

BLOCK CHAIN FOR AGRI FOOD EDU

modul2

Blockchains byggesten og blockchain mekanisme

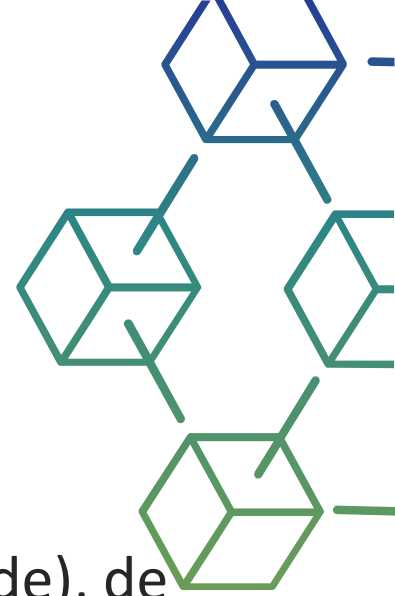
Blockchain til AgriFood Åbn uddannelsesressourcer
© 2023/2024 af Blockchain for AgriFood Konsortiet
er licenseret under [CC BY-SA 4.0](https://creativecommons.org/licenses/by-sa/4.0/)



Finansieret af Den Europæiske Union. Synspunkter og holdninger, der kommer til udtryk, er udelukkende forfatterens/forfatternes og er ikke nødvendigvis udtryk for Den Europæiske Unions eller Det Europæiske Forvaltningsorgan for Uddannelse og Kulturs (EACEA) officielle holdning. Hverken den Europæiske Union eller EACEA kan holdes ansvarlig herfor.

modulbeskrivelse

Modulet "Blockchains byggesten og blockchain-mekanismen" inkluderer principperne for skabelse af blockchain (hvad er en blok, og hvad er en kæde), de grundlæggende funktioner i det traditionelle, decentraliserede og distribuerede koncept for databaserne og egenskaberne og kravene af kryptografi og hash-funktioner og har som resultat. Der er også inkluderet en forklaring på forskellen mellem bevis på arbejde og bevis for staten og de vigtigste fordele ved blockchain i modulet.

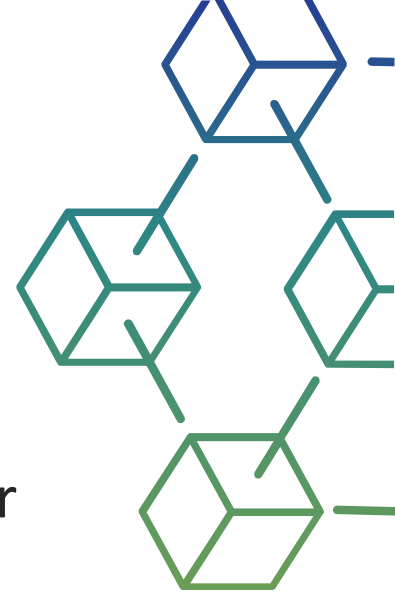


LæringResultater

Kandidater fra modulet vil erhverve grundlæggende teoretisk viden inden for blockchain-skabelse og krav til kryptografiske og hashing-funktioner. Viden fastlægges af et casestudie verificeret af en quiz.

Resultaterne er:

- Modul med undervisningsmateriale
- Casestudie
- Interaktiv aktivitet
- Quiz



indhold

01 Indledning

02 Grundlæggende komponenter: blokke, kryptografisk hashing, decentralisering

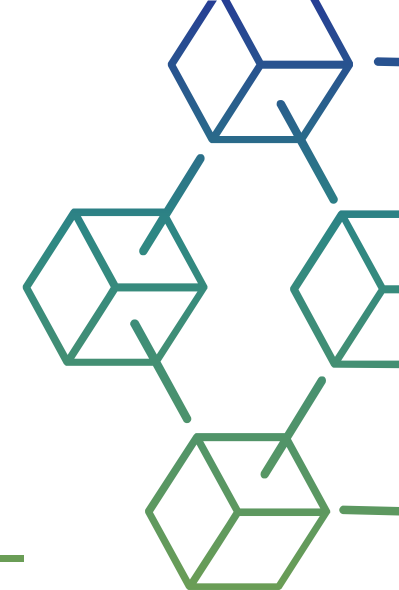
03 Hvaderde nøgle komponenter af deblockchain?

04 Hvaderde fordele af deblockchain?

05 Hvad er de forskel mellemen database og en blockchain?



Finansieret af Den Europæiske Union. Synspunkter og holdninger, der kommer til udtryk, er udelukkende forfatterens/forfatternes og er ikke nødvendigvis udtryk for Den Europæiske Unions eller Det Europæiske Forvaltningsorgan for Uddannelse og Kulturs (EACEA) officielle holdning. Hverken den Europæiske Union eller EACEA kan holdes ansvarlig herfor.



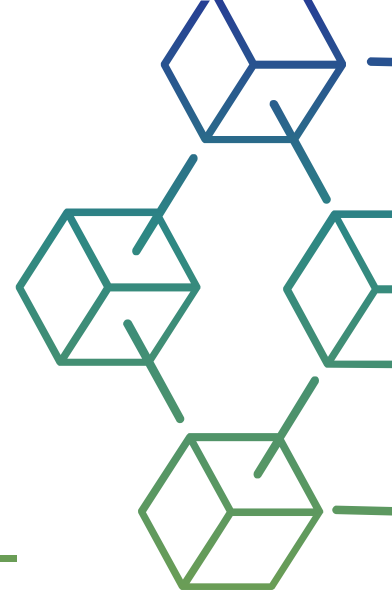
indhold

06 Hvordan erblockchainanderledes fra desky?

07 Hvad erblockchain som enservice?

08 Use case

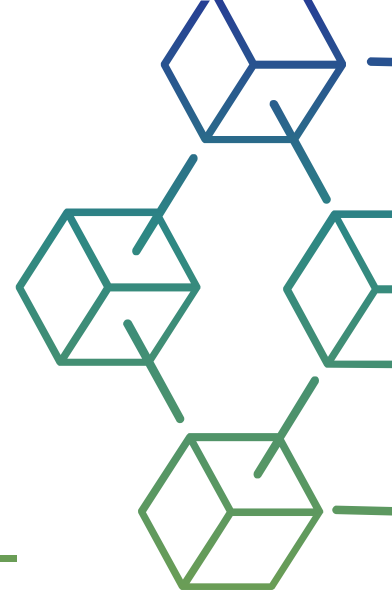
09 Konklusion



indhold

10 Interaktivlæringaktivitet

11 Quiz



01

INTRODUKTION TIL modul2

Byggestenene i blockchain
og blockchain mekanisme



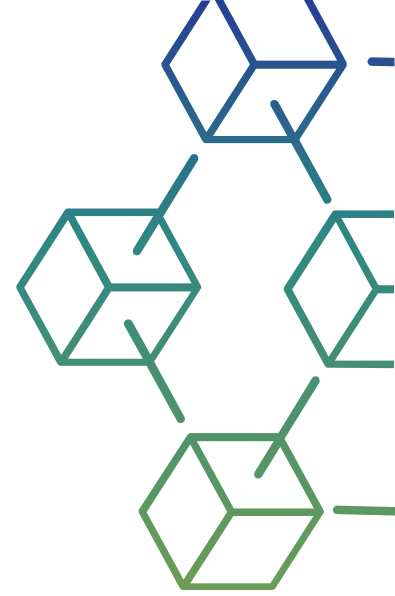
Indledning

Hvad er blockchain teknologi?

Blockchain teknologier er en fremskredendatabasemekanisme, der tillader gennemsigtig information deling inden for et forretningsnetværk. En blockchain-database består af data i blokke, der er forbundet sammen i en kæde.

Data er kronologisk konsekvent, fordi du ikke kan slette eller modificere den kæde uden konsensus fra det netværk. Som et resultat, kan du bruge blockchain-teknologi til at skabe en uforanderlig eller uforanderlig hovedbog for sporing af ordrer, betalinger, regnskaber, og andre transaktioner.

De systemer har bygget mekanismer, der forhindrer uberettiget transaktioner og sikrer konsistens i delte udsigt af disse transaktioner.



Indledning

Byggestenene i blockchain og blockchain mekanisme

Blockchain-byggesten og blockchain-mekanisme er nøglebegreber inden for digitale økosystemer og kryptovalutaer.

Blockchain er en teknologi, der gør det muligt at registrere transaktioner og begivenheder i et decentraliseret og uforanderligt system.

De grundlæggende byggesten i blockchain er følgende elementer:

- Blokke
- Uddelt hovedbog
- Kryptografi
- Konsensusmekanisme
- Uforanderlighed



Indledning

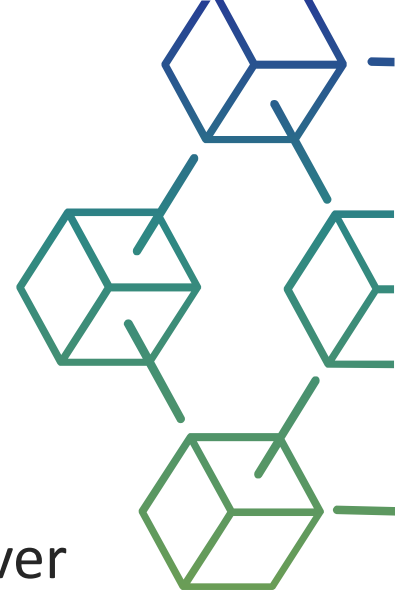
Byggestenene i blockchain og blockchain mekanisme

BLOKKE

Blockchain består af en kæde af blokke, hvor hver blok indeholder en liste over transaktioner og en unik identifikator (hash) for den foregående blok. Dette sikrer dataenes integritet.

DISTRIBUERET REGNSKAB

Blockchain er lagret på tusindvis af computere (noder) rundt om i verden. Hver node har en kopi af hele blockchainen, hvilket øger dens modstand mod udfald og angreb.



Indledning

Byggestenene i blockchain og blockchain mekanisme

KRYPTOGRAFI

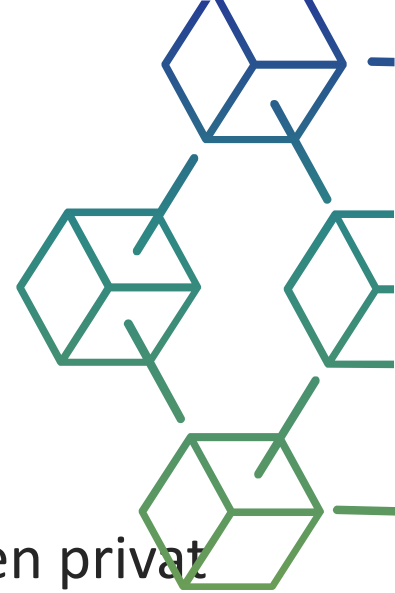
Asymmetrisk kryptografi bruges til at sikre transaktioner. Hver deltager har en privat og offentlig nøgle, som muliggør verifikation og signering af transaktioner.

KONSENSUSMEKANISME

Blockchain kræver noder for at opnå konsensus om gyldige transaktioner. Dette opnås normalt gennem forskellige konsensusalgoritmer såsom bevis for arbejde (PoW) eller bevis for indsats (PoS).

jegFORBYLDIGHED

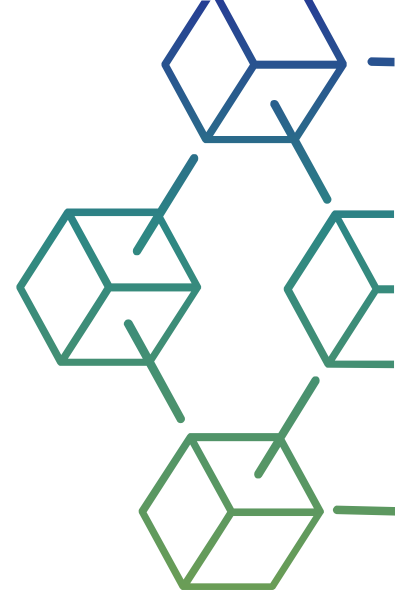
Når først data er lagret i blockchain, kan det ikke nemt ændres. Dette sikrer tillid og gennemsigtighed.



Indledning

Byggestenene i blockchain og blockchain mekanisme

- Blockchain-mekanismen sikrer dataintegritet og sikrer, at transaktioner er uomtvistelige.
- Blockchain har brede applikationer ud over kryptovaluta, herunder i finans, forsyningskæde, sundhedspleje og mange andre industrier.
- Dets fremtid afhænger af samfunds og virksomheders evne til at innovere og bruge sit potentiale til at løse reelle problemer og ændre den digitale verden.



02

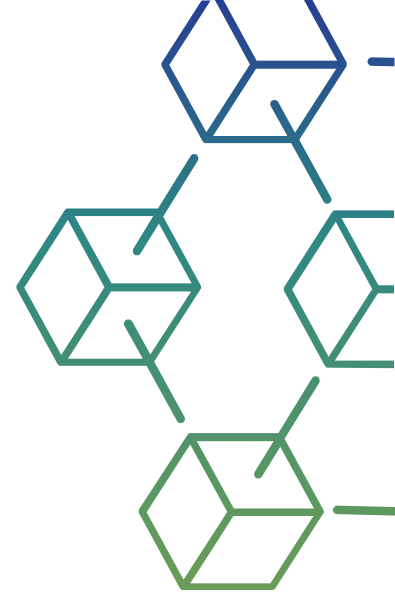
Grundlæggende
komponenter: blokke,
kryptografisk hashing,
decentralisering



Grundlæggende komponenter: blokke, kryptografisk hashing, decentralisering

Hvordan fungerer en Blockchain?

