



## Kapitola 6

# Úvod do Bitcoinu

### 6.0 Satoshi Nakamoto a vznik Bitcoinu

#### 6.1 Jak Bitcoin funguje?

##### 6.1.1 Nakamotův mechanismus konsensu (shody)

##### 6.1.2 Uživatelé systému

**Aktivita:** Vytváření konsensu v síti Peer-to-Peer

#### 6.2 Bitcoin jako kvalitní digitální peníze

##### 6.2.1 Úvod

##### 6.2.2 Vlastnosti Bitcoinu

**Aktivita:** Diskuse ve třídě - Je Bitcoin kvalitními penězi?

##### 6.2.3 Přijetí osobní odpovědnosti

**Pracovní sešit**

český překlad | 2024

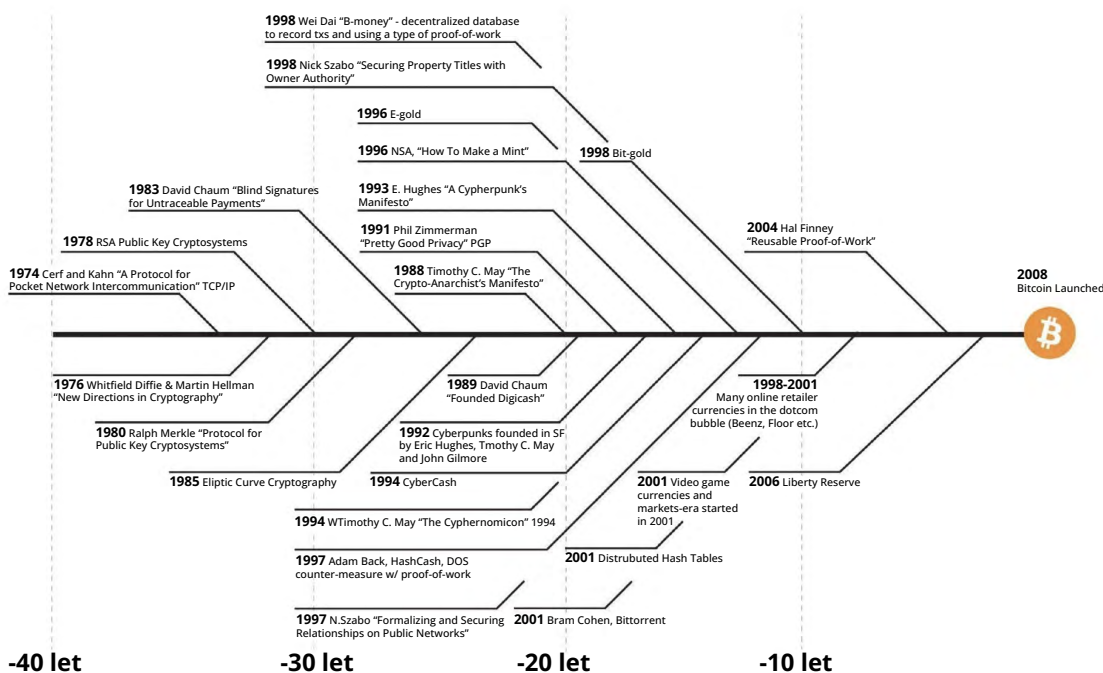
# Úvod do Bitcoinu

## 6.0 Satoshi Nakamoto a vznik Bitcoinu

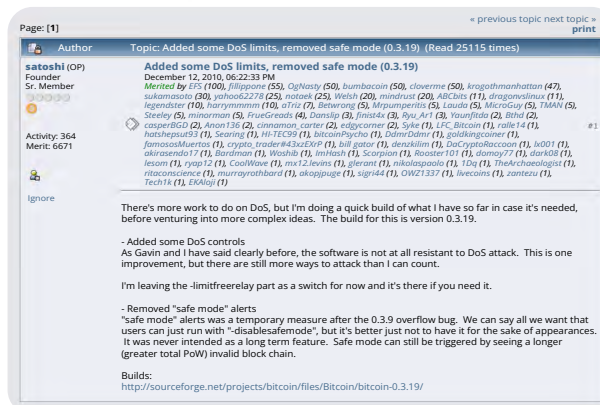
Mnoho lidí vzhledem ke všem projektům, které od 90. let zkrachovaly, automaticky odmítá jakoukoliv elektronickou měnu a považuje je za ztracené případy. Doufejme, že to bylo jen kvůli centrálně řízené povaze těchto systémů, která je odsoudila k zániku. Myslím si, že je to poprvé, co se pokoušíme o decentralizovaný systém, který není založen na důvěře.

