BITCOIN ZA 10 MINÚT

Všetko, čo treba vedieť o Bitcoine

Brought to you by Relai

ČO JE BITCOIN?

Bitcoin, najúspešnejšia kryptomena na svete, sa na nás valí z novinových titulkov. Mnohí by chceli na jeho vzostupe zarobiť, iní zostávajú skeptickí a niekoho to nezaujíma vôbec. Nemalým úspechom pritom je už fakt, že nová digitálna mena podnietila diskusie o peniazoch, investovaní a ekonómii všeobecne. Niekto v Bitcoine vidí len špekulatívne aktívum alebo ho považujú za bublinu, kým iní vyzdvihujú inovatívnosť, očakávajú od neho menovú revolúciu, či dokonca vykúpenie zo súčasného menového systému.

Rôzne štáty, vrátane Číny, považujú Bitcoin za hrozbu a vyhlásili kryptomenám vojnu. Iné vlády, napríklad v El Salvadore, Bitcoin postavili na úroveň zákonného platidla vo viere v pozitívne ekonomické dôsledky.

Ale čo to ten Bitcoin je? Sú to peniaze? Digitálne zlato? Zábavka pre ajťákov a špekulantov? Alebo snáď niečo úplne iné? V nasledujúcich odstavcoch tieto otázky do bodky zodpovieme a zblízka preskúmame digitálnu menu, aby sme lepšie pochopili jej filozofiu a fungovanie. Na to však musíme začať príbehom o samotných koreňoch Bitcoinu.

PRÍBEH BITCOINU

Začiatky Bitcoinu siahajú do raných deväťdesiatych rokov. Konkrétne v roku 1992 založila skupina programátorov e-mailovú diskusnú skupinu, v ktorej zdieľali svoje myšlienky na rôzne témy - kryptografiu, matematiku, politiku, či filozofiu. Začali si hovoriť Cypherpunks, čo je slovná hračka vzniknutá spojením slova cyberpunk (osoba zo sci-fi literatúry charakteristická oprávnene skeptickým pohľadom na spoločnosť) a cipher, teda šifra.

Cypherpunks

Hnutie Cypherpunks sa rozrástlo do veľkej a pestrej partičky. Napriek rozličným sféram pôsobenia ich spájalo presvedčenie, že Internet sa čoskoro stane jedným z najhorúcejších bojísk o ľudskú slobodu.

Cypherpunks sa rozhodli na ochranu pred ovládaním, špehovaním a cenzúrou Internetu a na jeho zachovanie v otvorenej, slobodnej podobe použiť mocnú zbraň - kryptografiu, šifrovanie informácií.

V roku 1993 vydali manifest, kde hlásali: “Cypherpunks píšu[počítačový] kód. Vieme, že niekto musí písať kód na obranu súkromia a [...] budeme to my, kto ho bude písať.” Šifrovanie sam o sebe však na slobodný internet nestačí. Pretože, a Cypherpunks o tom boli pevne presvedčení, Internet nemôže byť skutočne slobodný bez svojich vlastných peňazí. Peňazí nezávislých na štátoch, centrálnych bankách a firmách; teda kryptomeny, ktorá by bola slobodná a decentralizovaná ako Internet samotný.

Menové experimenty

Vytváranie nezávislých, digitálnych peňazí však prinieslo Cypherpunkom technologické výzvy. Už v roku 1990 prišiel kryptológ David Chaum s prvou kryptomenou eCash, ktorá nebola decentralizovaná, no pomocou šifrovania dokázala zabezpečiť užívateľom anonymitu. ECash sa však nedokázal dlhodobo presadiť v konkurencii ostatných online platobných systémov. Spoločnosť, ktorá za ním stála, po ôsmich rokoch zbankrotovala a eCash prestal existovať.

Prišli však nové pokusy a najznámejším bol E-Gold. Šlo o zlatom krytú kryptomenu otvorenú všetkým používateľom internetu. Založená bola v ére dot-com bubliny roku 1996 a dokázala si získať srdcia mnohých internetových užívateľov. V čase svojho vrcholu procesovala platby v hodnote dvoch miliárd vtedajších (nezabúdajme na infláciu) dolárov.
E-gold však doplatil na to, že bol ovládaný centrálnou inštitúciou - teda veľmi zraniteľný.
Čoskoro prišli problémy so zákonom - americká vláda sa rozhodla proti novej kryptomene zakročiť súdnou cestou. Roku 2008 bola firma stojaca za projektom uznaná súdom za vinnú z prania špinavých peňazí a porušení neslávneho Patriot Actu. Všetky jej aktíva boli zmrazené a E-gold bol donútený ukončiť svoje pôsobenie.

Tieto dva nevydarené pokusy však Cypherpunkom demonštrovali dve nové skutočnosti. Poprvé, eCash aj E-gold boli kolateralizované - kryté aktívami, ktoré prevádzkovateľ vlastnil. Kolaterál sa ukázal byť slabým miestom, nakoľko mohol byť - a v konečnom dôsledku aj bol - zhabaný štátom. Vyvstala tak potreba slobodnej kryptomeny bez centrálnych bodov, na ktoré by šlo zaútočiť - registrovaná spoločnosť, bankový účet alebo centralizované dátové úložisko. No a po druhé, bolo nad Slnko jasné, že vlády a regulátori budú sotva ochotní tolerovať neštátne digitálne peniaze.

Cypherpunks tak museli vyriešiť zostávajúcu otázku: Ako by mohli fungovať nezávislé digitálne peniaze bez centrálnej inštitúcie, ktorá by viedla účty a zabraňovala dvojitému použitiu tej istej mince?
Ak by sa problém dvojitej útraty podaril vyriešiť bez spoliehania sa na centrálnu autoritu, bola by šanca vytvoriť pre potreby internetu slobodné digitálne peniaze.

Mystický Akt stvorenia

Tieto skutočnosti priviedli Cypherpunkov k hľadaniu možných riešení pre kryptomenu bez kolateralizácie a centrálnej autority.
Dva najdôležitejšie projekty boli b-money (1998) a BitGold (2005). Boli to teoretické koncepty, ktoré neboli nikdy v praxi implementované, ale dizajnovo už boli veľmi blízke Bitcoinu. Šifrovanie malo byť asymetrické pomocou párov privátnych a verejných kľúčov a technológia Proof of Work

mala zabezpečovať tvorbu nových digitálnych mincí, ako sa to deje v prípade Bitcoinu. Jeho vynálezca vo svojom Whitepaperi potvrdil, že o týchto konceptoch vedel.

Pretože sa však b-money a Bitgold spoliehali na hlasovanie na konsenze (dohoda o tom, kto vlastní koľko menových jednotiek v danej chvíli), boli zraniteľné voči útokom, ktoré mohli hlasovanie zmanipulovať a teda skresliť stav vlastníctva jednotlivých menových jednotiek.

Riešenie tohto problému, ktorý stále bránil stvoreniu nových internetových peňazí, prišlo v piatok 31. októbra 2008. Toho dňa sa Bitcoinový Whitepaper, v ktorom Satoshi Nakamoto vysvetlil svoju predstavu o decentralizovanej platobnej sieti, objavil v schránkach ostatných Cypherpunkov. O dva mesiace neskôr, 3. januára 2009, bitcoinová sieť ožila.

Prvé reakcie na sieť neboli verejné. Niekoľko nadšencov začalo sieť testovať a reportovať jej chyby. Na začiatku to bol hlavne Nakamoto, kto držal sieť pri živote. Pomaly sa ale správy o nových internetových peniazoch začali šíriť po počítačových a technologických fórach a záujem o sieť začal rásť. Po roku už bitcoinová sieť mala viacerých užívateľov. Bitcoin ako taký však zatiaľ žiadnu hodnotu nemal.

Kto je Satoshi Nakamoto?

Bitcoinový Whitepaper, podobne ako e-mailová komunikácia jeho vynálezcu, boli podpísané menom Satoshi Nakamoto. Jeho skutočná totožnosť ostáva dodnes neznáma, lebo toto meno malo slúžiť len ako pseudonym. Na komunikáciu s podobne zmýšľajúcimi ľuďmi a neskôr komunitou developerov používal Nakamoto minimálne tri rôzne e-mailové adresy, ktoré boli starostlivo zašifrované, aby odosielateľova identita zostala skrytá.

Rôzni ľudia sa už pokúšali tvrdiť, že sú Satoshi Nakamoto. Dodnes to ale nikto z nich nedokázal vierohodne dokázať. Skutočný dôkaz, teda odoslanie Bitcoinu z jednej zo Satoshiho adries, totiž ešte nikto neposkytol.

Okrem toho skupina ľudí, ktorí s Nakamotom cez internet “osobne” komunikovali, je veľmi malá. Satoshi napísal svoj posledný odkaz bitcoinovej komunite 12. decembra 2010. Ten nejavil žiadne známky listu na rozlúčku - autor po ňom proste úplne prestal komunikovať.

Ukázalo sa, že sa nakoniec len presunul do širšej komunity. Nakamoto pokračoval v zhromažďovaní malej skupinky programátorov a informoval ich o ďalšom vývoji bitcoinovej siete. V apríli 2011 však poslal svoj posledný odkaz aj tejto skupine a tak, ako sa v roku 2008 záhadne objavil, o tri roky neskôr nadobro zmizol.