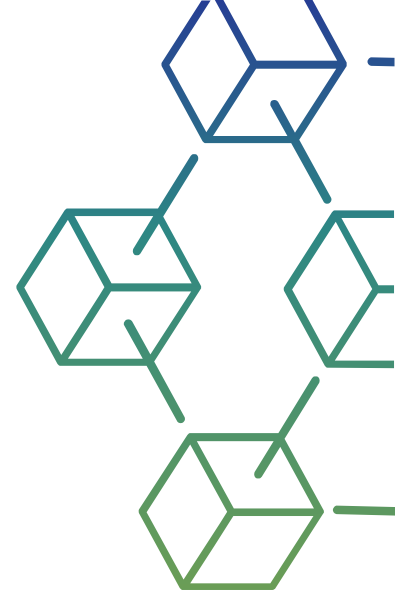
- Hver transaktion eller dataindtastning, kendt som en "blok", er sikkert forbundet med den forrige gennem kryptografisk hashing, hvilket skaber en kontinuerlig og manipulationssikker kæde af information.
- Fordi der ikke er nogen måde at ændre en blok på, er den eneste nødvendige tillid på det punkt, hvor en bruger eller et program indtaster data. Dette aspekt reducerer behovet for betroede tredjeparter, som normalt er revisorer eller andre mennesker, der tilføjer omkostninger og laver fejl.



Grundlæggende komponenter: blokke, kryptografisk hashing, decentralisering

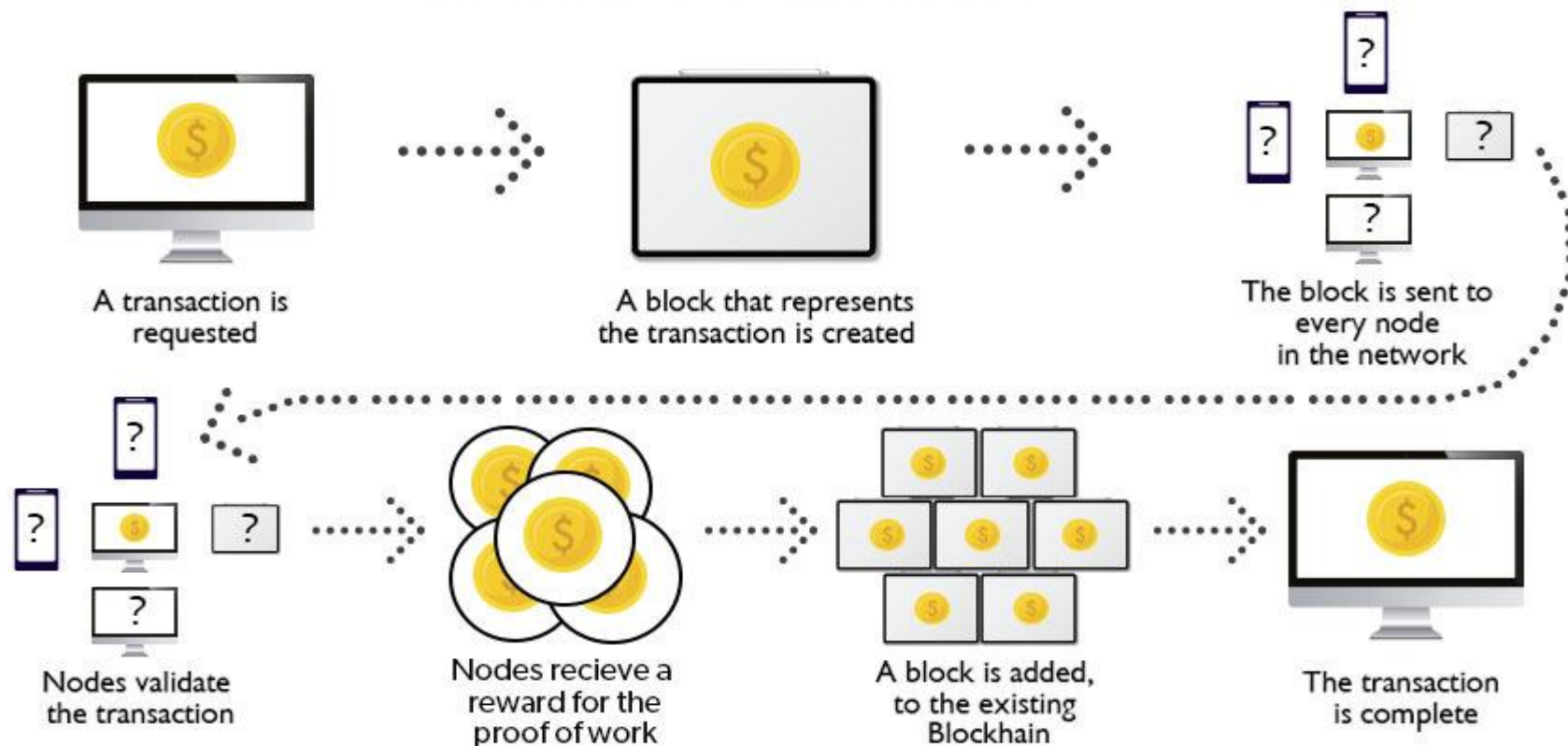
En blockchain består af programmer kaldet scripts, der udfører de opgaver, du normalt ville gøre i en database: Indtastning og adgang til information og lagring og lagring af dem et sted. En blockchain er distribueret, hvilket betyder, at flere kopier er gemt på mange maskiner, og de skal alle matche for at den er gyldig.

Blockchain samler **transaktion** oplysninger og indtaster dem i en **blok**, som en celle i et regneark, der indeholder information. Når den er fuld, køres informationen gennem en **krypteringsalgoritme**, som skaber et hexadecimalt tal kaldet **hash**



Grundlæggende komponenter: blokke, kryptografisk hashing, decentralisering

How Blockchain Works?

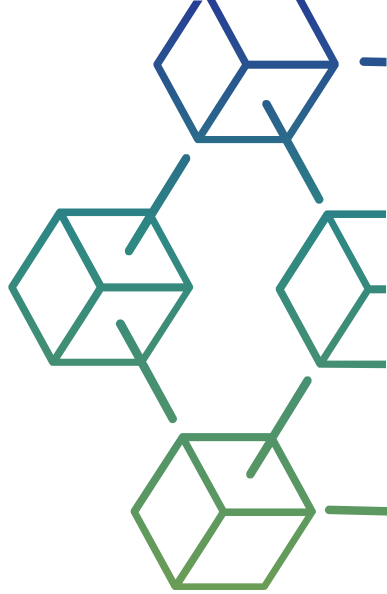


Figur 1 Hvordan blockchain fungererer (Kilde:<https://www.geeksforgeeks.org/how-does-the-blockchain-work/>)

Grundlæggende komponenter: blokke, kryptografisk hashing, decentralisering

Transaktionsprocessen i en blockchain kan opsummeres som følger:

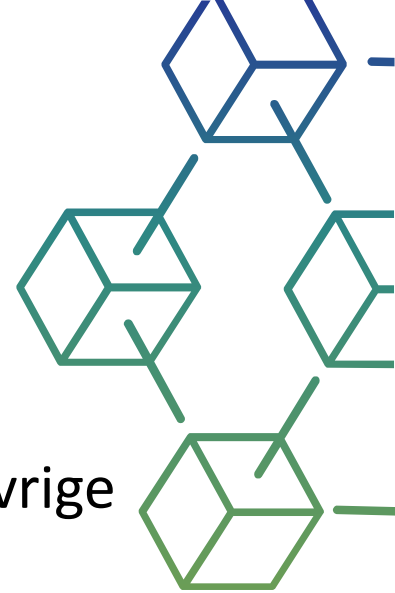
1. Facilitering af en transaktion
2. Verifikation af transaktion
3. Dannelse af en ny blok
4. Konsensus algoritme
5. Tilføjelse af den nye blok til blockchain
6. Transaktion gennemført



Grundlæggende komponenter: blokke, kryptografisk hashing, decentralisering

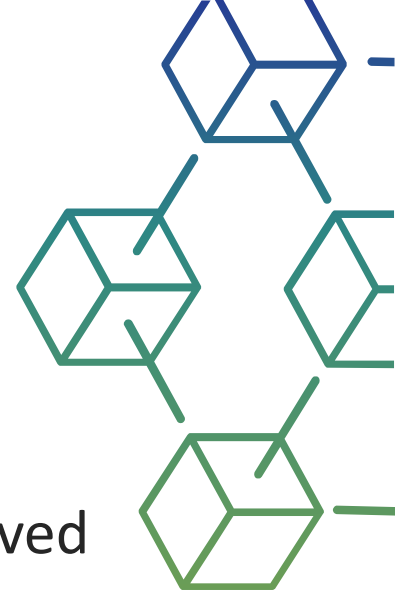
Hashen indtastes derefter i den følgende blokoverskrift og krypteres med de øvrige oplysninger i blokken. Dette skaber en række blokke, der er kædet sammen.

Transaktioner følger en bestemt proces, afhængigt af den blockchain, de finder sted på. For eksempel, på Bitcoins blockchain, hvis du starter en transaktion ved hjælp af din cryptocurrency-pung - applikationen, der giver en grænseflade til blockchain - starter det en sekvens af begivenheder.

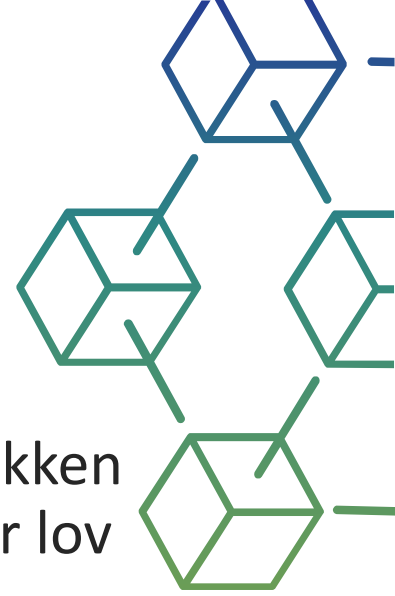


Grundlæggende komponenter: blokke, kryptografisk hashing, decentralisering

- 1. Facilitering af en transaktion:** En ny transaktion kommer ind i blockchain-netværket. Al den information, der skal transmitteres, er dobbeltkrypteret ved hjælp af offentlige og private nøgler.
- 2. Verifikation af transaktion:** Transaktionen overføres derefter til netværket af peer-to-peer-computere fordelt over hele verden. Alle noder på netværket vil tjekke for gyldigheden af transaktionen, f.eks. om en tilstrækkelig saldo er tilgængelig til at udføre transaktionen.
- 3. Dannelse af en ny blok:** I et typisk blockchain-netværk er der mange noder, og mange transaktioner bliver verificeret ad gangen. Når transaktionen er verificeret og erklæret en legitim transaktion, vil den blive tilføjet til mempool. Alle de verificerede transaktioner på en bestemt node danner en mempool og så mangemempoolsdanne en blok.



Grundlæggende komponenter: blokke, kryptografisk hashing, decentralisering

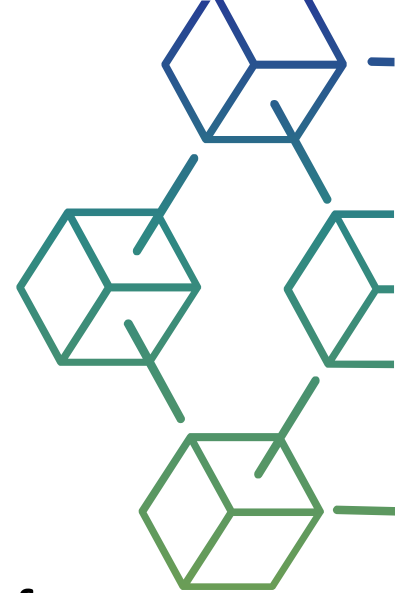


- 6. Konsensusalgoritme:** De noder, der danner en blok, vil forsøge at tilføje blokken til blockchain-netværket for at gøre den permanent. Men hvis hver node får lov til at tilføje blokke på denne måde, vil det forstyrre blockchain-netværkets funktion.
- 7. Tilføjelse af den nye blok til blockchain:** Efter at den nyoprettede blok har fået sin hashværdi og er autentificeret, er den nu klar til at blive tilføjet til blockchainen. I hver blok er der en hashværdi af den forrige blok, og det er sådan blokkene er kryptografisk forbundet med hinanden for at danne en blockchain. En ny blok bliver tilføjet til den åbne ende af blockchain.
- 8. Transaktion gennemført:** Så snart blokken er tilføjet til blockchain, er transaktionen gennemført, og detaljerne om denne transaktion gemmes permanent i blockchain. Alle kan hente detaljerne om transaktionen og bekræfte transaktionen.

Sammenligning med traditionelle databaser

De traditionelle databaser er centraliserede, foranderlige og optimeret til højhastighedsdatabehandling, mens blockchains er decentraliserede, uforanderlige og fokuserede på at give tillid og gennemsigtighed gennem konsensusmekanismer. Valget mellem de to afhænger af de specifikke behov for en given applikation.

