

# KINS 2021

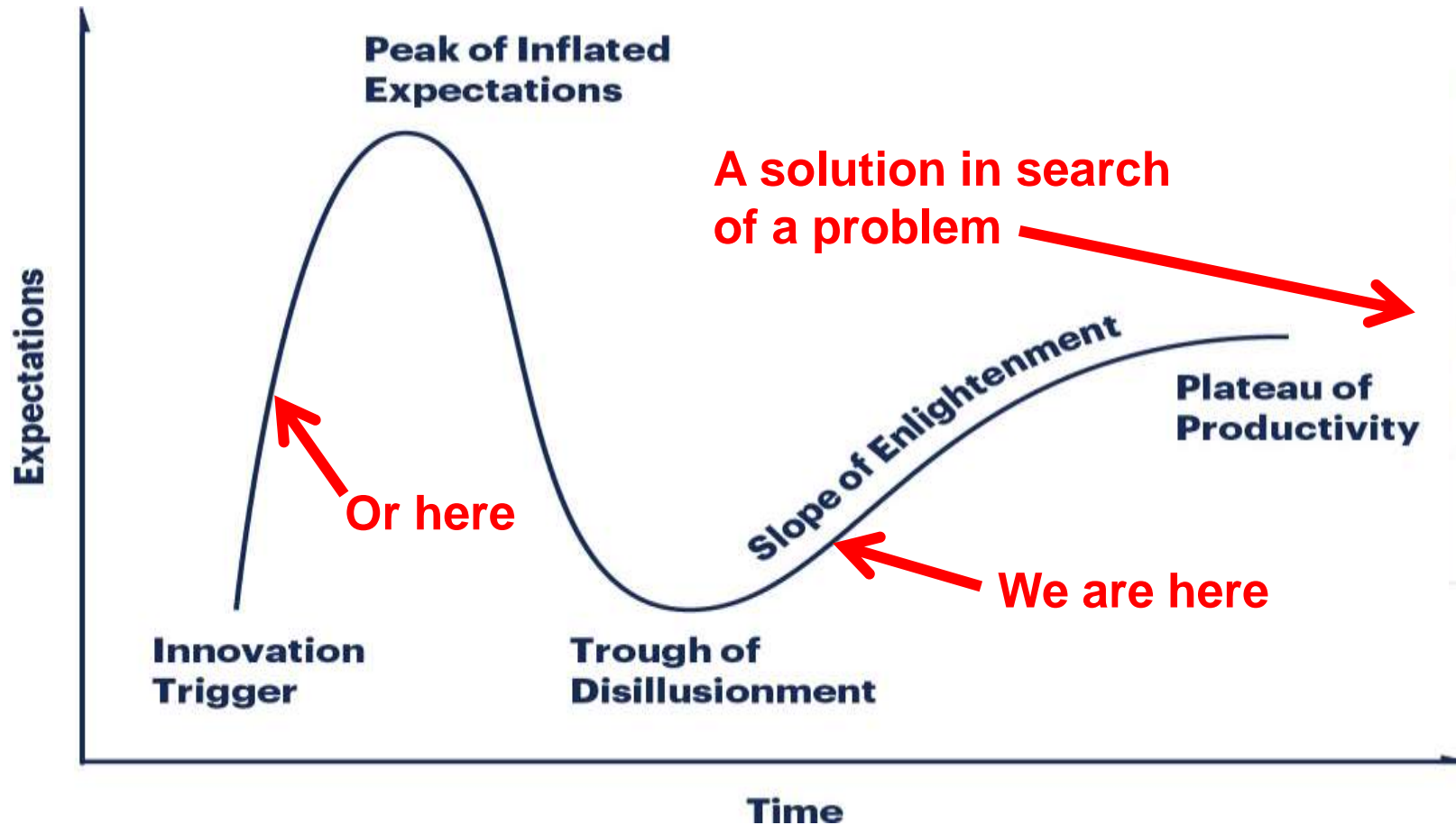
Blokkjeder - hemmer eller fremmer det personvernet?

