



POLITIET
KRIPOS

KRYPTOVALUTA – FCG 20.10.2022

Pub: Eirik Sneeggen

SEKSJON FOR ETTERFORSKNINGSSTØTTE, NC3



KRIPOS



Eirik Sneeggen

Politioverbetjent og fagspesialist innen kryptovaluta
NC3/ Kripos.

Har etterforsket saker som involverer kryptovaluta
siden 2014.

2014

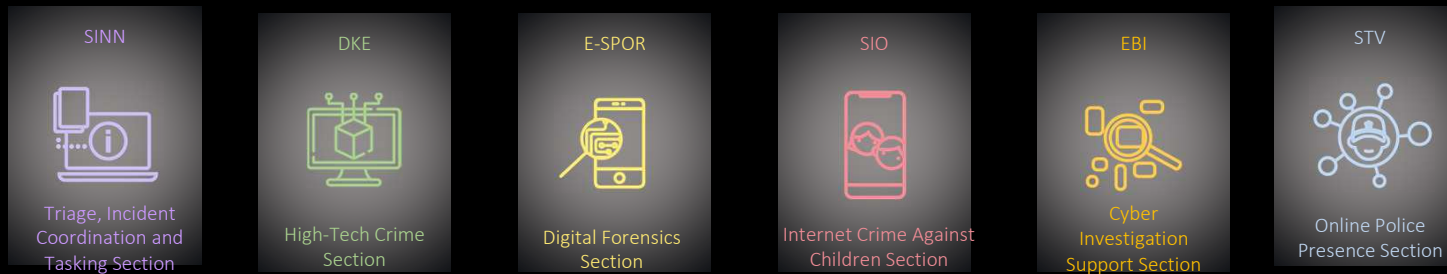
Darknet
Cybercrime
BTC



2022

Alle typer kriminalitet med
økonomiske motiv
Drap, kidnapping, ran,
investorbedrageri
Kjøp av overgrepsmateriale
Ether/ smartkontrakter/ DEFI, BTC,
privacy coins (Monero), mixing.

NC3 – Nasjonalt Cyberkrimsenter



NC3 opprettet som en avdeling på Kripos januar 2019:

Hovedoppgaver er å bekjempe cyberkriminalitet gjennom etterretning, metodeutvikling, forebygging, etterforskning, sikring av digitale spor samt patruljering på nett. Senteret vil spille en viktig rolle i å fremme informasjonsdeling og samvirke mellom private og statlige sikkerhetsaktører nasjonalt og internasjonalt. Målet er å være nasjonalt og internasjonalt ledende innen avdekking og bekjempelse av trusler og kriminalitet i det digitale rom.

Kryptovaluta en av de prioriterte fagområdene for NC3.

Hva er **KRYPTOVALUTA**?

Et **digitalt betalingsmiddel** som benytter seg av **kryptografi** for å sikre **transaksjoner** og kontroll over generering av nye **valutaenheter**. Kryptovalutaer benytter seg av desentralisert kontroll i motsetning til regulære valutaer hvor kontrollen normalt er sentralisert hos en statsbank.

DET FINNES **MANGE** KRYPTOVALUTAER



BITCOIN



ETHERIUM



NFT



MONERO

NFT – Non fungible tokens: Ikke underlagt hvitvaskingsreglene for kryptovaluta. Eierskap bevises gjennom kryptovaluta/ blockchain på kryptovalutaer som feks. Ethereum.

Cefi vs Defi innen kryptovaluta

Cefi:

- Tjenestene ligger på en sentralisert server, operert av et selskap.
- Brukerne må legitimere seg og opprette kontoer hos selskapet for å benytte seg av tjenestene.
- Ligner mer tradisjonelle finansielle tjenester, tilliten ligger hos tjenesten.
- Fungerer som et bindeledd mellom fiat og kryptovaluta.
- For politiet: Vi må anmode tjenesten om informasjon.

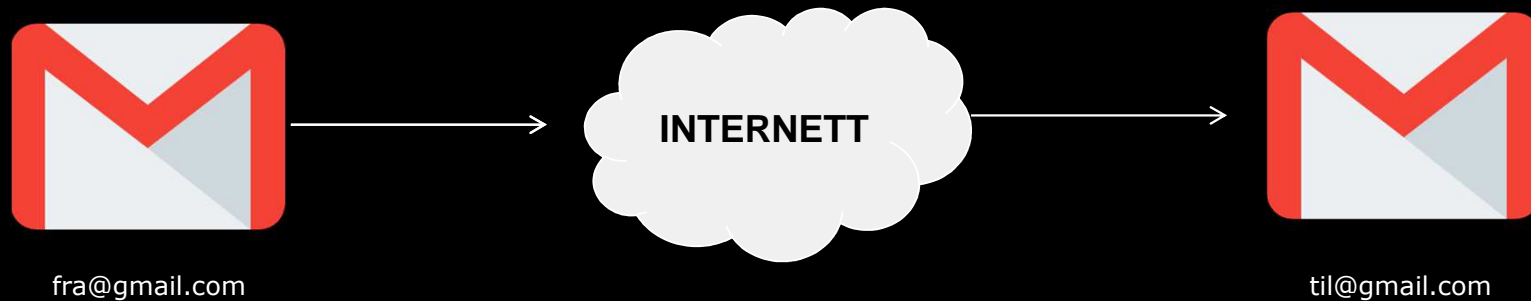
Defi:

- Tjenestene er regulert av smartkontrakter.
- Alle transaksjoner er synlige for alle. Teknologien ligger åpent tilgjengelig.
- Brukerne trenger ikke å opprette kontoer eller legitimere seg.
- Ingen veksling mellom krypto og fiat.
- For politiet: Vi må spore transaksjoner gjennom tjenesten.