Bitcoinový "Pizza Deň"

Ale ako vlastne prišiel Bitcoin k svojej cene? Na začiatku sa dal Bitcoin ťažiť a posielať hore-dole po bitcoinovej sieti medzi jednotlivými jej účastníkmi, ale digitálne jednotky nemali žiadnu cenu. Skupina ľudí, čo o Bitcoine vedeli, nehovoriac o tých, čo ho vedeli posielať, však bola stále malá.

To sa zmenilo 22. Mája 2010, keď sa na internetovom fóre bitcointalk.org objavila nezvyčajná požiadavka. 28 ročný László Hanyecz z Floridy ponúkol 10 000 bitcoinov osobe, ktorá mu objedná 2 pizze a ich doručenie k nemu domov. Študent z Kalifornie ponuku prijal a objednal mu dve pizze v hodnote 41 amerických dolárov.
Od tohto dňa bitoineri oslavujú "Pizza deň". Stal sa populárnym, pretože potvrdil tri veci:

- Bitcoiny majú hodnotu
- Bitcoiny sú vhodným prostriedkom na výmenu a platby
- Bitcoin je deflačná mena. Množstvo bitcoinov, ktoré do siete pribúdajú, sa zmenšuje, čo umožňuje Bitcoinu stúpať na hodnote

Dve pizze sa tak zapísali do učebníc histórie ako najdrahšie v dejinách ľudstva. Keby sme ich cenu prepočítali na cenu bitcoinu v decembri 2021, priblížila by sa neuveriteľnej pol miliarde amerických dolárov. To už je celkom vysoká čiastka. Príjemca tých 10 000 bitcoinov ich však takisto utratil. V rozhovore vyhlásil, že onedlho bitcoiny predal - zaplatil si nimi výlet. Pri dnešnej cene bitcoinu by zrejme opäť išlo o najdrahší výlet v dejinách.

Bitcoinový "Pizza deň tiež pôsobivo ilustruje, prečo je takzvané "hodlovanie" - odvodené z anglického "to hold" - držať - medzi bitcoinermi také populárne. Hodlovanie znamená držať svoje mince po dlhé časové obdobie s úmyslom nepredávať ich. Kto by koniec koncov chcel míňať svoje bitcoiny dnes, keď môžu byť o niekoľko rokov dvoj-, troj- alebo aj desaťnásobne drahšie?

AKO BITCOIN FUNGUJE?

Z histórie Bitcoinu už to najnutnejšie vieme, teraz je čas vysvetliť si, ako funguje. Cieľom bude vysvetliť si, ako pracuje bitcoinová sieť, aké problémy rieši a aké praktické výhody prináša.

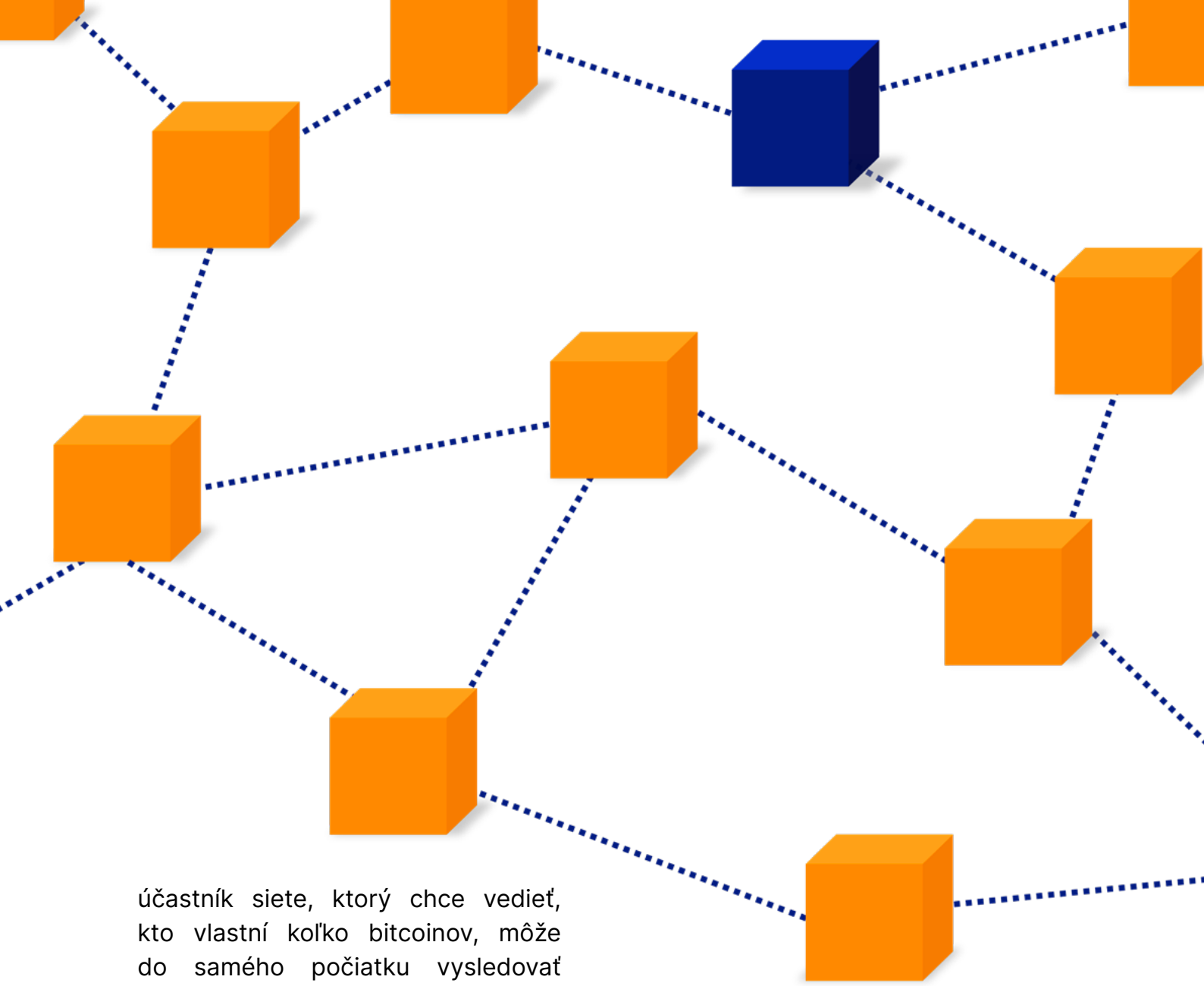
Bitcoin bol od začiatku zamýšľaný ako decentralizovaná sieť. Žiadny jednotlivý účastník siete nemá byť jej direktorom - moc robiť rozhodnutia a dohliadať na dodržiavanie pravidiel je rozdelená medzi všetkých členov siete. To je nesmierne dôležité, pretože žiadny jednotlivec, vláda, či spoločnosť nemôže sieť sama o sebe zmeniť, zmeny sú možné len prostredníctvom zhody väčšiny kolektívu.

Bitcoin funguje tak, že každý účastník siete má (vo svojom počítači) identickú kópiu najnovšej verzie účtovnej knihy, v ktorej sú zapísané zostatky účtov na každej peňaženke. Vo výsledku sa každý môže kedykoľvek presvedčiť, koľko ktorákoľvek adresa v danej chvíli drží bitcoinov. Tým pádom nikto nemôže tvrdiť (podvádzať), že drží viac bitcoinov, než v skutočnosti drží, lebo každý používateľ siete si dokáže skutočný stav overiť vo svojej kópii účtovnej knihy a a prípadného klamára usvedčiť.

Než bol Bitcoin spustený, decentralizované siete čelili dvom hlavným výzvam. Poprvé, ako zabezpečiť, že všetci účastníci dostávajú najnovšie aktualizácie zmien vo vlastníctve - to znamená informácie o bitcoinoch, ktoré boli presunuté, od koho a ku komu. Po druhé, ako si účastníci môžu overovať s absolútnou istotou, že získané informácie sú pravdivé.