Eirik Gulbrandsen, senioringeniør, Datatilsynet

21. oktober 2021



## Gartner Hype Curve





# 50+ BLOCKCHAIN REAL WORLD USE CASES

**GOVERNMENT**

Essentia develops world's first blockchain solution to manage international logistics hub together with Traffic Labs and the Finnish Government




**IDENTIFICATION**

Voter registration is being facilitated via a blockchain project in Switzerland spearheaded by Uport.



**MOBILE PAYMENTS**

The blockchain ledger that Ripple uses has been latched onto by a group of Japanese banks, who will be using it for quick mobile payments.




**INSURANCE**

A smart contract-based blockchain is being used by insurer American International Group Inc as a means of saving costs and increasing transparency.



**ENDANGERED SPECIES PROTECTION**

The protection of endangered species is being facilitated via a blockchain project that records the activities of these rare animals.




**CARBON OFFSETS**

IBM is using the Hyperledger Fabric blockchain in China to monitor carbon offset trading.



**ENTERPRISE**

Ethereum's blockchain can be accessed as a cloud-based service courtesy of Microsoft Azure.



**BORDER CONTROL**

Essentia has devised a border control system that would use blockchain to store passenger data in the Netherlands.




**SUPPLY CHAINS**

IBM and Walmart have partnered in China to create a blockchain project that will monitor food safety.



**HEALTHCARE**

A number of healthcare systems that store data on the blockchain have been pioneered including MedRec.



**SHIPPING**

Shipping is a natural fit for blockchain, and Maersk have been trialling a blockchain-based project within the maritime logistics industry.



**REAL ESTATE**

Blockchain is now being used to complete real estate deals, the first of which was conducted in Kiev by Propy.



**ENERGY**

Essentia is developing a test project that will help energy suppliers track the distribution of their resources in real time, whilst maintaining data confidentiality.



**LAND REGISTRY**

Land registry titles are now being stored on the blockchain in Georgia in a project developed by the National Agency of Public Registry.



**COMPUTATION**

Digital Currency Group are helping Amazon Web Services examine ways in which the distributed ledger technology can help improve database security.



**ADVERTISING**

New York Interactive Advertising Exchange has been experimenting with blockchain as a means of providing an ads marketplace for publishers.



**BORDER CONTROL**

Essentia is developing a blockchain project for border control that will allow customs agents to record passenger data from an array of inputs and safely store it.



**JOURNALISM**

Decentralized journalism, as enabled by blockchain technology, has the potential to prevent censorship and increase transparency, as Civil has shown.



**WASTE MANAGEMENT**

Waltonchain is using RFID technology to store waste management data on the blockchain in China.



**ENERGY**

Food importation is another industry where blockchain is proving its worth, with Louis Dreyfus Co trialling a soybean importation operation using this technology.



**DIAMONDS**

The De Beers Group is using blockchain to track the importation and sale of diamonds.



**FINE ART**

By storing certificates of authenticity on the blockchain, it's possible to dramatically reduce art forgeries, as one blockchain project is



**NATIONAL SECURITY**

For the past two years, the US Department of Homeland Security has been using blockchain to record and safely store data captured from its security cameras.



**TOURISM**

In a bid to boost its tourism economy, Hawaii is examining ways in which blockchain-based cryptocurrencies can be adopted throughout the US state.



**TAXATION**

In China, a tax-based initiative is using blockchain to store tax records and electronic invoices led by Miaocai Network.



**ENERGY**

Chile's National Energy Commission has started using blockchain technology as a way of certifying data pertaining to the country's energy usage as it seeks to update its electrical infrastructure.



**RAILWAYS**

Russian rail operator Novotrans is storing inventory data on a blockchain pertaining to repair requests and rolling stock.



