Co je to Bitcoin a proč vznikl?

Bitcoin je tu s námi již od roku 2009 a neustále nabývá na své popularitě. Většina lidí na světě o něm už slyšela, někteří jej již nakoupili a jiní ho dokonce stihli i prodat, avšak pouze zlomek světové populaci ví, co je to Bitcoin, jaké problémy řeší a proč se jedná o tak zásadní inovaci v oblasti peněz. A tato témata se pokusím v nadcházejících řádcích jednoduše vysvětlit. Prvně si zde popíšeme problémy současných peněz a až následně to, co vlastně Bitcoin je a jak tyto problémy řeší.

V roce 1971 přišel obrovský zlom v celé historii peněz. Tohoto roku totiž tehdejší americký prezident Richard Milhous Nixon jednostranně ukončil takzvaný Brettonwoodský systém a tím i veškerou návaznost amerického dolaru na zlato, co by podkladové aktivum.

Dokud byly měny navázány či kryty skutečnými penězi, především v podobě drahých kovů, byly obchodní banky limitovány v tom, kolik úvěrů mohou poskytnout, tedy kolik nových peněz mohou vytvořit. Mimochodem termíny *peníze* a *měna*, byť jsou často vzájemně zaměňovány, neznamenají to stejné, ostatně, proto jsou v češtině dvě různá označení pro platidlo. Měna je poukázka (peněžní substitut), chcete-li směnka na peníze. Historicky byly měny papírové bankovky, které byly kryty penězi v podobě drahých kovů, zejména zlata. Přičemž na samotných těchto bankovkách bylo napsáno, že na žádost bude držiteli vyplacena částka odpovídající směnnému poměru mezi měnou a penězi.