The Blockchain

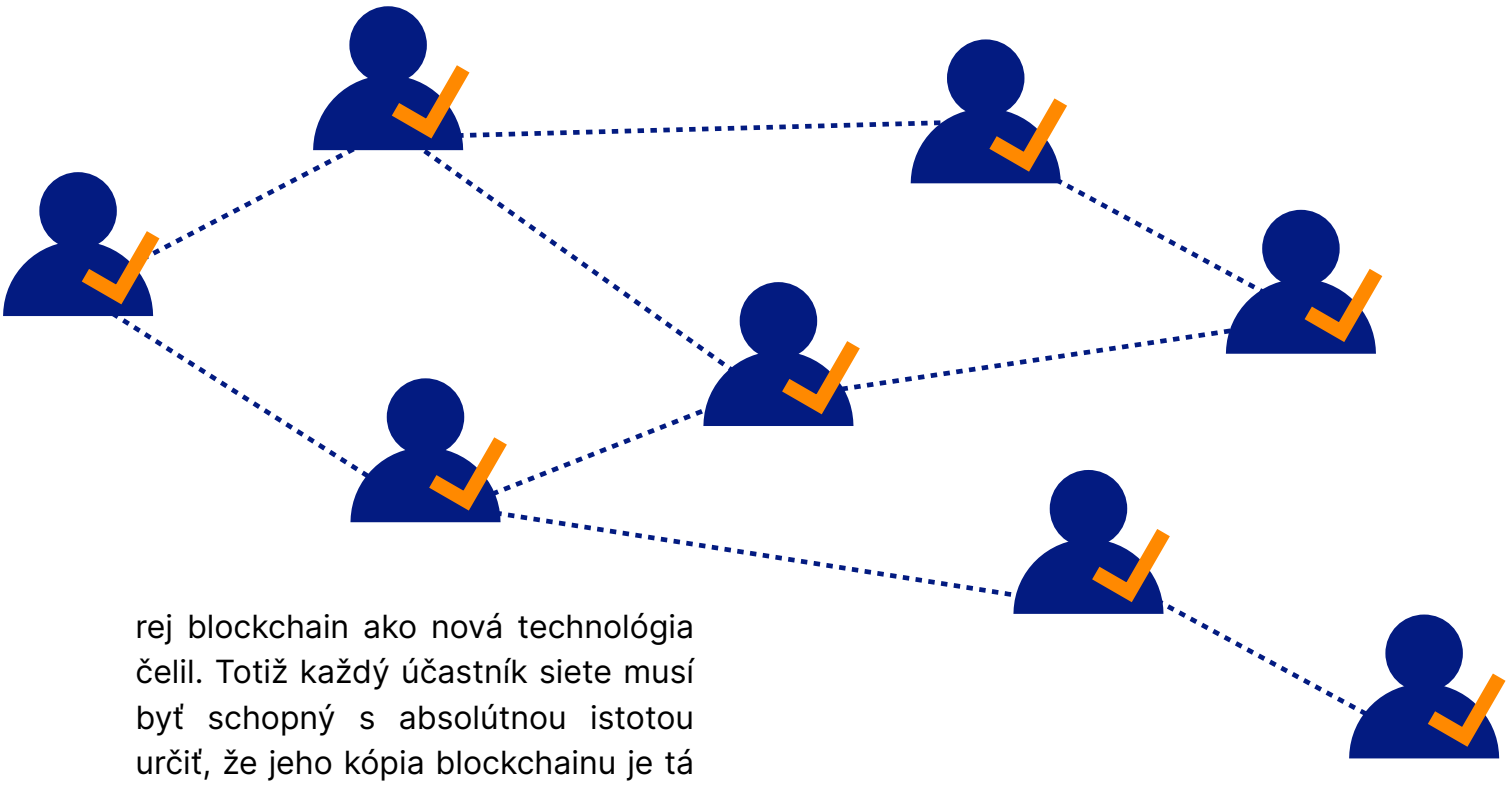
Tieto ťažkosti sa podarilo prekonať vďaka vynálezu blockchainu - reťazca jednotlivých blokov, v ktorých sú dáta uložené v chronologickom poradí. V prípade Bitcoinu sa všetky transakcie od vzniku Bitcoinu ukladajú v časovom poradí v stovkách tisícov blokov, ktoré si možno predstaviť ako jednotlivé strany v účtovnej knihe. Takto usporiadanú účtovnú knihu nazývame blockchain. Každý



účastník siete, ktorý chce vedieť, kto vlastní koľko bitcoinov, môže do samého počiatku vysledovať transakčnú históriu uloženú v blockchaine a určiť, kto presne vlastní koľko bitcoinov v súčasnosti. Ak teda niekto chce poslať bitcoin, najprv sa môže presvedčiť, že tieto konkrétne mince daný odosielateľ skutočne vlastní.

Až do tohoto bodu nejde o žiadnu novinku, pretože banky fungujú podobne. Ak chce zákazník utratiť jedno euro, banka (prostredníctvom automatizovaného systému) prehľadá históriu zákazníkových transakcií a zistí, či už eurá neutratil niekde inde a stále ich vlastní.
Jedinečnou vlastnosťou blockchainu ale je, že tieto informácie nie sú uložené na centralizovanom bankovom serveri, ale na počítačoch všetkých účastníkov siete (takzvaných nodoch - uzloch) a teda existujú v desiatkach tisícov kópií po celom svete. To je takisto dôvodom, prečo sa Bitcoin nedá jednoducho vymazať - ak by sa o to niekto chcel pokúsiť, musel by vymazať celé kópie blockchainu zo všetkých počítačov po celom svete naraz.

Tu sa však dostávame k výzve, kto-



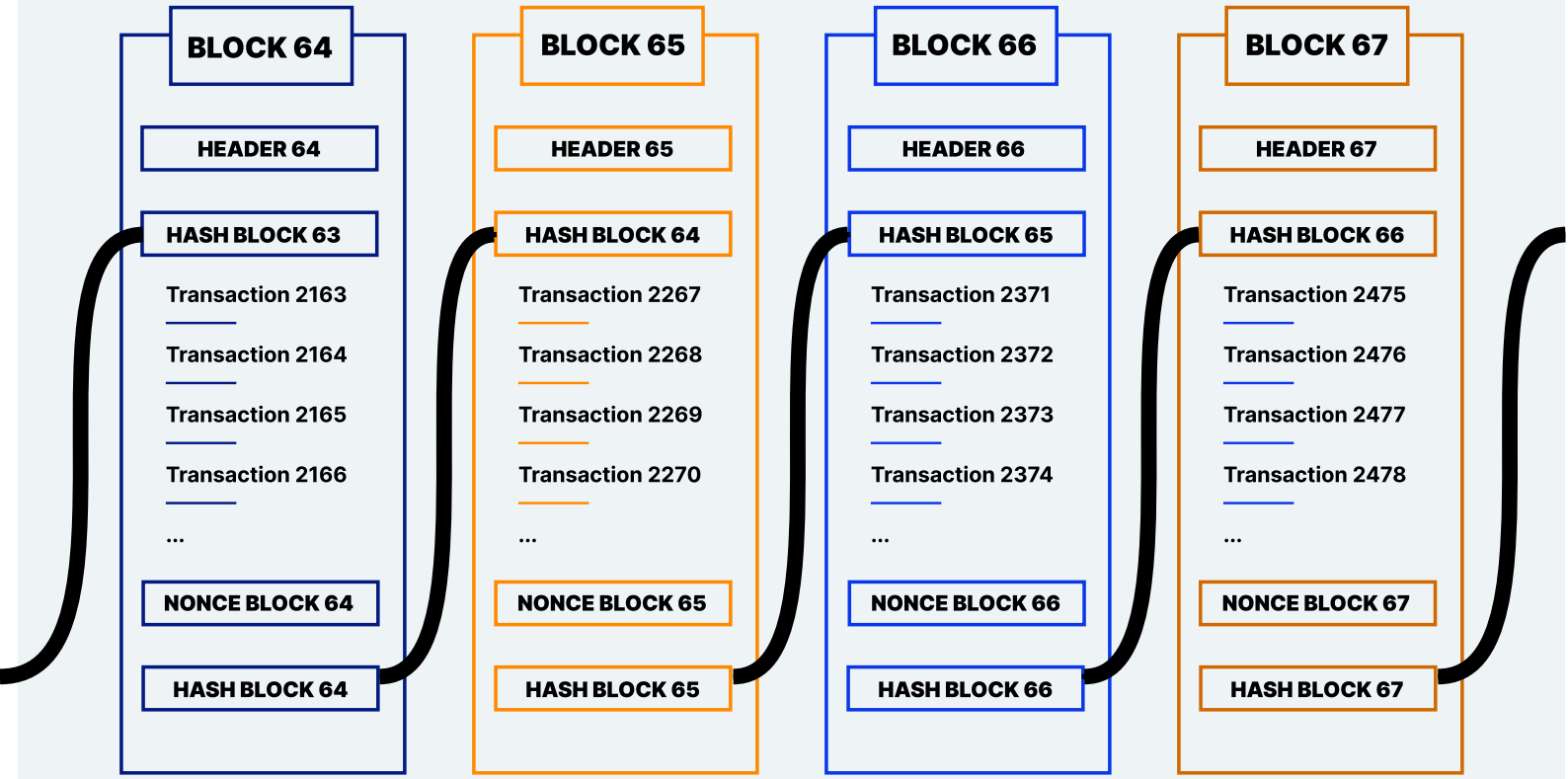
rej blockchain ako nová technológia čelil. Totiž každý účastník siete musí byť schopný s absolútnou istotou určiť, že jeho kópia blockchainu je tá správna a že sa žiadna chybná alebo podvodná transakcia do jeho blockchainovej kópie účtovnej knihy nedostala.
Pretože sa nové bloky s novými transakciami pridávajú každých (približne) 10 minút, celá účtovná kniha pomaly rastie a do jej kópií po celom svete sa priebežne musia zapisovať nové dáta.