Hva er **BITCOIN**?

BITCOIN LAR DEG SENDE PENGER GJENNOM INTERNETT

BITCOIN ER SOM E-POST



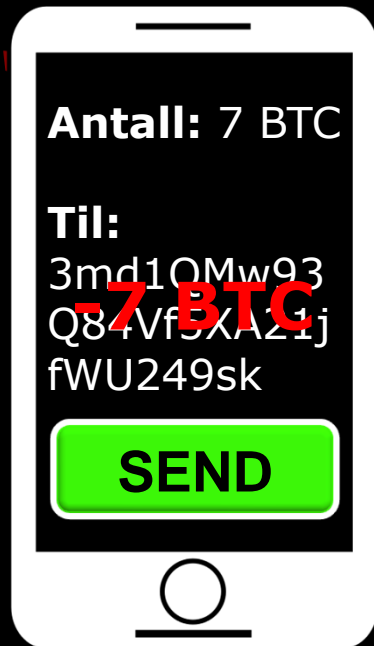
1aa5cmqmvQq8YQTEqcTmW7dfBNuFwgdCD

1bbwxJvTcMd2QYt1QMfELf3oJYui5WahD

HVORDAN FUNGERER **BITCOINS**?



SENDER



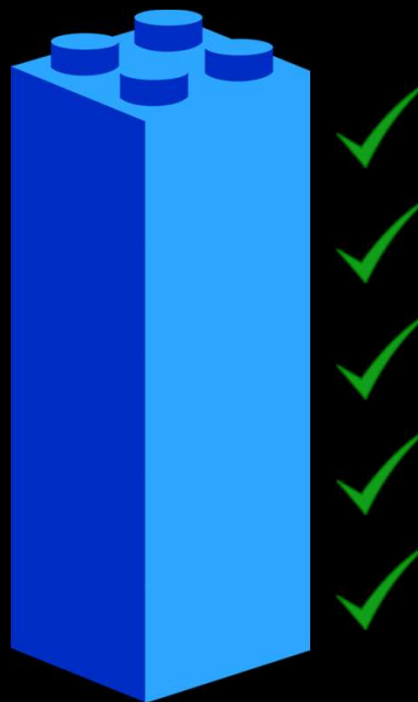
MOTTAKER



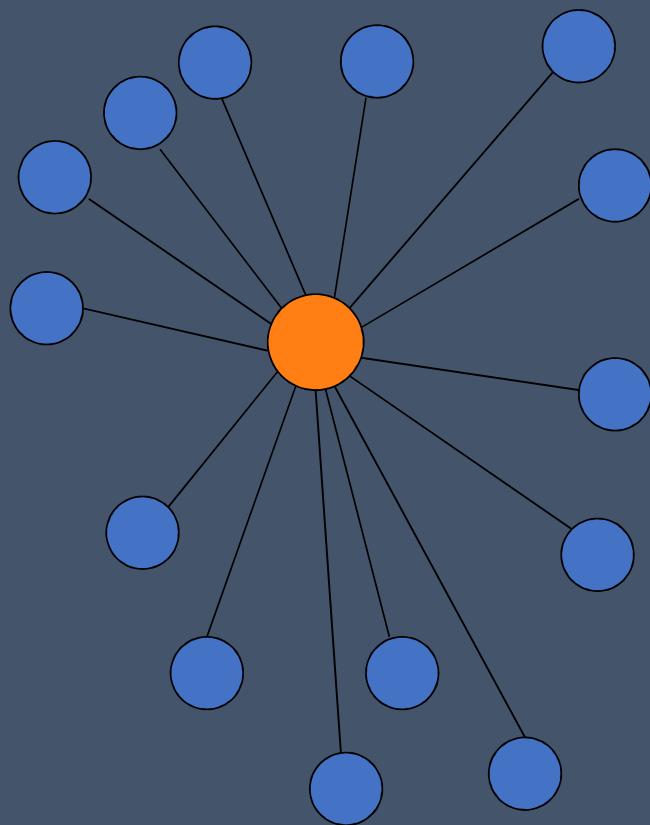
Hva er **BLOCKCHAIN**?

En blockchain er en **distribuert database** hvor hver node automatisk verifiserer tilføyer som gjøres på noen av de andre nodene