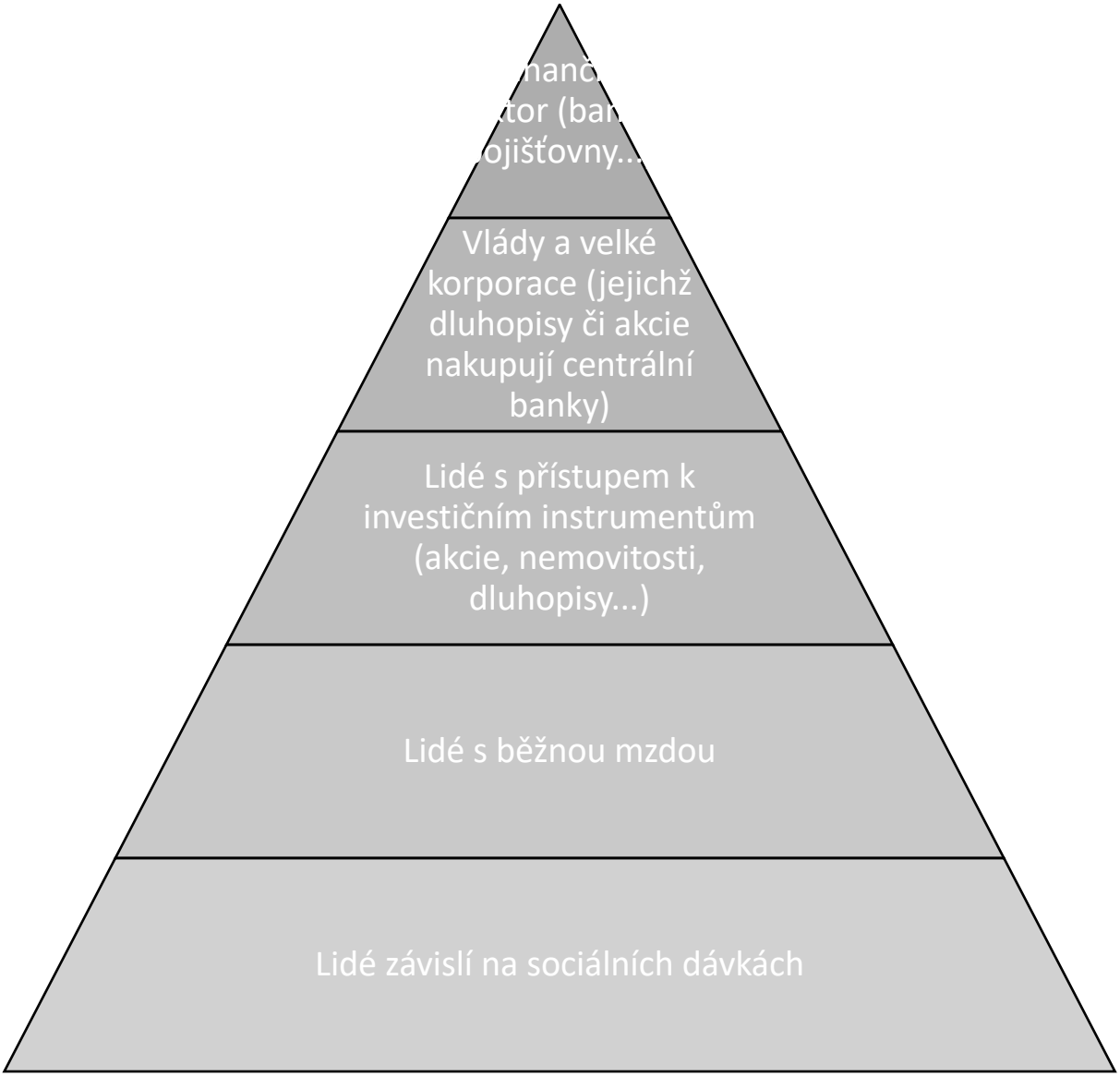
Avšak po zrušení návaznosti dolaru a s ním i ostatních měn na zlato se monetární politika stávala čím dál tím rozvolnější. Centrální banky začaly provádět expanzivní monetární politiku, tj. stlačovaly úrokové sazby níže a níže a tím motivovaly lidi k novým úvěrům a v poslední době začaly dokonce provádět i takzvané kvantitativní uvolňování. Kvantitativní uvolňování znamená nákup aktiv centrální bankou. To v praxi vypadá tak, že centrální banka nakoupí od finančních institucí určité cenné papíry, převážně státní dluhopisy, a tím zvýší likviditu komerčních bank. Tyto obchodní, chcete-li komerční banky tak mají více peněz k poskytování nových půjček. Čehož pochopitelně využívají, poskytují nové úvěry a tím i emitují nové peníze.

A není žádným překvapením, že v důsledku masivní tvorby nových měnových jednotek, v poslední době rostou i ceny spotřebních statků – cenová inflace. Z dlouhodobého hlediska je ale růst cen velkým problémem, a to hned z několika různých důvodů. Dlouhodobé znehodnocování peněz totiž ničí základní

ekonomický instrument – spoření. V dnešní době je už inflace tak vysoká, že jsou lidé bohužel nuceni (pokud nechtějí přijít o kupní sílu vlastních peněz) začínat s vysoce rizikovými investicemi a riskovat tak ztráty jejich celoživotních úspor.

Peníze, které se znehodnocují z definice nemohou být uchovatelem hodnoty, což je jedna ze základních funkcí peněz. Peníze jsou totiž pouze prostředek k přesunu hodnoty prostorem a časem. Peníze jsou prostředkem směny. Jejich prostřednictvím se ulehčuje směna statků. Ale k čemu jsou takové peníze, které mají časem menší a menší kupní sílu? Přeci jenom, peníze by si měly uchovat svoji hodnotu do té doby, než je opět směníme za jiné zboží. Pokud jsou peníze nevzácné a neuchovávají si svojí kupní sílu, neslouží jako prostředek k uspokojování vlastních potřeb, nýbrž jako nástroj k obohacování určité privilegované skupiny, která má k těmto nově vytvořeným penězům jako první přístup.