**ENTERPRISE**

Google is building its own blockchain which will be integrated into its cloud-based services, enabling businesses to store data on it, and to request their own white label version developed by Alphabet Inc



**MUSIC**

Arbit is a blockchain-based project led by former Guns N Roses drummer Matt Sorum seeking a fairer way to reward musicians for their creative efforts.



**FISHING**

Blockchain technology has been used to provide a transparent record of where fish was caught, as a means of ensuring it was legally landed.



# Blokkjeder - hemmer eller fremmer det personvernet?



Hva er blokkjeder egentlig?

Kryptovaluta; Bitcoin, Ethereum og «10 000» andre...

Ethereum; Smart Contracts

NFT – Non-Fungible Tokens...



Hva må man tenke på i et personvernperspektiv?

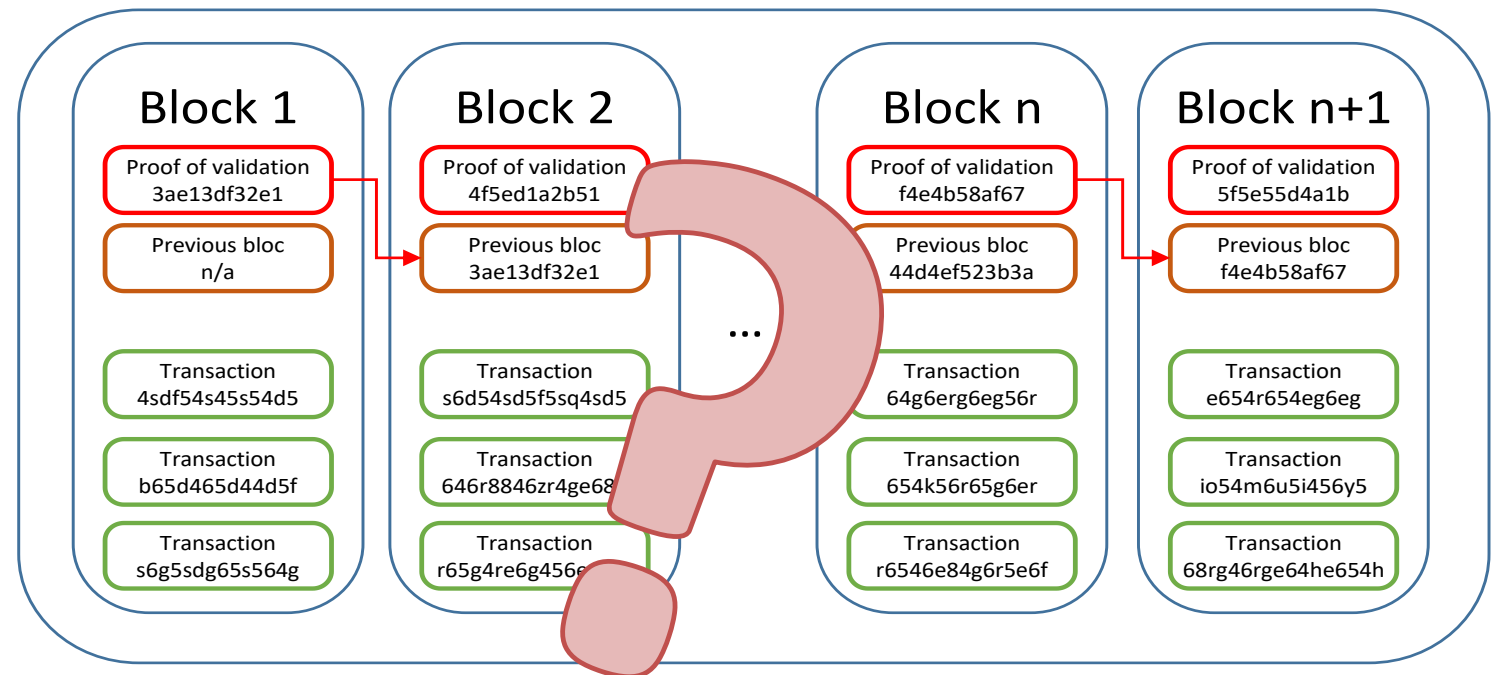
# Hva er en blokkjede?