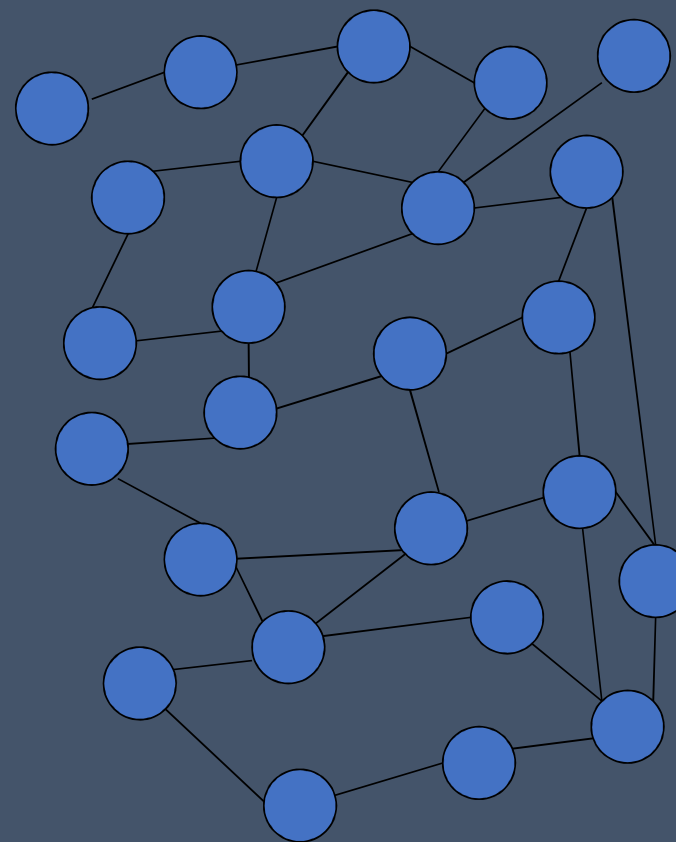
EN GODKJENT «BLOKK» KAN **IKKE ENDRES**



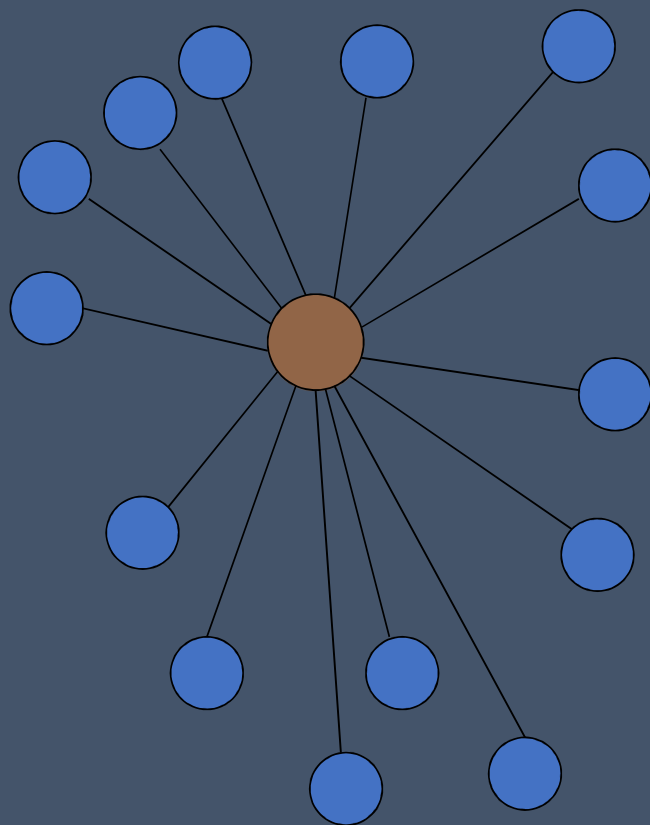
SENTRALISERT



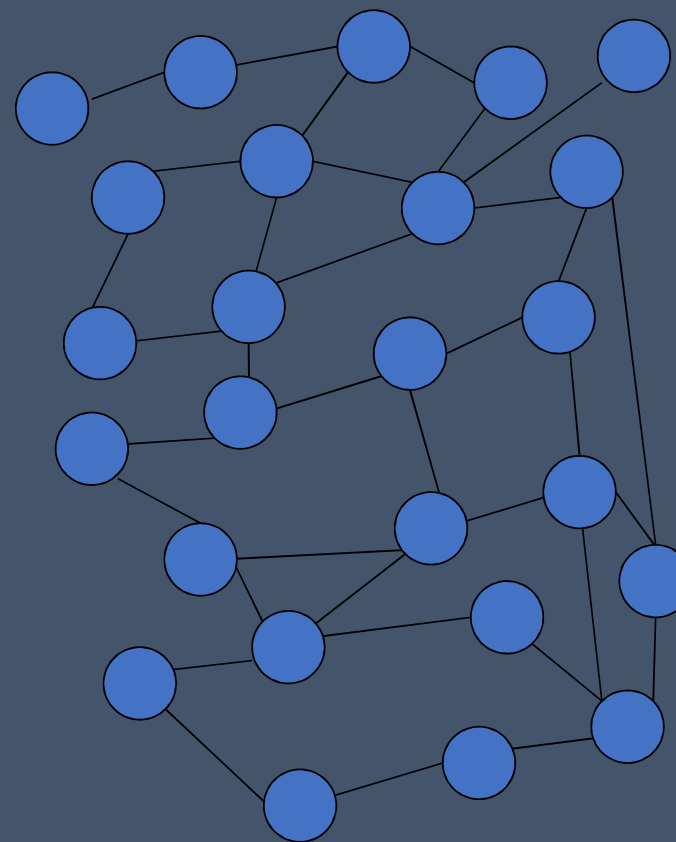
DESENTRALISERT OG DISTRIBUTUERT



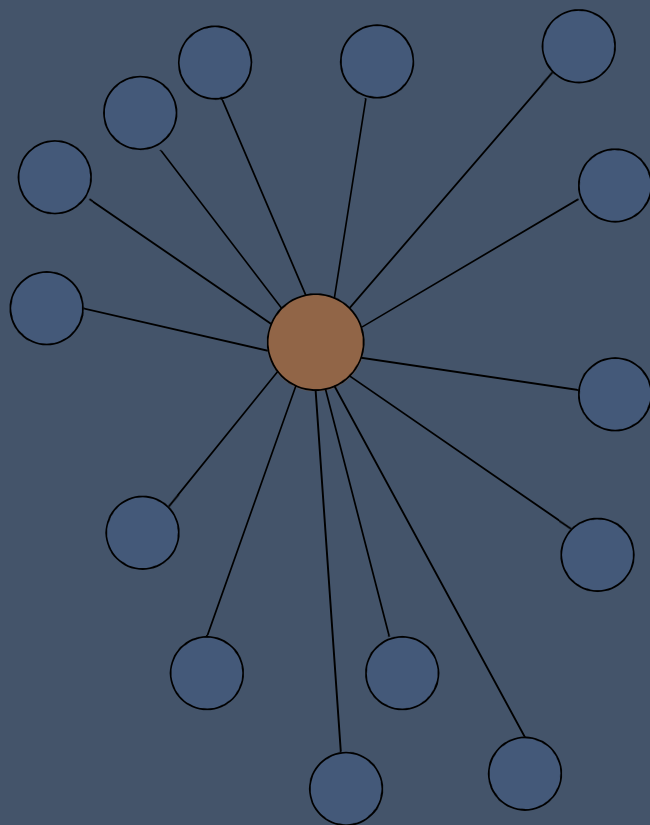
SENTRALISERT



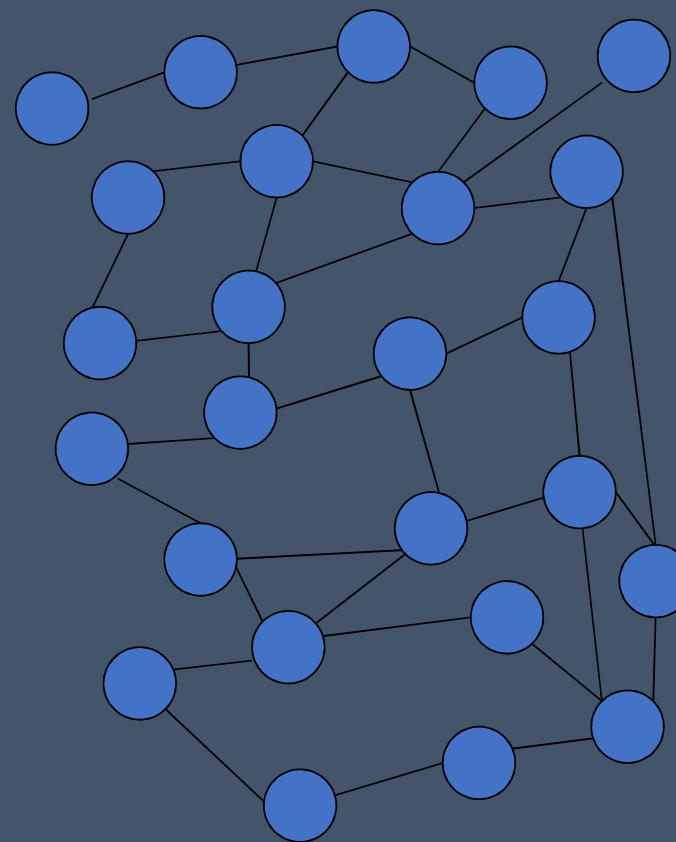
DESENTRALISERT OG DISTRIBUTUERT



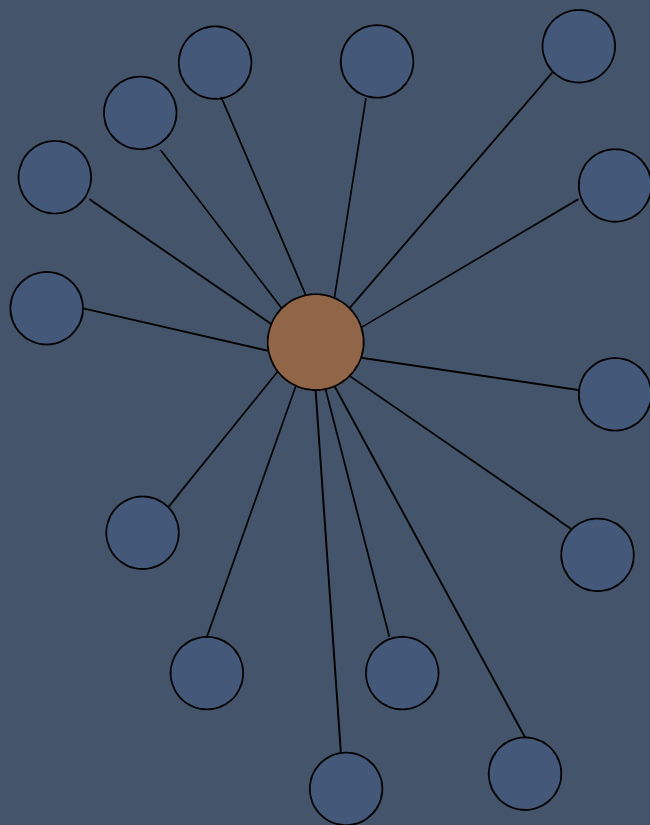
SENTRALISERT



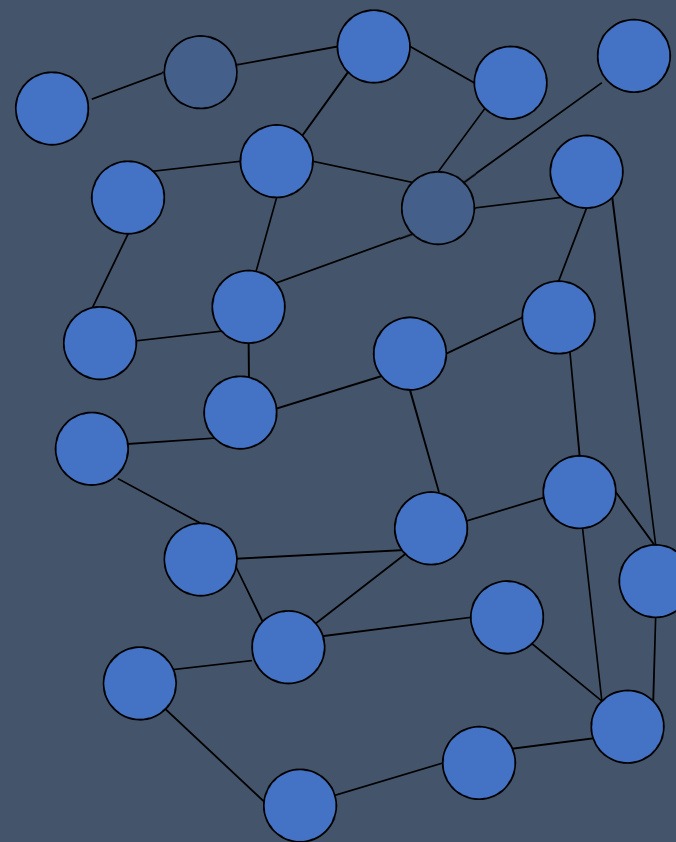