Satoshi Nakamoto

### Události před vznikem Bitcoinu - výsledek 40ti let výzkumu, vývoje a poptávky

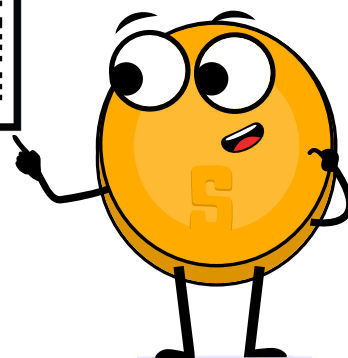


Jak jste se dočetli v předchozí kapitole, o vytvoření alternativního peněžního systému se pokusilo několik cypherpunkerů. V následující kapitole pokračuje příběh jednoho z nich: vizionáře jménem „Satoshi Nakamoto“. Tato pseudonymní osoba (muž, žena nebo skupina osob) byla dlouho, ještě před Bitcoinem, součástí kryptografických nadšenců, jako jsou počítačová vědci a hackeri, kteří se zapojovali do diskusí s cílem najít praktická řešení, jež by nahradila fiat systém.



V říjnu 2008 Nakamoto představil na kryptografickém mailing listu přelomový dokument s názvem „Bitcoin: A Peer-to-Peer Electronic Cash System“. Tento dokument položil základy decentralizovaného peer-to-peer (dále P2P) protokolu, který byl navržen tak, aby umožňoval bezpečné online transakce bez potřeby zprostředkovatelů.

Autorova vize byla jasná: vytvořit čistě P2P verzi elektronické hotovosti, která by se vymanila z kontroly mocných vlád a finančních institucí.



Přejdeme k 3. lednu 2009, kdy Nakamoto vytěžil první blok Bitcoinu, známý jako "genesis blok". Tím byla oficiálně spuštěna Bitcoinová síť, nový peněžní systém postavený na bezpečnosti bez nutnosti důvěry prostřednictvím decentralizované účetní knihy. V následujících měsících a letech se k této myšlence začalo přidávat a přispívat stále více nadšenců.

## Bitcoin Genesis Block Raw Hex Version

```
00000000 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000020 00 00 00 00 3B A3 ED FD 7A 7B 12 B2 7A C7 2C 3E .....;f1y{.2zC,>
00000030 67 76 8F 61 7F C8 1B C3 88 8A 51 32 3A 9F B8 AA .....gv.a.B.A~SQ2:Y,
00000040 4B 1E 5E 4A 29 AB 5F 49 FF FF 00 1D 1D AC 2B 7C .....K.^J)=_iyy...~+|
00000050 01 01 00 00 00 01 00 00 00 00 00 00 00 00 00 00 .....
00000060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000070 00 00 00 00 00 00 FF FF FF FF 4D 04 FF FF 00 1D .....
00000080 01 04 45 54 68 65 20 54 69 6D 65 73 20 30 33 2F .....The Times 03/
00000090 4A 61 6E 2F 32 30 30 39 20 43 68 61 6E 63 65 6C .....Jan/2009 Chancel
000000A0 6C 6F 72 20 6F 6E 20 62 72 69 6E 6B 20 6F 66 20 .....lor on brink of
000000B0 73 65 63 6F 6E 64 20 62 61 69 6C 6F 75 74 20 66 .....second bailout f
000000C0 6F 72 20 62 61 6E 6B 73 FF FF FF FF 01 00 F2 05 .....or banksyyy..d.
000000D0 2A 01 00 00 00 43 41 04 67 8A FD B0 FE 55 48 27 .....*....CA.gSý"bUH'
000000E0 19 67 F1 A6 71 30 B7 10 5C D6 A8 28 B0 39 09 A6 .....gñ|q0..Ö"(a9.¡
000000F0 79 62 E0 EA 1F 61 DE B6 49 F6 BC 3F 4C EF 38 C4 .....ybâe.ab*I0k?Ll8A
00000100 F3 55 04 E5 1E C1 12 DE 5C 38 4D F7 BA 0B 8D 57 .....ou.â.â.b\8M+0..W
00000110 8A 4C 70 2B 6B F1 1D 5F AC 00 00 00 00 .....šLp+kn._~....
```

Poté, co se v roce 2011 ukázalo, že Bitcoinová síť může úspěšně fungovat i bez svého tvůrce, poslal Nakamoto e-mail dalšímu vývojáři na Bitcoinu, ve kterém oznámil, že se stahuje ze scény a předává budoucnost Bitcoinu do „dobrých rukou“. Čili lidem, kteří sdílejí jeho vizi.