Tieto čerstvo pridané bloky musí každý člen siete overiť. Overenie prebieha pomocou nemenných pravidiel, ktoré sú definované v zdrojovom kóde bitcoinovej siete. Tieto pravidlá presne určujú, ktoré transakcie sú povolené a ktoré nie. Každý užívateľ, ktorý si stiahne kópiu blockchainu, preto môže overiť, či všetky transakcie prebehli v súlade s danými pravidlami. Ak niektorá transakcia pravidlá poruší, tzn. je neplatná alebo podvodná, účastníci siete (uzly) ju odmietnu a nezapíše sa do blockchainu.

Ťažba pomocou Proof-of-Work (PoW)

Bitcoinová sieť takisto potrebuje mechanizmus na obmedzovanie pridávania nových blokov. Keby mohol nové transakcie a bloky do účtovnej knihy pridávať ktokoľvek, blockchain by sa nestíhal updatovať po celom svete dostatočne rýchlo a sieť by sa utopila v chaose.

Aby sa tomu predišlo, Bitcoin pracuje s mechanizmom nazvaným Proof-of Work, čo by sa dalo preložiť ako Dôkaz o vykonanej práci. Aby si niekto zaslúžil právo pridať do blockchainu nový blok, musí poskytnúť dôkaz o vykonanej práci. Jednoduchým prirovnaním pre tento proces by mohlo byť hľadanie ihly v kope sena. Komu sa prvému podarí ihlu nájsť, môže pridať do blockchainu nový blok, čiže pripísať novú stranu do existujúcej účtovnej knihy. Navyše bude autor tohoto bloku odmenený novovzniknutými bitcoinami a poplatkami za



Hlavička, výsledok hashovacej funkcie predchádzajúceho bloku, všetky transakcie aktuálneho bloku a Nonce (náhodné číslo) sa vložia do matematickej funkcie. Číslo Nonce sa mení, kým výsledok funkcie hash nemá dostatočný počet predchádzajúcich núl. Tento proces sa nazýva ťažba.

transakcie zapísané v ním vytvorenom bloku. V momente, keď je nový blok pridaný, začína tento proces hľadania odznovu.

V praxi ťažiari vykonávajú matematickú hashovaciu funkciu (hashovací algoritmus SHA-256) v snahe nájsť špecifické číslo. Hashové číslo predchádzajúceho bloku, transakcie zahrnuté do súčasného bloku a náhodné číslo (tzv. kryptografická nonca) sa spolu preženú spomenutým algoritmom. Tento proces sa opakuje mnohokrát (na konci septembra 2022 vykonala celá ťažobná sieť dohromady zhruba 250 000 000 000 000 000 000 výpočtov za sekundu), zakaždým so zmeneným náhodným číslom, až kým sa z hashovacej funkcie nedostane číslo s čo najmenším počtom núl na začiatku. Napríklad blok číslo 700 000 vytvorený 11. septembra 2021, mal platné hashovacie číslo 0000000000000000590fc0f3eba193a278534220b2b37e 9849e1a770ca959.

Celý tento zložitý proces hľadania daného čísla sa tiež nazýva ťažením bitcoinu a má dve hlavné funkcie: po-prvé spája bloky matematicko-kryptografickým spôsobom tak, aby ich mohol ktokoľvek jednoducho overiť. Zároveň znemožňuje zmenu poradia, v ktorom boli vytvorené. Podruhé tento mechanizmus odďaľuje vznik nových blokov, takže v priemere vzniká každý blok v priemere každých 10 minút. Každý užívateľ bitcoinovej sie-

te tak dostáva dostatok času, aby si stiahol ten istý, najnovší stav blockchainu.

21 miliónov bitcoinov

Hoci sa do blockchainu stále pridávajú nové bloky a ťažiari si za to pripisujú odmeny v podobe nových bitcoinov, celkový počet bitcoinov je obmedzený na 21 miliónov. Nikdy nebude existovať viac. Toto množstvo však zďaleka nebolo v obehu od samého začiatku fungovania Bitcoinu. Naopak, vznikajú postupne podľa striktne určeného plánu.

Keď bol Bitcoin spustený, zdrojový kód softvéru uvoľňoval ťažiarom 50 nových bitcoinov pri každom novovzniknutom bloku - teda zhruba každých 10 minút. O štyri roky neskôr sa toto množstvo zmenšilo na polovicu. Proces nazývaný Halvingom, teda Polením, sa odohráva každých 210 000 blokov, teda približne štyri roky. Momentálne (9/2022) je v obehu už viac ako 19 z 21 miliónov bitcoinov. Zbytok sa bude v podobe odmeny za nájdenie nového bloku ťažiť až do roku 2140. Potom budú ťažiari odmeňovaní len prostredníctvom transakčných poplatkov.

Striktne obmedzené množstvo bitcoinov je jeho fundamentálnou vlastnosťou, ktorá ho robí extrémne vzácnou komoditou. Táto absolútna digitálna vzácnosť je tiež dôležitým základom, ktorý z Bitcoinu robí uchovávateľa hodnoty v dlhodobom horizonte a dôvodom, prečo sa o bitcoine hovorí ako o digitálnom zlate alebo zlate 2.0.

Výsledok: Digitálne zlato

Preskúmaním schopností bitcoinovej siete sme získali obraz o dôležitosti tohto vynálezu. Po prvý raz v dejinách je na svete digitálny tovar, ktorý je dostupný v dokonale obmedzenom množstve. Bitcoin nie je možné kopírovať alebo duplikovať.
Vďaka tomu je bitcoin nazývaný digitálnym majetkom. Pretože tak ako každý kúsok zeme je jedinečný a existuje len v jednej jednotke, Bitcoin je tiež jedinečný a každý jeho diel existuje v digitálnom priestore v danom čase len raz.
Ďalšou unikátnou vlastnosťou Bitcoinu je, že jeho jednotky môžu byť skutočne a nedeliteľne vlastnené. Len osoba, ktorá vlastní privátny kľúč, teda kombináciu číslic a písmen pozostávajúcu zo 64 znakov, môže disponovať priradeným bitcoinom. Inými slovami, Bitcoin sa nedá ukradnúť, skonfiškovať alebo zablokovať. Toto umožňuje jeho vlastníkovi absolútnu moc nad jeho vlastnými finančnými zdrojmi bez ohľadu na to, či je milionárom, disidentom alebo stíhaným dlžníkom. Po prvý raz od vynájdenia počítača je možné skutočne a úplne vlastniť digitálne aktívum.

PREČO BITCOIN?

Kde sa vzal celý ten humbug okolo Bitcoinu? Možnosť naozaj a úplne vlastniť digitálne aktívum môže byť revolučné, ale načo by to komu vôbec malo byť dobré?

Najlepší z oboch svetov

V minulých storočiach slúžili ako prostriedok výmeny drahé kovy a neskôr hotovosť v podobe mincí a bankoviek. Ich výhodou bolo, že mohli byť ľubovoľne skladované a použité ako platba za tovar alebo služby. Porekadlo, že hotovosť je sloboda vytlačená na papieri, to skvele zhrňuje. Nevýhodou drahých kovov a hotovosti však bola ich nevhosť na použitie v digitálnom priestore Internetu. Nakoniec sa v predvečer online nakupovania udomácnili medzi ľuďmi kreditné a debetné karty.

Ako však stúpala popularita digitálnych peňazí na bankových účtoch na úkor hotovosti, začali sa objavovať ich nevýhody spôsobené prítomnosťou banky ako tretej strany. Napríklad ak táto tretia strana vyhlásila insolvenciu, vlastník účtu mohol o svoje peniaze prísť. Alebo, ako tomu bolo na Cypre (civilizovaná, členská krajina EÚ) v roku 2013, výbery z účtu boli drasticky obmedzené a zlegalizovalo sa vyvlastnenie majetku v podobe úspor na účtoch a ľudia stratili prístup k svojim vlastným peniazom. Takisto sa stáva, že klient banky nemusí byť schopný poslať peniaze svojim príbuzným, ak žijú v sankcionovaných krajinách ako je Kuba alebo Irán a musí dúfať, že mu tretia strana v podobe banky alebo regulátora prevod povolí. Pamätníci z východného bloku si možno spomenú, ako sa “strácali” bankovky z poštovej korešpondencie s príbuznými žijúcimi v Kanade, USA alebo Západnom Nemecku. S prechodom z papierových na digitálne peniaze uložené na bankových účtoch strácame kontrolu nad našimi vlastnými peniazmi. Až doteraz bolo toto nevýhodou nášho života v digitálnom svete.

