BITCOIN PÅ 10 MINUTTER

Alt det du altid gerne har villet vide om Bitcoin

Brought to you by Relai

HVAD ER BITCOIN?

Bitcoin, der er verdens mest succesfulde kryptovaluta, skaber overskrifter overalt på kloden. Mange vil gerne profitere på dens succes, andre er ligeglade eller skeptiske.

Den digitale valuta har været udgangspunkt for utallige diskussioner om penge, investeringer og teknologi. Nogle ser Bitcoin som ren spekulation, eller afskriver det som værende en boble, imens andre taler om innovation, monetær revolution eller endda redning fra det nuværende monetære system.

Nogle nationer, herunder Kina, ser Bitcoin som en trussel og har erklæret kryptovalutaen krig. Andre regeringer, som for eksempel El Salvadors, har introduceret Bitcoin som officielt betalingsmiddel i håbet om økonomisk vækst.

Men hvad er Bitcoin? Er det penge? Digitalt guld? En dille for IT-specialister og spekulanter?
Eller noget helt andet? I de følgende afsnit vil vi komme til bunds i disse spørgsmål og tage et nærmere kig på den digitale valuta, så vi bedre kan forstå filosofien og funktionaliteten bag Bitcoin. For at opnå dette, er det vigtigt at starte ved selve begyndelsen: med historien om Bitcoins oprindelse.

BITCOIN HISTORIE

Begyndelsen til Bitcoin daterer sig tilbage til de tidlige halvfemsere. I 1992 startede en gruppe af IT-specialister en e-mail liste, så de kunne udveksle idéer med ligesindede om kryptografi, matematik, politik og filosofi. De kaldte sig selv "Cypherpunks" – et ordspil skabt af "cyberpunk" (en person i sci-fi-litteraturen, der er skeptisk i forhold til samfundet – og med rette) og "cipher" (at kryptere).

Cypherpunkerne

Cypherpunkerne udviklede sig hurtigt til en broget flok. På trods af deres vidt forskellig baggrund var de forenede omkring deres overbevisning om, at Internettet snart ville blive en af de mest omstridte arenaer for menneskelig frihed.
For at beskytte sig selv mod truslen om kontrol, overvågning og censur af Internettet og bevare et frit og åbent Internet, benyttede Cypherpunkerne sig af et stærkt våben: krypteringen af information.

I deres manifest fra 1993 fremfører de: "Cypherpunks skriver [computer] kode. Vi ved at nogen er nødt til at kode software for at forsvare privatlivets fred, og [...] vi vil skrive det.

Men kryptografi alene ville ikke være nok til at sikre et frit Internet. Fordi, og Cypherpunkerne var overbeviste om dette, Internettet kan ikke være ægte frit, hvis det ikke har sine egne penge. Penge der er uafhængige af stater, centralbanker og virksomheder; en kryptovaluta så fair og decentraliseret som Internettet selv.

Monetære eksperimenter

Men skabelsen af uafhængige digitale penge gav Cypherpunkerne nogle tekniske udfordringer. Kryptografen David Chaum havde så tidligt som i 1990 skabt eCash, den første kryptovaluta, der ikke var decentraliseret, men sikrede anonymitet takket være kryptografi. Men eCash var på sigt ikke i stand til at gøre sig gældende overfor andre online betalingssystemer. Virksomheden bag projektet måtte indgive konkursbegæring efter 8 års drift, og eCash er siden forsvundet.

Andre forsøg fulgte af hvilke E-Gold skilte sig ud. E-Gold var en kryptovaluta understøttet af fysisk guld, og som var åben for alle. Etableret i dotcom æraen i 1996 slog virksomheden igennem blandt sine ligemænd, og omsatte transaktioner for en værdi på mere end 2 milliarder dollars om året, da den var på sit højeste.

Men E-gold var kontrolleret af en centraliseret institution, og var derfor sårbar overfor angreb. Snart fulgte juridiske problemer, og den amerikanske stat anlagde sag mod E-Gold. I 2008 blev E-Gold af en amerikansk domstol kendt skyldig i hvidvask og overtrædelse af den såkaldte "Patriots Act". Alle aktiver blev indefrosset og E-Gold var nødsaget til at stoppe alle aktiviteter.

Disse fejlslagne forsøg beviste to ting for Cypherpunkerne. For det første, både eCash og E-Gold var understøttet af aktiver stillet som sikkerhed. Disse aktiver havde vist sig at være et svagt punkt, idet de kunne beslaglægges af stater. Derfor skulle en fri kryptovaluta ikke have noget centralt angrebspunkt, såsom en virksomhed, en bankkonto eller en centraliseret server lokation. For det andet, hverken stater eller regulerende myndigheder har nogen interesse i digitale penge, der er uafhængige af staten.

For Cypherpunkerne bestod det basale spørgsmål, til hvilket der endnu ikke var fundet en løsning, endnu: Hvordan kan uafhængige digitale penge fungere uden en centralt placeret enhed, der holder regnskab og sikrer at de samme penge ikke bliver brugt mere end én gang? Hvis det var muligt at løse dobbelt-forbrugs-problemet (nemlig det at holde styr på at den enkelte digitale mønt ikke bliver brugt flere gange samtidigt) uden at være nødt til at stole på en central enhed, så ville det måske være muligt at frembringe uafhængige digitale penge skabt til Internettet.

En mytisk skabelse

Af disse grunde begyndte Cypherpunkerne at diskutere mulige designs for en kryptovaluta uden en centralt placeret enhed (der kunne angribes) og uden aktiver (der kunne beslaglægges). To af de mest vigtige koncepter var b-money (1998) og Bit-Gold (2005). Disse teoretiske idéer, som aldrig blev implementeret i praksis, var allerede meget lig Bitcoin i de-

res design. Et offentligt/privat nøgle par var påtænkt for kryptering og en Proof-of-Work-mekanisme tilføjet for skabelsen af yderligere digitale mønter, som også er tilfældet for Bitcoin. I sin oprindelige beskrivelse af Bitcoin (også kendt som The Bitcoin Whitepaper på engelsk) bekræfter opfinderen af Bitcoin kendskab til b-money og BitGold.

Men idet b-money og BitGold støttede sig til en afstemnings-mekanisme for at opnå konsensus (afklaringen af hvem der ejer hvilke monetære enheder på det givne tidspunkt), var de sårbare overfor angreb, der kunne manipulere sådanne afstemninger og derfor fordreje det reelle ejerskab.

Dette var det sidste problem der stod i vejen for skabelse af en ny form for penge specifikt for Internettet, og en løsning til dette problem blev fremlagt fredag d. 31. oktober 2008. På denne dag blev The Bitcoin Whitepaper, hvori Satoshi Nakamoto forklarer hans koncept for et decentraliseret betalingssystem, e-mailet til Cypherpunkerne. To måneder senere, d. 3. januar 2009, gik Bitcoin netværket live.

Indledningsvis var der ikke mange reaktioner eller meget opmærksomhed omkring netværket. Nogle få entusiaster begyndte at teste netværket og rapportere fejl. I begyndelsen var det dog hovedsageligt Satoshi Nakamoto selv der holdt netværket kørende. Langsomt blev nyheden om det nye netværk spredt til computer- og teknik-forums og interessen for netværket steg støt. Efter et år havde Bitcoin netværket allerede nogle brugere, men Bitcoin selv (den digitale valuta) havde endnu ingen værdi.

Hvem er Satoshi Nakamoto?

Både ”The Bitcoin Whitepaper” og e-mail korrespondance fra opfinderen af Bitcoin blev signeret med navnet Satoshi Nakamoto. Der er dog stadig ingen der kender den sande identitet af opfinderen af Bitcoin, da det tyder på, at navnet er et alias. Nakamoto brugte mindst tre forskellig e-mail adresser, der alle var grundigt krypterede for at skjule afsenderens sande identitet, til at kommunikere med ligesindede og sidenhen fællesskabet af Bitcoins softwareudviklere.

Forskellige personer har påstået at være Satoshi Nakamoto. Men indtil videre har ingen været i stand til at bevise deres påstande. Det ultimative bevis ville være at sende Bitcoin fra en af de Bitcoin adresser der efter al sandsynlighed tilhører Satoshi, men det har ingen endnu været i stand til.

Desuden er den gruppe af mennesker der har kommunikeret ”personligt” med Satoshi Nakamoto via Internettet meget lille. Satoshi Nakamoto skrev sin sidste besked til Bitcoin fællesskabet d. 12. december 2010, men den var ikke formuleret som en afsked – Satoshi stoppede ganske enkelt med at kommunikere efterfølgende.