Ačkoli Nakamotova identita zůstává dodnes záhadou, záměr vytvořit měnu jako Bitcoin nebyl nikdy tajemstvím. Nakamoto jej v podstatě vytvořil proto, aby odebral moc několika málo lidem a vrátil ji mnoha lidem vytvořením alternativy v podobě decentralizovaného, otevřeného a transparentního peněžního systému, který odděluje peníze od státu. Vznik Bitcoinu byl Nakamotovou reakcí na finanční krizi z roku 2008, která měla dopad na všechny občany po celém světě a zároveň opět obohatila elitní třídu. Bitcoin byl Nakamotovou odpovědí na korupci a křehkost fiat systému. Satoshi položil základy nové revoluce a odešel od ní, místo aby si nárokoval jakékoliv uznání.

# Úvod do Bitcoinu

V následujících letech se Bitcoin začal rychle rozvíjet a stal se symbolem naděje, nezávislosti a odolnosti, který se postavil fiat systému a poskytl bezpečný přístav finančních transakcí odolných vůči cenzuře. Bitcoin je protokol s otevřeným zdrojovým kódem, což znamená, že nikdo nemá moc jej vlastnit nebo ovládat. Jeho zdrojový kód je veřejný a otevřený pro kohokoli, kdo se na něm chce podílet.

Nakamotův sen o transparentním a bezpečném finančním systému bez hranic žije dál a přispívá ke globální revoluci, které jsme dodnes svědky. Běžní lidé každý den dobrovolně opouští fiat systém a vstupují do světa Bitcoinu. Příznivci svobody po celém světě zakládají bitcoinová centra - takzvané bitcoinové cirkulární ekonomiky. Dokonce i celé země, které hledají alternativní cestu, jako například El Salvador, který v roce 2021 jako první stát oficiálně adoptoval Bitcoin jako zákonné platidlo.

## 6.1 Jak Bitcoin funguje?

### 6.1.1 Nakamotův mechanismus konsensu (shody)

Bitcoin má spoustu funkcí, vlastností a jeho pomyslná „králičí nora“ sahá velmi hluboko. Naštěstí, pokud do světa Bitcoinu vstoupíte poprvé, nemusíte k jeho používání dokonale rozumět tomu, jak funguje. Totéž platí pro používání internetu.

Většina lidí neví, jak funguje protokol TCP/IP, a přesto denně posílají e-maily, zprávy a zveřejňují obsah na svém účtu na sociálních sítích. Totéž platí pro řízení auta. Většina lidí přesně neví, jak auto funguje mechanicky, přesto umí řídit. Bitcoin v tomto není výjimkou.



Nicméně Bitcoin zatím není široce rozšířený. Jedná se o poměrně novou technologii, podobně jako byl v 90. letech internet. Z tohoto důvodu může být výhodné pochopit základy Bitcoinu jednoduchým, méně technickým způsobem.

Klíčovou myšlenku Bitcoinu lze shrnout do jedné věty: Bitcoin je soubor pravidel, na kterých se shodli lidé na internetu. Můžete si to představit jako hraní stolní hry s přáteli. Když hrajete deskovou hru, jako jsou Monopoly, jste s ostatními hráči domluveni na konkrétních pravidlech. Jedním z pravidel hry Monopoly je, že se přijímají pouze speciální "monopolní bankovky". Pokud by Jan (jeden z hráčů) porušil pravidla tím, že by místo monopolních bankovek použil na koupi domu toaletní papír, ostatní hráči by Honzovi řekli, že je podvodník, a jednoduše by s ním přestali hrát. Zkrátka, abyste mohli hrát hru, musíte se mezi sebou dohodnout na souboru pravidel a od těchto pravidel se neodchylovat, jinak vás budou ostatní hráči ignorovat.

