LIKE

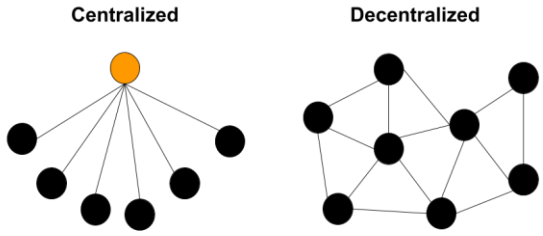
DIGITAL (UD)DANNELSE

Projekt om Blockchain og Bitcoin

Du har sikkert hørt ord som Blockchain og Bitcoin blive brugt, men det er de færreste der egentlig ved hvad de betyder, og hvad mulighederne med dem er. I dette projekt vil du lære mere om disse ting.

Projektet indeholder en del praktiske øvelser, der foregår på hjemmesiden https://anders.com/blockchain/ som er lavet af Anders Brownworth. Her kan du også se hans videoer der forklarer mange af de samme emner som projektet handler om.

Centraliserede og decentraliserede databaser



Når du overfører penge til eller fra din bank foregår det gennem et *centralt* register: Bankens database holder styr på de forskellige saldoer, og alle transaktioner foregår igennem den.

a. Diskuter hvilke fordele og ulemper der kan være ved en sådan centraliseret struktur.

Bitcoin er en *decentraliseret* valuta. Hvilket betyder at handlen med den ikke foregår igennem nogen officiel myndighed: Alle kan frit handle med enhver anden uden nogen mellemmænd. Og alle har en kopi af hele databasen og alle transaktioner der nogensinde er blevet foretaget.

b. Diskuter tilsvarende hvilke fordele og ulemper der kan være ved en decentraliseret struktur.

Blockchain er den underliggende teknologi der gør det decentraliserede element af Bitcoin muligt. Vi vil i de kommende afsnit kigge på hvordan Blockchain er bygget op.

Hash-funktioner

En *hash-funktion* har ikke noget med stærk tobak at gøre, men er derimod en algoritme der tager et stykke tekst og laver det om til en kode. Den hash-funktion vi skal beskæftige os med her i projektet hedder *SHA-256*. SHA er en forkortelse for *Secure Hashing Algorithm*, og tallet 256 viser at koden man får ud er på 256 bits, altså en liste af 256 nuller eller ettaller.

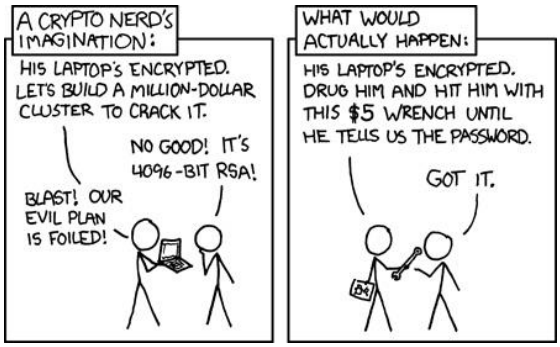
LIKE

Gå nu ind på siden https://anders.com/blockchain/hash.html (Eller vælg ”Hash” i menuen hvis du allerede har klikket på linket ovenfor). Du kan nu skrive en tekst i feltet og se den tilsvarende hash-kode nedenfor. Den er skrevet i noget der hedder *hexadecimal*, men du behøver ikke at vide andet end at det er en smart måde at få de 256 bits til at fylde mindre når man skriver dem ud og som et menneske (lidt) nemmere kan læse.

Leg med at skrive forskellige tekster i feltet, og se på de tilsvarende hash-koder. Overvej følgende, og skriv dine erfaringer ned:

a. Hvor meget ændrer hash-koden sig når du ændrer lidt i teksten?
b. Er hash-koden tilfældig? Prøv at skrive det samme i feltet to gange og sammenlign.

Selvom det er nemt for computeren at lave en hash-kode ud af en tekst er det ikke nemt at gå den anden vej: Hvis du får givet en hash-kode vil det være meget svært at gætte en tekst der giver lige præcist denne hash-kode; der er ikke ret meget andet at gøre en at gætte sig frem (se dog billedet til højre).



c. Kan du forklare hvorfor det er sådan ud fra dine svar til delspørgsmål a og b?
d. Hvor mange forskellige hash-koder på 256 bits findes der? (Husk der er to muligheder for hver bit)?

