjøp og salg av kryptovaluta i Norge er menn (92 prosent) under 30/45år (50/85 prosent). Den virkelig store veksten i kryptovaluta-handel så vi i 2017. Til transaksjonene benyttes både utenlandske og norske vekslere.

Hva er en kryptovalutaveksler?

En kryptovalutaveksler er en aktør som tilbyr tjenester for å veksle ordinær valuta til kryptovaluta, eller omvendt. Tilbydere av slike vekslingstjenester ble ved ikrafttredelse av ny hvitvaskingsforskrift 15. oktober 2018 rapporteringspliktige etter hvitvaskingsloven.[2] Dette innebærer at vekslerne blant annet pålegges å gjennomføre kundetiltak og å rapportere mistenkelige transaksjoner til ØKOKRIM. I tillegg ble vekslerne registreringspliktig hos Finanstilsynet. Vekslerne fikk frist til å registrere seg hos Finanstilsynet innen 15. januar 2019.[3] Fra og med 11. okt. 2019 startet Finanstilsynet å gjennomføre egnethetsvurderinger (inkludert politiattest) som en del av registreringsprosessen.[4]

---

[1] NTAES, «Temarapport nr.1: Kryptovaluta», 2018.

[2] Jf. forskrift 14. september 2018 nr. 1324 § 1–3.

[3] Finanstilsynet, «Hvitvaskingslovens anvendelse for virtuell valuta», 2018.

[4] Finanstilsynet, «Hvitvaskingsregelverket: Innføring av egnethetskrav for tilbydere av vekslings- og oppbevaringstjenester for virtuell valuta», 2019.

Desentraliserte vekslere
En desentralisert veksler (DEX) tilrettelegger for at privatpersoner kan kjøpe og selge kryptovaluta direkte imellom hverandre, uten å gå via en tredjepart. Eksempel på desentralisert veksler er tjenesten localbitcoins.com som fungerer som en møteplass for kjøpere og selgere av kryptovaluta, samtidig som man kan veksle imellom krypto- og ordinær valuta. Flere av de desentraliserte vekslerne gjennomfører ikke identitetskontroll, noe som gjør de mer attraktive for kriminelle.[5]

Finanstilsynet mener at aktører som annonserer mot det norske markedet må følge det norske regelverket. Financial Action Task Force (FATF) påpeker imidlertid at vekslere som har registrert seg i en annen jurisdiksjon, men som tilbyr sine tjenester i for eksempel Norge, er en utfordring. Spesielt når det kommer til transaksjoner som krysser landegrenser, kan det bli uklart hvilke personer som er involvert, og hvilket land som har det juridiske ansvaret for reguleringen og overvåkningen.[6]

Norske rapporteringspliktige kryptovalutavekslere
Før rapporteringsplikten trådde i kraft 15. oktober 2018 var det 10-15 tilbydere av vekslingstjenester i Norge. Kun et fåtall av disse valgte å registrere seg hos Finanstilsynet da registreringsplikten trådte i kraft. Pr. 11. august 2020 er det hos Finanstilsynet registrert ni tilbydere av oppbevaring- og veksling av kryptovaluta.

Blant de rapporteringspliktige vekslerne, er det enkelte av de involverte som kan knyttes til bedrageri- og narkotikakriminalitet.

For anti-hvitvaskingsarbeidet er det en sårbarhet at vekslere av kryptovaluta i hovedsak er aktører med manglende erfaring og rutiner for rapportering av mistenkelige transaksjoner. Flere av de registrerte vekslerne er også små enkeltmannsforetak/aksjeselskap med begrensede ressurser til å drive kontroll av kunder. Anonymiteten som kryptovaluta tilbyr gir også grunnleggende utfordringer med kundekontrollen for aktørene.