Han tilbagetrækning var dog kun i forhold til det bredere fællesskab. Nakamoto fortsatte med at samle en mindre gruppe af kerne-programmører omkring sig, og han informerede dem om den videre udvikling af Bitcoin netværket. Men d. 11. april 2011 sendte han også en sidste besked til denne gruppe. På ligeså mystisk vis som Nakamoto dukkede op i 2008 forsvandt han igen tre år senere.

Bitcoin's "Pizza Day"

Men hvordan fik Bitcoin værdi til en start? I starten kunne Bitcoin udvindes (på engelsk: "mine") og sendes frem og tilbage mellem brugerne på netværket, men de digitale enheder havde ingen værdi. Ikke mindst fordi gruppen af personer der kendte til Bitcoin, samt kunne sende og modtage det, stadig var meget lille.

Dette ændrede sig d. 22. maj 2010 da en usædvanlig forespørgsel dukkede op på Internet forummet bitcointalk.org.En 28-årig mand ved navn Laszlo Hanyecz fra Florida tilbød 10,000 Bitcoin til enhver, der kunne bestille to pizzaer leveret til hans hjem. En studerende fra Californien slog til og fik to store pizzaer til en værdi af $41 leveret til hans hjem. Dernæst sendte Hanyecz ham de 10,000 Bitcoin.

Siden den dag er d. 22. maj årligt blevet fejret af Bitcoinere som Bitcoin "Pizza Dag". Dagen blev populær da den illustrerer tre ting:

- Bitcoin har en værdi
- Bitcoins er brugbare som overførsel af værdi og betaling

- Bitcoin som en valuta er defaltionær.

Antallet af nye Bitcoin bragt i cirkulation er støt faldende, hvilket kan føre til en stigning i værdien.

De to pizzaer er gået over i historiebøgerne som de dyreste i verden. Hvis man udregner hvad de kostede med prisen for Bitcoin i december 2021, så blev der betalt utrolige 460 millioner US dollars for dem. Det er enormt mange penge. Men modtageren af de 10,000 Bitcoin har også allerede brugt dem. I et interview udtaler han, at han solgte dem ikke længe efter for at betale for en rejse – til den nutidige pris for Bitcoin sandsynligvis også den dyreste rejse i historien.

Bitcoins "Pizza Dag" illustrerer også

på overbevisende vis hvorfor "Hodling" – udledt af "to hold" – er så populært blandt Bitcoinere. "Hodling" betyder at man beholder sine Bitcoins over længere perioder med hensigten om (muligvis) aldrig at sælge dem. Hvem ønsker at bruge sine Bitcoin i dag, hvis de kunne vise sig være det dobbelte, det tredobbelte eller endda ti gange mere værdifulde i de kommende år?

The Bitcoin „Pizza Day" also impressively illustrates why ‚hodling' - derived from ‚to hold' - is so popular among Bitcoiners. 'Hodling' means keeping one's Bitcoin over extended periods with the intent of (possibly) never selling them. After all, who wants to spend their Bitcoin today when they could be worth double, triple, or even ten times as much in the years to come?

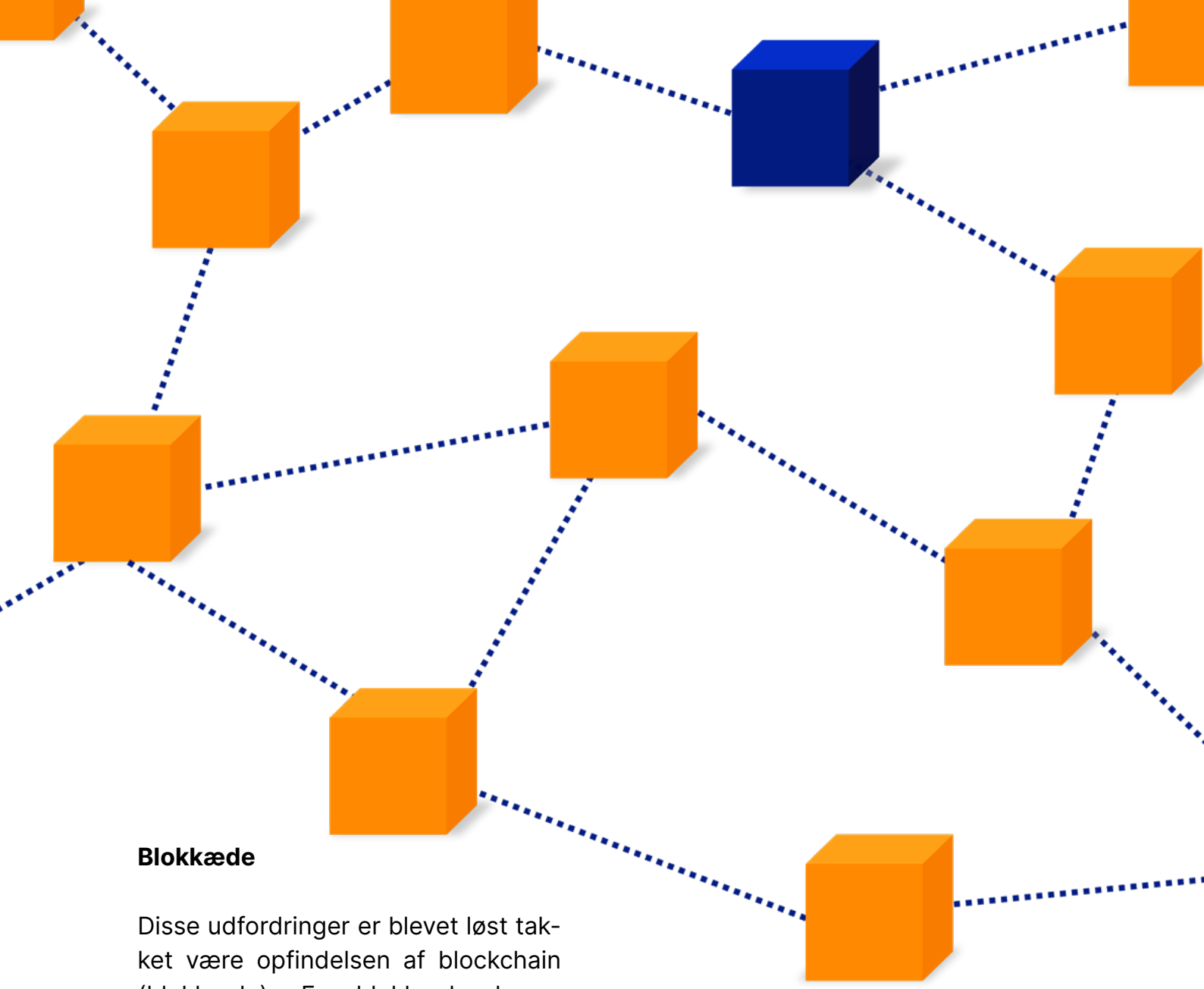
HVORDAN FUNGERER BITCOIN?

Efter at have hørt om Bitcoins historie, vil vi nu dykke ned i hvordan de virker. Målet er at forstå, hvordan Bitcoin netværket fungerer, hvilke problemer det løser og hvad dets praktiske fordele er.

Intentionen bag Bitcoin er at være et decentraliseret netværk. Ingen netværksdeltager skal være i stand til at bestemme over netværket alene – beslutningstagning og supervision er distribueret imellem alle deltagere. Dette er vigtigt, for det betyder at intet individ, ingen regering eller stat og ingen virksomhed kan ændre netværket enkeltvis, men ændringer er kun mulige kollektivt.

Bitcoin virker således, at alle deltagere i netværket har en identisk kopi af den seneste opgørelse af ejerskab i hovedbogen (regnskabet så at sige, kaldet "the ledger" på engelsk) – og som et resultat heraf ved alle hvem der på det givne tidspunkt ejer hvilke Bitcoin. Derfor kan ingen påstå at eje flere Bitcoins end de faktisk gør, fordi enhver netværksdeltager kan tjekke påstanden mod deres kopi af hovedbogen og bevise at den er usand.