A decentralized, distributed ledger wherein transactions are verified by and immutably\* recorded across the network, not a single central authority.

\* unchangeable object

En desentralisert, skrivbar database som ikke kan endres i ettertid.



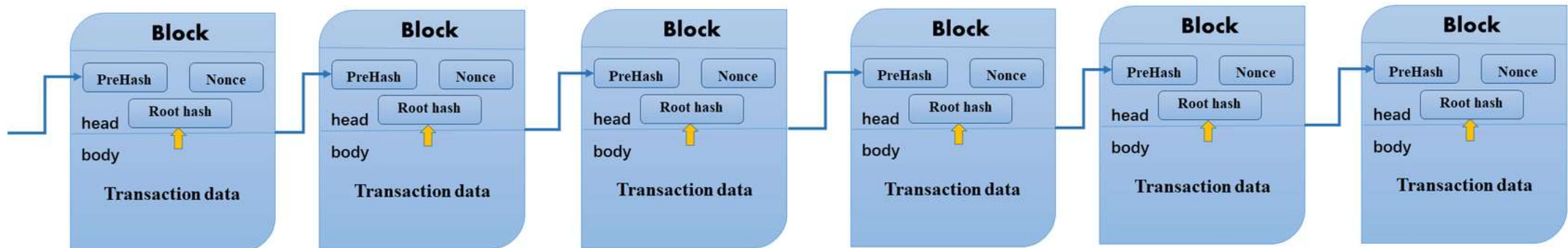
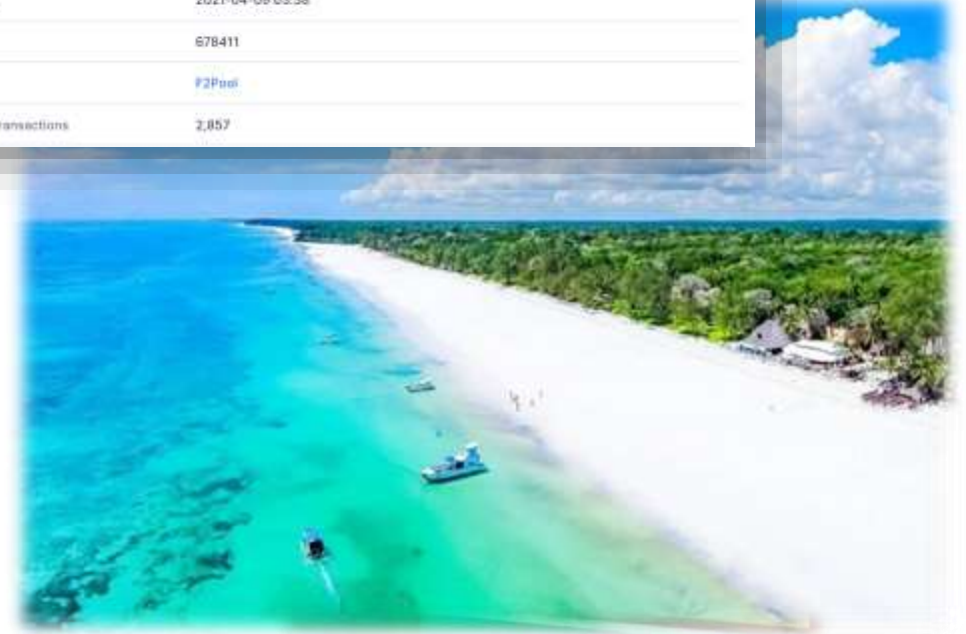