- *Centralisering vs. decentralisering*
- *DataStruktur*
- *AdgangKontrollere*
- *Konsensus Mekanisme*
- *Uforanderlig vs. Foranderlig Data*
- *Transaktion Hastighed og Skalerbarhed*
- *Bruge Sager*

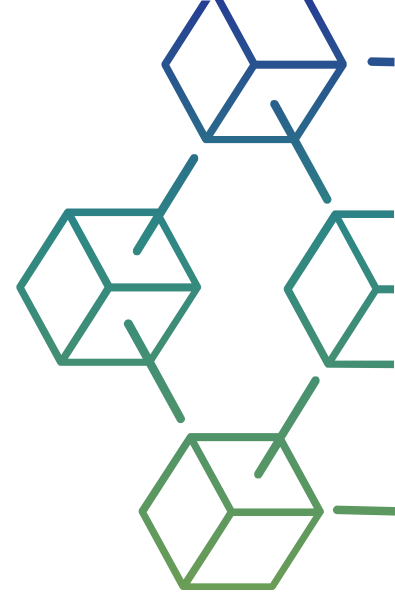


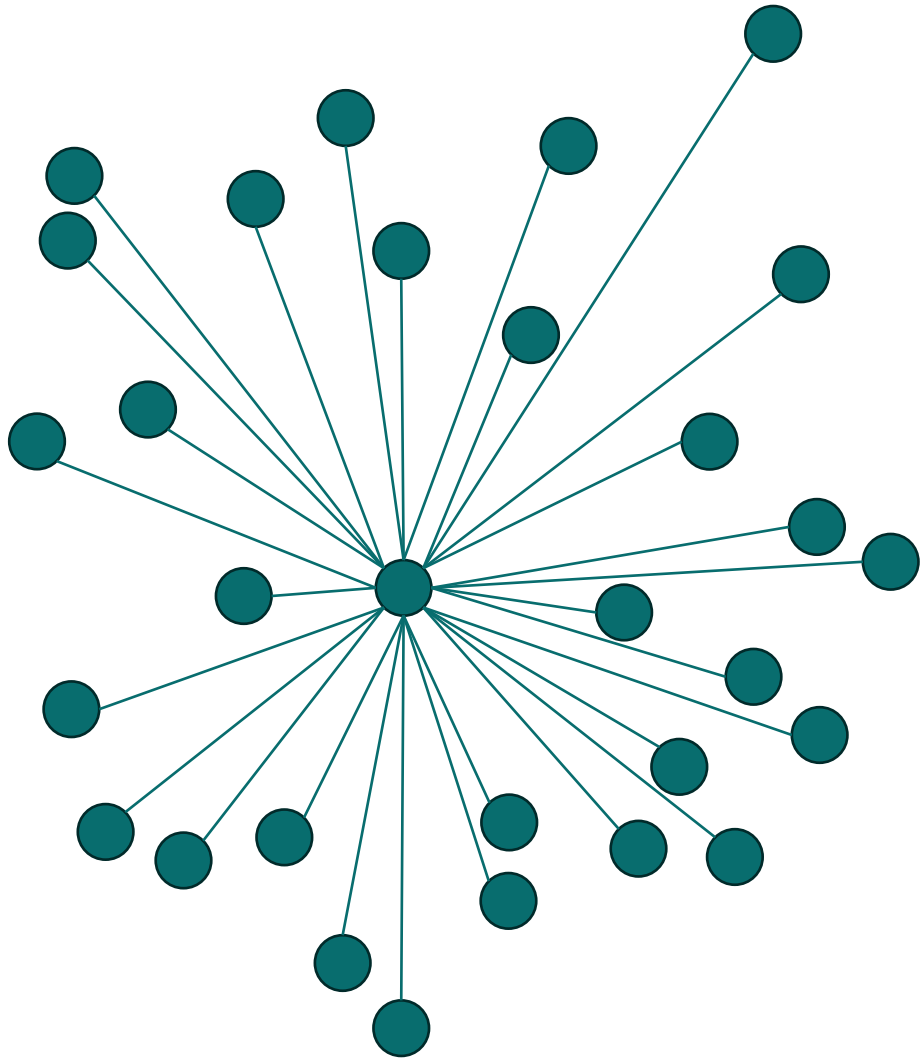
Sammenligning med traditionelle databaser

Centralisering vs. decentralisering

Traditionelle databaser: Traditionelle databaser er centraliserede systemer, hvor en enkelt enhed (f.eks. en virksomhed eller organisation) har kontrol over databasen. De er afhængige af en central server eller en klynge af servere til at administrere og gemme data.

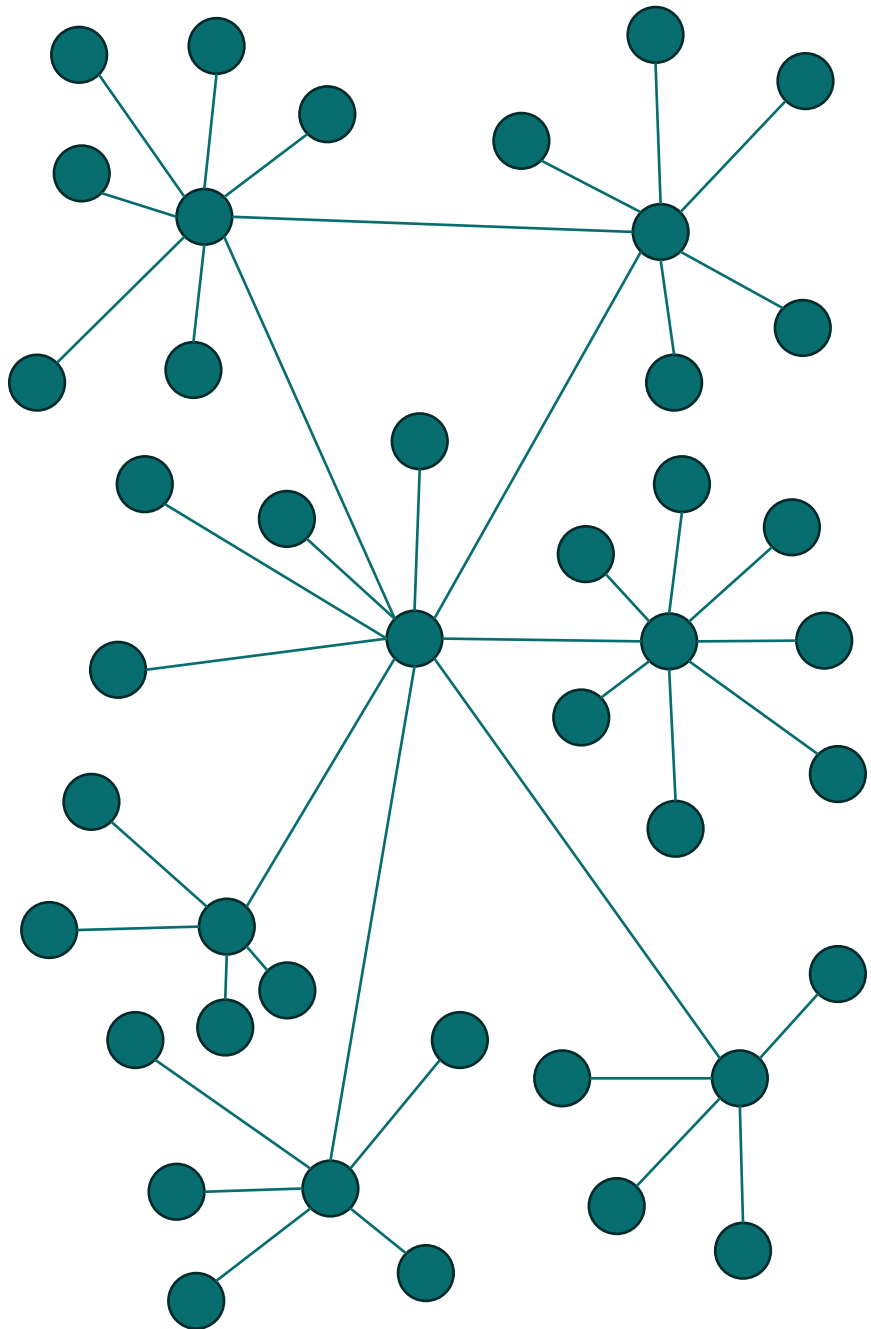
Blockchain: Blockchains er decentraler netværk, hvor data er fordelt på tværs af flere noder (computere) i et netværk. Der er ingen central autoritet eller enkelt kontrolpunkt, hvilket gør dem modstandsdygtige over for censur og manipulation.





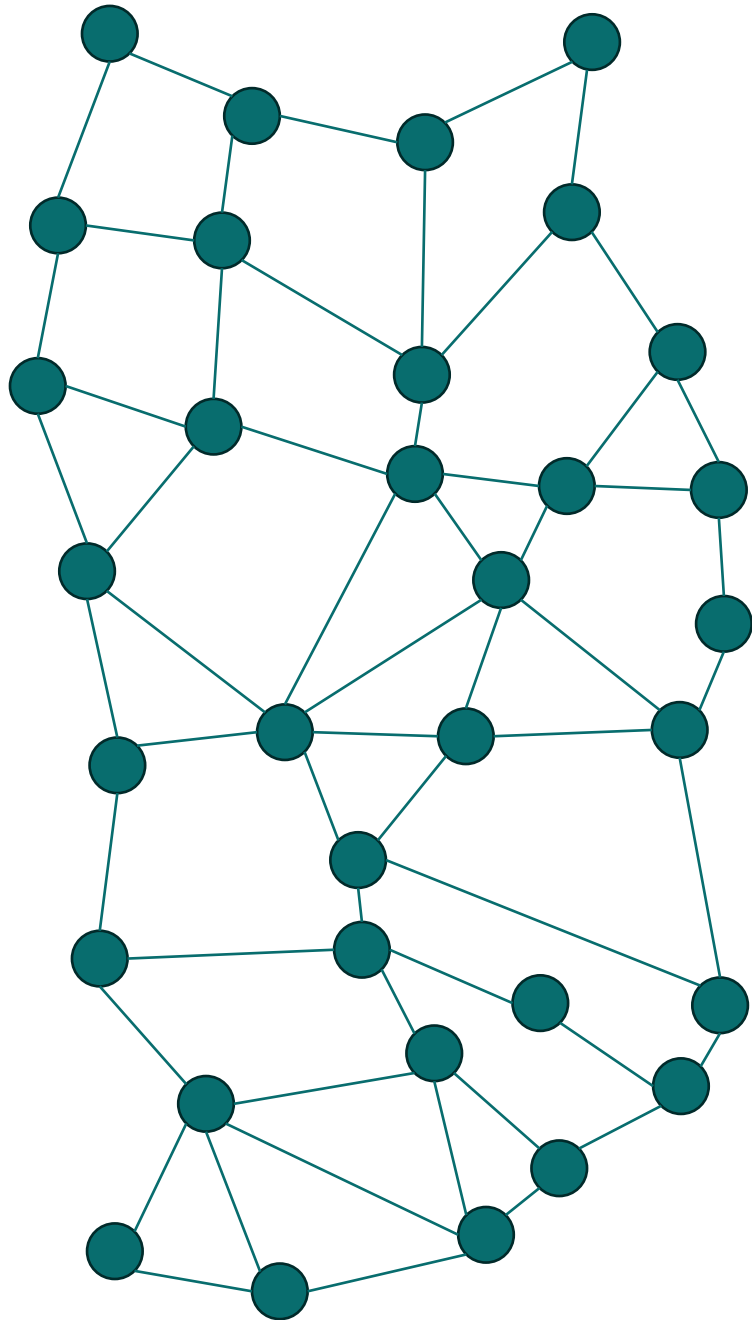
Centraliseret

*Alle noder er forbundet
under en enkelt myndighed.*



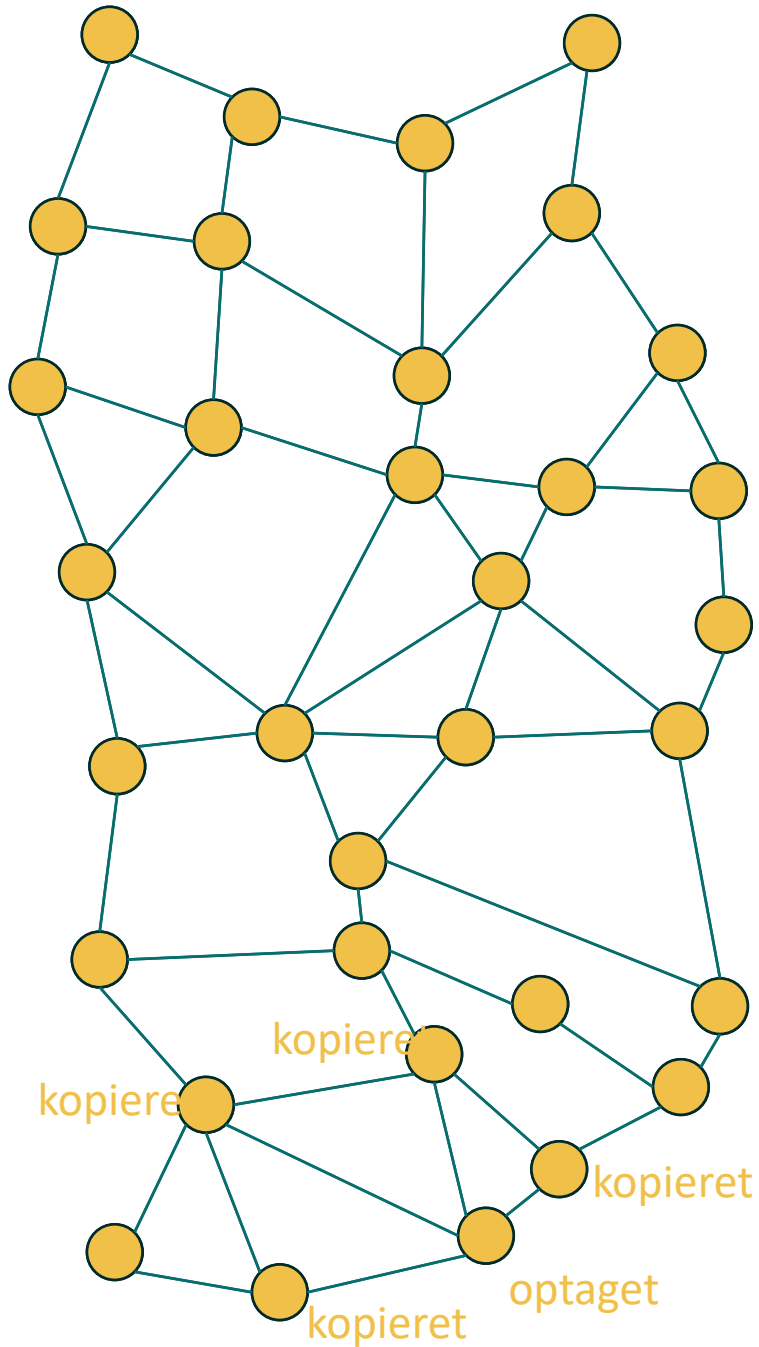
Decentraliseret

Ingen enkelt myndighedsserver styrer noderne, de har alle en individuel enhed.