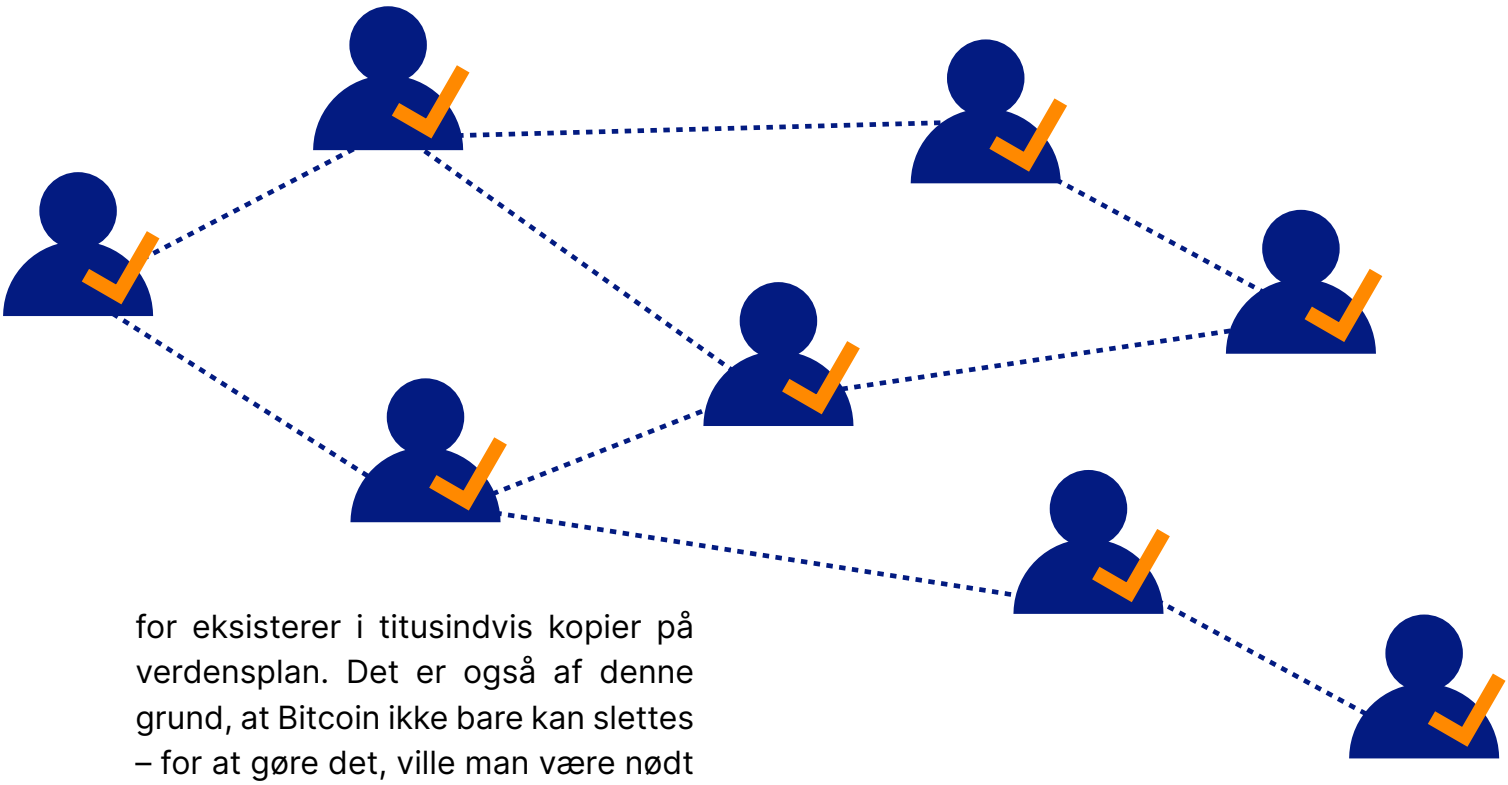
Før Bitcoin blev igangsat, havde decentraliserede netværk to store udfordringer. For det første, hvordan kan det sikres, at alle netværksdeltagere modtager de seneste opdateringer vedrørende ændringer i ejerskab, dvs. informationen om hvilke Bitcoins er blevet overført og til hvem. Og for det andet, hvordan kan netværksdeltagerne verificere med absolut sikkerhed, at informationen de modtager er korrekt.



Blokkæde

Disse udfordringer er blevet løst takket være opfindelsen af blockchain (blokkæde). En blokkæde lagrer informationer og data i kronologisk orden. I Bitcoins tilfælde er alle transaktioner siden skabelsen af Bitcoin lagret kronologisk i titusindvis af blokke, der tilsammen udgør Bitcoin-blokkæden. Enhver netværksdeltager der ønsker at vide hvem der ejer hvilke Bitcoin, kan spore transaktionshistorikken på Bitcoin-blokkæden og afgøre præcist hvem der ejer hvilke Bitcoin på ethvert givent tidspunkt. Det betyder, at hvis en person ønsker at sende en Bitcoin, kan enhver verificere om denne Bitcoin virkeligt tilhører den person.

Indtil videre er denne mekanisme ikke nogen nyskabelse, idet banker benytter sig af en lignende proces. Hvis en kunde ønsker at bruge en Schweizisk Franc, kigger banken i transaktionshistorikken for at se om den Franc stadig tilhører kunden, eller om den allerede er blevet brugt (sendt til en anden person). Den unikke karakteristik ved en blokkæden derimod er, at denne information ikke bliver lagret på en central bank server, men på alle netværksdeltagernes computere (såkaldte ”full nodes”) og der-



for eksisterer i titusindvis kopier på verdensplan. Det er også af denne grund, at Bitcoin ikke bare kan slettes – for at gøre det, ville man være nødt til at slette kopierne af blokkæden på alle netværksdeltagernes computere på samme tid.

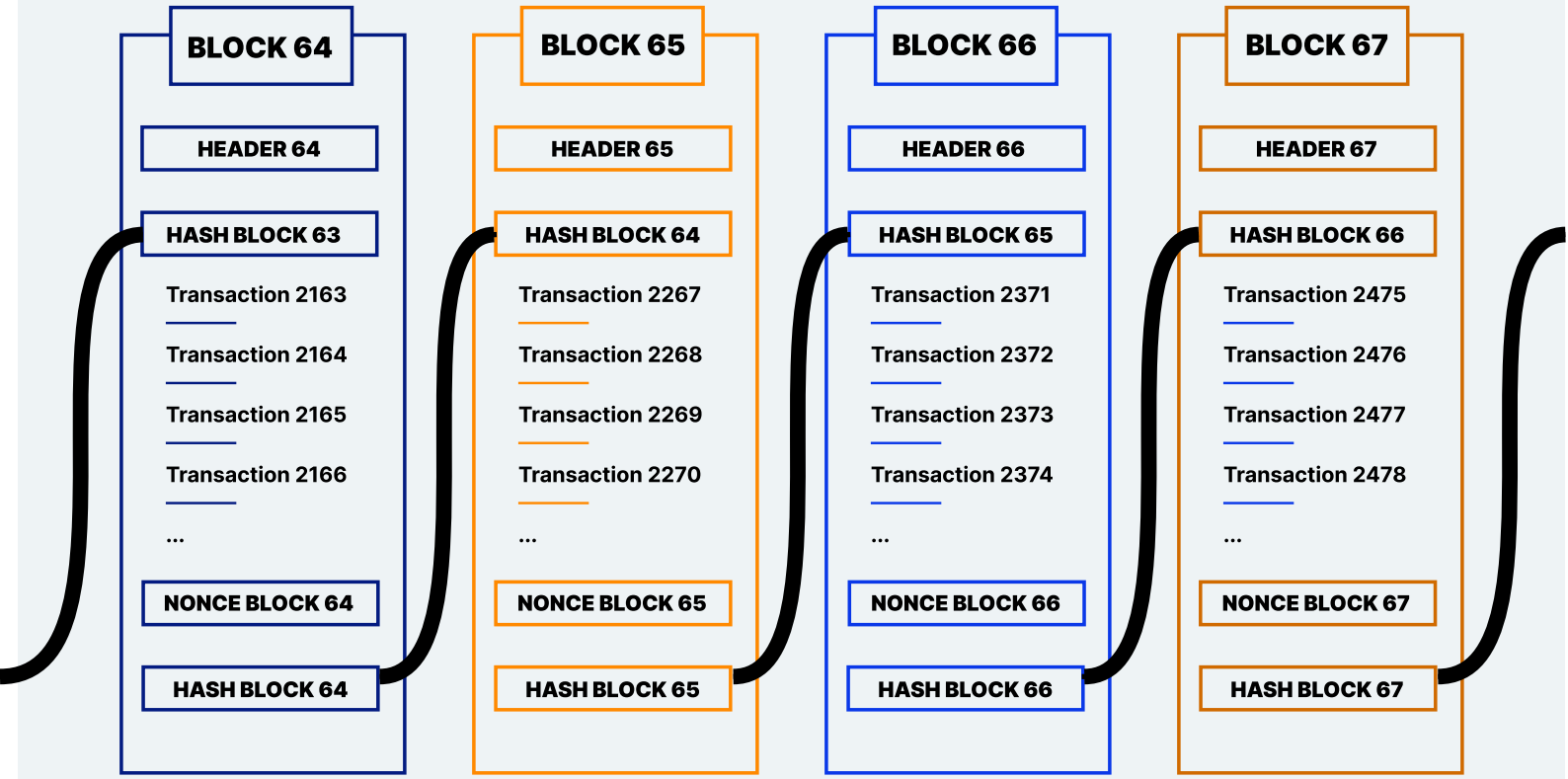
Men udfordringen for blokkæder er, at alle netværksdeltagerne skal være i stand til at afgøre med absolut sikkerhed at deres kopi af blokkæden er den korrekte, og at ingen fejlagtige eller svigagtige transaktioner finder vej til deres kopi af hovedbogen (the ledger). Idet nye blokke med nye transaktioner tilføjes blokkæden hvert 10. minut, betyder det at blokkæden konstant vokser og kontinuerligt skal opdateres på alle netværksdeltageres computere rundt omkring i verden.