DESENTRALISERT OG DISTRIBUTUERT



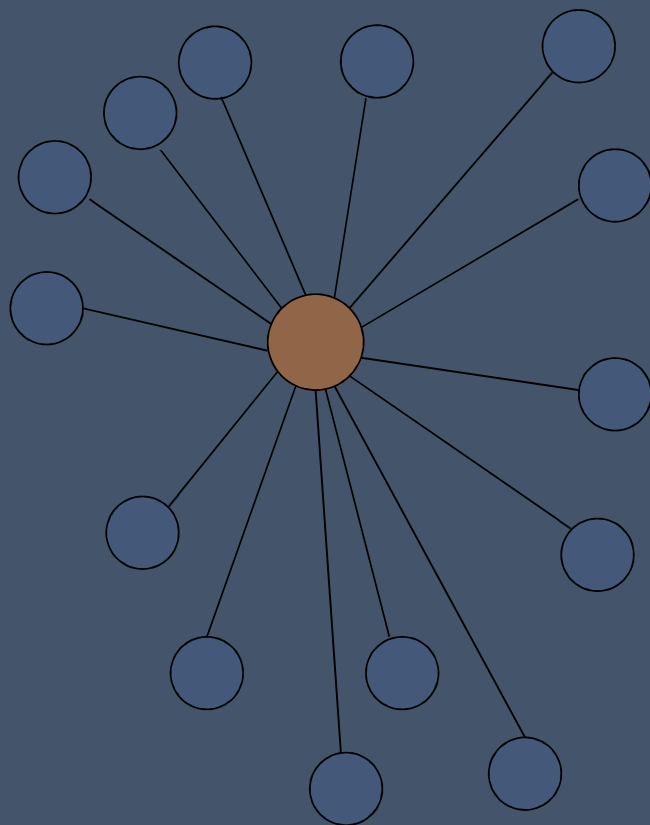
SENTRALISERT



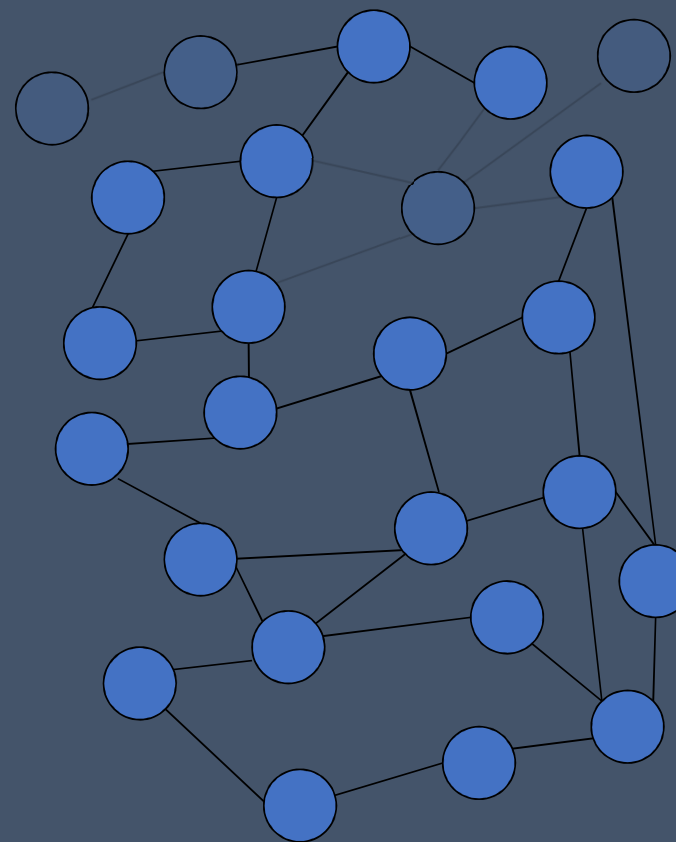
DESENTRALISERT OG DISTRIBUTUERT



SENTRALISERT



DESENTRALISERT OG DISTRIBUTUERT



Kryptovaluta bedre enn kontanter?

– Jeg synes ikke bitcoin fortjener et ensidig kriminelt stempel. Personlig vil jeg heller se fysiske kontanter forsvinne enn bitcoin, sier politiadvokat Richard Beck Pedersen.

Politiet har knekt bitcoin-koden: – Kriminelle vender tilbake til kontanter

Kripos mener de puster kriminelle i nakken når det kommer til bruk av kryptovaluta.



KRYPTOPOSITIVT: Politadvokat Richard Beck Pedersen mener blokkjedefteknologi er et viktig verktøy for å ta kriminelle. Foto: Jan Olav Niesvold NTB scanpix

- Transaksjoner **offentlige** i blockchain
- **Historiske data** blir tatt var på
- Kryptovaluta **pseudoanonymt**, politiet har gode muligheter til å identifisere hvem som står bak!