Distribueret

*Hver knude er uafhængig og
forbundet med hinanden.*



Transaktion i distribueret netværk

Transaktionen registreres i en node og kopieres til hinanden.

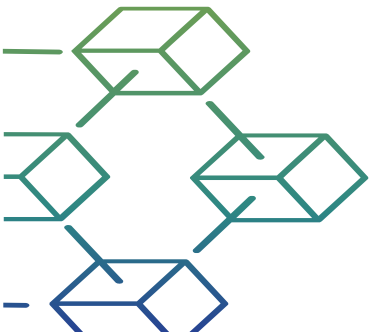
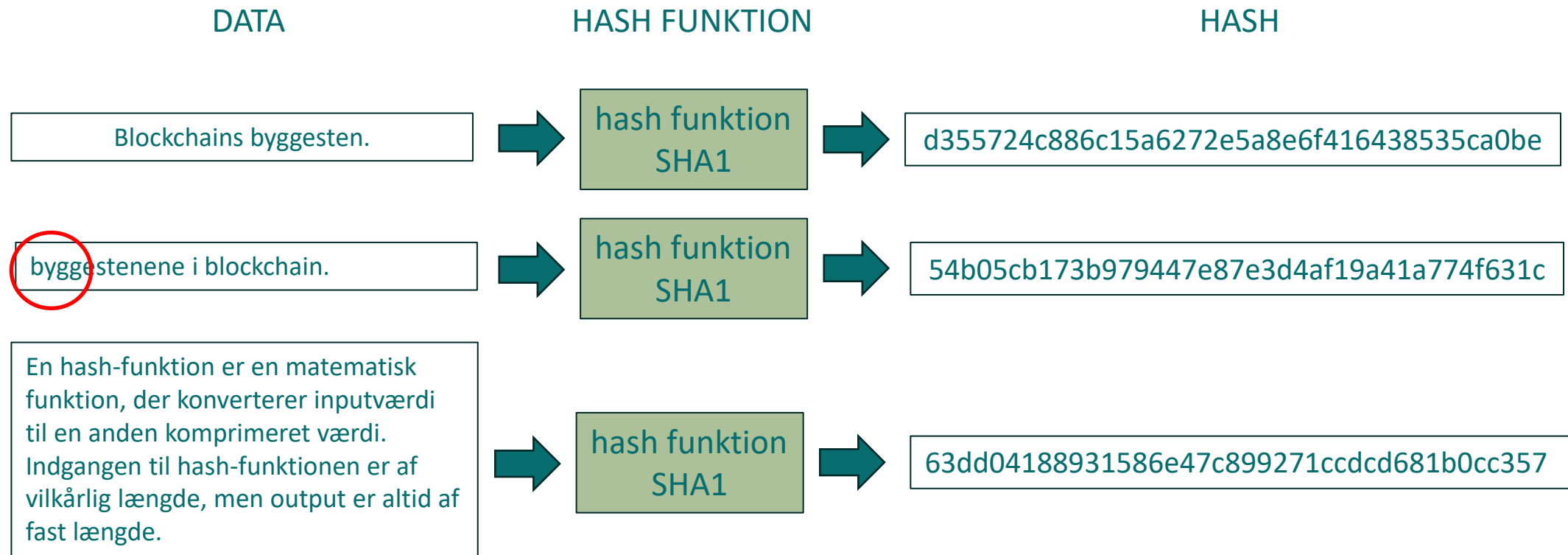
Hash funktion

En hash-funktion er en matematisk funktion, der konverterer inputværdi til en anden komprimeret værdi. Indgangen til hash-funktionen er af vilkårlig længde, men output er altid af fast længde.

Hash-funktioner er ekstremt nyttige og vises i næsten alle informationssikkerhedsapplikationer.



Uenestående udgang af hash-funktion



SHA1 er ikke nok i denne tid

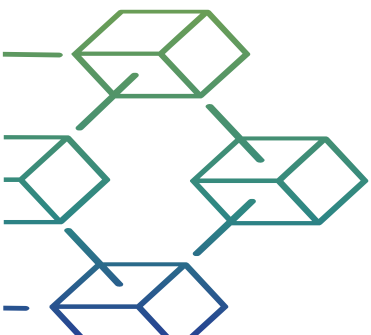
Blockchains byggesten.



hash funktion
SHA3-512



33322d615333e9faa2109c35997cf144876cc75ba76059454b28c81d2fa1c286a68679a00afb
baa71e9170ffc3bdaf6fbef504552a1845350180450000000000000000

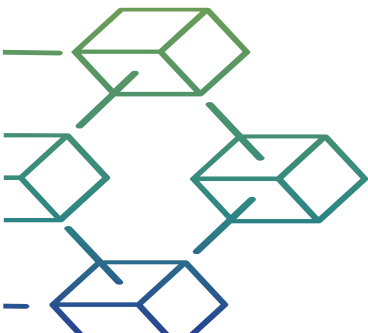


Modstand før billede

Denne egenskab betyder, at det burde være beregningsmæssigt svært at vende en hash-funktion.

Med andre ord, hvis en hashfunktion h producerede en hashværdi z , så burde det være en vanskelig proces at finde enhver inputværdi x , der hashes til z .

Denne egenskab beskytter mod en angriber, der kun har en hashværdi og forsøger at finde inputtet.



Kollisionsmodstand

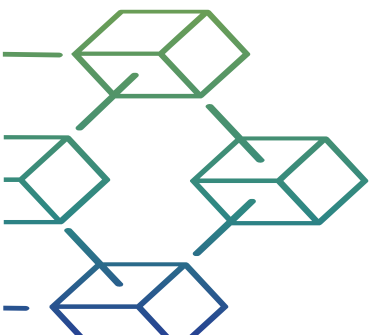
Denne egenskab betyder, at det burde være svært at finde to forskellige input af enhver længde, der resulterer i den samme hash. Denne egenskab omtales også som kollisionsfri hash-funktion.

Med andre ord, for en hashfunktion h , er det svært at finde to forskellige input x og y , således at $h(x) = h(y)$.

Da hash-funktion er komprimerende funktion med fast hash-længde, er det umuligt for en hash-funktion ikke at have kollisioner. Denne egenskab kollisionsfri bekræfter kun, at disse kollisioner burde være svære at finde.

Denne egenskab gør det meget vanskeligt for en angriber at finde to inputværdier med samme hash.

Også, hvis en hash-funktion er kollisionsbestandig, så er den anden pre-image resistent.

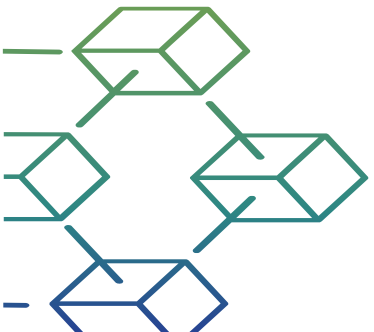


Anden Pre-Image Resistance

Denne egenskab betyder, at givet et input og dets hash, burde det være svært at finde et andet input med den samme hash.

Med andre ord, hvis en hashfunktion h for et input x producerer hashværdi $h(x)$, så burde det være svært at finde en anden inputværdi y , således at $h(y) = h(x)$.

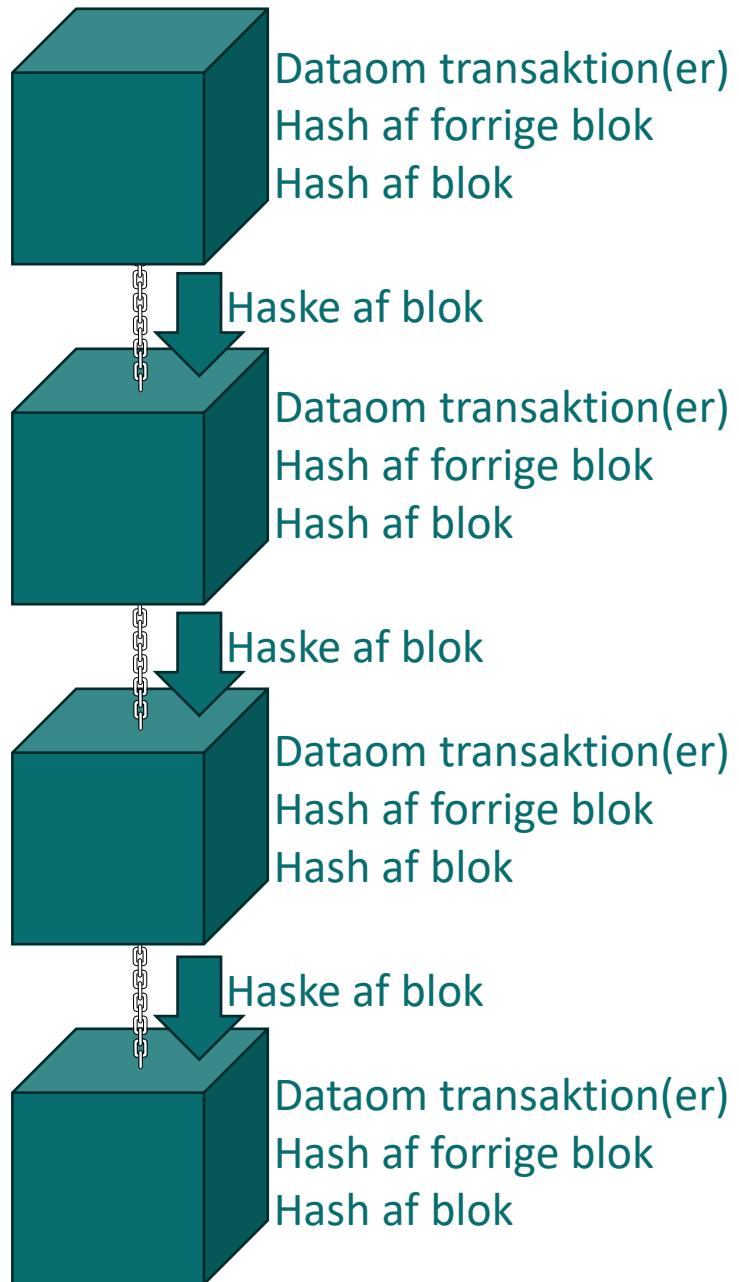
Denne egenskab for hash-funktion beskytter mod en hacker, der har en inputværdi og dens hash, og ønsker at erstatte en anden værdi som legitim værdi i stedet for den oprindelige inputværdi.