Norske uregistrerte vekslere av kryptovaluta
Kryptovalutavekslere som ikke har registrert seg hos Finanstilsynet, slik de er lovpålagt, faller i kategorien

> Tilbydere av vekslingstjenester mellom krypto- og ordinær (fiat) valuta er registreringspliktig hos Finanstilsynet, samt rapporteringspliktig iht. hvitvaskingsloven.

[5] EUROPOL, «Internet Organised Crime Threat Assessment (IOCTA)», 2018.
[6] FATF, «Guidance for a risk-based approach: Virtual assets and virtual asset service providers», 2019.

uregistrerte vekslere, og bedriver ulovlig virksomhet. Disse opererer anonymt under alias. Vekslingen foregår som regel ved vanlig nettbankoverføring[7] som tilbys på nettsider som localbitcoins.com. I tillegg tilbyr enkelte oppgjør via betalingsapplikasjoner.

I begynnelsen av august 2020 anslår ØKOKRIM at det var 10–20 uregistrerte vekslekontoer innrettet mot det norske markedet. Av disse er det enkelte som skiller seg ut som svært aktive.

Omtrent samtlige av de uregistrerte vekslerne, hvor man kjenner identiteten til vedkommende, har knytninger til annen kriminalitet, som narkotika-, skattesvik-, bedrageri og hvitvasking. Enkelte vekslere av kryptovaluta er villig til å motta kontantbeløp da dette er mer lukrativt fordi folk er villige til å betale ekstra for å unngå hvitvaskingsregelverket. De antas å være spesielt egnet for bruk til kriminelle formål.

Hvordan benyttes kryptovaluta til kriminalitet?

Kryptovaluta kan enkelt overføres, oppbevares og veksles i ordinær valuta i utlandet. Den potensielt vanskelige sporbarheten gjør dette til en svært attraktiv metode å skjule utbytte fra kriminelle handlinger, hvitvaske penger samt finansiere ny kriminell aktivitet.[8]

Betalingsløsning i ulike typer kriminell handling

Det finnes flere eksempler på at kryptovaluta benyttes som betalingsmiddel i sammenheng med annen kriminell aktivitet. ØKOKRIM har observert transaksjoner hvor selve vekslingen er lovlig, men hvor transaksjonen er betaling for en kriminell handling. Kryptovaluta benyttes også ved oppgjør for narkotika,[9 10 11] og som betalingsmiddel på det mørke nettet hvor ulovlige varer/tjenester omsettes, slik som narkotika, seksuelle overgrep mot barn, våpen og stjålne person- og bankopplysninger.[12 13]

Muldyr

En metode for hvitvasking er bruk av såkalte muldyr. Dette er personer uten en åpenbar tilknytning til den kriminelle virksomheten/personen, som får betalt for å ta imot innbetalinger, veksle de til/fra kryptovaluta og overføre beløpet videre for oppdragsgiveren.[14]

> Omtrent samtlige av de identifiserte uregistrerte vekslerne har knytninger til annen kriminalitet, som narkotika-, skattesvik-, bedrageri og hvitvasking.

Forhåndsbetalte kort/Bitcoin plastic

Bitcoin plastic er et forhåndsbetalt debetkort hvor brukeren fyller på verdi ved bruk av kryptovaluta. Brukeren trenger kun å opprette konto hos selskapet og får deretter tilsendt bankkortet i posten. Han vil deretter være anonym ved bruk av dette kortet.[15 16]

Skattesvindel

Kryptovaluta er et eget formuesobjekt som får skattemessig betydning både ved kjøp, salg og beholdning. I tillegg er inntekt fra såkalt mining (utvinning) av kryptovaluta og fra vekslingstjenester skattepliktig. Området er relativt nytt og markedet er under utvikling, så misforståelse hos skattepliktige kan forekomme, men bevisste skatteunndragelser er også sannsynlig.