# Hva er en blokkjede?



- digitale signaturer signerer transaksjoner
  - privat nøkkel
  - offentlig nøkkel
- → «body» (defineres av «token»-format)
- hashfunksjoner (avtrykksfunksjon) + tidsstempling = blokkjede / tidskjede / tillitskjede
  - «låser» et sett med transaksjoner (SHA256)
- proof-of-work (bevis på benyttet datakraft)
  - en hash med en definert egenskap
    - ledende nuller – «00000000000000000006c9fa...» (19)
  - gjetting av riktig «nonce» (et tilfeldig tall) er «diamanten i gruen»

Hash	00000000000000000006c9fad44b7137429b238d99d50396df13f6c444f9194
Confirmations	2,736
Timestamp	2021-04-09 03:38
Height	678411
Miner	F2Pool
Number of Transactions	2,857



# Blokkjeder og smarte kontrakter

---

# Blokkjeder → smarte kontrakter

---



## Difficult to change

Changing smart contract processes is almost impossible, any error in the code can be time-consuming and expensive to correct.

## Possibility of loopholes

According to the concept of good faith, parties will deal fairly and not get benefits unethically from a contract. However, using smart contracts makes it difficult to ensure that the terms are met according to what was agreed upon.

## Third party

Although smart contracts seek to eliminate third-party involvement, it is not possible to eliminate them. Third parties assume different roles from the ones they take in traditional contracts. For example, lawyers will not be needed to prepare individual contracts; however, they will be needed by developers to understand the terms to create codes for smart contracts.

## Vague terms

Since contracts include terms that are not always understood, smart contracts are not always able to handle terms and conditions that are vague.

## Autonomy and savings

Smart contracts do not need brokers or other intermediaries to confirm the agreement; thus, they eliminate the risk of manipulation by third parties. Moreover, the absence of intermediary in smart contracts results in cost savings.

## Redundancy

All the documents stored on blockchain are duplicated multiple times; thus, originals can be restored in the event of any data loss.

## Safety and security

Smart contracts are encrypted, and cryptography keeps all the documents safe from infiltration.

## Speed

Smart contracts automate tasks by using computer protocols, saving hours of various business processes.

## Accuracy

Using smart contracts results in the elimination of errors that occur due to manual filling of numerous forms.





## Smart Contract Platforms

- Ethereum – Simple contracts using Solidity; widely adopted
- EOS – High throughput; removal of transaction fees; scalability; DPOS (democracy as a POS); WASM language
- Stellar – Virtually no cost; connects banks, payment systems and people; five-second confirmation time; DTI issues
- Cardano – functional programming approach; robust platform; Plutus/Haskell
- Neo – “Ethereum of China”; smart economy; javascript
- Hyperledger Fabric – Linux Foundation; modular architecture; scalable

<https://blockgeeks.com/guides/different-smart-contract-platforms/>



## Example of a Smart Contract

```
contract Mortal {
    /* Define variable owner of the type address */
    address owner;

    /* This function is executed at initialization and sets the owner of the contract */
    function Mortal() { owner = msg.sender; }

    /* Function to recover the funds on the contract */
    function kill() { if (msg.sender == owner) selfdestruct(owner); }
}

contract Greeter is Mortal {
    /* Define variable greeting of the type string */
    string greeting;

    /* This runs when the contract is executed */
    function Greeter(string _greeting) public {
        greeting = _greeting;
    }

    /* Main function */
    function greet() constant returns (string) {
        return greeting;
    }
}
```

<https://www.ethereum.org/greeter>

Solidity is a contract-oriented, high-level language for implementing smart contracts. It was influenced by C++, Python and JavaScript and is designed to target the Ethereum Virtual Machine (EVM)



## Features of a Smart Contract

Smart Contracts are automated, self-executing contracts with specific instructions written on its code (in the blockchain) which get executed when certain conditions are met:

- Deterministic – Same output given the same inputs
- Terminable – Predetermined steps, fees or completeness
- Isolated – Preventing tainting of entire ecosystem
  
- Electronic agreement
- Uses blockchain technology and coding
- No third party (TI) required to validate contract