Disse nyligt tillagte blokke skal være verificerbare for alle. Verifikationen foretages ved at benytte uforanderlige regler, der er definerede i computerkoden for Bitcoin netværket. Disse regler definerer nøjagtigt hvilke transaktioner der er tilladte og hvilke der ikke er. Alle brugere der downloader en kopi af blokkæden, kan derfor verificere om alle transaktioner er i overensstemmelse med de givne regler. Hvis en transaktion ikke overholder reglerne, f.eks. hvis den er fejlagtig eller svigagtig, bliver den afvist af netværksdeltagerne (full nodes) og bliver derfor ikke inkluderet i blokkæden.

Proof-of-Work (PoW) udvinding

I tillæg, har Bitcoin netværket en mekanisme der begrænser tilføjelsen af nye blokke. Hvis nye transaktioner og blokke kunne tilføjes af enhver, så ville netværket ende i kaos, da blokkæden ikke ville være i stand til opdatere sig på verdensplan til den samme version hurtigt nok.

For at undgå dette arbejder Bitcoin med en såkaldt Proof-of-Work mekanisme. For at opnå retten til at tilføje en ny blok til blokkæden, må man føre bevis for at man har udført et arbejde (proof of work). En sim-



Overskriften/header'en, resultatet af den forrige bloks hash-funktion, alle transaktioner i den aktuelle blok og en nonce (tilfældigt tal) sættes i en matematisk funktion. Nonce'en ændres, indtil resultatet af hashfunktionen har nok forudgående nuller. Denne proces kaldes udvinding/mine-drift.

pel illustration af denne proces er en gruppe personer der leder efter en nål i en høstak. Den der finder nålen først, får lov til at tilføje en ny blok til blokkæden. Vedkommende får som belønning desuden nye Bitcoin enheder (udvinding) samt transaktionsgebyrer i relation til blokken. Så snart blokken er tilføjet blokkæden begynder processen forfra igen.

I virkeligheden foregår udvindingen ved at udføre en matematisk hash-funktion (SHA-256 hash-algoritme) i søgningen efter specifikke tal. Hash-nummeret for den forrige blok, transaktionerne for den aktuelle blok og et tilfældigt tal (nonce) hashes sammen. Det tilfældige tal ændres, indtil hash-funktionen spytter et resultat ud med et minimum antal foranstillede nuller. For eksempel havde blok #700000, oprettet den 11. september 2021, det gyldige hashnummer: 00000000000000000590fc0f3eba193a278534220b2b37e 9849e1a770ca959.

Søgningen efter dette tal, også kaldet udvinding ("mining" på engelsk), har to formål: For det første binder det blokkene sammen på matematisk-kryptografisk vis således at alle nemt kan verificere den korrekte rækkefølge. På samme tid gør Proof-of-Work mekanismen det tæt på umuligt at ændre denne rækkefølge. For det andet så forsinker denne mekanisme tilføjelsen af nye blokke således at, i gennemsnit, en ny blok tilføjes til

blokkæden hvert 10. minut. Det betyder at alle netværksdeltagerne rundt omkring i verden får tid nok til at kunne opdatere til den samme og seneste version af blokkæden.

Altså er de der foretager udvindingen (miners), dem der holder Bitcoin netværket kørende. Takket være dem bliver nye transaktioner processeret og tilføjet til blokkæden. "Full nodes" delen af netværksdeltagerne opretholder opdaterede kopier af hovedbogen (the ledger), monitorerer at reglerne bliver overholdt og sikrer dermed at ingen fejlagtige transaktioner bliver inkluderet i blokkæden.

21 millioner Bitcoin

Selvom der konstant tilføjes flere blokke til Bitcoin-blokkæden, og de der udfører udvindingen (miners) belønnes for dette arbejde med nye Bitcoins, er det samlede antal Bitcoin begrænset til 21 millioner Bitcoin. Der vil aldrig være mere end 21 millioner Bitcoin. Men disse 21 millioner mønter var ikke i omløb fra begyndelsen. De frigives af Bitcoin-koden i henhold til en streng foruddefineret frigivelsesplan.

Da Bitcoin blev lanceret, frigav koden 50 nye Bitcoin til de der udfører udvindingen cirka hvert 10. minut. Fire år efter lanceringen er antallet af Bitcoins frigivet pr. ti minutter halveret. Denne proces kaldes ‚halvering' og beskriver det faktum, at blokbelønningen for minearbejdere falder med det halve hvert 4. år. I øjeblikket er der allerede 19 millioner Bitcoin i omløb. Det resterende antal Bitcoin (op til 21 millioner) vil blive udvundet indtil år 2140. Derefter vil de der udfører udvindingen kun blive kompenseret via transaktionsgebyrer.

Den strengt begrænsede mængde af Bitcoin-enheder er en af de grundlæggende egenskaber ved kryptovalutaen og gør Bitcoin til en ekstrem mangelvare. Denne absolutte digitale knaphed er også en vigtig forudsætning for Bitcoins funktion som lagring af værdi over lange perioder og er årsagen til, at Bitcoin ofte kaldes digitalt guld eller guld 2.0.

Resultatet: digital ejendom

Ved at se på alle egenskaber i Bitcoin netværket i kombination, kan man se vigtigheden af denne opfindelse. For første gang i historien eksisterer der et digitalt gode, der kun er tilgængeligt i et strengt begrænset antal. Bitcoins kan ikke kopieres eller duplikeres.

Takket være denne præstation omtales Bitcoin ofte som digital ejendom. For ligesom hvert stykke jord på denne jord er unikt og kun eksisterer én gang, er hver Bitcoin-enhed også unik og eksisterer kun én gang i det digitale rum.

Og disse Bitcoin-enheder kan virkelig ejes. Kun den person, der er i besiddelse af den tilsvarende private

nøgle, som er en kombination af tal og bogstaver bestående af 64 tegn, kan flytte den tilhørende Bitcoin. Med andre ord, uden denne private nøgle kan Bitcoin ikke stjæles, konfiskeres eller blokeres. Dette giver ejeren mulighed for at have absolut kontrol over vedkommendes økonomiske ressourcer, uanset om vedkommende er millionær, politisk flygtning eller en forfulgt kreditor. For første gang siden opfindelsen af computeren er det muligt virkelig at eje digitale aktiver.

HVORFOR BITCOIN?

Men hvorfor al denne hype omkring Bitcoin? Muligheden for virkelig at eje et digitalt aktiv kan være revolutionerende. Men hvorfor skulle nogen ønske at eje Bitcoin i første omgang?

Det bedste fra begge verdener

I tidligere århundreder blev ædelmetaller og senere kontanter i form af mønter og pengesedler brugt som betalingsmiddel. Disse havde den fordel, at de kunne opbevares og bruges uafhængigt af tredjeparter. Ordsproget „kontanter er trykt frihed" opsummerer dette meget godt. Ulempen ved ædelmetaller og kontanter er dog, at de er svære at bruge i det digitale rum. Senest siden fremkomsten af nethandel er debet- og kreditkort derfor blevet etableret i den brede befolkning.

Men nu hvor de fleste mennesker bruger digitale penge på bankkonti i stedet for kontanter, stiger de modpartsrisici, de står over for. Hvis for eksempel et pengeinstitut erklærer sig insolvent, kan kundernes opsparing gå tabt. Eller, som det skete på Cypern i 2013, hvis kontanthævninger er stærkt begrænset, kapitalkontrol er på plads, og der sker tvungen ekspropriation på opsparingskonti, så har folk ikke længere kontrol over deres egne penge. Eller, som det nu er tilfældet i mange vestlige lande, hvis bankkunder ikke må sende penge til slægtninge, fordi de bor i Cuba eller Iran, er de afhængige af en tredjepart til at godkende alle deres transaktioner.