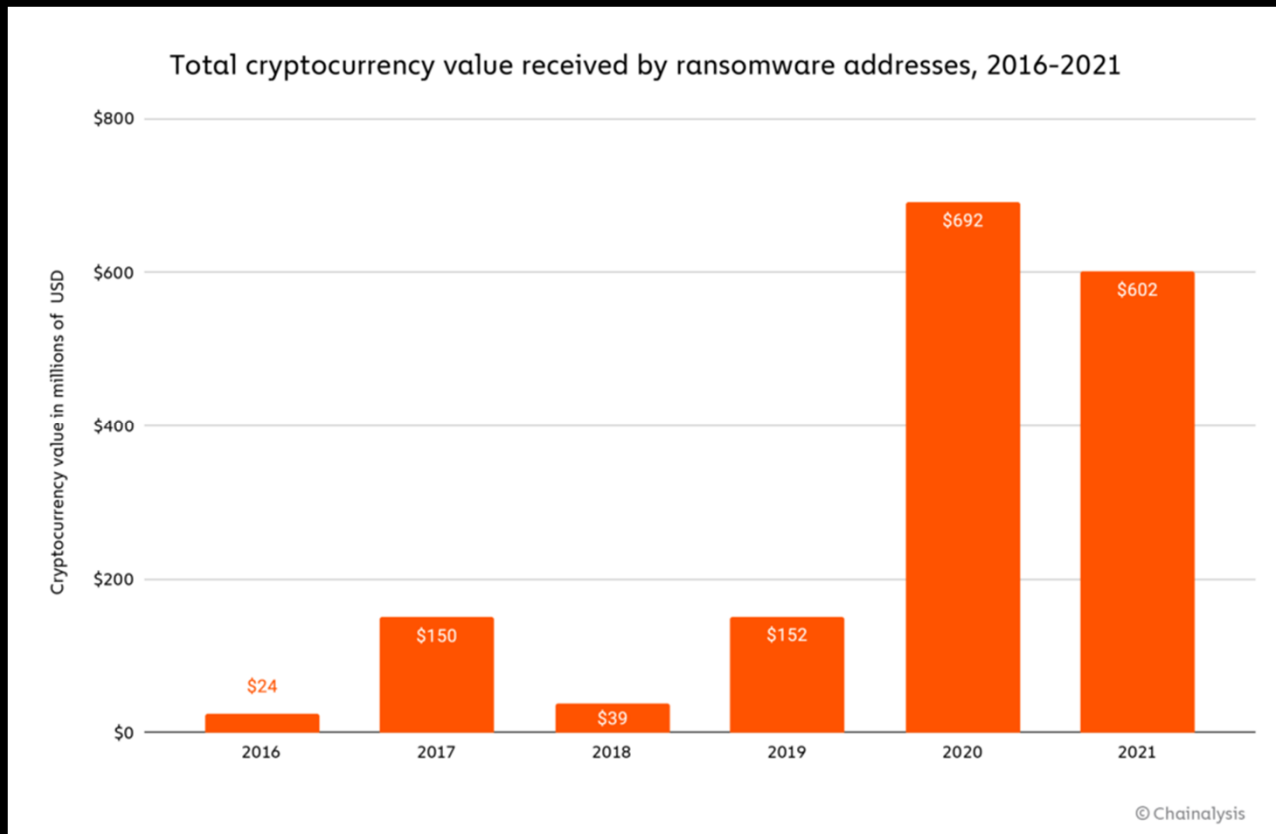
Crime as a **service**

The continued increase of cyber- and computer-related crime is to a large degree enabled through the evolution and maturation of the criminal markets that provide all the necessary tools, goods and services to novice and established criminals. Network intrusions and social engineering are components of a multitude of attack vectors.

Internet Organised Crime Threat Assessment (IOCTA) 2021 (Europol)

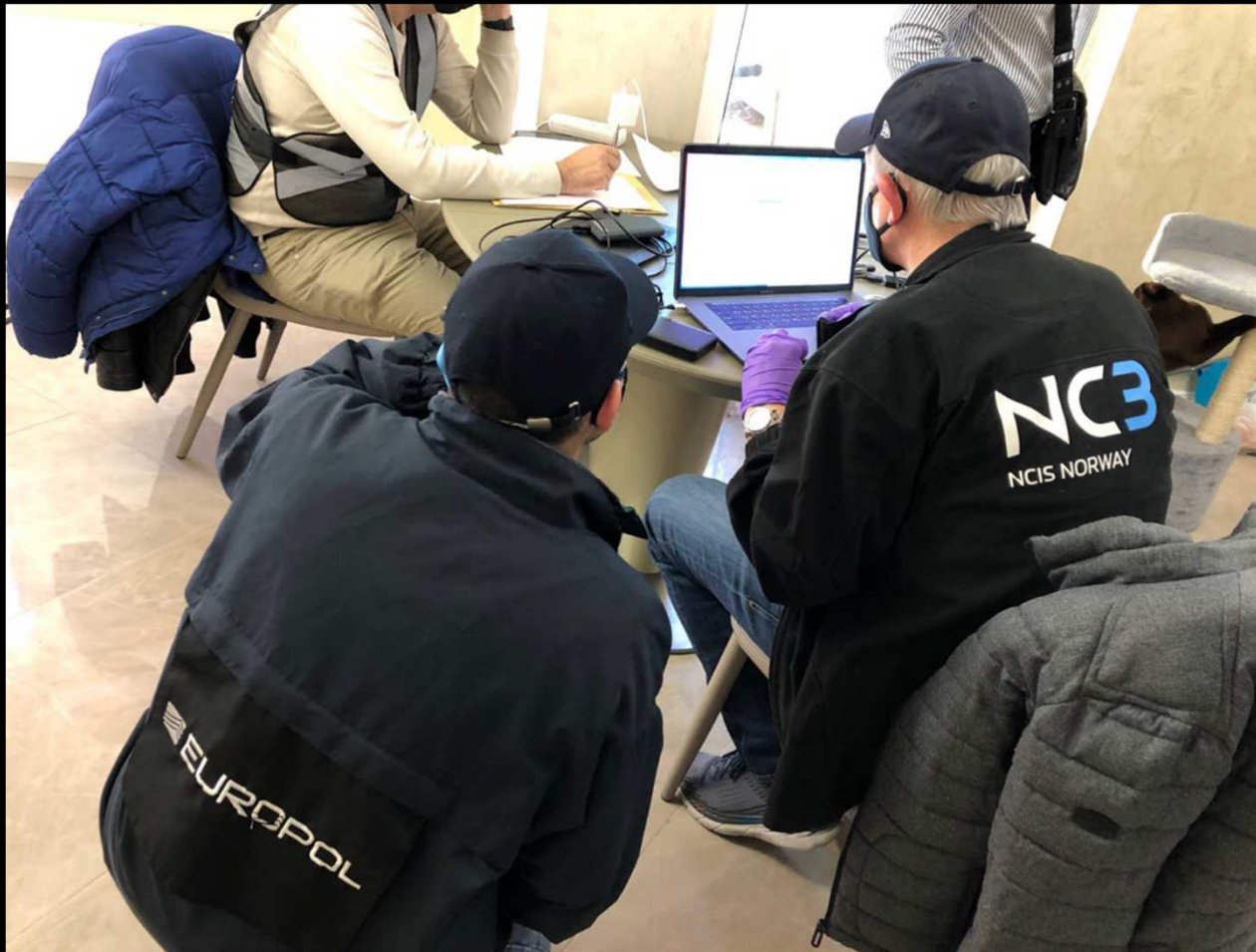
- Kriminelle nettverk samarbeider **over landegrensene**
- Kriminelle **kjøper tjenester** av hverandre og deler erfaringer
- Kryptovaluta – bruk av falske identitetspapirer, avanserte mixing transaksjoner, kriminelle betalinger over landegrensene og hvitvasking. Slik tjenester tilbys også i Norge.