*<https://blockgeeks.com/guides/different-smart-contract-platforms/>*

# Blokkjeder og NFT (non-fungible tokens)

---



# Blokkjeder og NFT (non-fungible tokens)



ERC20 / ERC 721 / ERC 1155



# Blokkjeder og NFT (non-fungible tokens)



ERC20 / ERC 721 / ERC 1155



MATTEO GIANPIETRO ZAGO

# Blokkjeder og personvern

---



## Risiko knyttet til blokkjedeteknologien:

- Generelle (standardisering)
- Sikkerhetsrelaterte (KIT)
- Juridiske (databehandler, håndhevelse av rettigheter)

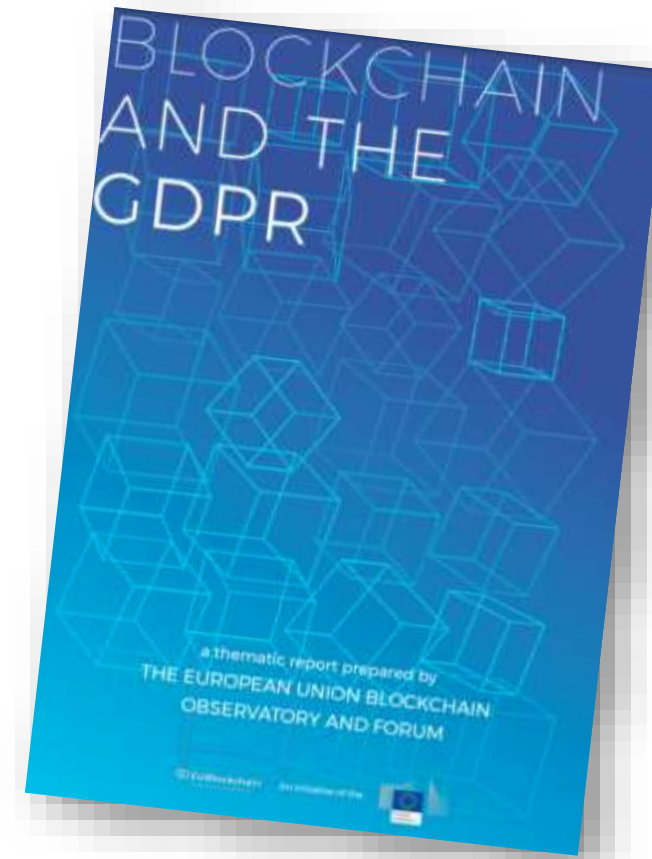




- EDPBs Technology Expert Subgroup jobber med å utarbeide en veileder om Blockchain-teknologien
- Sentrale problemstillinger:
  - Behandling og ansvar
  - Forenlighet med personvernprinsippene
  - Innebygd personvern
  - Risiko og DPIA
  - De registrertes rettigheter



\* European Data Protection Board



[https://www.eublockchainforum.eu/sites/default/files/reports/20181016\\_report\\_gdpr.pdf](https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf)



- Personopplysninger kan lagres i blockchain:
  - I brukeridentifikator (f eks digitale signaturer)
  - I payload data («body»)
- Utfordring: Personopplysninger lagret på en åpen blokkjede vil alltid være synlig for alle brukere
  - Vurder nødvendigheten av de ulike arkitektoniske elementene i blokkjeder
  - Personopplysninger bør i størst mulig grad lagres «off-chain»
- Hvem er behandlingsansvarlig?
  - Noder verifiserer gyldigheten av «blokker»
  - Aktører samler inn opplysninger brukt i transaksjoner og legger det inn i blokkjeden



- Teknologien er nøytral ift. flere prinsipper:
  - Rettferdighet, åpenhet, formålsbestemthet, riktighet
  - Ikke teknologien i seg selv som utgjør en utfordring, opp til behandlingsansvarlige
- Utfordrende ift.:
  - Dataminimering (lagring over tid)
  - Lagringsbegrensning (sletting, f eks når formål er oppnådd)
  - Integritet og tilgjengelighet (inkl nødløsninger)
- Om lovlighetsprinsippet:
  - Ikke samme behandlingsgrunnlag for alle transaksjoner
  - Bevisstgjøre brukere av konsekvensen av «åpen bok»