Práve Bitcoin ponúka riešenie tejto dilemy. Dokonale spĺňa požiadavky na digitálnu hotovosť, pretože je

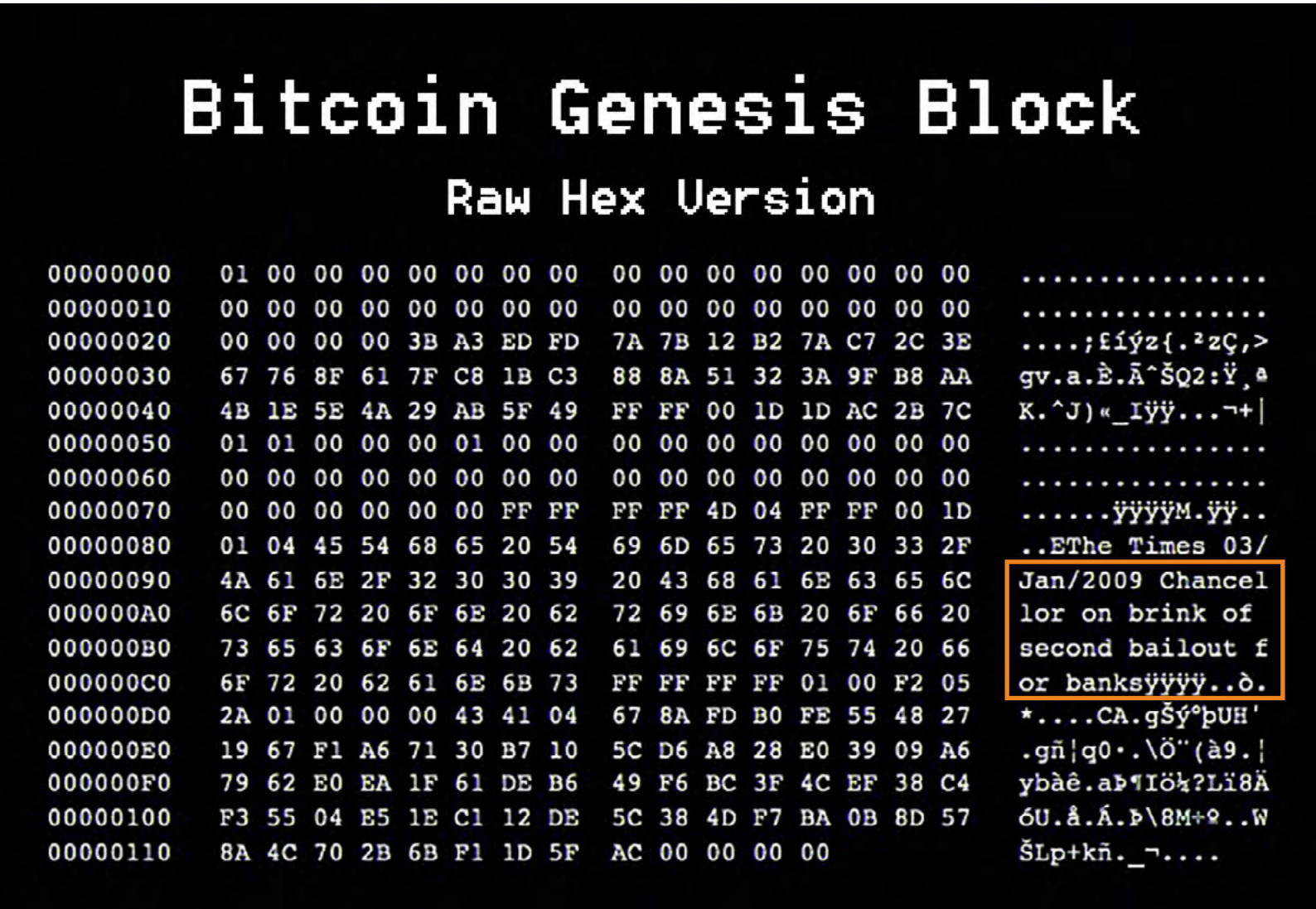
na to navrhnutý. Zároveň umožňuje ukladať hodnotu v podobe digitálneho vlastníctva bez potreby spoliehať sa na tretiu stranu (banky). Vlastníci tak Bitcoin, lepšie povedané privátne kľúče k nemu, môžu mať uložený pod vlastným matracom alebo kdekoľvek inde to uznajú za bezpečné.

Dokonalé načasovanie

Bitcoin vznikol počas globálnej finančnej krízy v rokoch 2008/09. V prvom bloku svojho blockchainu, nazvanom tiež Genesis block, zanechal Satoshi Nakamoto silný odkaz. Citoval v ňom titulok z britských He The Times, ktorý hlásal: "Chancellor on brink of second bailout for banks - Minister financií (je) na pokraji druhého záchranného balíčka pre banky"

Týmto činom Satoshi vyjadril kritický postoj voči štátu, ktorý Cypherpunks zdieľali. Počas finančnej krízy v roku 2008 použili centrálne banky nesmierne množstvá novo vytvorených peňazí na záchranu komerčných bánk. V konečnom dôsledku však túto záchranu zaplatili sporitelia rozriedením svojich úspor v zväčšenej zásobe peňazí. Tento fakt cypherpunkom opäť potvrdil opodstatnenosť ich nedôvery voči štátu a centrálnym bankám a upevnil ich presvedčenie o potrebe nezávislých peňazí.

Taká istá procedúra, len v ešte väčšom meradle, sa odohrala po vypuknutí pandémie Covid-19. Len v roku 2020 sa zásoba všetkých peňazí v USA zvýšila o 50%. V iných



krajinách, EÚ alebo Švajčiarsko nevynímajúc, tlačenie digitálnych peňazí stále pokračuje. Priamym následkom tejto politiky sú rekordne nízke, dokonca záporné, úrokové sadzby a silný rast cien aktív.

Zabezpečenie proti devalvácii meny

Práve preto bol Bitcoin spustený v najlepšom možnom čase. Tlačenie peňazí a otázniky s ním spojené boli sotvakedy väčšie ako dnes. S obmedzeným množstvom na 21 miliónov poskytuje Bitcoin príjemnú zmenu oproti donekonečna rastúcim súvahám centrálnych bánk. Jeho obmedzená ponuka poskytuje človeku ochranu pred znehodnocovaním kapitálu, ktoré sa v posledných dekádach deje u všetkých mien po celom svete.

Vďaka svojmu špecifickému nastaveniu zabezpečuje Bitcoin zachovanie kúpnej sily v dlhodobom časovom horizonte. Pretože je absolútne vzácny, mal by túto úlohu spĺňať dokonca lepšie ako zlato, ktorého množstvo sa každoročne zvyšuje o 1-2%. Navyše sú náklady na uloženie a transakcie u Bitcoinu v porovnaní so zlatom výrazne nižšie, čo tiež prispieva k lepšiemu uchovaniu hodnoty v priebehu času.

Ochrana majetku

Ďalším problémom, ktorý Bitcoin rieši, je ochrana vlastníctva. Kým zlato alebo hotovosť musia byť bezpečne uschované, čo generuje nemalé náklady, Bitcoin môže byť uložený a presúvaný doslova zadarmo. Akékoľvek, aj obrovské množstvá môžu byť presunuté po celom svete (vrátane Iránu alebo KĽDR) v kóde pozostávajúcom z dvanástich alebo dvadsiatich štyroch slov. Ak si ich raz zapamätáte a zničíte, nikto vám ich nemôže ukradnúť. To robí Bitcoin bezpečným a umožňuje jeho vlastníkovi vziať si ho až do hrobu, pokiaľ si to praje.

NÁKUP BITCOIN

V podstate existujú dva spôsoby, ako sa k bitcoinu dostať. Buď sa dá zarobiť vyťažením, alebo zakúpením od iného držiteľa. Pretože ťažba sa pri súčasných cenách energií stala pre domácich ťažiarov extrémne nevýhodnou, ostáva nováčikom druhá možnosť - kúpiť si ho.

Krypto burzy a brokeri

Najjednoduchší spôsob, ako si kúpiť bitcoin, sú burzy alebo brokeri. Fungujú veľmi podobne ako online platformy na obchod s cennými papiermi. Po otvorení osobného účtu sa prostredníctvom bankového prevodu alebo kreditnej karty na účet na burze presunú finančné prostriedky - Franky, Eurá, Doláre, či Koruny. Po ich pripísaní je možné Bitcoin niekoľkými klikmi nakupovať alebo predávať za aktuálnu trhovú cenu, a to 24 hodín denne, nonstop. V Európe je možné bez registrácie, overovania dokladov alebo predchádzajúceho vkladu peňazí nakupovať prostredníctvom aplikácie Relai, ktorá je určená výhradne pre Bitcoin.

Peer-to-peer, teda osobne

Ako alternatíva k zmenárňam a burzám sa dá Bitcoin nakupovať a predávať osobne medzi známymi ako s vexlákmi z čias socializmu. To umožňuje väčšiu anonymitu, nakoľko v procese nie je nutné odhaľovať svoju identitu ani iné osobné dáta. Je to však spojené s určitým bezpečnostným rizikom.

Bitcoinové bankomaty

Takisto existuje možnosť nakupovať bitcoin alebo vyberať hotovosť z bitcoinových automatov. Možno v nich používať hotovosť alebo platobnú kartu a vo väčšine krajín nie je potrebná kontrola identity (na Slovensku áno).

Bezpečné uloženie bitcoinu

Po získaní bitcoinu vyvstáva otázka

jeho bezpečného uloženia. Bitcoin aj ostatné kryptomeny sú postavené na princípe “Nemáš kľúče, nemáš peniaze”. Na skutočné vlastníctvo bitcoinu je teda potrebné vlastniť privátny kľúč k adrese, na ktorej je pripísaný.