Løsepengevirus - Ransomware



- Store mørketall
- BTC ofte betalingsmiddelet
- Rammer mange norske bedrifter

Løsepengevirus - Ransomware



- Erfaring med Hydro-saken, Lockergoga ransomware
- Norsk Hydro betalte ikke, men store kostnader for virksomheten.
- 71 land rammet, flere tusen virksomheter utsatt for skadevaren.
- Stor internasjonal etterforskning, med NC3 som koordinator.
- Flere forhold forebygget, både i Norge og utlandet.

Løsepengevirus – Utbyttet

Motparten:

- Kriminell organisert gruppe
- Utbyttet ender ofte i **Russland**, Ukraina og Kina
- Motparten kan være **statlig aktør** – Lazarus – Nord Koreansk hackergruppe.
- Utbyttet finansierer ny kriminalitet, øker profesjonaliteten og kan i verste fall brukes til **masseødeleggelsesvåpen**.

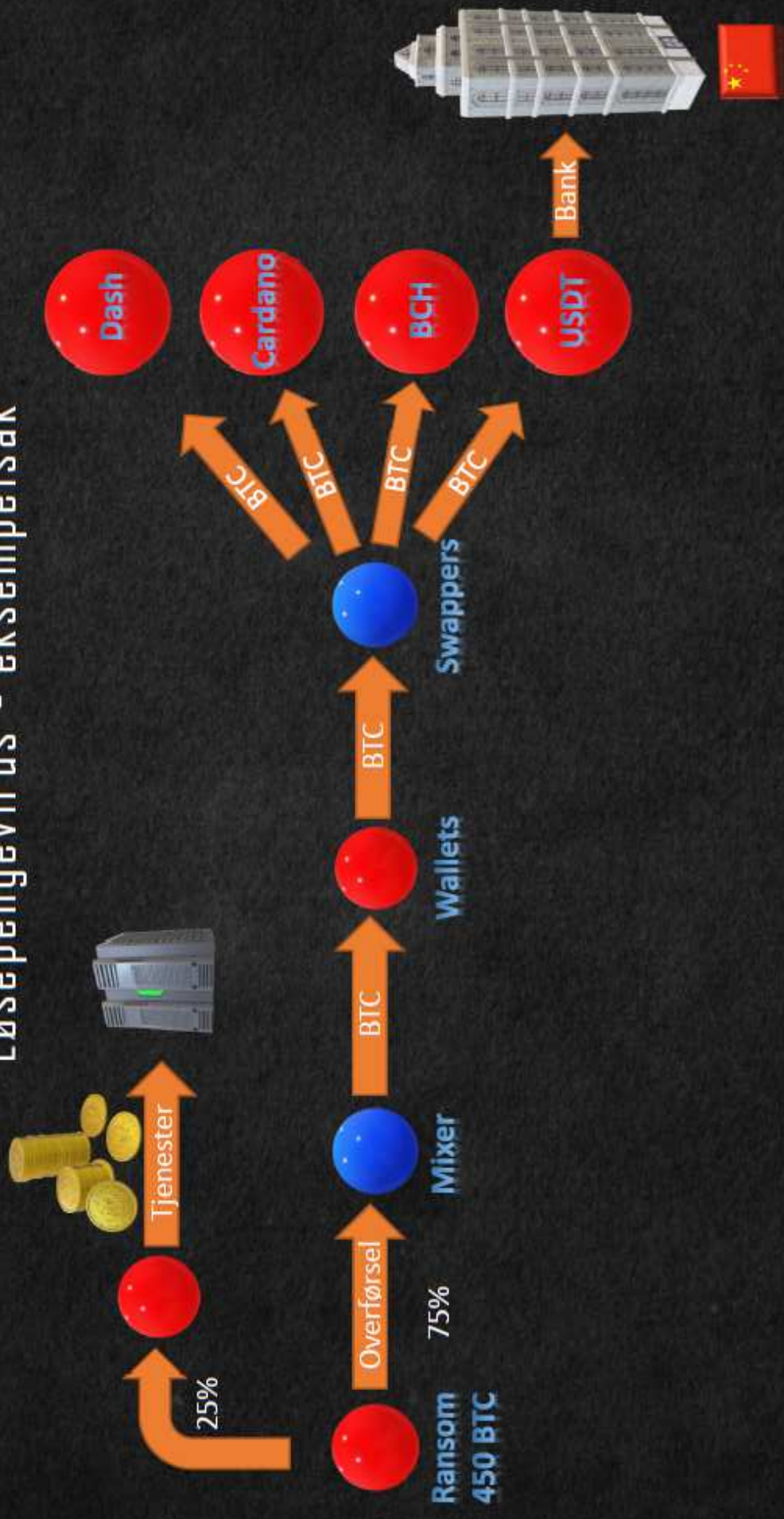
Hvitvaskingsloven:

