Så fungerar blockkedjan med smarta kontrakt och stablecoins

Stablecoins och andra kryptovalutor är digitala pengar registrerade på blockkedjor. Exemplet visar hur *stablecoins* kan användas tillsammans med smarta kontrakt, alltså digitala kontrakt som verkställs automatiskt. Stablecoins kan även användas oberoende av smarta kontrakt.

AV JOHAN JARNESTAD OCH KRISTOFER DITTMER

Kontrakt förhandlas

Säljaren och köparen kommer överens om pris och andra köpvillkor som behöver stå i kontraktet, som i ett traditionellt kontrakt.

Kontrakt digitaliseras

Kontraktet omvandlas till ett smart kontrakt som är programmerat att automatiskt verkställa en överföring av *stablecoins* när kontraktets villkor är uppfyllda.

Smart kontrakt fästs på blockkedjan

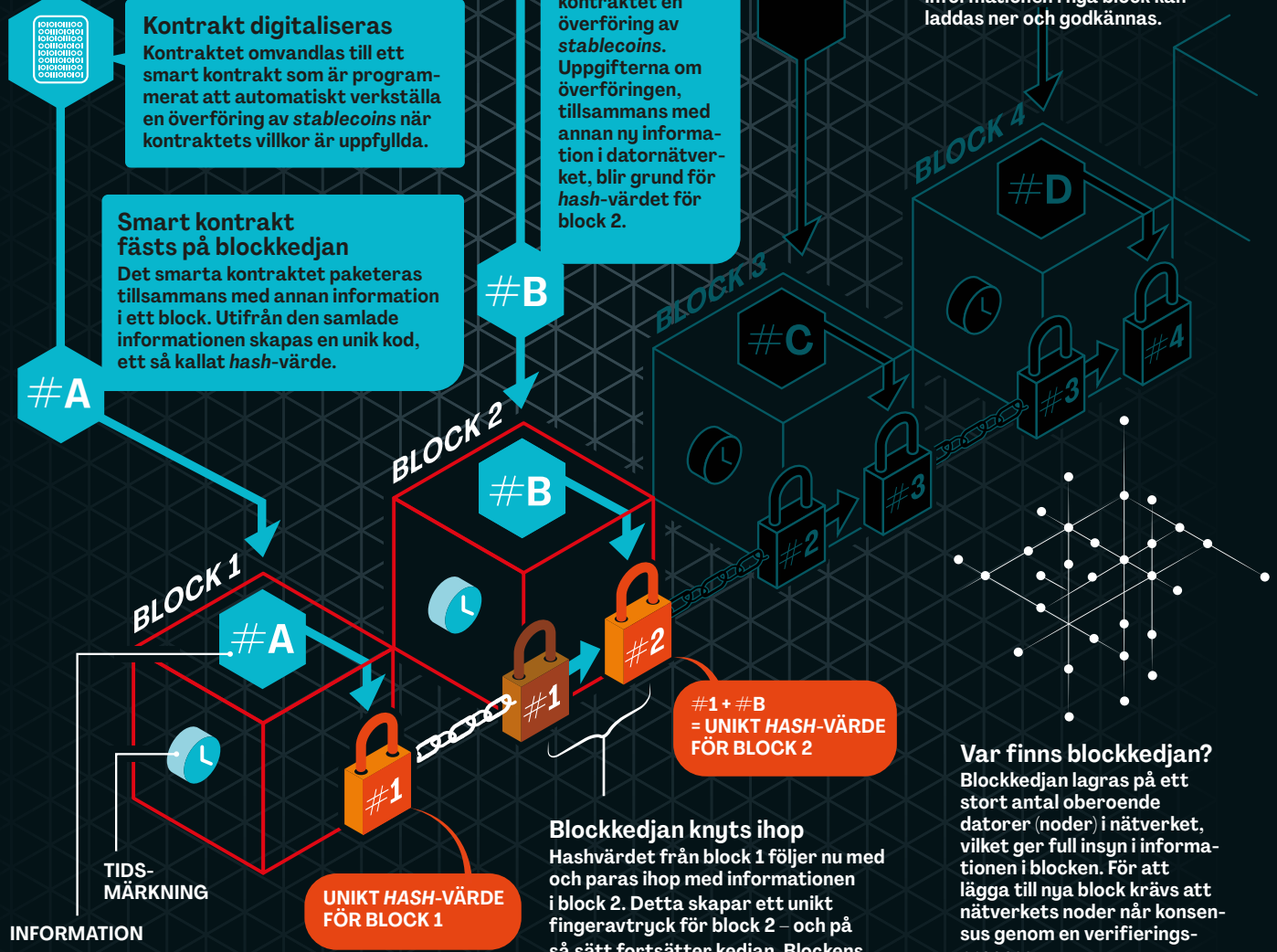
Det smarta kontraktet paketeras tillsammans med annan information i ett block. Utifrån den samlade informationen skapas en unik kod, ett så kallat *hash*-värde.

Kontraktets villkor uppfylls

När villkoren är uppfyllda verkställer det smarta kontraktet en överföring av *stablecoins*. Uppgifterna om överföringen, tillsammans med annan ny information i datornätverket, blir grund för *hash*-värdet för block 2.

Oändligt lång

I teorin kan en blockkedja bli hur lång som helst, men tillväxttakten begränsas av att nya block behöver verifieras av nätverksdeltagarna. Hastigheten i deras internetuppkoppling och datorernas processorkraft påverkar därför hur snabbt informationen i nya block kan laddas ner och godkännas.



Blockkedjan knyts ihop

Hashvärdet från block 1 följer nu med och paras ihop med informationen i block 2. Detta skapar ett unikt fingeravtryck för block 2 – och på så sätt fortsätter kedjan. Blockens beroende av varandra gör att ingen kan förfalska uppgifterna i dem.

Var finns blockkedjan?

Blockkedjan lagras på ett stort antal oberoende datorer (noder) i nätverket, vilket ger full insyn i informationen i blocken. För att lägga till nya block krävs att nätverkets noder når konsensus genom en verifieringsprocess.

Forskning & Framsteg
Bild: Johan Jarnestad