Pokiaľ je bitcoin deponovaný na účte na burze, vlastní kľúče k nemu ona a fakticky ho ovláda. Ak dôjde k jej hacknutiu, bankrotu, či spreneveře, bitcoin môže byť pre užívateľa navždy stratený.

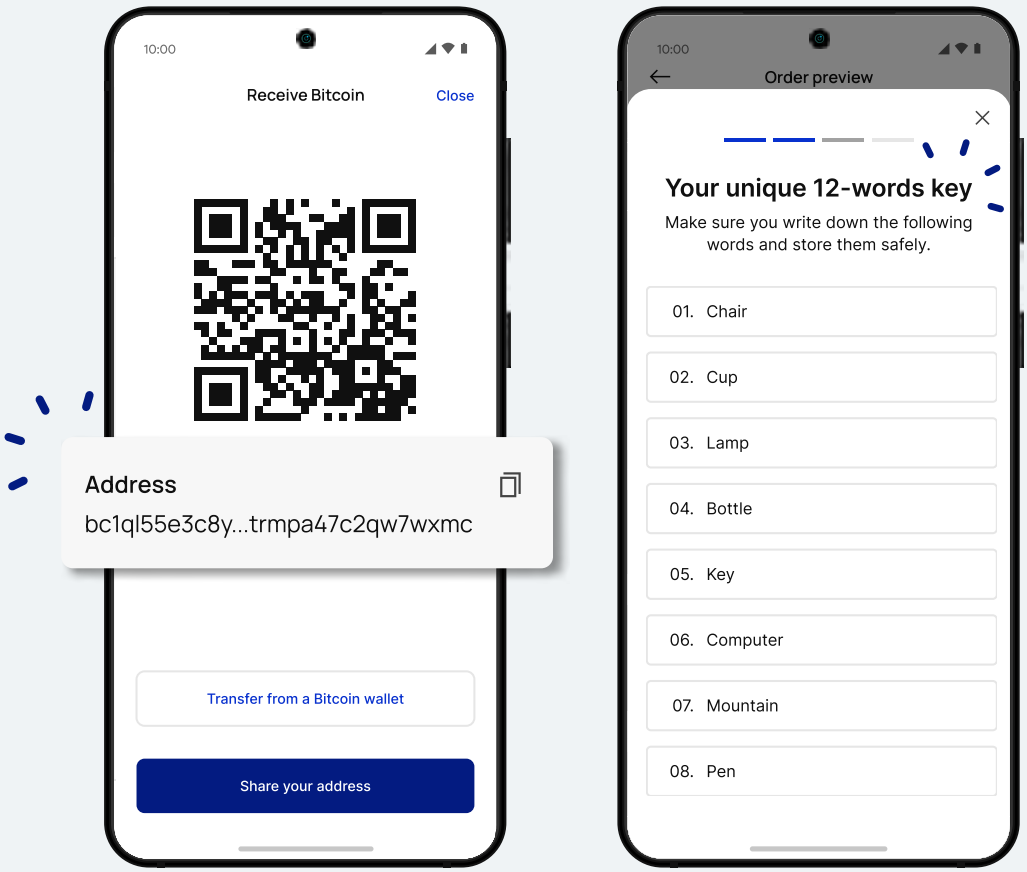
Vlastná úschova

Na rozdiel od bankového účtu, bitcoin funguje ako hotovosť, a teda umožňuje uloženie svojich menových jednotiek na osobnej peňaženke. To dáva človeku možnosť byť svojou vlastnou bankou a absolútne ovládať svoj bitcoin. Samozrejme, s týmto prichádza zodpovednosť. Privátny kľúč, ktorý často existuje vo forme reťazca dvanástich alebo dvadsiatich štyroch slov, treba bezpečne uložiť. Nesprávne alebo nedbalé používanie privátnych kľúčov môže skrze stratu alebo hacknutie viesť k nevratnej strate bitcoinu.

Peňaženky: digitálne peňaženky

Digitálne peňaženky pomáhajú bezpečne skladovať bitcoin - alebo presnejšie povedané, kľúče k nemu. Bitcoin existuje v blockchaine a na peňaženku sa presunúť nedá. Je pripísaný k adrese a kľúč uložený v peňaženke ním umožňuje disponovať.

Peňaženky teda vznikli na jednoduchú a bezpečnú úschovu privát-



nych kľúčov. Okrem toho umožňujú odosielanie a prijímanie bitcoinu na adresu spojenú s kľúčmi pomocou niekoľkých klikov. To z nich robí užitočný nástroj na používanie bitcoinu.

Softvérové peňaženky

Najpoužívanejšie peňaženky sú softvérové. Existujú v podobe aplikácií pre počítače alebo smartfóny. Počas inštalácie sa privátny kľúč zobrazí v podobe dvanástich alebo dvadsiatich štyroch slov - takzvaného seedu. Tento reťazec slov následne reprezentuje adresy, na ktoré sa dajú odosielať bitcoiny a tie sa potom zobrazia v peňaženke. Ktokoľvek tento reťazec slov pozná, preto môže disponovať s bitcoinom na danej peňaženke. Z tohto dôvodu musí byť tento reťazec uchovaný v analógovej forme (napríklad rukou napísaný na papieri, ručne vyrazený do oceľového plechu a podobne), aby nemohlo prostredníctvom hacku dôjsť k odcudzeniu privátneho kľúča k peniazom. Navyše, ak by bolo zariadenie, na ktorom je nainštalovaná peňaženka, stratené alebo zničené, dá sa nová peňaženka vytvoriť na novom zariadení a po zadaní seedu v novej aplikácií možno opäť disponovať so svojimi peniazmi.

Softvérové peňaženky majú tú výhodu, že sa dajú rýchlo nainštalovať a veľmi jednoducho sa používajú. Pretože sú ale nainštalované na zariadeniach pripojených k internetu, existuje u nich vždy riziko hackerského útoku.

Hardvérové peňaženky

Ak potrebujete vyššiu úroveň zabezpečenia svojich prostriedkov, stojí za zváženie peňaženka hardvérová. Je to malé zariadenie podobné USB kľúču, ktoré sa v prípade potreby pripája k počítaču. Zariadenie je navrhnuté tak, aby sa ani počítač nakazený vírusom alebo iným škodlivým softvérom nemohol dostať k privátnym kľúčom.

Aj pri nastavovaní hardwarovej peňaženky sa generuje seed, ktorý treba opäť uložiť v analógovej podobe (v žiadnom prípade ho nezapisovať do počítača, fotiť mobilom alebo si fotografiu neukladať na zariadenie s prístupom k internetu). Ak sa hardvérová peňaženka stratí, opäť je možné peňaženku s pomocou seedu obnoviť na novom zariadení. Príkladmi hardwarových peňaženiek sú Trezor alebo BitBox.