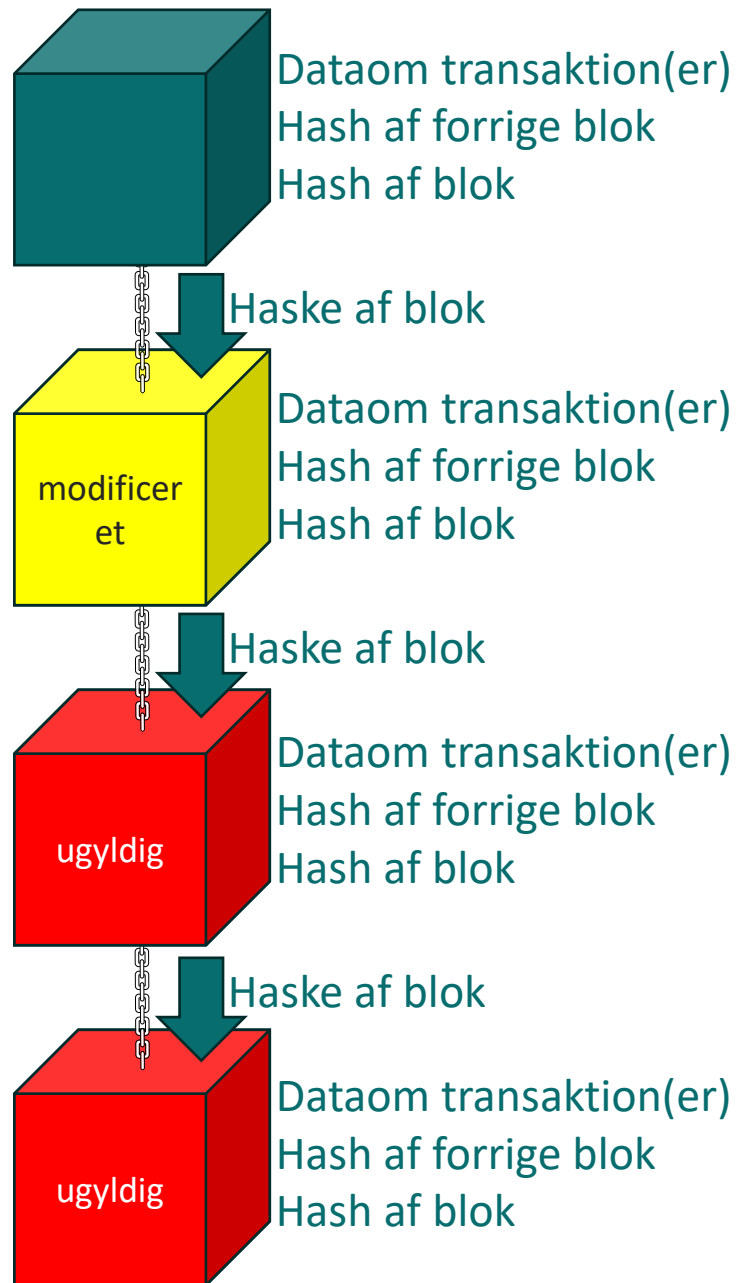
Blockchain

Blok = data + hash af
tidligere blok + hash
Kæde = kæde mellem
blokke



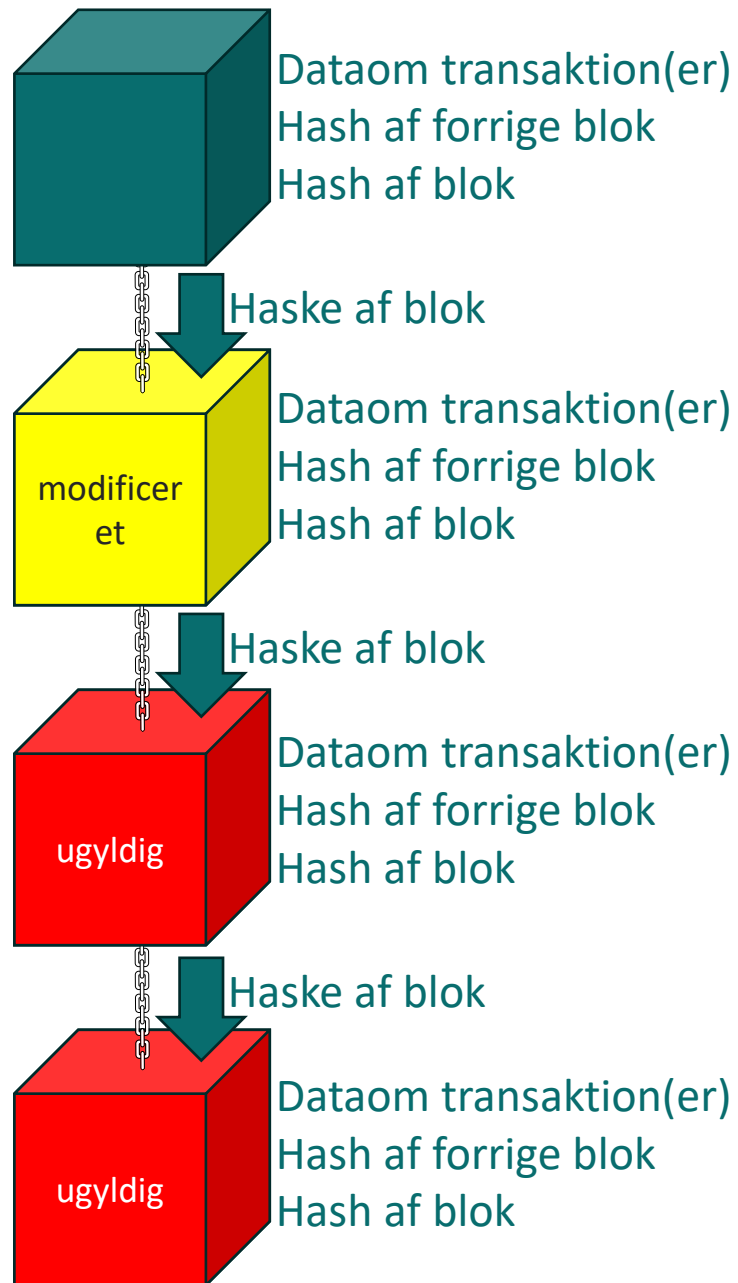


*Alle transaktioner registreres
i "blokke"*



Hvis er én blok (én transaktion i én blok) ændret

Værdien af hash-funktionen er anderledes



Hvis hackeren ønsker at ændre én blok (data i én blok), skal han ændre alle næste blokke og alle kopier af blokke i distribueret netværk

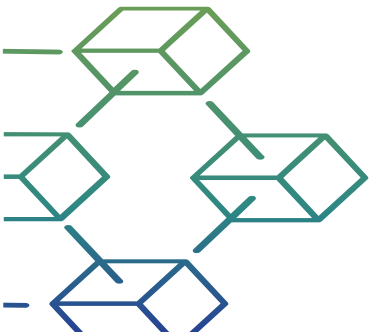
Næsten umuligt

(har brug for gigantisk computerkraft, elektricitet osv.)

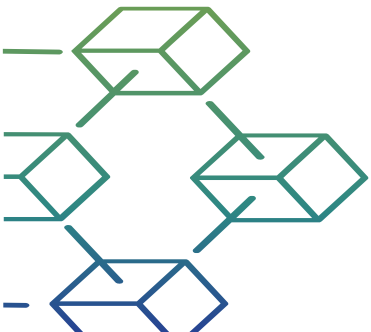
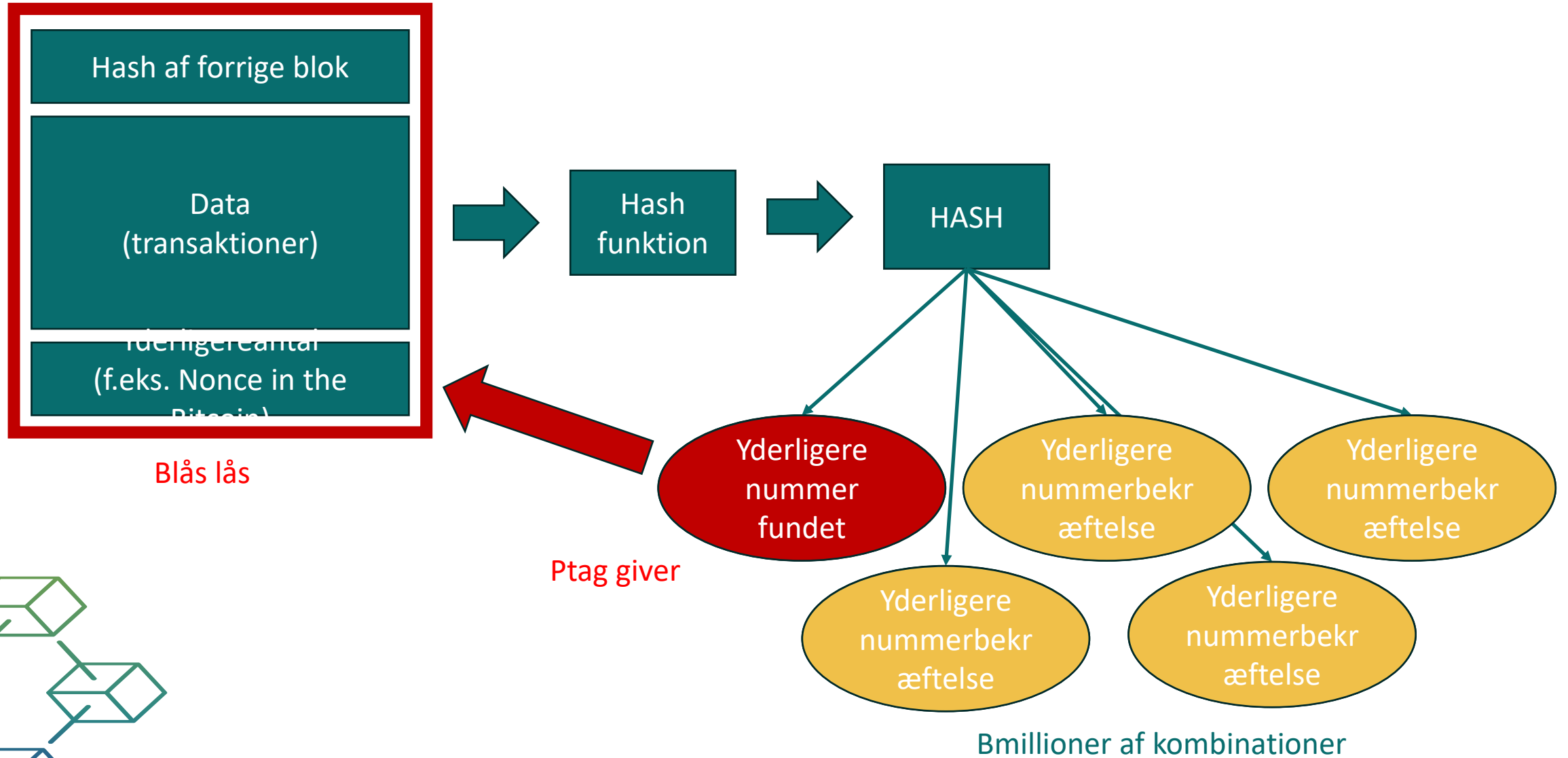
Bevis for arbejde

Bevis for arbejde (PoW) er en form for kryptografisk bevis, hvor den ene part (beviseren) beviser over for andre (verifikatorerne), at en vis mængde af en specifik beregningsmæssig indsats er blevet brugt.

Verifikatorer kan efterfølgende bekræfte disse udgifter med minimal indsats fra deres side.



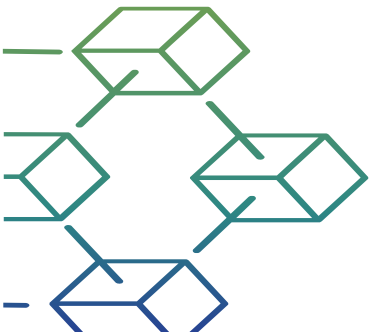
Bevis for arbejde



Bevis for indsats

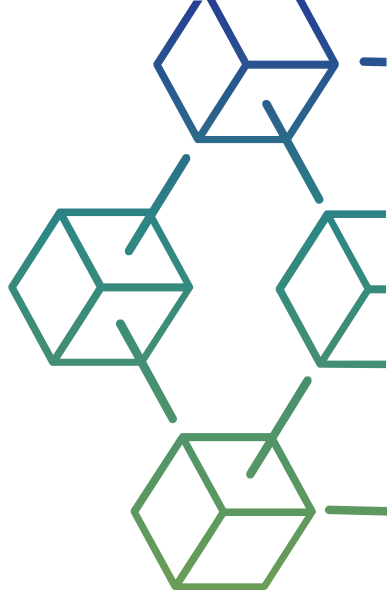
Bevis for indsats (PoS) protokoller er en klasse af konsensusmekanismer for blockchains, der fungerer ved at vælge validatorer i forhold til deres mængde af beholdninger i den tilknyttede kryptovaluta.

Dette gøres for at undgå de beregningsmæssige omkostninger ved proof-of-work (POW)-ordninger.

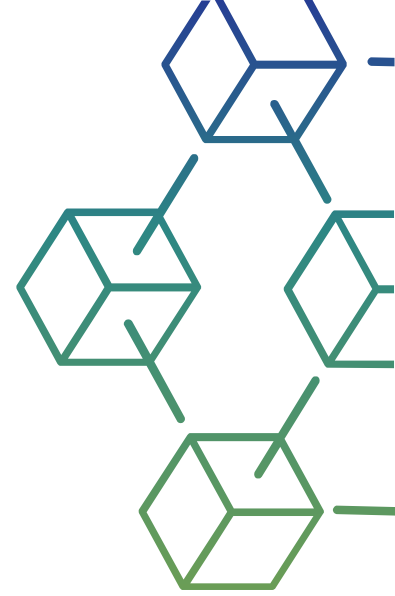


De 3 niveauer af blockchain

1. Blockchain 1.0: De oprindelse af de moderne blockchain
2. Blockchain 2.0: Smartkontrakter
3. Blockchain 3.0: Decentraliseret virksomhedsniveau anvendelse



Sammenligning med traditionelle databaser



DataStruktur

Traditionelle databaser: Traditionelle databaser bruger tabeller til at organisere data på en struktureret måde, typisk efter et foruddefineret skema.

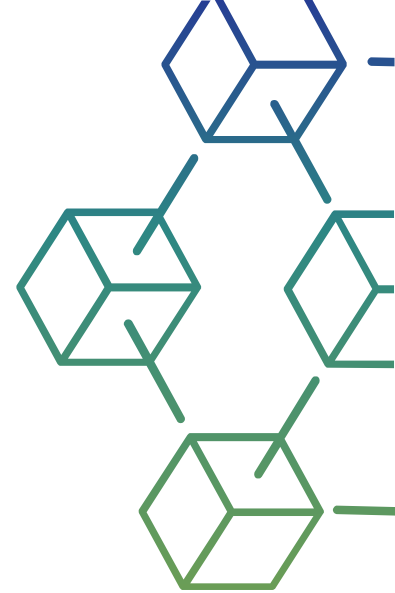
Blockchain: Blockchains bruger en hovedbogsstruktur, hvor data er organiseret i blokke, og hver blok indeholder en liste over transaktioner eller dataindtastninger. Strukturen er typisk mindre stiv, hvilket giver mulighed for mere fleksibilitet i datatyper og formater.