Jedním z velmi neintuitivních, byť naprosto zásadních dopadů tvorby peněz je totiž takzvaný Cantillonův efekt. Tento efekt popisuje, jak se vlivem tvorby nových peněz přerozděluje jejich kupní síla, a to od držitelů těchto peněz k jejich emitentům. A to protože, ten, kdo má brzký přístup k novým penězům, může za tyto peníze nakupovat statky, v jejichž cenách ještě nejsou nijak projeveny samotné nově vzniklé peníze – ceny jsou i přes růst měnové zásoby stále stejně nízké, jako před vznikem těchto peněz. A to jsou konkrétně lidé, kteří mají investiční instrumenty, jako jsou například nemovitosti či akcie, kde se pomocí bankovních úvěrů dostávají tyto nově vzniklé peníze, a to, protože většina spotřebitelů, kterým banky poskytují úvěr, si tyto peníze půjčují buďto k nákupu nemovitostí – hypoteční úvěr anebo k financování aktivity vlastního podniku – korporátní úvěr. A na druhou stanu lidé, ke kterým se tyto peníze dostanou až později jsou na tom hůře, poněvadž nakupují zboží a služby za ceny, v nichž je zakomponována skutečnost, že došlo k růstu měnové zásoby, v jejímž důsledku rostou ceny statků. Celý inflační peněžní systém si lze představit jako jednu velkou pyramidu, v níž, čím blíže jste k novým penězům, tím lépe pro vás, to však na úkor lidí, ke kterým se tyto nové peníze dostanou až později. Vše závisí pouze na tom, jak blízko jste ke tvorbě nových peněžních jednotek. Důležité je ale zmínit, že se tento efekt bude objevovat u veškerých peněz, jejichž zásoba se v průběhu čase navyšuje.



Znázornění toho, v jakém pořadí se kdo dostává k novým penězům

Důležité je také zmínit, že současné měny stojí a padají pouze na důvěře k jejich emitentům – bankám. K jejich tvorbě nejsou potřeba prakticky žádné náklady a jejich množství není do budoucna predikovatelné – státní měny nemají předvídatelnou monetární politiku.

O vyřešení problému, že stát zneužívá svého postavení v tvorbě peněz a jeho instituce – centrální banky provádí čím dál tím expanzivnější monetární politiku, čímž znehodnocují peníze všem jejím držitelům a prohlubují Cantillonův efekt, se snažila jistá skupina cypherpunků již na přelomu 20. a 21. století s projekty, jako byl Liberty dollar, e-gold či Bit Gold. Avšak všechny tyto alternativy k současným státním měnám měly jeden velký problém – centralizaci. Centralizované služby mohou fungovat relativně dobře (díky svojí jednoduché správě), jsou však extrémně fragilní, křehké, chcete-li. Centralizované systémy jsou totiž vysoce

zranitelné, stačí pouze jeden „kámen úrazu“ a celý systém je u konce. V tomto případě byly pomyslnými body zkázy sklady se zlatem a stříbrem, které tyto digitální tokeny kryly, a identita zakladatelů těchto projektů.

Ačkoliv je ve Spojených státech naprosto legální konkurovat americkému dolaru, jakožto zákonnému platidlu (neplést s padělaním zákonného platidla, to je federální zločin), když vám, co by státu, soukromé společnosti postupně oslabují váš monopol na tvorbu peněz, ze kterého mimo jiné i díky Cantillonově efektu profitujete, nějaký zákon, který by vás v této činnosti mohl omezit, potažmo celý váš podnik ukončit, se vždy nalezne.

