Blockchain – alt-i-ett-teknologien

Ved hjelp av blockchain-teknologien vil det til en lavere pris enn i dag bli mulig å utføre transaksjoner i tilnærmet sanntid og dokumentere disse uten bruk av ekstern tredjepart som garanterer for transaksjonenes riktighet eller holder rede på eierforholdene. Forsøk på juks avdekkes med det samme.

Redaktør Alf Asklund

Ved bruk av blockchain-teknologi verifiseres og lagres alle transaksjoner hos alle i nettverket i helt identiske kopier.

Startet med Bitcoin

blockchain er foreløpig mest kjent for å være den teknologien som har gjort det mulig å lage et digitalt betalingsmiddel som Bitcoin. Selv om Bitcoin ikke understøttes av noe lands myndighet eller noen form for underliggende verdier, regnes det som sikkert at ingen klarer å forfalske betalinger eller bruke sine Bitcoins mer enn én gang. Det er en forutsigbar tilførsel av nye Bitcoins inn i markedet og det totale antall Bitcoins vil aldri overstige et forhåndsdefinert antall. Bitcoin er i tillegg et tilnærmet anonymt betalingsmiddel.

Teknologien bak er mest interessant

Egenskapene som ligger i teknologien som gjør Bitcoin mulig – blockchain teknologien – er imidlertid mye mer interessant enn selve betalingsmiddelet Bitcoin.

En blockchain er et nettverk av datamaskiner (strengt tatt en distribuert databasemodell),[1] der alle medlemmer av nettverket sitter på en kopi av en felles reskontro (transaksjonsoversikt). Alle i nettverket har innsyn i reskontroen, men det kan ikke gjøres endringer i den. Reskontroen er bygd som en lenket liste eller kjede av blokker, der hver blokk inneholder transaksjonene som er blitt gjort i et gitt tidsrom.

Verifisert og dokumentert

Alle transaksjoner som gjøres er verifiserte og lagres hos alle i nettverket i helt identiske kopier. Det finnes altså ikke én enkelt

1 Streng tatt ikke ett nettverk av maskonger, en distribuert databasemodell. Ikke ett nettverk av maskiner.

liste med transaksjoner, men et tilnærmet uendelig antall med lister. Et forsøk på å gjøre en endring/forfalskning på tidligere oversikter vil derfor vises i alle kopier. Bruk av en teknologi benevnt som hashing sikrer mot forfalskninger. Hashing innebærer å omgjøre en rekke med data til en kort streng/nøkkel som representerer de originale dataene.

Eliminerer tredjepart

Ved hjelp av blockchain-teknologi er det mulig å gjøre transaksjoner mellom personer som ikke nødvendigvis må stole på hverandre. På det viset elimineres behovet for en bekreftelse fra en tredjepart for riktigheten av dataene. Sikkerheten tas altså vare på av teknologien og av deltagerne i et nettverk i fellesskap.

Slik skjer en transaksjon

En typisk transaksjon illustreres nedenfor. Hele prosessen kan gjøres i løpet av 3–10 sekunder.

1. En person i nettverket lager en transaksjon som deretter sendes i nettverket – inkludert en digital signatur.
2. Meldingens ekthet bekreftes ved at den digitale signaturen dekrypteres. Dette gjøres av den i nettverket (Noden) som er blitt gitt fullmakten til dette. Den bekreftede transaksjonen plasseres i en pool av bekreftede transaksjoner.
3. Ventende transaksjoner samles i en blokk, som er en oppdatert versjon av reskontroen/transaksjonslisten. Etter en gitt tid sender Noden blokken ut i nettverket for endelig verifisiering.
4. Den endelige verifiseringen gjør Noden i nettverket gjennom en interaktiv prosess som krever godkjennelse fra en majoritet i nettverket.
5. Hvis alle transaksjoner blir godkjente, hektes den siste blokken på blokkjeden og en oppdatert versjon av reskontroen/transaksjonslisten sendes ut i nettverket.

Når det gjelder Bitcoin, skjer valget av Noden som kan hekte siste blokk i blokkjeden ved hjelp av en slags loddtrekning. Tilfeldigheten som ligger i valg av den som får skriveprivilegiet, er en ekstra sikkerhet mot forfalskning.

Bitcon er basert på at alle som ønsker det kan delta i nettverket. Transaksjoner og eierskap skjer under full anonymitet og privilegiet med å godkjenne transaksjoner loddes ut. Med andre ord snakker vi om et åpent og anonymisert system.

Fjerner anonymiseringen

Basert på en blockchain 2.0-plattform er det mulig å lage løsninger for verifiserte transaksjoner der deltakerne i nettverket må legitimere seg og ha tillatelse for å være med i nettverket, de som godkjenner transaksjonene er kjente og listen over transaksjoner viser hvem som eier hva og til hvilken tid. At anonymiteten er fjernet, gjør også at de enkelte aktørene kan stilles til ansvar i forhold til eksisterende lover og regler.

Ideen bak åpne nettverk

Hele ideen er å kunne overføre verdier eller bekrefte informasjon i tilnærmet sanntid til en veldig lav kostnad uten at dette må bekreftes av noen eksterne og uten at informasjonen om eierforholdene/informasjonen må lages i ett sentralt register. Kostnadbesparelsen ligger i at ingen eksterne må garantere for sikkerheten eller holde rede på hvem som eier hva. Dette fordi det definerte nettverket sørger for at alle transaksjoner gjennomføres og dokumenteres på sikkert vis.

Et stort antall bruksområder

Når det gjelder bruksområde, er det vel bare fantasien som setter grenser, men blockchains egenskaper passer i hvert fall svært godt for omsetning av standardiserte finansielle eiendeler (som jo i prinsippet er standardiserte kontrakter), eller for å registrere for eksempel eiendomsrett/bruksrett etc. til faste eiendommer i et land.

Passer på regnskapet

Vi kan også tenke oss at en blokk kan inneholde regnskapet til en virksomhet og at denne settes i en blokk-kjede med regnskapet til alle andre virksomheter i Norge – eller i verden for den saks skyld. Alle i nettverket ville da kunne se om noen prøver å gjøre en eneste liten endring i et hvilket som helst av disse regnskapene. Det går an å tenke seg at det samme vil måtte kunne gjøres med deler av et enkelt regnskap. Kundereskontroen kan for eksempel være en blokk – som deretter settes sammen med alle andre deler av regnskapet – i en blokk-kjede. Enhver form for uautorisert endring i noen deler av regnskapet vil dermed vises med det samme.

De mest entusiastiske ser også for seg at blockchain 2.0 vil gjøre det mulig å drive hele organisasjoner ved at en lang rekkefølge av arbeidsoppgaver legges inn i et stort system. Dette uten at det i all hovedsak er bruk for mennesker i administrasjonen. Men dit er det (heldigvis?) langt frem – om det noen gang kommer så langt.

Whitepaper

For de som ønsker å sette seg inn i blockchains virkemåte og mulige bruksområder, anbefales et såkalt whitepaper utarbeidet av EVRY med tittelen *blockchain – Powering the Internet of Value* som kan lastes ned fra: evry.com/globalassets/insight/bank2020/bank-2020---blockchain-powering-the-internet-of-value---whitepaper.pdf