Made in Switzerland

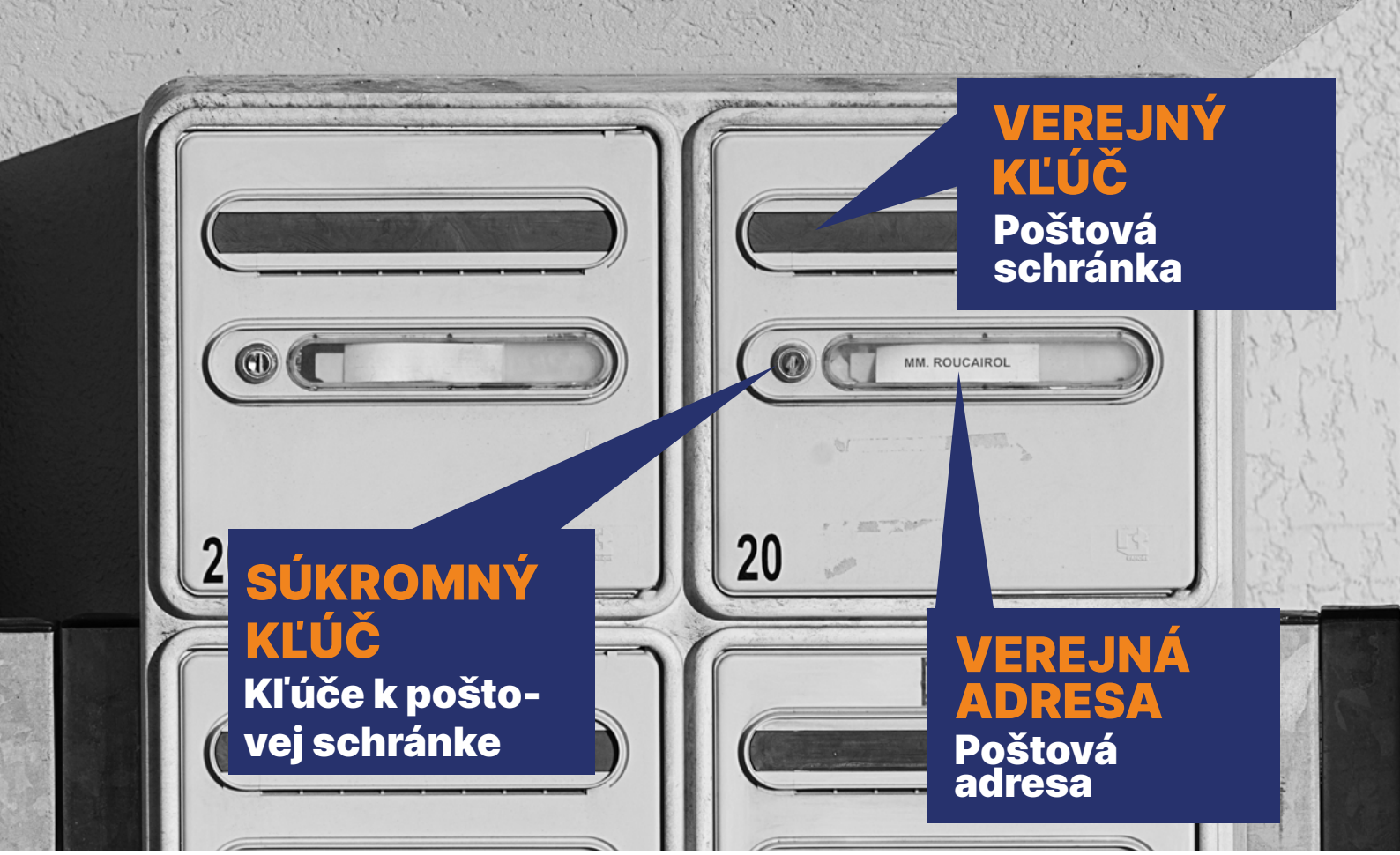
EUROPE'S EASIEST BITCOIN APP

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.



Posielanie a prijímanie bitcoinu

Posielanie a prijímanie bitcoinu je veľmi jednoduché. Každá peňaženka má svoju verejnú adresu vygenerovanú z takzvaného privátneho kľúča. Táto adresa slúži na prijímanie, podobne ako IBAN. Ktokoľvek túto adresu dostane, môže poslať bitcoiny na k nej prislúchajúcu peňaženku. Adresy sa často zobrazujú vo forme QR kódov, čo ďalej zjednodušuje ich obsluhu.

Ak chcete niekomu bitcoin poslať, môžete alebo ručne zadať jeho adresu v peňaženke alebo fotoaparátom načítať QR kód. Transakčný poplatok na zaradenie transakcie do blockchainu sa automaticky stiahne z odosielateľovej adresy. Veľkosť transakčného poplatku sa rôzni závislosti od zaťaženia bitcoinovej siete a možno si ju vyhľadať tu. Prevod trvá minimálne jeden blok, teda asi 10 minút. Transakčný poplatok motivuje ťažiarov zaradiť transakciu do bloku, teda zapísané sú transakcie s najvyššími poplatkami a tie s nižšími sa môžu zaradiť až v neskorších blokoch. To umožňuje odosielateľom ušetriť na poplatkoch, ak im transakcia neponáhľa.

Platenie pomocou Bitcoinu

Keď bol Bitcoin vytvorený, verilo sa, že jedného dňa sa bude každodenne využívať na platby za tovar a služby. Teoreticky je to dnes bez problémov možné. Niektoré vládne daňové úrady, neziskové organizácie a hlavne rastúci počet firiem Bitcoin ako platobný prostriedok prijímajú.
Ale pretože transakcie s Bitcoinom môžu stáť niekoľko (občas dokon-

ca desiatok) eur a trvajú vždy minimálne 10 minút, dávajú zmysel len pri väčších platbách. Pre lacné a rýchle platby je potrebné alternatívne riešenie.

Lightning network - rýchlejšia a lacnejšia

Preto bola nad Bitcoinom vybudovaná ďalšia vrstva. Táto sieť nazývaná Lightning, teda blesková, umožňuje platby v priebehu sekúnd a s minimálnou cenou. V krajinách ako El Salvador táto sieť už funguje. Na Slovensku takisto rapídne stúpa počet miest, kde sa prostredníctvom lightningu dá platiť za tovar, či služby. Ide nie len o eshopy (Alza), ale aj kaviarne, reštaurácie, či holičstvá. Konkrétnych obchodníkov možno nájsť napríklad tu a tu.

Každodenné platby sa preto v budúcnosti budú odohrávať práve skrze Lightning Network. Jej vývoj beží na plné obrátky. Pomocou aplikácie Tweetoshi tak napríklad umožňuje dávať "dýško" prostredníctvom požívateľom twitteru a najnovšie ju implementoval aj komunikačný softvér Telegram. Aplikácia Strike posunula možnosti siete ešte ďalej a umožňuje jej prostredníctvom platby po celom svete v rôznych menách. Očakáva sa preto, že v budúcnosti sa do bitcoinového blockchainu budú zapisovať len skutočne veľké transakcie, kým všetky ostatné sa budú odohrávať na Lightning Networku.

Pretože sa cel Lightning posielajú hlavne menšie transakcie, používajú sa pri nich ako účtovná jednotka Satoshi alebo Saty. 1 bitcoin sa rovná 100 000 000 Satoshi.

Pre používanie Lightning Network je potrebná peňaženka, ktorá ju podporuje, napríklad Muun, Phoenix alebo Blixt. Vybrať si medzi nimi možno na základe erudície, ktorú už užívateľ v používaní má a vyberú si úplní začiatočníci aj skúsení bitcoineri, ktorí si ju budú vedieť pripojiť k vlastnému uzlu.
1 Bitcoin is equal to 100,000,000 Satoshis. To use the Lightning Network, a Lightning wallet must be set up.

POHĽAD DO BUDÚCNOSTI

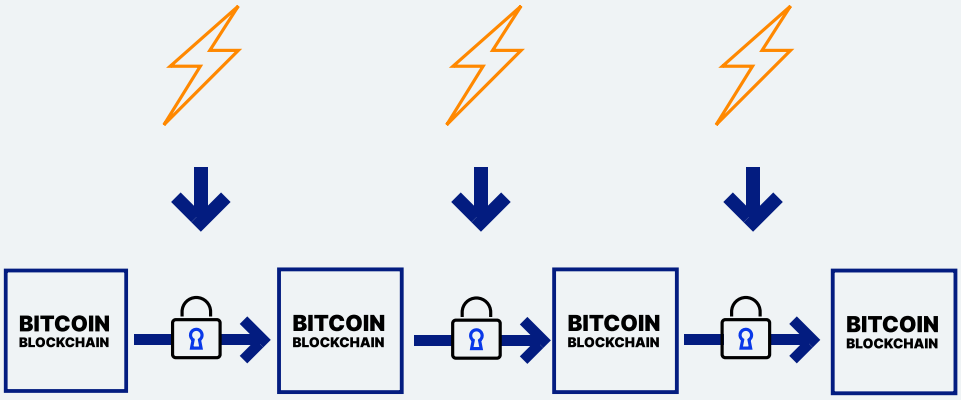
Za viac ako desať rokov svojej existencie Bitcoin prešiel mnoho dobrého aj zlého. Verejnosť ho po veľkých pádoch ceny mnohokrát zatracovala, považovala za mŕtvy alebo zabudnutý. Bitcoin sa však bez ohľadu na to postupne šíril po celom svete.

Bitcoin a energia

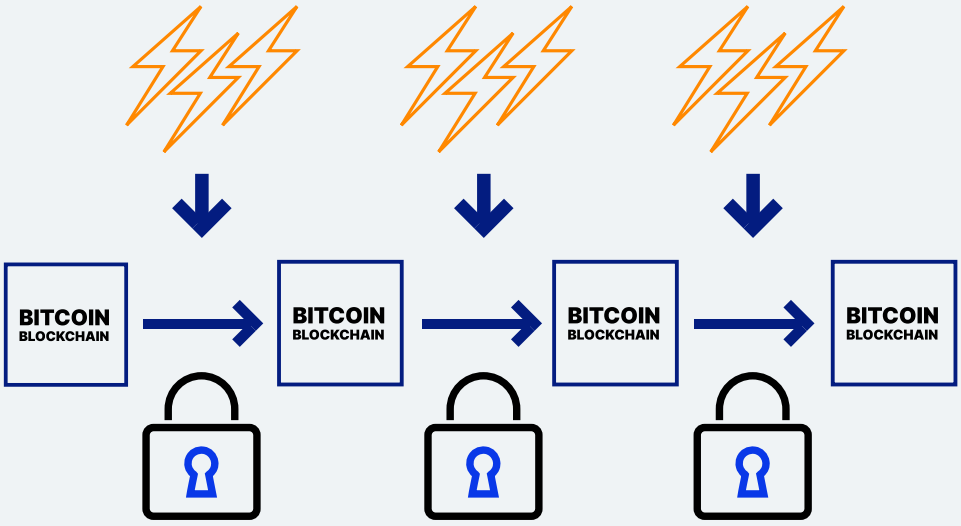
Jednou z prvých pripomienok, ktoré sa k vývoju Bitcoinu vznášajú, je množstvo energie, ktoré sa pri ťažbe Bitcoinu spotrebúva. To je v súčasnosti už v celosvetovom meradle významné a bude zrejme v budúcnosti stúpať spolu so stúpajúcim záujmom ľudí a firiem o ťažbu.
Počas debát o Bitcoine a energiách je však dôležité porozumieť, že množstvo energie, ktoré ťažba spotrebúva, je kriticky dôležité pre bezpečnosť siete. Čím viac energie priteká, tým bezpečnejšou sa sieť stáva. Aby niekto mohol blockchain zmeniť, musel by vlastniť nadpolovičnú väčšinu výpočtového výkonu siete - a teda investovanej energie aj hardvéru. Pretože sa však miliónom počítačov po celom svete ekonomicky opláca podieľať sa na ťažbe, stáva sa takýto útok menej a menej pravdepodobným. To je dôvodom, prečo je tak extrémne dôležitý hashovací výkon siete a spotreba elektriny s ním spojená.