A tak všechny z těchto projektů dopadly neslavně: Zakladatel Liberty dollaru – Bernard Von NotHaus byl odsouzen za padělání peněz a hrozil mu trest až 25 let za mřížemi. Nakonec dostal „pouhých“ 6 měsíců domácího vězení a tříletou podmínku. Přičemž veškeré drahé kovy, které za tímto projektem stály, byly státem zkonfiskovány. Tu tehdy nejpopulárnější a nejrozšířenější alternativu ke státním měnám – e-gold, kterou ve svých nejlepších letech dokonce používalo více než 5 000 000 lidí po celém světě, zakázala americká vláda s odůvodněním, že se skrze ni perou špinavé peníze a financují další trestné činy. Částečně měla vláda skutečně pravdu, protože se e-gold díky své anonymitě, kterou umožňoval, skutečně používal i k ilegálním činnostem, avšak se nejednalo o primární využití těchto digitálních peněz. Koneckonců, každou technologii je možné použít k dobrým, ale i špatným účelům. Kdybychom však zakazovali veškeré inovace jenom kvůli tomu, že se dají použít i k nehezkým účelům, svět by se nikam neposouval, nezažíval by žádný pokrok, který zlepšuje život lidem na celém světě. Kdyby ale americká vláda skutečně chtěla omezit, potažmo znemožnit existenci černého trhu, musela by si prvně zamést před svým vlastním prahem a zakázat hotovost, která se, ze všech platidel, nejčastěji používá k nelegálním transakcím. Tedy je zřejmé, že vlády mají zcela jiné motivace znemožňovat konkurenci peněz, nežli ochránit své vlastní občany před šedou/černou ekonomikou. A poslední ze zde zmíněných projektů, Bit Gold, byl pouze koncept jednoho z nejlepších světových kryptografů Nicka Szaba, který nebyl nikdy uveden do praxe. Možná právě kvůli tomu, jak neslavně dopadly předchozí, podobné projekty.

Skupině cypherpunků bylo jasné, že tudy cesta nevede a je zapotřebí vynaleznout nový systém, ve kterém není jediné, zranitelné místo, ze kterého by byl tento systém ovládán. S decentralizovaným systém, tj. systémem, který nemá jedno centrum, nýbrž je distribuován mezi více různých subjektů, které jej spravují, se ale také pojí určité problémy. A to konkrétně například, jak

dosáhnout shody, konsenzu chcete-li, mezi jednotlivými uživateli sítě bez centrální autority, která by určovala, co je pravda a co ne. V IT terminologii se tento problém nazývá *problém byzantských generálů*.

U peněz by tento problém mohl vypadat následovně: Máme dva členy transakce – Alici a Boba, řekněme, že by Alice chtěla poslat Bobovi 1 minci. Co ji ale brání v tom, s tou samou mincí provést další transakci s jiným členem, třeba s Cyrilem? Nic. V digitálním světě můžete totiž naprosto jednoduše zkopírovat transakci a ostatní uživatelé této sítě nemají, jak rozpoznat, která z těchto transakcí je ta správná. Tento problém tak dostal jméno *problém dvojí útraty* (angl. double-spending problem). Ovšem, jak jej vyřešit?

1. *Centralizovaně*
   Nejjednodušším řešením je postavit mezi Alici, Boba a všechny uživatele daných peněz autoritu, banku, která bude spravovat databázi, ve které bude mít uloženy veškeré transakce, které kdy proběhly. Tedy uvidí například to, že Alice poslala Bobovi 1 minci, tudíž ji už nemá a nemůže ji poslat Cyrilovi. Banka jednoduše znemožní Alici dvojí útratu téže mince. Problém vyřešen, kde je problém? Problém spočívá v samotném centru. Všechny transakce jsou totiž postaveny na důvěře k autoritě, které nic nebrání v tom, aby svého postavení zneužila. Má nad všemi transakcemi moc, pomocí které může určité uživatele cenzurovat. Samozřejmě je zde i již dříve zmíněný problém s centralizací, a sice zranitelnost. Tato databáze je totiž takzvaný *honey pot*, tj. přímo vybízí útočníky, aby na ni zaútočili. Centralizace sice řeší problém dvojí útraty, ale vytváří jiné, velké problémy.