Tyveri av kryptovaluta

EUROPOL og Chainalysis har rapportert at flere vekslere, spesielt de som også tillater oppbevaring av kryptovaluta, har blitt hacket og kundenes midler stjålet.[17] De rapporterer om cyberangrep mot vekslere hvor tyveriet i mange tilfeller utgjør titalls-, og i enkelte tilfeller over hundre millioner amerikanske dollar.[18] Chainalysis mistenker at velorganiserte og kompetente organisasjoner/stater står bak.

---

[7] En escrow-konto er en konto for mellomlagring av midler som skal overføres mellom to eller flere parter. Disse tilbys gjerne av en tredjepart.

[8] Finanstilsynet, «Risikovurdering: Hvitvasking og terrorfinansiering», 2019.

[9] EUROPOL, «Internet Organised Crime Threat Assessment (IOCTA)», 2017.

[10] EUROPOL, «Internet Organised Crime Threat Assessment (IOCTA)», 2018.

[11] NTAES, «Bedrageri mot næringslivet», 2019.

[12] National Crime Agency UK, «National Strategic Assessment of Serious and Organised Crime», 2019.

[13] Finanstilsynet, «Risikovurdering: Hvitvasking og terrorfinansiering», 2019.

[14] Finanstilsynet, «Risikovurdering: Hvitvasking og terrorfinansiering», 2019.

[15] EUROPOL, «Internet Organised Crime Threat Assessment (IOCTA)», 2018.

[16] Coinbase, «Coinbase.com/card», 2020.

[17] EUROPOL, «Internet Organised Crime Threat Assessment (IOCTA)», 2018.

[18] Chainalysis, «Crypto Crime report», January 2019.

Hvitvasking
Vi ser også en ny modus hvor aktører lyver om at kryptovaluta er opphavet til midler som egentlig stammer fra straffbare handlinger.

Modus for bruk av kryptovalutavekslere til hvitvasking

ØKOKRIM erfarer at kriminelle ofte benytter en av tre metoder for å hvitvaske kriminelt utbytte via kryptovaluta.

1. Den første innebærer at de/den kriminelle har mottatt en bankoverføring av ulovlig ervervede midler og nå ønsker å veksle ordinær valuta om til en kryptovaluta, og deretter sende utbyttet utenlands. Alternativt er rekkefølgen motsatt, altså at de kriminelle vil veksle kryptovaluta som er utbytte fra annen kriminell handling om til en ordinær valuta.
2. Den andre er at et bedragerioffer veksler egen ordinær valuta til kryptovaluta, og sender kryptovalutaen til den kriminelle, eventuelt får veksleren til å gjøre dette.[19]
3. Den tredje og siste metoden innebærer at kriminelle får kontroll over nettbanken til offeret og overfører penger derifra til seg selv via en kryptovalutaveksler ved å utgi seg for å være offeret. I bedragerisaker, hvor offeret har gitt fra seg bank- og personopplysninger, tar de kriminelle og overfører pengene fra bankkontoen til en kryptovalutaveksler. Deretter blir pengene vekslet til kryptovaluta og sendt videre til den kriminelles kryptovalutakonto (wallet).

I alle disse eksemplene er det vanskelig for veksleren å vite den ordinære valutaens opphav, eller om den som ønsker å veksle er et bedragerioffer.

Et eksempel på en mer avansert hvitvaskingsoperasjon ble avdekket i 2018 da spanske, amerikanske og finske myndigheter gikk til aksjon mot finske kryptovalutavekslere. Disse ble brukt av spanske narkotikaselgere til å veksle ordinær valuta som stammet fra kriminalitet om til bitcoin, for deretter å veksle kryptovalutaen om til Colombianske pesos og sette de inn i Colombianske banker.[20]

[19] Finanstilsynet, «Risikovurdering: Hvitvasking og terrorfinansiering», 2019.
[20] EUROPOL, «Internet Organised Crime Threat Assessment (IOCTA)», 2018.

Bruk av kryptovaluta er en svært attraktiv metode for å skjule utbytte fra kriminelle handlinger, hvitvaske penger samt finansiere ny kriminell aktivitet.