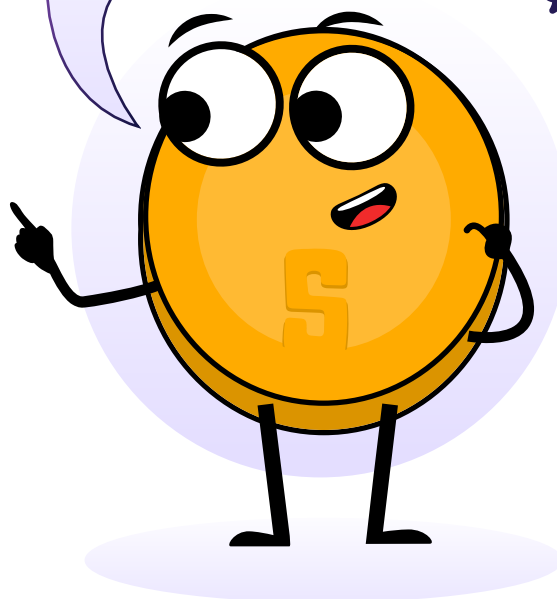
A takto v podstatě Bitcoin funguje. Bitcoin je síť lidí, kteří se shodují na stejném souboru pravidel. Tato pravidla jsou matematicky vázána, zapsána v počítačovém kódu a přijímána každým, kdo software bitcoinu používá. Pravidla platí pro všechny účastníky stejně, což znamená, že každý je buď dodržuje a je součástí ekosystému a pokud je nedodržuje, síť jej odmítne a nemůže se dál účastnit.

Například jedno z pravidel zní: „Nikdy nebude více než 21 milionů bitcoinů“. Pokud si někteří lidé budou chtít vytvořit 1 milion bitcoinů navíc, nebude jim to nic platné, protože by byli automaticky identifikováni a odmítnuti všemi ostatními. Právě díky tomu je bitcoin tak robustní.

*Nezáleží na tom, kdo jste nebo odkud pocházíte, pokud vstoupíte do ekosystému Bitcoinu, musíte hrát podle stejného souboru pravidel jako kdokoli jiný.*

To platí i pro všechny lidi, kteří měli ve světě fiat obrovskou kontrolu a vliv. Ve světě Bitcoinu není žádný prostor pro podvádění nebo sabotáž. Se všemi se zachází stejně a nikdo s tím nemůže nic udělat.

Věděli jste, že od roku 2009 odolal Bitcoin více než desítkám tisíc pokusů o hacknutí, manipulaci nebo jakoukoliv změnu v protokolu? Bitcoin dokázal, že ho nikdo nedokáže zastavit, ovládnout ani zmanipulovat.



# Úvod do Bitcoinu

## 6.1.2 Uživatelé systémy

Abychom lépe pochopili decentralizaci Bitcoinu, musíme se hlouběji ponořit do různých rolí v síti. Ve světě Bitcoinu hrají různí účastníci odlišné, ale harmonické role, které přispívají k bezchybnému fungování sítě.

### 1. Těžaři: Architekti bezpečnosti

Těžaři jsou základním pilířem Bitcoinu. Jsou to lidé nebo skupiny lidí, kteří v zákulisí pracují na zabezpečení sítě prostřednictvím mechanismu zvaného Proof-of-Work (PoW). Tito účastníci disponují speciálními počítači, které obsahují velký výpočetní výkon. Tento výkon dodávají do celé sítě a snaží se vytěžit jednotlivé bloky (soutěží s ostatními těžaři). Dále ověřují transakce a přidávají nové bloky obsahující transakce do decentralizované účetní knihy (tzv. blockchainu). Jejich účast zajišťuje nezměnitelnou podobu účetní knihy a chrání ji před vnějšími útoky.



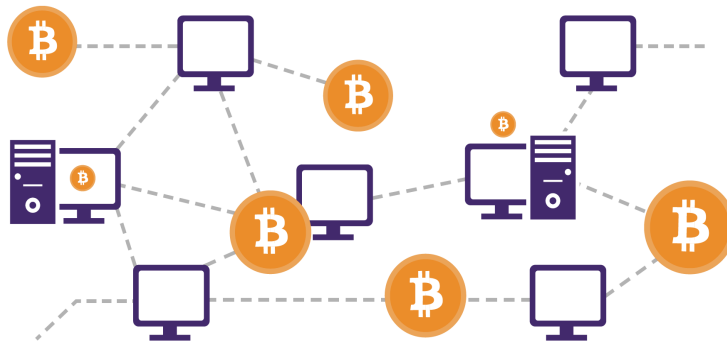
Těžaři, kteří vyřeší „hádanku“ nejrychleji, jsou díky své „usilovné práci“ odměněni v podobě nově vzniklých bitcoinů.