En computer der er optimeret til at gætte tekster der svarer til en given hashkode, kan typisk teste 10^{12} muligheder i sekundet. Den skal i gennemsnit gætte lige så mange gange som der er mulige hashkoder for at løse problemet.

e. Hvor mange sekunder tager dette maskinen?

Universets alder er anslået til at være $4{,}1 \cdot 10^{17}$ sekunder.

f. Hvor mange gange universets alder er svaret fra delspørgsmål e?

For en mere detaljeret forklaring af hvor store tal vi egentlig taler om kan du se denne video: https://www.youtube.com/watch?v=S9JGmA5_unY

En blok

Den grundlæggende byggesten i Blockchain er – forhåbentlig ikke overraskende – *blokken*.

Gå ind på siden https://anders.com/blockchain/block.html (Eller vælg ”Block” i menuen). Som man kan se består blokken ud over tekst af et tal kaldet en *nonce*. Både tekst og nonce bidrager til hash-funktionen.

a. Prøv at ændre på tekst og nonce for at efterprøve dette. Lægger du mærke til noget andet der ændrer sig?

D·U·D·E

LIKE

En blok, hvis hash-kode starter med fire nuller vil vi kalde *underskrevet* (på engelsk *signed*). På siden angiver farven om en blok er underskrevet eller ej.

a. De fire cifre svarer til 16 bits. Hvor mange forskellige koder på 16 bits findes der?

   Hvis man har en tekst man gerne vil underskrive, kan man altså lede efter en nonce der gør de første fire cifre til nuller. I gennemsnit skal man kun kigge lige så mange muligheder igennem som tallet du fandt i delspørgsmål b.

b. Ved at trykke på ”Mine” leder siden efter en nonce der passer til teksten. Gør dette for ti forskellige tekster og skriv hver nonce ned. Hvad er gennemsnittet? Sammenlign med svaret på delspørgsmål b.

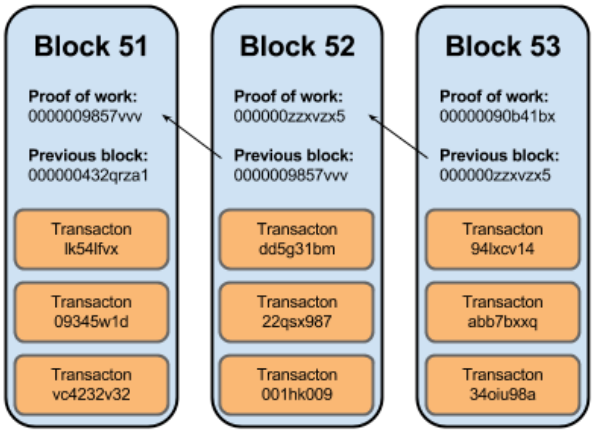
En sådan nonce der svarer til en tekst kaldes for *proof-of-work* for blokken. Den beviser nemlig man har gjort arbejdet med at *mine* en kode der passer. Altså at ”grave” efter en passende nonce. Mere om Bitcoin-mining senere.

Ideen i Bitcoin og andre *kryptovalutaer* er, at lade teksten i blokken repræsentere transaktioner. ”Transaktioner af hvad?”, kan man naturligt spørge. For så vidt eksisterer Bitcoin kun som tal i disse blokke, men det at man kan handle med dem giver dem i sig selv en potential værdi – men det er jo dybest set samme ide der ligger bag almindelig valuta!

På hjemmesiden – der er en slags ”legeplads” for Blockchain - skal der kun fire nuller i starten af hash-koden (eller 16 bits) før blokken er underskrevet. I virkeligheden kræver man at et noget større antal bits først i hash-koden er nuller. Dette gør det svært, men ikke umuligt at finde nonce/proof-of-work for en blok. For Bitcoin vokser antallet af påkrævede nuller med tiden.

Kæder af blokke: Blockchain

Vi ønsker nu at kæde flere blokke sammen i en *kæde*. Med tiden kan kæden blive forlænget med flere blokke. Der er altså en første blok i kæden, og herefter hægtes der flere på.



Gå ind på siden https://anders.com/blockchain/blockchain.html (Eller vælg ”Blockchain” i menuen). Nu afhænger hash-koden for hver enkelte blok ikke kun af tekst og nonce, men også af proof-of-work for blokken der kommer før den! Figuren til højre viser dette (teksten er den orange del af blokkene).