Sammenligning med traditionelle databaser

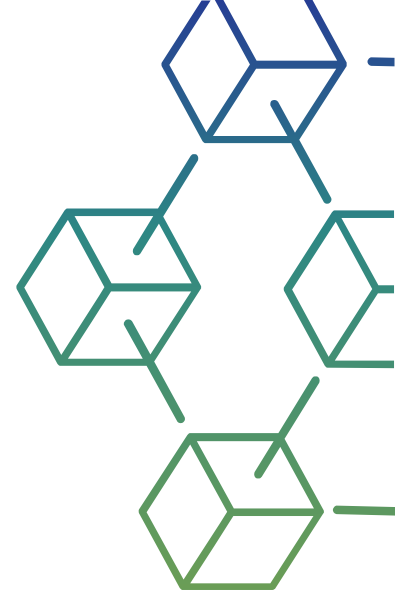
AdgangKontrollere

Traditionelle databaser: Adgangskontrol administreres af en centraliseret myndighed, og tilladelser kan gives eller tilbagekaldes for forskellige brugere eller roller.

Blockchain: Adgangskontrol styres ofte gennem kryptografiske nøgler. Brugere har kontrol over deres private nøgler, hvilket giver dem mulighed for at interagere med blockchain uden at stole på en central myndighed. Offentlige blockchains er typisk tilladelsesløse, mens private blockchains kan have forskellige niveauer af adgangskontrol.



Sammenligning med traditionelle databaser



Konsensus Mekanisme

Traditionelle databaser: Traditionelle databaser er ikke afhængige af en konsensusmekanisme blandt flere parter. De antager, at de data, der er gemt i databasen, er nøjagtige.

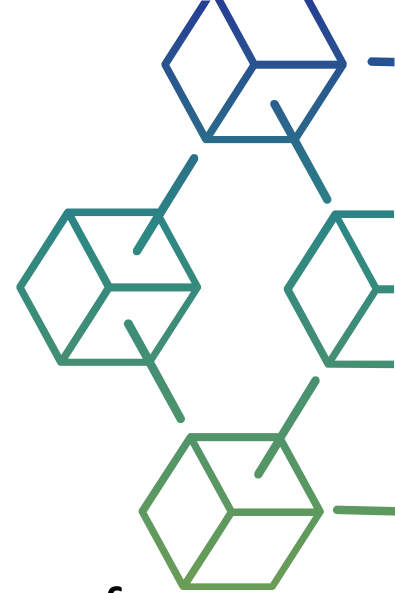
Blockchain: Blockchains bruger konsensusmekanismer (f.eks. Proof of Work, Proof of Stake) til at validere og blive enige om status for hovedbogen. Dette sikrer, at alle deltagere i netværket har et fælles og aftalt syn på dataene.

Sammenligning med traditionelle databaser

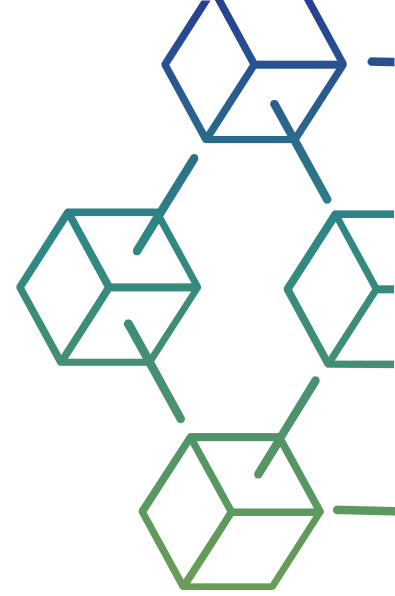
Uforanderligvs.ForanderligData

Traditionelle databaser:Data i traditionelle databaser kan ændres eller slettes af autoriserede brugere med de nødvendige tilladelser.

Blockchain:Når først data er registreret på blockchain, er de typisk uforanderlige og modstandsdygtige over for ændringer. Denne uforanderlighed er et kernetræk ved blockchain-teknologi.



Sammenligning med traditionelle databaser



TransaktionHastighed ogSkalerbarhed

Traditionelle databaser: Traditionelle databaser er ofte optimeret til høje transaktionshastigheder og kan nemt skaleres ved at tilføje flere servere eller ressourcer.

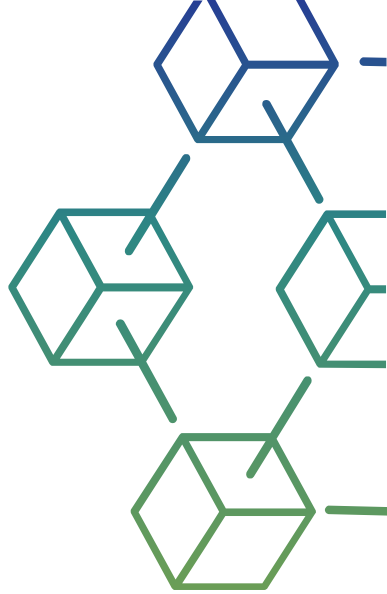
Blockchain: Offentlige blockchains, især dem, der bruger Proof of Work, kan have langsommere transaktionsbehandlingshastigheder og skalerbarhedsudfordringer. Der udvikles dog forskellige løsninger og teknologier for at forbedre skalerbarheden af blockchain.

Sammenligning med traditionelle databaser

Brugsager

Traditionelle databaser: Traditionelle databaser er velegnede til applikationer, der kræver høj gennemstrømning, lav latenstid og centraliseret kontrol, såsom banksystemer og e-handelsplatforme.

Blockchain: Blockchains er bedst egnede til applikationer, der kræver decentralisering, tillid, gennemsigtighed og sikkerhed, såsom kryptovalutaer, forsyningskædesporing, stemmesystemer og smarte kontrakter.



03

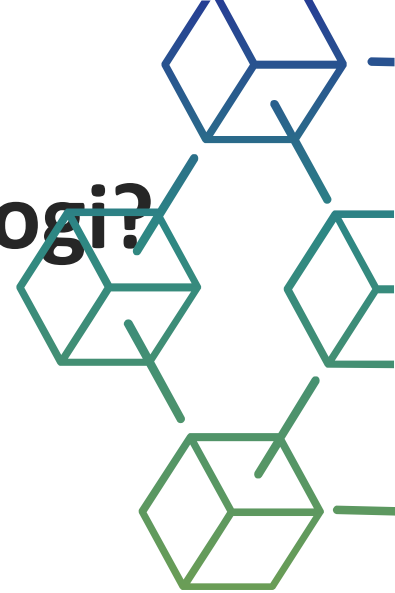
Hvaderde nøgle
komponenter
af blockchain teknologi?



Hvad er nøglekomponenterne i blockchain-teknologi?

Blockchainarkitekturharde følge vigtigste komponenter:

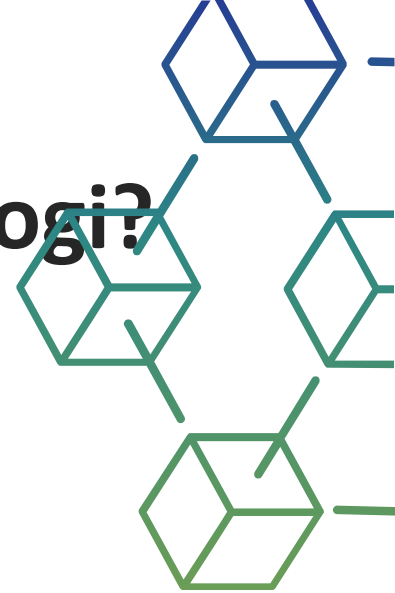
- 1. En distribueret hovedbog**
- 2. Smarte kontrakter**
- 3. Offentlig nøglekryptering**



Hvad er nøglekomponenterne i blockchain-teknologi?

1. En distribueret hovedbog

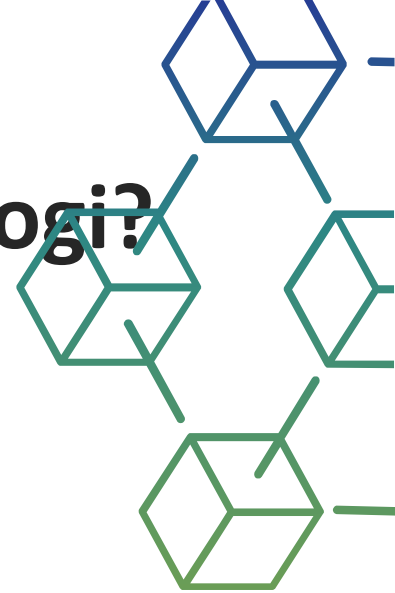
En distribueret hovedbog er en del af databasen i et blockchain-netværk af butikker der udfører transaktioner, såsom en digital fil at alle i det netværk kan redigere. Hos de fleste tekstredaktører, nogen med redigeringsrettigheder kan slette hele filen. Imidlertid, distribueret hovedbog-teknologier har strenge regler om hvem kan redigere og hvornår de kan redigere. Du kan ikke slette poster engang de er blevet optaget.



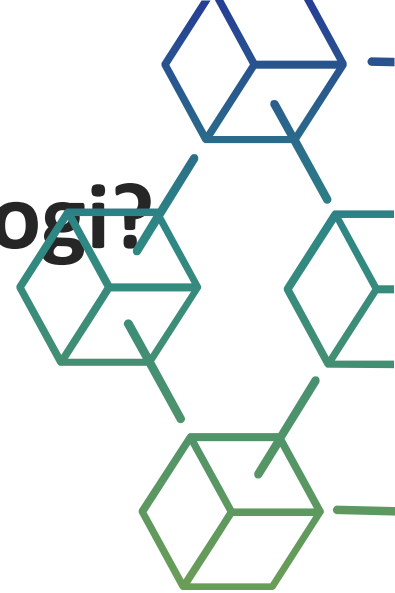
Hvad er nøglekomponenterne i blockchain-teknologi?

2. Smarte kontrakter

Virksomheder bruges smart kontrakt til selvstyre forretning kontrakter uden de behov for en assisterende tredjepart. Det er de programmer gemt på blockchain system at løbe automatisk når forudbestemt forhold er opfyldt. De løber hvis så check så at transaktioner kan være afsluttet selv sikkert. For eksempel, et logistik selskab kan have en smart kontrakt at automatisk gøre betaling engang gods er ankom på destination.



Hvad er nøglekomponenterne i blockchain-teknologi?



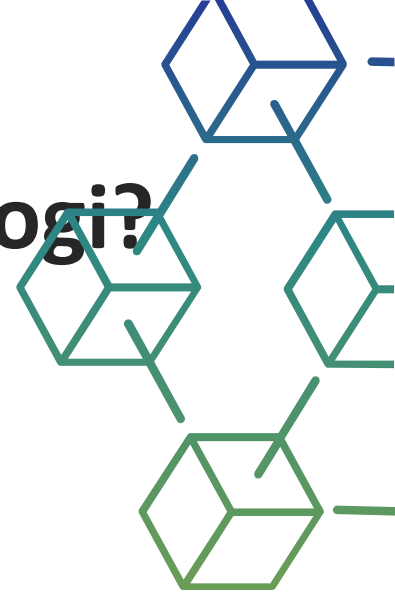
3. Offentlig nøglekryptering

Offentlig nøgle kryptografi er-ensikkerhed funktion til unikt identificere deltagere i blockchain netværk. Denne mekanisme genererer to sæt af nøgler for netværk medlemmer. En nøgle er en offentlighed nøgle at er fælles til alle i netværk. De andre er en privat nøgle at er enestående til hver medlem. De privat og offentlige nøgler arbejde sammen til låse op data i den hovedbog.

Hvad er nøglekomponenterne i blockchain-teknologi?

3. Offentlig nøglekryptering

For eksempel, John og Jill er to medlemmer af det netværk. John optegner en transaktion, der er krypteret med hans private nøgle. Jill kan dekryptere den med hendes offentlige nøgle. På denne måde, Jill er overbevist om, at John lavede den transaktion. Hvis Jill offentlig nøgle ville ikke have arbejdet, hvis Johns private nøgle havde været manipuleret med.



04

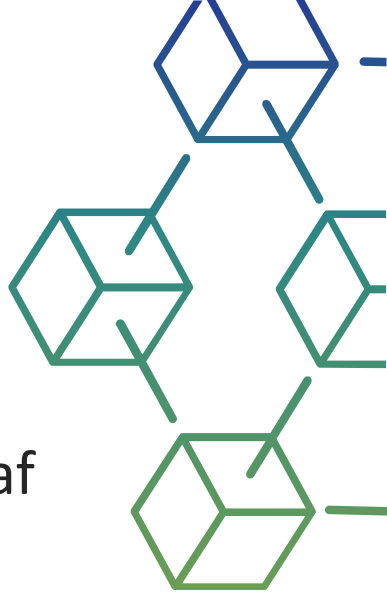
Hvaderde fordele
af blockchain teknologi?



Hvad er fordelene af blockchain-teknologi?

Blockchain teknologibringer mange fordele til aktiv transaktion ledelse. Vil du vide mere om de forskellige fordele, så læs de følgende underafsnit:

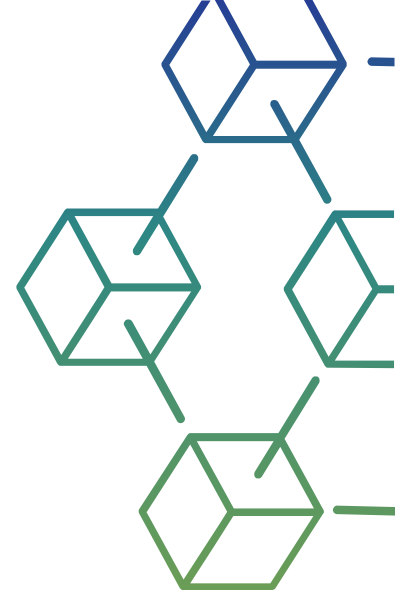
- 1. Avanceret sikkerhed**
- 2. Forbedret effektivitet**
- 3. Hurtigere revision**



Hvad er fordelene af blockchain-teknologi?