Med skiftet fra papirbaserede til digitale penge, stående på bankkonti, har vi i sidste ende ikke længere kontrol over vores egne penge. Indtil nu har denne ulempe dog været den pris, vi skulle betale for at deltage i et digitaliseret liv.

Bitcoin tilbyder en løsning på det-

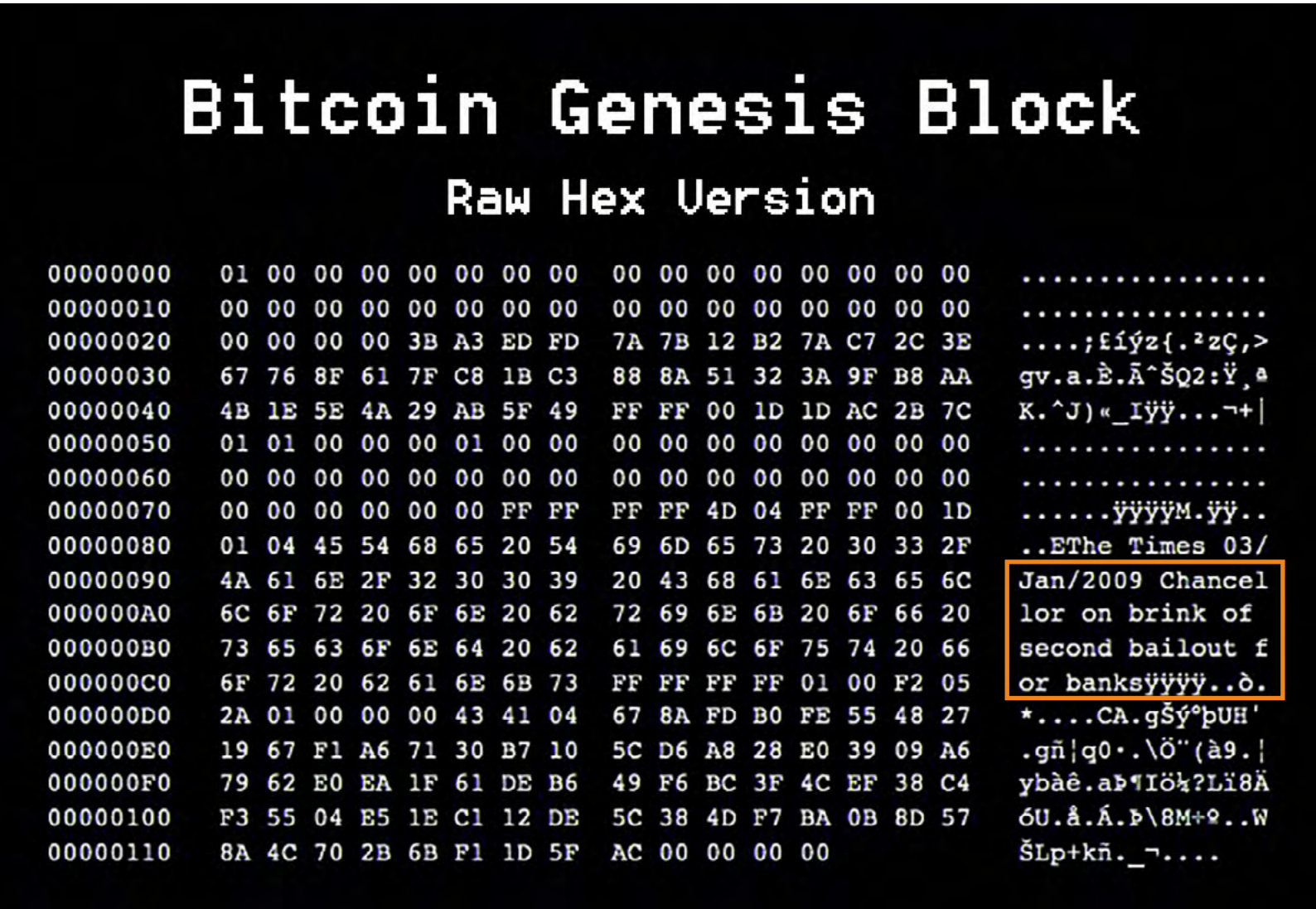
te dilemma. Som digitale penge er de ideelle til brug i det digitale rum. Samtidig kan Bitcoin opbevares som digital ejendom uden at skulle forlade sig på tredjeparter (banker) for opbevaring. Så Bitcoin-ejere kan opbevare deres mønter – i form af de private nøgler – under madrassen, eller hvor de nu synes, det er sikrest.

Perfekt timing

Bitcoin blev skabt midt i den globale finanskrise i 2008/09. På den første blok af Bitcoin-blokkæden – også kaldet Genesis-blokken – efterlod Satoshi Nakamoto et stærkt budskab. Han citerede en overskrift offentliggjort i avisen The Times, der lyder: „ Chancellor on brink of second bailout for banks."

Med denne handling udtrykte Satoshi Cypherpunkernes statskritiske filosofi. I finanskrisen i 2008 satte centralbankerne enorme mængder nye penge i omløb for at redde bankerne. I sidste ende betalte opsparerne dog for det, da deres opsparing mistede værdi gennem udvanding af pengemængden. Dette faktum bekræftede endnu en gang Cypherpunkerne i deres mistillid til staten og centralbankerne og forstærkede deres overbevisning om, at der var et presserende behov for penge der var uafhængige af staten.

Den samme metode, bare i endnu større skala, er blevet gentaget med udbruddet af Covid-19-pandemien.



Alene i 2020 blev den amerikanske pengemængde udvidet med 50 procent, og i andre lande – inklusive Schweiz – kører den digitale trykpresse konstant. En direkte konsekvens af dette er rekordlave renter – endda negative renter i Schweiz – og høj inflation i aktiver.

Afdækning af risiko for valutadevaluering

Bitcoin blev derfor lanceret på det bedst mulige tidspunkt. Sjældent har pengespørgsmålet været mere relevant og spørgsmålstegnene større end i dag. Med sit begrænsede udbud på 21 millioner giver Bitcoin en behagelig kontrast til centralbankernes endeløst voksende balancer. Dets begrænsede udbud giver beskyttelse mod udvanding af ens kapital, som det er blevet observeret med alle valutaer verden over i de sidste årtier.

På grund af dets specifikke opbygning er Bitcoin designet til at sikre bevarelsen af købekraft over tid. Da Bitcoin er knap, burde den være endnu bedre til denne opgave end guld, som har en nettotilgang på 1-2% hvert år. Derudover er omkostningerne ved opbevaring og transport af Bitcoin også væsentligt lavere sammenlignet med guld, hvilket også giver mulighed for bedre værdibevarelse over tid.

Ejendomsbeskyttelse

Et andet problem, som Bitcoin afhjælper, er beskyttelsen af ejendom. Mens guld eller kontanter normalt skal opbevares sikkert, med store omkostninger til følge, for at beskytte dem mod tyveri, kan Bitcoin opbevares og transporteres til næsten ingen omkostninger. Selv betydelige beløb kan tages med overalt i verden med en kode bestående af tolv eller fireogtyve ord. Når først den er blevet husket og fysisk ødelagt, kan denne kode ikke stjæles af nogen, hvilket gør Bitcoinen bag koden sikker og tillader dens ejer at tage dem med i graven, hvis det ønskes.

KØB BITCOIN

Der er to måder at anskaffe sig Bitcoin på. Enten tjener du Bitcoin som udvinder (mining), eller også køber du Bitcoin af en anden person. Da udvinding med hjemmeenheder (computere) er blevet praktisk talt umuligt i dag, er den eneste vej tilbage for nytilkomne at købe Bitcoin.

Kryptobørser & mæglere

Den nemmeste måde at købe Bitcoin på er gennem en kryptobørs eller en mægler. Disse fungerer på samme måde som aktiehandelsplatforme. Efter åbning af en personlig konto kan schweizerfranc, euro eller amerikanske dollars overføres via bankoverførsel eller kreditkort. Når pengene er ankommet på den personlige konto på børsen, kan Bitcoin købes 24/7 med få klik til den aktuelle markedspris. I Europa er det muligt at købe Bitcoin uden registrering, verifikation eller krav om først at skulle indbetale penge med den populære Bitcoin-dedikerede investeringsapp Relai.