D·U·D·E

LIKE

Hvis kæden skal være anerkendt skal samtlige blokke være underskrevet. Til at starte med er alle nonces på siden valgt så dette er tilfældet.

a. Prøv at ændre teksten i en af blokkene. Hvordan ændrer det på hvilke blokke der er underskrevet eller ej? Hvad sker der når man prøver at mine nye nonces? Start evt. forfra et par gange og prøv at ændre andre blokke. Skriv dine observationer ned.
b. Hvilke blokke er "sværest" at rette i?

Distribueret konsensus

Som vi har set er det svært at rette på indholdet i en blockchain, særligt hvis man vil ændre på en blok langt tilbage i kæden. Men vi har også set det ikke er umuligt. Så hvad gør man for at sikre sig imod dette?

Svaret er, at data er *distribueret*. Det betyder at alle der benytter kryptovalutaen har sin egen kopi af hele databasen, altså alle kæder af blokke.

Gå til https://anders.com/blockchain/distributed.html (Eller naviger til "Distributed" i menuen). Her er der vist en simpelt eksempel hvor der er tre brugere af samme blockchain.

a. Vælg en af de tre brugere, og ændr på teksten i en af blokkene. Brug "Mine" til at underskrive de resterende blokke i kæden. Sammenlign hash-koden for sidste blok i hver kæde.

Ved at stole på flertallet af brugere ser vi altså at vi sikre os mod ændringer i kæden: Hvis hash-koden ikke stemmer overens med den konsensus der er, bliver kæden ikke accepteret.

Ovenstående afsnit viser i princippet alle ideerne bag Blockchain. Der er selvfølgelig en masse detaljer der er udeladt, men forhåbentlig er du nu lidt klogere på denne nye teknologi.

Andre anvendelser

Inden vi går mere i detaljer med mining af Bitcoins er det værd at nævne at Blockchains kan bruges til andet og mere end kryptovaluta. Manglen på mellemmænd, og det faktum at alle har adgang til hele historien for hver blok gør Blockchain ideel til en række andre formål.

D·U·D·E

LIKE

a. Undersøg hvad nogle af disse anvendelser kunne være. Du kan f.eks. starte med at se nærmere på WePower, Ethereum eller ProPy.

Mining af Bitcoin

Vi vender nu tilbage til Bitcoin. Du har måske overvejet hvordan man tilføjer nye blokke til en kæde. I store træk foregår det på den måde, at man annoncerer de transaktioner man gerne vil lave, hvorefter alle kan konkurrere om at finde proof-of-work der kan underskrive den nye blok, der dermed kan tilføjes til kæden. Den der først finder en sådan bliver belønnet i Bitcoins – der kommer altså løbende flere og flere Bitcoins i omløb.

Denne proces kaldes Bitcoin-mining, og der er kamp om at vinde dette kapløb. Derfor er der mange minere der har investeret i store computer-clusters der afprøver nonces i døgndrift. Sådanne clusters bruger meget energi – rigtig meget endda! Hvilket har givet grund til bekymring af miljøhensyn. Særligt fordi mange af disse clusters befinder sig i Kina hvor energi er billig og kulbaseret.

Tabellen viser det estimerede globale Bitcoin-mining-energiforbrug ved starten af de første seks måneder i 2018:

Måned	Januar	Februar	Marts	April	Maj	Juni
Forbrug i TWh/år	36,80	46,68	52,69	58,83	64,17	69,66

Kilde: digiconomist.net

Til sammenligning er Danmarks energiforbrug 32 TWh pr. år.

a. Brug regression til at finde en model af formen $y = ax + b$, hvor x er antallet af måneder siden Januar 2018, og y er energiforbruget i TWh/år.
b. Tegn et residualplot for regressionen.
c. Beregn residualspredningen og vurder modellens gyldighed.
d. Hvad er energiforbruget i starten af 2020 ifølge modellen?

Energiforbrug pr. land kan ses på
https://en.wikipedia.org/wiki/List_of_countries_by_electricity_consumption

e. Hvilket lands energiforbrug ligger svaret i delspørgsmål d tættest på?

Der arbejdes heldigvis på alternativer til proof-of-work.

f. Undersøg ideen bag *proof-of-stake*.

D·U·D·E