1. Avanceret sikkerhed

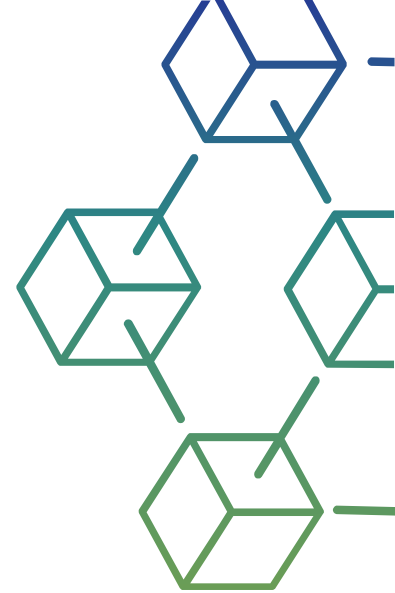
Blockchainsystemer giver et højt niveau af sikkerhed og tillid til moderne digitale transaktioner kræves. Der er altid en frygt for at nogen vil manipulere underliggende software til frembringelse af falske penge for sig selv. Men blockchain bruger de tre principper af kryptografi, decentralisering, og konsensus til at skabe et højt sikkert underliggende softwaresystem, der er næsten umuligt at manipulere. Der er intet enkelt punkt for fiasko, og en enkelt bruger ikke kan forandre de transaktionsoptegnelser.



Hvad er fordelene af blockchain-teknologi?

2. Forbedret effektivitet

Business-to-business transaktioner kan tage meget af tid og skabe operationelle flaskehalse, især når overholdelse og tredje-partiregulerende kroppe er involveret. Gennemsigtighed og smarte kontrakter i blockchain gøre sådanne forretningstransaktioner hurtigere og mere effektive.



05

Hvad er forskellen mellem en database og en blockchain?

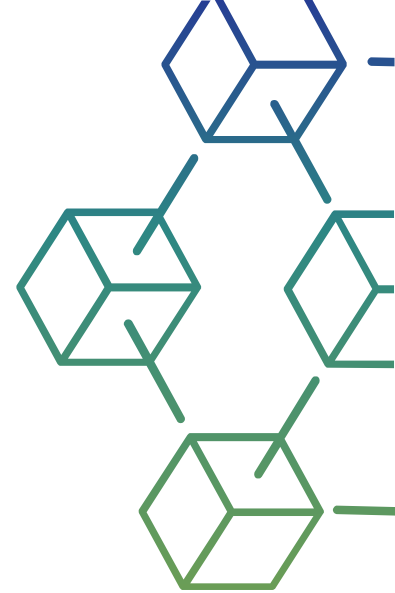


Hvad er fordelene af blockchain-teknologi?

3. Hurtigere revision

Virksomheder skal være i stand til sikkert frembringe, udveksle, arkivere og rekonstruere transaktioner, som kan revideres.

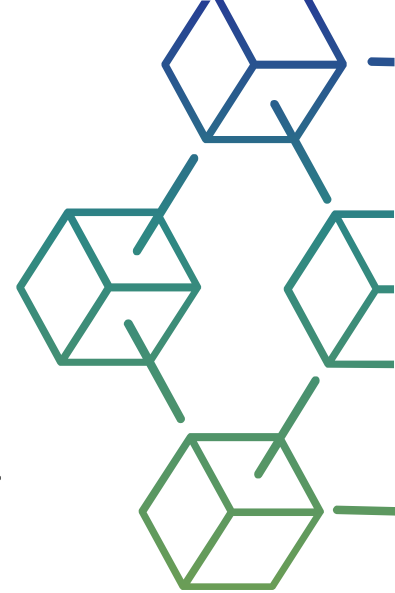
Blockchainoptegnelser er kronologisk uforanderlig, hvilket betyder at alle optegnelser altid består af den samme data. Denne datagennemsigthed gør revision og forarbejdning meget hurtigere.



Hvad er de forskel mellem database og en blockchain?

Blockchain er en særlig type af database styresystem, der har mere funktioner end en fast database. Vi beskriver nogle væsentlige forskelle mellem en traditionel database og en blockchain i følgende liste:

- Blockchains decentraliserer kontrollen uden skadelige stole på eksisterende data. Denne er ikke muligt i andre database systemer.
- Virksomheder involveret i en transaktion ikke kan dele deres hele database. Men i blockchain netværk, hver virksomhed har en kopi af den hovedbog, og det system automatisk fastholder konsistens mellem de to hovedbøger.
- Skønt i de fleste database systemer du kan redigere eller slette data, i blockchain du kan kun indsætte data.



06

Hvordan
erblockchainanderledes
fra desky?

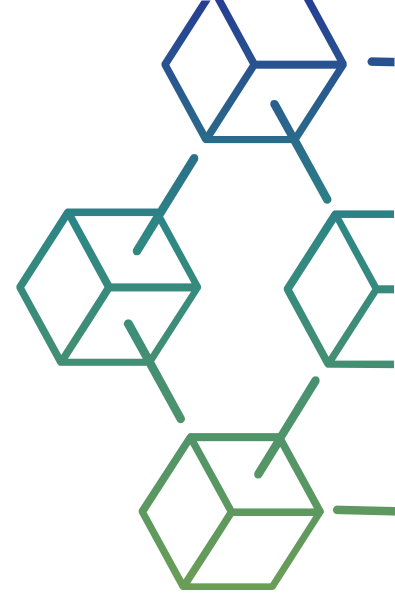


Hvordan er blockchain anderledes fra desky?

Det er nemt at få adgang til cloud tjenester, der kan være tilgængelige online. Du kan få adgang til software som en service (SaaS), produkt som en service (PaaS), og infrastruktur som en service (IaaS) fra desky.

Skyudbydere styre deres hardware og infrastruktur og give dig adgang til disse cloud ressourcer over de internet. De giver mange flere ressourcer end blot databasestyring.

Hvis du mangler til det offentlige blockchain-netværk, du behøver ikke dine hardware ressourcer til butik dine hovedbogkopi. Du kunne bruge en server fra desky for denne formål også. Nogle skyudbydere også tilbyder komplet Blockchain som en service (BaaS) fra desky.



07

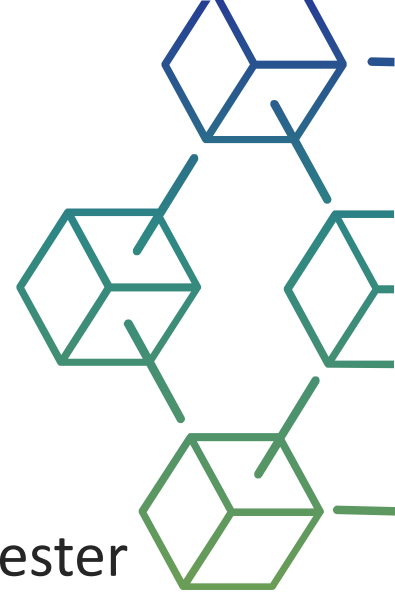
Hvad er blockchain som
enservice?



Hvad er blockchain som en service?

Blockchain som en Service (BaaS) er enklare blockchain service at-entredjepart giver i sky. Du kan udvikle blockchain applikationer og digitalt tjenester mens de cloud udbydere forsyninger de infrastrukturer og blockchain bygning værktøjer.

Alledu have at gøre er tilpasse eksisterende blockchain teknologi, hvilke gør blockchain adoption hurtigere og mere effektiv.



08

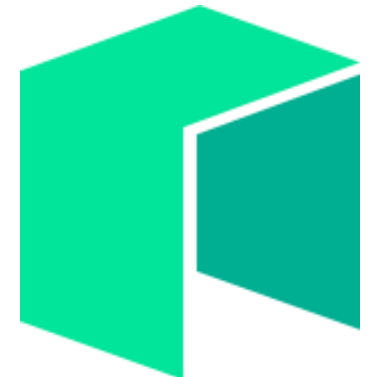
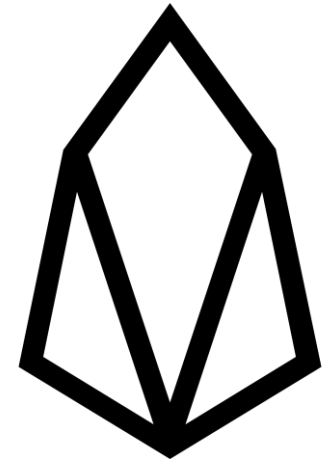
Use Case



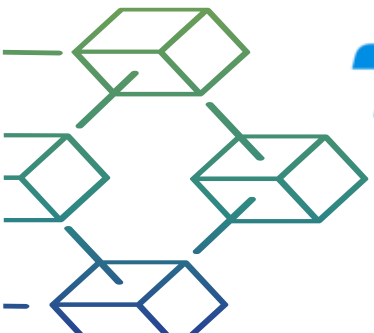
Cryptocurrency – den første bredt anvendte blockchain

- Moderne kryptovalutaer brugte blockchain

- Bitcoin
- Litecoin
- Ethereum
- XRP
- EOS
- NEO
- Stellar
- Monero
- Dash
- ...



Dash



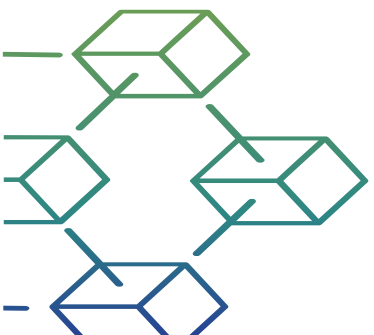
09

Konklusion



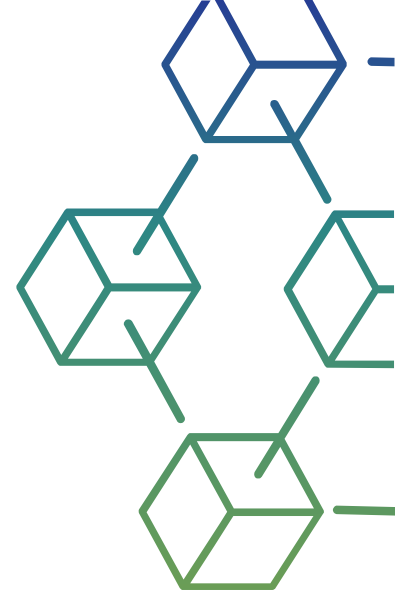
Konklusion

Blockchain teknologier er fremskredne databasemekanismer, der tillader gennemsigtig information deling inden for et forretningsnetværk. Blockchain er gjort op af en kæde af blokke, hvor hver blok indeholder en liste af transaktioner og en uafhængig identifikator (hash) af den tidligere blok. Dette sikrer integritet af data. Blockchain er et decentraliseret netværk, hvor data er fordelt over flere noder (computere) i et netværk. Der er ingen central myndighed eller enkelt punkt af kontrol, der fremstiller dem modstandsdygtig til censur og manipulation. Blockchain er gemt på tusindvis af computere (noder) omkring verden. Hver node har en kopi af den hel blockchain, hvilket stiger dens modstand til udfald og angreb.



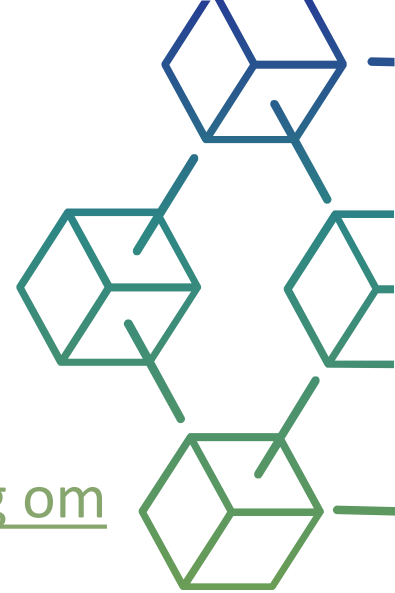
Video

- [Hvordan fungerer en blockchain - Simpelt forklaret](#)[6:00]
- [Blockchain på 7 minutter](#)[7:03]
- [Blockchain forklaret](#)[10:23]
- [Hvad er en Blockchain? \(Animeret + Eksempler\)](#)[8:27]
- [Blockchain-teknologi forklaret\(2 timers kursus\)](#)[1:54:53]
- [Blockchain Basics & Kryptografi](#)[1:17:37]



Links

- [BlockChain-principper, type og anvendelse og hvorfor du skal bekymre dig om det?](#)
- [Designprincipper for blockchain](#)
- [Principper for blockchains](#)
- [Principper for vellykkede Blockchain-implementeringer](#)
- [Grundlæggende blockchain-sikkerhed](#)
- [Blockchain-design – Udforsk Blockchain-principperne](#)
- [Blockchain-teknologi: principper og anvendelse i medicinsk billeddannelse](#)