§ 27. Gjennomføring av mistenkelig transaksjon

*(1) Rapporteringspliktige **skal ikke** gjennomføre mistenkelige transaksjoner før Økokrim er underrettet. Økokrim kan i særlige tilfeller forby gjennomføring av en transaksjon.*

(2) Dersom det er umulig å stanse transaksjonen, eller dersom stans av transaksjonen kan vanskeliggjøre undersøkelser av person som kan dra fordel av en mistenkelig transaksjon, skal Økokrim varsles umiddelbart etter at transaksjonen er gjennomført.

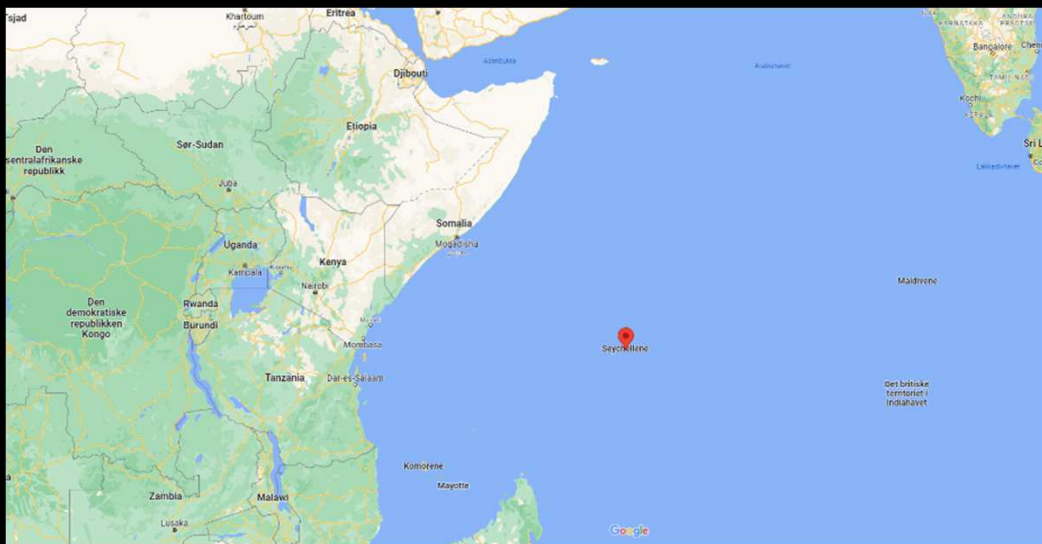
Løsepengevirus - eksempel sak



Utfordringer i etterforskningen

- Kryptovaluta utfordrer politiet på **kompetanse** og kapasitet
- **Ressurskrevende** saker, utenlandske aktører, kriminelle nettverk som operer i flere land.
- **Jurisdiksjon** – politiet er avhengig av informasjon fra kryptovaluta tjenester.

De største kryptovalutavekslerne registrert i skatteparadiser:



XXX in Seychelles is only registered as an International Business Company (IBC) under the name XXX, and it is not physically operating in Seychelles. We have attempted to communicate with them on previous occasions and they have not given us a feedback. As currently we have no laws to regulate Virtual Asset Service Providers (online platforms) we are not able to do anything further in regards to supplying the information requested. You must communicated directly with XXX to receive this. Please let us know if you require any further information or assistance with this matter.

Bankenes rolle med kryptovaluta – entry og exit til kryptovaluta:

Kriminelle med behov for å veksle fiat til kryptovaluta:

- Muldyr
- Falske identifikasjonspapirer
- VPN/ TOR
- Offeret i en tvangssituasjon: Ransomware m.fl
- Offeret er villedet: Investorbedrageri. Any desk.

Kriminelle med behov for å veksle kryptovaluta til fiat:

- Utenlandske tjenester. Coinbase, Binance m.fl
- Utenlandske betalingskort.

Hvordan kan bankene avdekke dette?

- Brå endring i transaksjonsmønster.
- Alder, kjønn.
- VPN/TOR deteksjon.
- KYC – snakk med kunden, har vedkommende kunnskap om kryptovaluta.

Tilslutt: Ansatte i bankene trenger **økt kunnskap** om kryptovaluta og tilgang til **sporingsverktøy**. Sporingsverktøy vil lett avsløre om kunder forsøker å skjule opprinnelsen til midlene.

Oppsummering:

- Kryptovaluta er **sporbart**
- **Sporene** ligger der til evig tid
- Sporene er lett tilgjengelig for politiet
- **Useriøse tjenester** en stor utfordring – politiet ønsker økt fokus på motpartsrisiko.
- Mixere, privacy coins og jurisdiksjon utfordrer.
- **Teknologien** utvikles raskt, vi må henge med i svingene.

Takk for oppmerksomheten!