2. *Decentralizovaně*
   Dlouho panoval názor, že k dosažení konsenzu a vzájemné důvěry mezi různými členy určité sítě, musí existovat jistá autorita, která dohlíží na správný chod této sítě a rozhoduje o, v případě peněz, správnosti transakcí. Celý tento narativ dokázal až v roce 2008 změnit určitý člověk nebo skupina lidí s pseudonymem *Satoshi Nakamoto*, který zveřejnil takzvaný *white paper* s názvem Bitcoin: A Peer-to-Peer Electronic Cash System. V tomto technickém návodu Satoshi popisuje fungování nové formy digitálních peněz – Bitcoinu. Problém dvojí útraty vyřešil tak, že mezi veškeré účastníky těchto peněz umístil databázi, ke které mají všichni uživatelé přístup. Distribuované veřejné databázi – účetní knize se říká *Blockchain*. Přičemž tuto databázi spravují samotní uživatelé, tedy pomyslnou „pravdu“ neurčuje jeden centrální bod, nýbrž je výsledkem vzájemné shody uživatelů v síti, kteří mají pozitivní motivace nepodvádět,

respektive, negativní motivace podvádět. Blockchain umožňuje lidem, kteří si navzájem nedůvěřují, bezpečně vytvářet záznamy bez nutnosti přítomnosti prostředníka, jako je banka nebo notář. *Zabezpečováním této účetní knihy a dalšími technickými prvky Bitcoinu se budeme detailněji zabývat hned v nadcházejícím článku.

Nyní si ale pojďme říct něco o monetární politice Bitcoinu. Monetární politika Bitcoinu je nastavena tak, že předem známe jeho konečné množství, nikdy jej nebude více než 21 000 000 (respektive 20 999 999,9769) mincí. Tato politika je navíc předvídatelná, přesně víme, kdy vznikne kolik nových mincí, což je oproti státním měnám obrovská výhoda. U *fiat* měn, tj. státem emitovaných měn s vynuceným oběhem, totiž množství nově vzniklých peněžních jednotek závisí pouze na rozhodnutí cílů centrálních bank, tedy na jednání malé skupiny centrálních plánovačů v oblasti peněz. A tyto cíle se často v průběhu času mění. U fiat měn zkrátka nevíme, kdy se kolik nových jednotek platidla vytvoří. Navíc je jejich měnová zásoba výrazně elastická, tj. mění se v závislosti na ekonomické situaci v daných státech. Mezitím Bitcoin má fixní, přesně danou monetární politiku, která je zajištěna matematikou a technologiemi, o kterých bude řeč v příštím článku, nikoliv důvěrou k autoritě v tvorbě peněz, která svého postavení zatím vždy zneužila.

U Bitcoinu se navíc snižuje tempo růstu nových mincí, a to až do roku 2140, od tohoto roku již nebudou vznikat nové peněžní jednotky. Co to znamená? Bitcoin bude dlouho dezinflační, tj. bude se zpomalovat tempo růstu měnové zásoby (a to exponenciálně) a po roce 2140 bude zcela deflační, tj. bude se snižovat jeho měnová zásoba, a to, protože sem tam někdo ztratí své bitcoiny (respektive *privátní klíče* ke svým *UTXOs*). Tedy Bitcoin má silné předpoklady k tomu, aby u něj byl Cantillonův efekt velmi nízký a po roce 2140 úplně nulový. Navíc musíme vzít v úvahu, že u Bitcoinu jsou vysoké náklady pro vznik nových mincí, tudíž se tak rychle nedostávají do oběhu, čímž snižují právě dopady tohoto efektu. Jinými slovy, z peněz, které dnes známe (fiat, drahé kovy, bitcoin...) bude Cantillonův efekt nejnižší (nikoliv však žádný, respektive do roku 2140 ne) právě u Bitcoinu.