Navyše počítače ťažiace Bitcoin majú výhodu, že sa môžu nachádzať kdekoľvek na svete. Pretože ich zárobok je nepriamo úmerný cene elektriny, sú umiestnené často na miestach, kde je energie nadbytok a tá je preto lacná. Z dlhodobého hľadiska to

Čím menej energie v podobe výpočtového výkonu sa spotrebuje na vytvorenie block-chainu Bitcoinu, tým ľahšie je ho neskôr zmeniť.



Čím viac energie v podobe výpočtového výkonu sa použije na vytvorenie bitcoinové-ho blockchainu, tým ťažšie je ho neskôr zmeniť.



budú často miesta, kde je dostupná energia z obnoviteľných zdrojov, ale nie je tam pre ňu ekonomicky zmysluplné využitie.

Podľa informácií z Rady bitcoinových ťažiarov pochádza momentálne zhruba 56% elektriny využitej na ťažbu z obnoviteľných zdrojov a toto číslo stabilne rastie. Mnohí experti sú presvedčení, že v budúcnosti dosiahne hodnotu 100%.

Dovtedy však množstvo energie spotrebované na ťažbu Bitcoinu bude prinášať otázku, či bezpečné a nemanipulovateľné peniaze skvele uchovávajúce hodnotu v čase stoja za túto energiu alebo nie.

El Salvador - Bitcoin ako národná mena

A few years ago, visionaries already Už pred niekoľkými rokmi si viacerí vizionári uvedomovali možnosť, že by sa Bitcoin mohol stať zákonným platidlom v niektorých štátoch. V lete 2021 tá chvíľa prišla a El Salvador sa stal prvou krajinou na svete, ktorá uznala Bitcoin ako zákonné platidlo. V predajniach, reštauráciách, či u poskytovateľov najrôznejších služieb sa tak dá platiť nielen americkými

dolármi, ale tiež Bitcoinom. Na tieto účely bola vytvorená a pre potreby obyvateľstva poskytnutá nová peňaženka fungujúca na Lightning Network, teda umožňujúca rýchle platby s minimálnymi poplatkami.

Iné krajiny ako Ukrajina, Brazília alebo Panama už momentálne tiež zvažujú prijatie podobných zákonov. Ak by iné krajiny príklad El Salvadoru nasledovali, zdvihlo by to dopyt po Bitcoine, ale čo je ešte dôležitejšie, podčiarklo by to dôveryhodnosť Bitcoinu ako peňazí. Prijatie Bitcoinu ako zákonného platidla v ďalších a ďalších krajinách preto predstavuje rozhodujúcu fázu v globálnom adaptačnom procese Bitcoinu.

Zákony a regulácie

Tento vývoj priviedol štáty, centrálne banky, ale aj firmy do kontaktu s kryptomenami. Rôzne štáty, vrátane Švajčiarska, vydali legislatívu a ďalšie pravidlá týkajúce sa kryptomien. Toto privítalo mnoho účastníkov trhu, nakoľko s tým prišla legislatívna istota pre kryptomeny aj potenciálnych investorov.

Regulácie sú na dohľad aj v USA, ktoré doteraz vyznávali prístup laissez-faire /nechať na pokoji, neintervenovať/. Presná forma týchto nových regulácií bude určite pod drobnohľadom kryptokomunity, nakoľko budú mať vplyv na celý sektor, v ktorom sa točia bilióny dolárov.

Iné kryptomeny

Bitcoin už dnes zďaleka nie je jedinou kryptomenou. V súčasnosti existuje cez 20 000 rôznych kryptomien a kryptoaktív. Tieto mince a žetóny majú iné charakteristiky a funkcie a nie všetky z nich boli navrhnuté ako meny alebo peniaze. Niektoré viac pripomínajú akcie, ktoré odrážajú vo svojej cene úspech daného projektu. Iné sú požadované na prístup k určitej službe a ešte iné, takzvané meme tokeny sú proste zábavkou.

Aby sa predišlo stratám, je viac než vhodné sa pred investovaním na danú menu alebo projekt pozrieť zblízka, prípadne sa im proste a jednoducho rovno vyhnúť.

Digitálne meny centrálnych bánk (CBDC)

Kryptomeny sú v procese prechodu z fázy neregulovaného Divokého Západu k regulovanému svetu kryptofinancií. Tento vývoj neprežili centrálne banky celkom nedotknuté a vznikli myšlienky, že centrálne banky by mali samy vydávať svoje vlastné kryptomeny. Tieto Digitálne meny centrálnych bánk, známe viac pod anglickou skratkou CBDCs by, ako tvrdia ich proponenti, v sebe spojili stabilitu štátnej meny s výhodami kryptomien postavených na blockchainoch. V skratke tvrdia, že by vytvorili digitálnu hotovosť.

V závislosti na ich dizajne, CBDCs

môžu nabrať fundamentálne odlišné formy. Rôzne krajiny už testujú takéto meny v pilotnej prevádzke a iné ich dokonca plne spustili. V každom prípade sa pozorne očakáva spustenie takýchto mien v ekonomicky silných menových teritóriách ako USA, EÚ alebo Čína.

Konkurencia peňazí

Naša spoločnosť si už za posledné dekády tak privykla na štátne meny, že iné formy peňazí sú pre väčšinu jej členov sotva predstaviteľné. Ale nie tak dávno ešte boli rôzne meny cirkulujúce paralelne v eknomomike celkom bežnou vecou. Ako platidlo sa používali bankovky od rôznych bánk, mince vyrazené z rôznych kovov s rôznymi menovými hodnotami..

S bitcoinom sú neštátne peniaze opäť k dispozícií ako alternatíva k štátnym menám. Doteraz väčšina vlád Bitcoin tolerovala. Do určitej miery to bolo vďaka jeho decentralizovanej povahe, ktorá sťažovala prípadný útok naň. Pre občanov toto znamená digitálnu alternatívu peňazí súbežne so zlatom alebo striebrom. V budúcnosti bude zaujímavé pozorovať výsledky tejto novej menovej konkurencie.

BITCOIN, ČO S NÍM?

Ak sa pýtate sami seba, ako naložiť so všetkými týmito informáciami, dovoľte mi niečo navrhnúť. Vstup do sveta Bitcoinu nestojí veľa, trocha času a (voliteľne) nejaké peniaze. Spoznáte však technológiu, ktorá môže zmeniť náš svet a budúcnosť.

Takže: vytvorte si účet na kryptoburze alebo, ešte lepšie, stiahnite si peňaženku na svoj smartfón a kúpte si bitcoin za 20 alebo 50 eur. Alebo poproste kamaráta, aby vám nejaký na vašu peňaženku poslal. Aspoň si ho trocha "ohmatáte" a zistíte, ako to funguje.

Pretože ak sa Bitcoin presadí a stane sa tak všadeprítomný ako internet, nebudete o ňom vedieť len teoreticky, ale už s ním budete mať vlastnú skúsenosť. Občas je toto veľký rozdiel, pretože vám to dá pojem o danej technológií a postaví vás to pred väčšinu ľudí.

ABOUT

O AUTOROVI

Daniel Jungen je ekonóm a finančný novinár špecializujúci sa na kryptomeny. Daniel spoluzakladateľom InsightDeFi, a výskumnej kancelárie zameranej na kryptomeny. Spolu so svojimi partnermi z InsightDeFi, publikujú dvojtýždenník (v nemčine) o Bitcoine DeFi a krypte všeobecne.

O RELAI

Relai bolo založené vo Švajčiarsku Julianom Linigerom a Ademom Bilicanom po tom, ako mali problém nájsť bezpečný, bezproblémový spôsob na na nákup bitcoinu. Relai sprístupňuje šetrenie a investovanie v bitcoine všetkým. Výhradne bitcoinová aplikácie je navrhnutá tak, aby bola čo najjednoduchšia a intuitívna, ako sa len dá, čím umožňuje komukoľvek v Európe nakupovať a predávať bitcoin v priebehu minút bez potreby sa registrovať, overovať alebo vkladať peniaze popredu. Je nezávisle auditovaná a užívatelia cez ňu preinvestovali vyše 35 miliónov švajčiarskych frankov vďaka jej schopnosti priniesť im nové spôsoby sporenia a investovania.

Zistite viac na Relai.app.

Poďakovanie za preklad: @lednicky_j .
Na záver ďakujeme @tulkooo2 za poskytnutie poznámok a spätnej väzby