Peer-to-peer

Som et alternativ til kryptobørser kan Bitcoin også købes direkte fra andre markedsdeltagere via peer-to-peer platforme uden at involvere en børs. Dette giver mulighed for større anonymitet, da ingen persondata skal afsløres i processen.

Bitcoin ATMs

Der er også mulighed for at hæve Bitcoin via hæveautomater. Disse er allerede tilgængelige i mange lande, herunder Schweiz, Tyskland, og Østrig.Hos Bitcoin-hæveautoma-

ter kan Bitcoin hæves anonymt med kontanter eller kreditkort. Hverken en konto eller en eksisterende kryptopung er nødvendig.

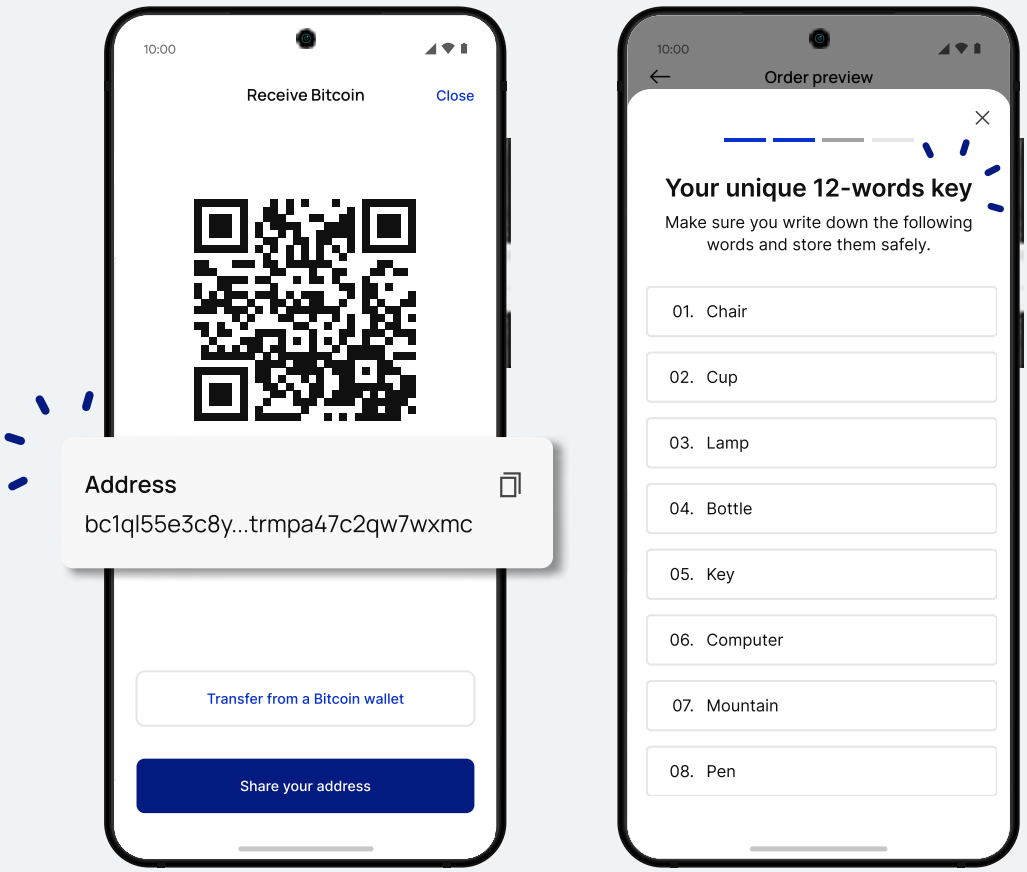
Opbevar Bitcoin sikkert

Når først Bitcoins er blevet erhvervet, opstår spørgsmålet om sikker håndtering og opbevaring. Bitcoin og kryptovalutaer er styret af princippet: „ikke dine nøgler, ikke dine mønter". For virkelig at eje din Bitcoin skal du være i besiddelse af de tilsvarende private nøgler. Dette lidt tekniske udtryk betyder, at du først rigtig har kontrol over din Bitcoin, hvis du gemmer dem i en personlig digital pung, som du har de private nøgler til.

Så længe Bitcoins er deponeret på en kryptobørs, er de under børsens kontrol. Hvis børsen er hacket, går konkurs eller er svigagtig, kan dine Bitcoin gå tabt for altid.

Egen varetægt

I modsætning til en bankkonto giver Bitcoin dig mulighed for at gemme dine pengeenheder i en personlig pung. Dette giver dig mulighed for at være din egen bank og har den fordel, at du har absolut kontrol over din Bitcoin. Til gengæld følger der hermed også ansvar. Den private nøgle, som ofte kommer i form af tolv eller fireogtyve ord, skal opbevares og opbevares sikkert af ejeren af den/de respektive Bitcoins selv. Forkert eller uagtsom håndtering kan føre til uigenkaldeligt tab af Bitcoins.



Punge: digitale punge

Digitale punge hjælper til sikkert at opbevare Bitcoin, eller mere præcist, private nøgler. Selve Bitcoin er altid gemt på blockchain og kan ikke overføres til en pung. Kun adgangsnøglerne til Bitcoin kan opbevares i en pung.

Så punge blev skabt til at opbevare de private nøgler sikkert og på en enkel måde. Desuden gør de det muligt at sende og modtage Bitcoin med blot et par klik. Således er punge et nyttigt værktøj til at håndtere Bitcoin.

Softwarepunge

De mest almindelige punge er softwarepunge. Softwarepunge kan konfigureres som desktop-applikationer eller som smartphone-apps. Under opsætningen vises de private nøgler til pungen i form af tolv eller fireogtyve ord (seed sætning). Disse ord er synonyme med Bitcoin i den pung. Den, der kender disse ord, har kontrol over mønterne. Derfor skal ordene nedskrives analogt, gerne på papir, i hemmelighed og opbevares sikkert. Skulle computeren eller smartphonen nogensinde gå tabt eller blive stjålet, kan pungen til enhver tid genoprettes med disse ord.

Softwarepunge har den fordel, at de kan sættes op hurtigt og er nemme at bruge. Men da softwarepunge er computerprogrammer installeret på en enhed og forbundet direkte til internettet, er der altid en risiko for hackerangreb.

Hardwarepung

Hvis du værdsætter sikkerhed, bør du bruge en hardwarepung i stedet. Disse små enheder gemmer adgangskoderne til Bitcoin på en USB-stick-lignende enhed, der kun er forbundet til computeren, når det er nødvendigt. Enheden er designet på en sådan måde, at selv en computer, der er inficeret med skadelig software, ikke kan få adgang til koderne.

Når du opretter en hardwarepung, genereres der tolv eller fireogtyve ord (seed phrase), som skal skrives ned analogt og opbevares sikkert. Hvis hardwarepungen nogensinde går tabt, kan den gendannes ved hjælp af ordene. Eksempler på hardwarepunge er BitBox og Trezor.