10

Interaktivlæringaktivitet

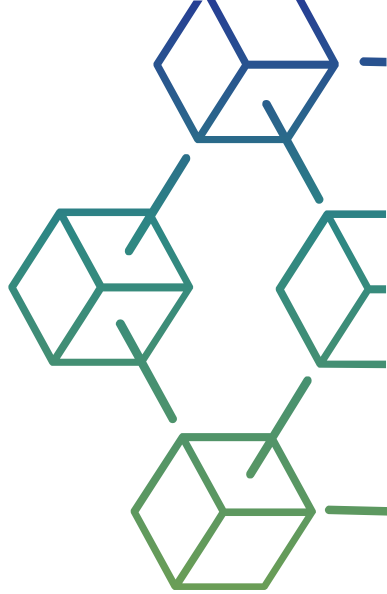


Lav 5blokke underblockchain

1. Brug onlineværktøj til hash

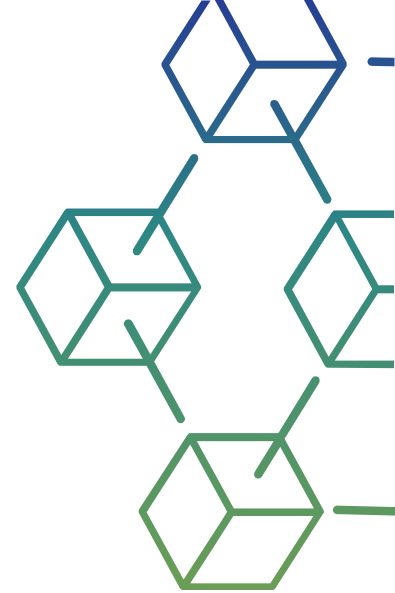
<https://emn178.github.io/online-tools/sha256.html>

2. Brug SHA256 og lav hashes af 5 blokke – indholdet er på næste slide



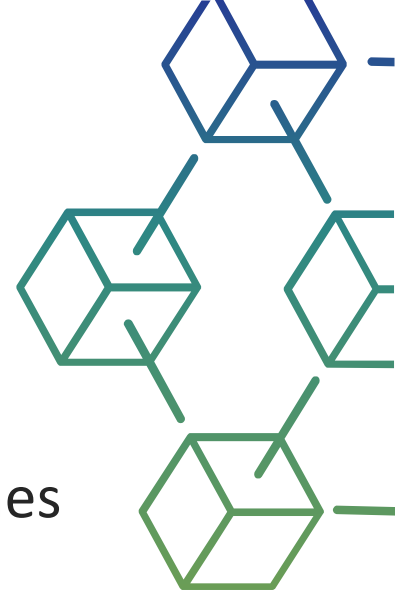
Lav 5 blokke underblockchain

1. 1st blokere indhold:
2023-01-01T10:34:12+1,JonhNewman, JaneNewman, 236,23, EUR
e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
2. 2nd blokere indhold:
2023-01-01T10:35:28+1,SteveJohnson, RichardMcCay, 100,00 EUR
brug hash fra hash-funktionen af 1st blok
3. 3rd blokere indhold:
2023-01-01T10:35:33+1,CharlesTann, ElisabethBronson,100,00,EUR
brug hash fra hash-funktionen af 3rd blok
4. 4th blokere indhold:
2023-01-01T10:35:59+1,RogerBlackburn, LisaTann,50,00,EUR
brug hash fra hash-funktionen af 3rd blok
5. 5th blokere indhold:
2023-01-01T10:36:01+1,RichardMoss, EdwardMorris,85,00,EUR
brug hash fra hash-funktionen af 4th blok



Prøv at:

1. Foretag de samme små ændringer i 2nd blokere og sammenligne nye hashes
2. Brug en anden hash-funktion – topmenu – Hash
 1. SHA1
 2. SHA2-512
 3. SHA3
 4. ...
3. Brug dit indhold af blok for har funktion



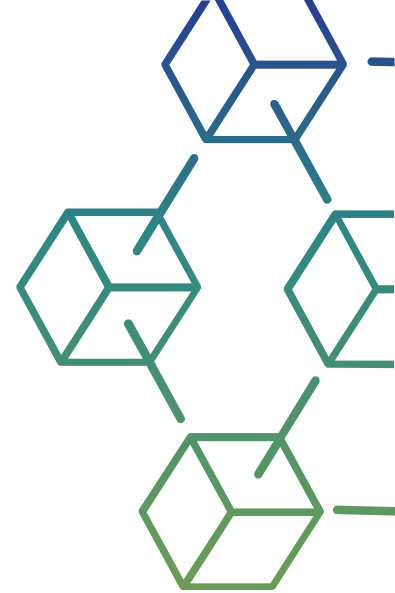
11

Quiz



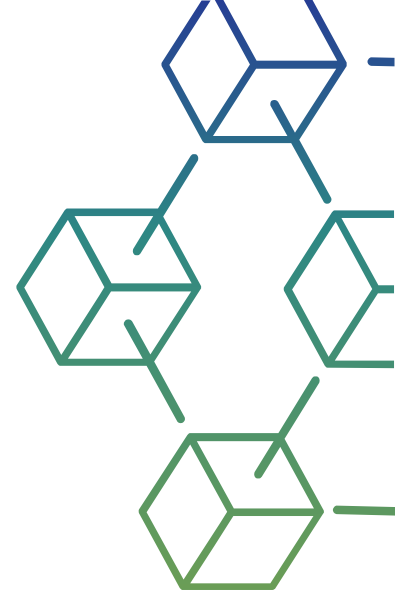
Quiz

1. Hvad er et nøglekrav for en sikker hash-funktion:
 - a) Kollisionsmodstand
 - b) Redundans
 - c) Forudsigelighed
 - d) Linearitet



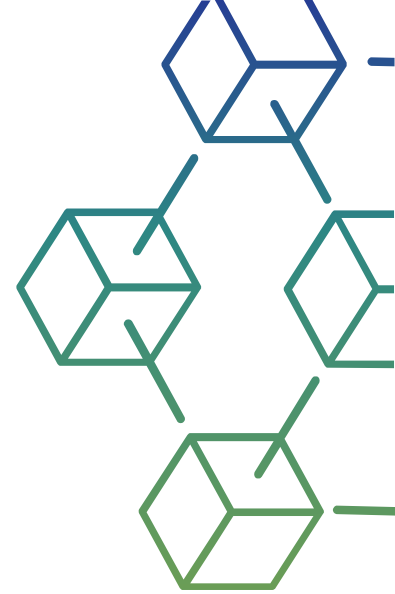
Quiz

2. Hvad kendetegner en centraliseret databasearkitektur?
- a) Enkelt kontrol- og myndighedspunkt
 - b) Distribueret datalagring på tværs af flere noder
 - c) Autonom beslutningstagning af hver node
 - d) Høj modstand mod censur og manipulation



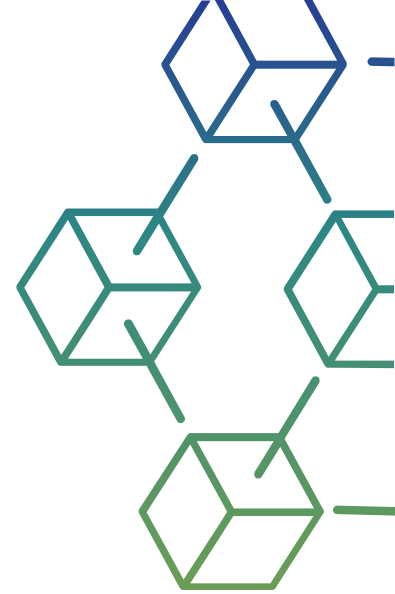
Quiz

3. Hvad er et nøgletræk ved en decentraliseret databasearkitektur?
- a) Flere "centrale" noder
 - b) Enkelt kontrol- og myndighedspunkt
 - c) Centraliseret beslutningstagning af en udpeget node
 - d) Lav redundans og fejltolerance



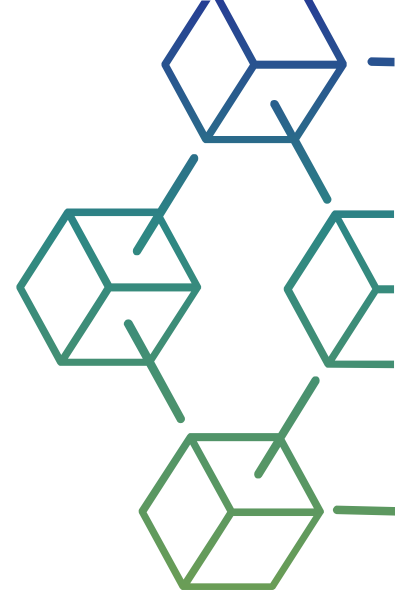
Quiz

4. Hvad er en definerende egenskab ved en distribueret databasesystem?
- a) Data gemmes på tværs af flere noder i et netværk
 - b) Centraliseret kontrol og autoritet over hele databasen
 - c) Mangel på redundans for øget ydeevne
 - d) Begrænset skalerbarhed på grund af en enkelt-node-arkitektur



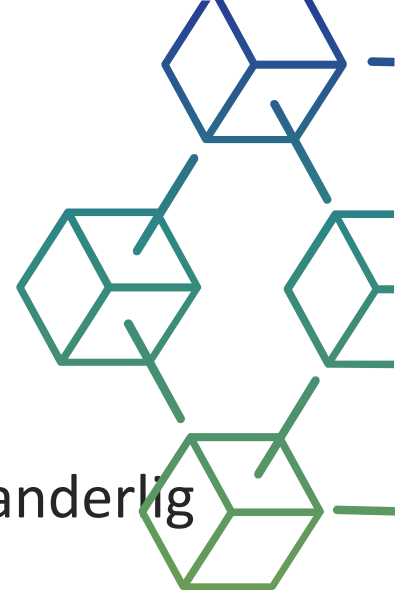
Quiz

5. Hvad beskriver bedst en hash i forbindelse med datalogi og kryptografi?
- a) Et output med fast størrelse genereret af en hash-funktion, der repræsenterer den unikke digitale signatur af inputdata
 - b) En streng med variabel længde, der bruges til datalagring i databaser
 - c) En programmeringskonstruktion til optimering af datahentning i algoritmer
 - d) En realtidskrypteringsmetode til sikring af kommunikationskanaler



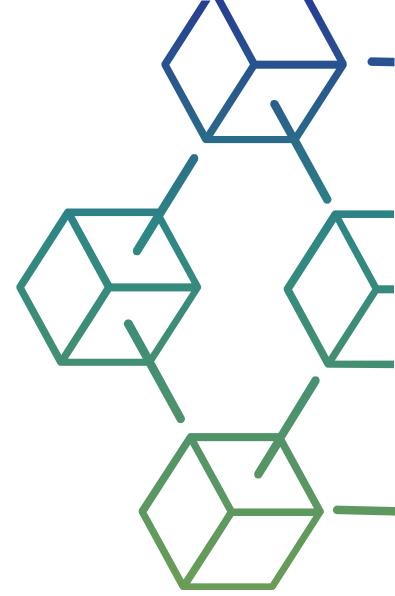
Quiz

6. Hvilken komponent er ansvarlig for at opretholde en kronologisk og uforanderlig registrering af transaktioner i en blockchain?
- a) Blok
 - b) Node
 - c) Smart kontrakt
 - d) Konsensus algoritme



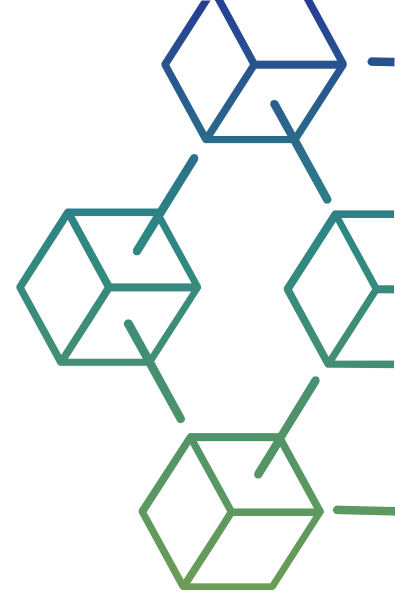
Quiz

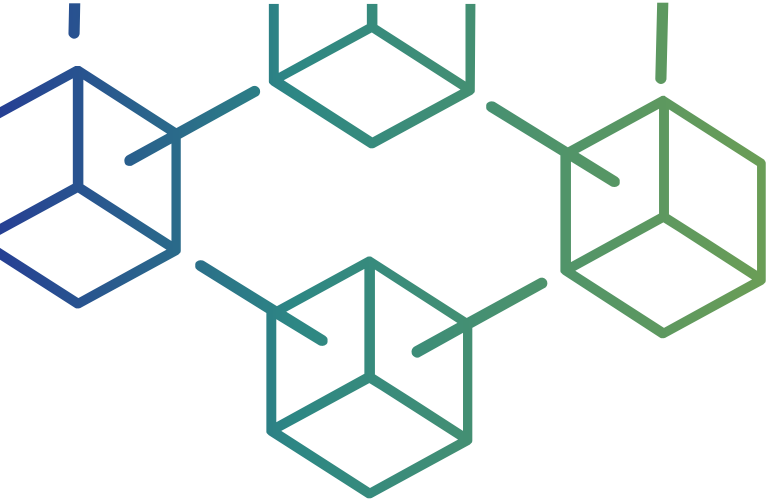
7. Hvad er en vigtig differentiator mellem en blockchain og en traditionel database?
- a) Blockchain tilbyder decentraliseret og distribueret kontrol, mens traditionelle databaser typisk er centraliserede
 - b) Traditionelle databaser giver hurtigere transaktionsbehandling sammenlignet med den langsommere karakter af blockchain
 - c) Blockchain er afhængig af et enkelt kontrolpunkt, hvorimod traditionelle databaser bruger et distribueret netværk til kontrol
 - d) Traditionelle databaser er i sig selv modstandsdygtige over for manipulation, mens blockchain er mere modtagelige for datamanipulation.



Quiz

8. Hvor blev blockchain-teknologi først implementeret?
- a) Finansiering og kryptovaluta
 - b) Sundhedspleje og lægejournaler
 - c) Sociale medier og netværk
 - d) E-handel og online detailhandel





<https://blockchainforagrifood.eu/>

Tak

Har du spørgsmål?