- Innsynsrett og dataportabilitet ikke problematisk
- Rett til sletting og rett til å protestere
  - Behandles samlet fordi ved protest må opplysninger slettes
  - Sletting kan muligens oppnås ved å gjøre personopplysningene praktisk utilgjengelige
    - Slette referansenøkkel – spørsmål om dette tilsvarer reell sletting
- Rett til retting
  - Ikke mulig å endre opplysninger som allerede er i blokkjeden
  - Opplysninger må eventuelt «slettes» og så lage ny transaksjon med korrigerede opplysninger.





- Blokkjedeteknologien har iboende egenskaper som kan være vanskelig å forene med kravet om innebygd personvern
- Kan være mulig å løse utfordringene case by case ved å ta i bruk key design and default elements fra veileder om innebygd personvern.



## Programvareutvikling med innebygd personvern

Denne veilederen skal hjelpe norske virksomheter å forstå og etterleve kravet om innebygd personvern i personvernregelverket. Den er utarbeidet i samarbeid med sikkerhetsekspertene og programutviklere i privat og offentlig sektor. Veilederen har også vært på høring i flere virksomheter og organisasjoner.

### 1. Innledning

### 2. Innebygd personvern - hva er det?

### 3. Oppplæring

### 4. Krav

### 5. Design

### 6. Koding

### 7. Test

### 8. Produksjonssetting

### 9. Forvaltning



## Blockchain krever DPIA (Data Protection Impact Assessment)

- “Innovative use or applying new technological or organisational solutions” utgjør en sannsynlighet for høy risiko jf. DPIA-veilederen



### Vurdering av personvernkonsekvenser (DPIA)

En vurdering av personvernkonsekvenser (Data Protection Impact Assessment - *DPIA*) skal sikre at personvernet til de som er registrert i løsningen ivaretas. Dette er en plikt etter personvernregelverket. Artikkel 35 definerer når det er påkrevd å gjøre en DPIA, hva den skal inneholde og hvem som skal gjennomføre den.

<https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdere-personvernkonsekvenser/vurdering-av-personvernkonsekvenser/>

## Innhold

1. Innledning
2. Når må man gjennomføre en vurdering av personvernkonsekvenser?
3. Risiko og risikovurdering
4. Når er det høy risiko?
5. Hvordan gjennomføre en DPIA?
6. Når skal det gjennomføres forhåndsdrøftelse med Datatilsynet?
7. Eksempler på eksisterende rammeverk i EU

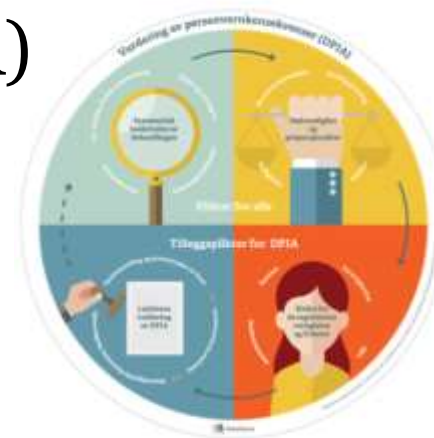


Blokkjeder har egenskaper som både fremmer og utfordrer personvern

Utfordringer kan adresseres gjennom arkitektur og løsningsdesign

Bruk prinsippene beskrevet i veileder «Innebygd personvern»

Bruk av blokkjeder vil høyst sannsynlig kreve personvernkonsekvensutredning (DPIA)



Eirik Gulbrandsen, Senioringeniør, Datatilsynet  
eirik.gulbrandsen@datatilsynet.no



postkasse@datatilsynet.no  
Telefon: +47 22 39 69 00

**datatilsynet.no**  
**personvernbloggen.no**