Made in Switzerland

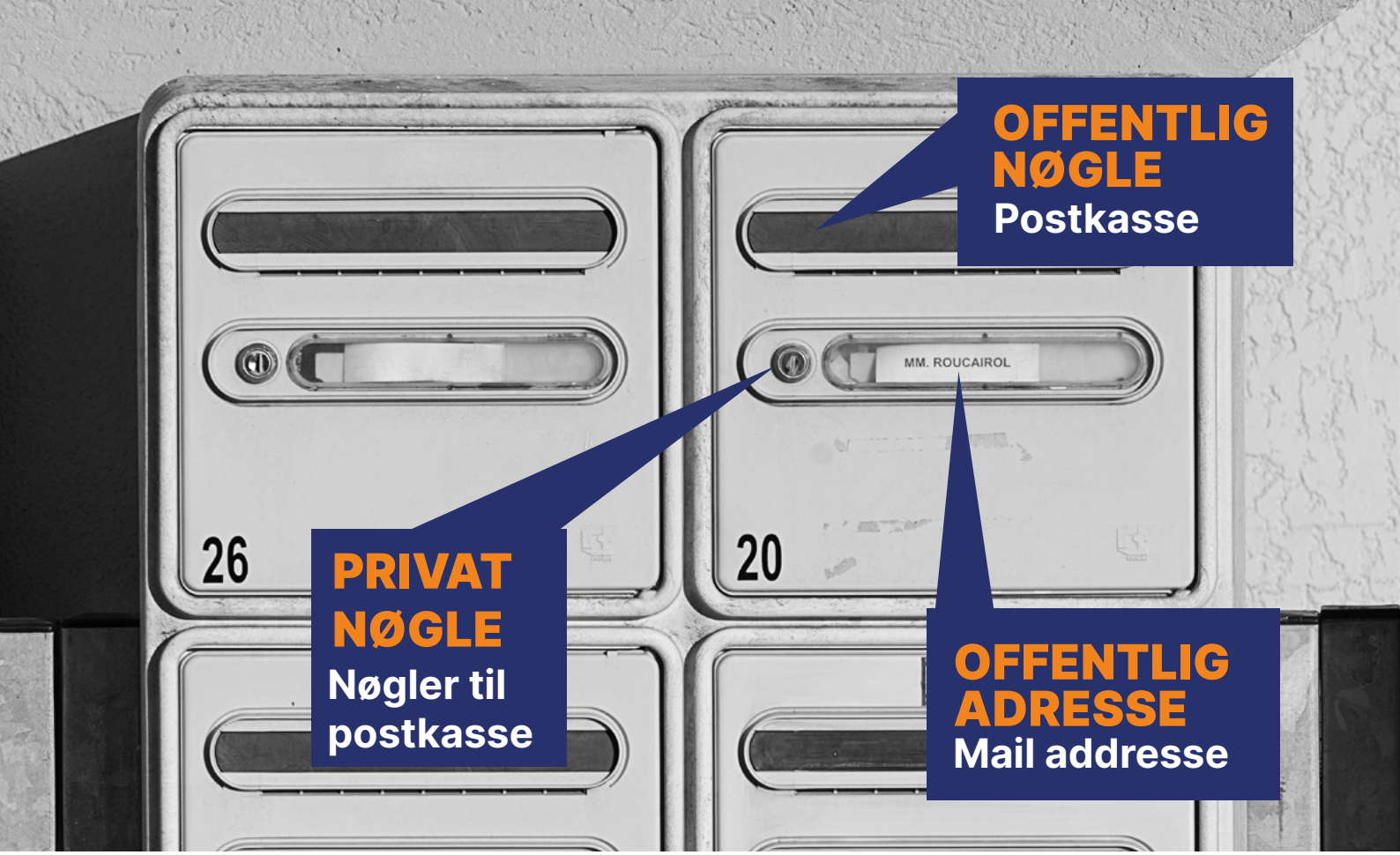
EUROPE'S EASIEST BITCOIN APP

Relai

Download on the App Store

GET IT ON Google Play

Buy bitcoin in 1 minute from as little as 10 EUR/CHF without verification.



Send og modtag Bitcoin

Det er meget nemt at sende og modtage Bitcoin. Hver Bitcoin-pung har sin offentlige adresse genereret fra den såkaldte offentlige nøgle. Dette fungerer som modtagende adresse, svarende til et IBAN. Enhver, der har denne adresse, kan sende Bitcoin til den tilsvarende pung. Adressen vises ofte som en QR-kode, hvilket yderligere forenkler håndteringen.

Hvis du vil sende Bitcoin til nogen, kan du enten indtaste modtagerens Bitcoin-adresse i din pung under ‚send' eller scanne den tilsvarende QR-kode. De påløbne transaktionsgebyrer trækkes automatisk fra afsenderens pung. Størrelsen af transaktionsgebyrerne varierer afhængigt af netværkets belastning og kan slås op here. Det tager i gennemsnit 10 minutter for overførslen at nå frem til modtageren. Det kan dog også tage længere tid, afhængigt af antallet af transaktionsgebyrer, som du er villig til at betale.

Betal med Bitcoin

Da Bitcoin blev skabt, håbede man, at Bitcoin en dag kunne bruges til at betale for hverdagsvarer. Og i teorien er det muligt i dag. Nogle statslige skatteafdelinger, non-profit organisationer og et stigende antal virksomheder accepterer Bitcoin som betalingsmiddel. Men da transaktioner via Bitcoin-netværket kan koste flere francs og tage mindst 10 minutter, giver dette kun mening for større beløb. For at sende Bitcoin billigt og hurtigt er der brug for en alternativ løsning.

Lightning-netværket - hurtigere og billigere

Derfor blev der bygget et ekstra lag oven på Bitcoin-netværket. Dette netværk, kaldet Lightning, gør det muligt at betale med Bitcoin på få sekunder til en minimal pris. I lande som El Salvador er Lightning-netværket allerede i aktivt og succesfuldt brug.

At betale for hverdagsvarer med Bitcoin vil derfor i høj grad foregå via Lightning-netværket i fremtiden. Udviklingen på dette område kører for fuld fart. Twitter introducerede for eksempel for nylig en ‚tip'-funktion, der bruger Lightning-netværket. Appen Strike tilbyder desuden verdensomspændende betalinger i forskellige valutaer uden omkostninger via Lightning-netværket. Det må derfor forventes, at der i fremtiden kun vil blive afregnet større beløb direkte via Bitcoin-netværket, mens alle andre transaktioner vil køre via Lightning-netværket.

Da der primært sendes mindre beløb gennem Lightning-netværket, bruges Satoshis eller kort Sats som regningsenhed i stedet for Bitcoin. 1 Bitcoin er lig med 100.000.000 Sats. For at bruge Lightning-netværket skal der konfigureres en Lightning-pung.

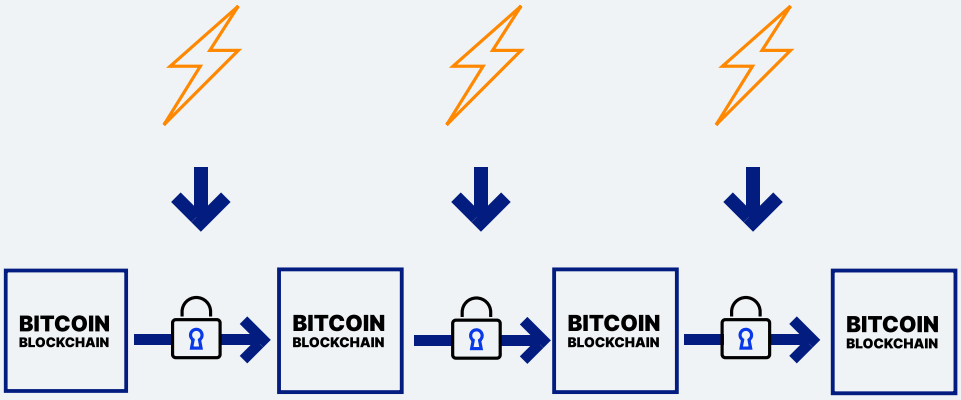
ET KIG IND I FREMTIDEN

I sine mere end ti års eksistens har Bitcoin gennemgået mange op- og nedture. Kryptovalutaen blev erklæret død eller faldt i glemmebogen blandt offentligheden flere gange efter store kurstab. Bitcoin har dog spredt sig ubønhørligt rundt om i verden i løbet af det sidste årti.

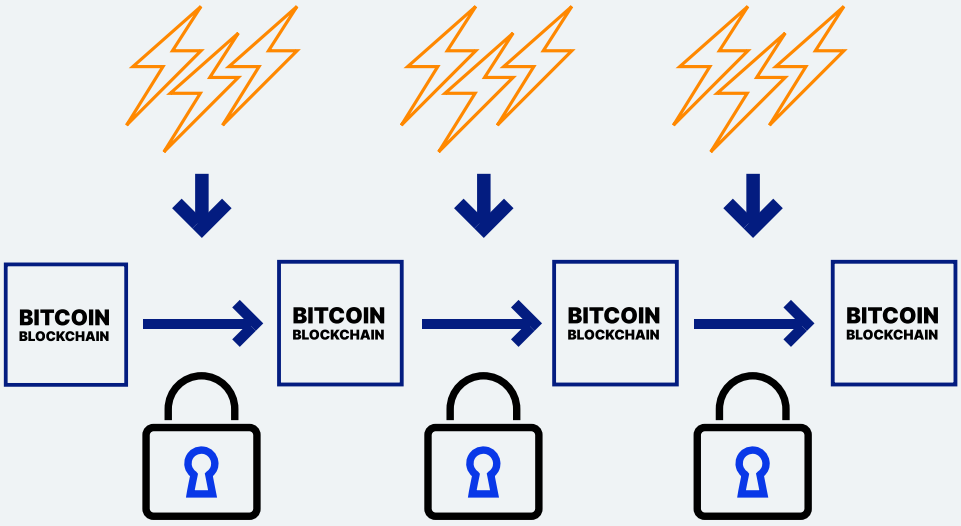
Bitcoin og energi

En af de første bekymringer, der ofte rejses vedrørende udviklingen af Bitcoin, er Bitcoin-netværkets energiforbrug. Bitcoin-minedrift forbruger allerede en betydelig mængde elektricitet på verdensplan. Og dette forbrug vil sandsynligvis stige i fremtiden, efterhånden som flere mennesker kommer ind i Bitcoin-minedrift.

Jo mindre energi i form af computerkraft der bruges til at bygge Bitcoin blokkæden, jo lettere er det at ændre den senere.



Jo mere energi i form af computerkraft der bruges til at skabe Bitcoin Blokkæden, jo sværere er det at ændre den senere.



Når man taler om Bitcoin og energi, er det vigtigt at forstå, at mængden af energi, der strømmer ind i Bitcoin-netværket, er afgørende for netværkets sikkerhed. Jo mere energi, der strømmer ind i netværket, jo mere sikkert er det. Dette skyldes, at for at Bitcoin blokkæden kan ændres, skal den samme mængde computerkraft - og dermed energi - som blev investeret for at skabe blokkæden i første omgang bruges igen. Men med millioner af computere verden over, der leverer computerkraft til Bitcoin-netværket, er det næsten umuligt for en person, en organisation eller en stat nogensinde at samle nok computerkraft til at foretage selv de mindste ændringer i blokkæden. Derfor er hashpower og det tilhørende energiforbrug en vigtig sikkerhedsfunktion i Bitcoin-netværket.

Desuden har Bitcoin-minecomputere den fordel, at de kan placeres hvor som helst i verden. Da Bitcoin-minedrift har brug for den billigst mulige elektricitet for at være rentabel, placerer den sig ofte steder, hvor der er meget overskud og derfor billig energi. På længere sigt vil det sandsynligvis være steder, hvor der er meget vedvarende energi, da det giver den billigste strøm.

Ifølge Bitcoin Mining Council bruger Bitcoin-minearbejdere i øjeblikket omkring 56% vedvarende energi, og tendensen er stigende. Mange Bitcoin-eksperter mener, at Bitcoin-minedrift vil blive drevet af op til 100 % vedvarende energi i fremtiden.

Indtil det er tilfældet, koger Bitcoins energiforbrug dog ned til spørgsmålet om, hvorvidt sikre og uforfalskede penge og beskyttelse af opsparinger er dette energiforbrug værd - eller ej.

El Salvador - Bitcoin som national valuta

For et par år siden troede visionære allerede, at det var muligt, at Bitcoin en dag ville blive anerkendt som lovligt betalingsmiddel af nationalstater. I sommeren 2021 var tiden kommet: El Salvador var det første land i verden, der introducerede Bitcoin som lovligt betalingsmiddel. I butikker, restauranter og hos alle slags serviceudbydere kan betaling ikke kun ske med amerikanske dollars, men også med Bitcoin. Til dette formål blev borgerne forsynet med en tilpasset Bitcoin-pung, som muliggør betalinger via Lightning-netværket på få sekunder og til en minimal pris.

Andre lande som Ukraine, Brasilien og Panama diskuterer i øjeblikket lignende lovudkast. Skulle andre lande følge El Salvadors eksempel, vil dette på den ene side yderligere øge efterspørgslen efter Bitcoin og endnu vigtigere understøtte Bitcoins troværdighed som ‚penge'. Accepten af Bitcoin som lovligt betalingsmiddel i flere og flere lande repræsenterer derfor en afgørende fase i Bitcoins globale tilpasningsproces.

Love og regler

Denne udvikling har ført til, at nationalstater, centralbanker og virksomheder er nødt til at beskæftige sig intensivt med kryptovalutaer. Forskellige stater, herunder Schweiz,har udstedt regler og retningslinjer vedrørende kryptovalutaer. Dette skridt hilses velkommen af mange markedsdeltagere, da det skaber retssikkerhed for både kryptoprojekter og de involverede investorer.

Regler er også på vej i USA, som hidtil har taget en laissez-faire-tilgang. Den nøjagtige form, disse nye reguleringslove i USA vil antage, bliver nøje overvåget af det globale kryptosamfund, da de vil have en stor indflydelse på hele kryptosektoren.

Andre kryptovalutaer

Bitcoin er langtfra den eneste kryptovaluta i dag. Der er nu over 16.000 forskellige kryptovalutaer og aktiver. Disse mønter og tokens har forskellige karakteristika og funktionaliteter og er ikke alle designet som ‚valutaer' eller penge. Nogle er mere som aktier, idet deres værdi afspejler succesen med et kryptoprojekt. Andre er forpligtet til at gøre brug af en bestemt tjeneste. Og atter andre -

såkaldte meme-tokens - er primært sjove valutaer.

For at undgå tab er det derfor tilrådeligt at se nærmere på den respektive valuta og projektet bagved, før der foretages nogen investering.

Centralbanks digitale valutaer (CBDC)

Kryptovalutaer er i overgang fra en ureguleret Wild-West-fase til en reguleret kryptofinansverden. Denne udvikling har ikke efterladt centralbanker uskadt, og der er rejst spørgsmål om ikke centralbanker bør udstede deres egne kryptovalutaer. Disse „Central Bank Digital Currencies" eller CBDC'er ville, siger fortalere, kombinere stabiliteten af en statsvaluta med fordelene ved en blokkæde-baseret valuta. Kort sagt ville de skabe digitale kontanter, så at sige.

Men afhængigt af dens design kan en CBDC antage fundamentalt forskellige former.
Forskellige lande har lanceret pilotforsøg med forskellige typer CBDC'er, og CBDC'er er allerede blevet lanceret i nogle få lande. Det bliver dog spændt afventet om, og i hvilken form økonomisk stærke valutaområder som USA, EU eller Kina, vil lancere deres CBDC'er.

Pengekonkurrence

Vores samfund er blevet så vant til statsvalutaer i de seneste årtier, at andre typer penge næppe var tænkelige for mange indtil for nylig. Men for ikke så længe siden var det en del af hverdagen at have forskellige typer penge cirkulerende sideløbende. Der var pengesedler fra forskellige banker, mønter lavet af forskellige metaller og andre monetære værdier, der kunne bruges som betalingsmiddel.

Med Bitcoin er ikke-statslige valutaer nu tilgængelige igen som et alternativ til statsvalutaer. Indtil videre har flertallet af regeringer tolereret Bitcoin. Til en vis grad kan dette være takket være dens decentraliserede karakter, som gør Bitcoin svær at angribe. For borgerne betyder det, at et digitalt alternativ til statens penge nu er tilgængeligt ved siden af guld og sølv. Effekterne af denne yderligere monetære konkurrence bliver spændende at observere i fremtiden.

BITCOIN, HVAD NU?

Hvis du spørger dig selv, hvad du skal gøre med alle disse oplysninger, så lad mig komme med et forslag. At komme ind i Bitcoins verden koster ingenting, hverken tid eller penge. Men du vil lære en teknologi at kende, der er ved at ændre vores verden og fremtiden.

Derfor: Opret en konto på en kryptobørs eller download en pung på din smartphone og køb Bitcoin for 50 CHF. Eller få en kollega til at sende dig noget Bitcoin til din pung. Men få fingrene i Bitcoin mindst én gang.

For skulle Bitcoin slå igennem og blive lige så allestedsnærværende som internettet, vil du ikke kun kende til det teoretisk, men også selv have brugt Bitcoin. Nogle gange gør dette hele forskellen, da det giver dig et førstehåndsindtryk af teknologien, og gør at du er et skridt foran et flertal af befolkningen.

OM

FORFATTEREN

Daniel Jungen er økonom og finansjournalist med ekspertise i kryptoaktiver. Daniel er medstifter af InsightDeFi, en research virksomhed, der specialiserer sig i alt der har med krypto at gøre. Sammen med hans partnere hos InsightDeFi udgiver de hver anden uge et nyhedsbrev (tysk) om Bitcoin, DeFi og Crypto.

RELAI

Grundlagt i Schweiz af Julian Liniger og Adem Bilican, efter at de havde problemer med at finde et sikkert, problemfrit sted at købe bitcoin, muliggør Relai bitcoin-opsparing og -investering i let tilgængelig form for alle. Den bitcoin-dedikerede app er designet til at være enkel og intuitiv, hvilket gør det muligt for alle i Europa at købe og sælge bitcoin inden for få minutter, uden behov for registrering, verifikation eller indbetalinger. Uafhængigt revideret og med over 35 millioner CHF i bitcoin investeret gennem sin platform, giver Relai brugerne muligheden for nye måder at opspare og investere på.

Lær mere på Relai.app.

Dieses Büchlein ist auch auf Deutsch erhältlich.