Těžaři bitcoinů jsou rozprostřeni po celém světě, čímž chrání síť před centralizací a zajišťují, aby bezpečnost sítě zůstala robustní a distribuovaná.

### 2. Uzly: Kontrola pravosti

Bitcoinový uzel může provozovat téměř každý na této planetě. Uzly hrají svou roli v síti tím, že na svých osobních počítačích provozují bitcoinový software, v němž udržují kopii celé účetní knihy. Uzly ověřují transakce a zajišťují, aby všichni účastníci dodržovali pravidla konsensu (shody).

Díky rozdělení odpovědnosti za ověřování konsensu mezi síť uzlů zůstává Bitcoin odolný proti útokům a zachovává si svou důvěryhodnou povahu. Uzly hrají klíčovou roli při udržování neměnného stavu účetní knihy a přispívají k decentralizovanému charakteru Bitcoinu.





## 3. Uživatelé: Nezávislí účastníci

Jsou hybnou silou bitcoinové sítě, jelikož se podílejí na provádění transakcí. O uživatelích můžete uvažovat jako o běžných lidech, kteří prostě žijí své životy, ale kteří se také určitým způsobem podílejí na integraci Bitcoinu. Někteří uživatelé například spoří své finanční prostředky do bitcoinu. Jiní, jako například občané Salvadoru mohou používat bitcoin jako peníze na nákup potravin a také mohou dostávat bitcoin ve formě výplaty.

Bitcoin posiluje postavení uživatelů tím, že odstraňuje potřebu zprostředkovatelů, jako jsou banky a vlády, a umožňuje přímé P2P transakce. To také znamená, že uživatelé mají nad svými penězi plnou kontrolu, což jim poskytuje určitou suverenitu a nemožnost konfiskovat jejich majetku.

## 4. Vývojáři: Architekti inovací

Měnový systém budoucnosti se nevybuduje sám od sebe, ani se neujme celosvětově eticky správným způsobem bez vynaložení úsilí. Zde přicházejí ke slovu vývojáři Bitcoinu a projekty postavené na bitcoinové síti.

Vývojáři uplatňují své technické znalosti, aby vylepšili a inovovali bitcoinový protokol. Tito lidé přispívají do zdrojového kódu, navrhuji vylepšení a řeší zranitelnosti, čímž zajišťují, aby se síť vyvíjela v reakci na všechny typy výzev. Open-source povaha Bitcoinu vybízí ke spolupráci, a proto umožňuje vývojářům z celého světa přispívat k jeho růstu.

Krása tohoto decentralizovaného přístupu zabraňuje tomu, aby si kontrolu nad protokolem uzurpoval jeden subjekt. To se děje prostřednictvím procesu založeném na konsensu. Vývojáři navrhuji změny a pouze ti s nejlepšími nápady, které jsou v souladu s širokou vizí lepšího světa, získají podporu komunity. To umožňuje transparentní a demokratický vývoj Bitcoinu, dokud nebude připraven pro 8 miliard lidí.

Na bitcoinových projektech se podílejí různé skupiny, od neziskových organizací, přes korporace až po skupiny nadšenců či jednotlivce, kteří vytvářejí inovativní produkty. Jedná se o lidi, kteří společně pracují na konkrétním projektu nebo lidi, kteří se zaměřují na širší poslání Bitcoinu, které směřuje ke kolektivní svobodě.

Bitcoinové projekty hrají klíčovou roli při utváření a podporování adopce Bitcoinu a snaží se vytvořit budoucnost, která upřednostňuje posílení pravomocí a svobody všech obyvatel.

## Symfonie

Decentralizaci bitcoinu si lze představit jako symfonický hudební orchestr, v němž všichni hráči hrají na různé nástroje a společně vytvářejí tu nejkrásnější hudbu. V bitcoinové síti není žádný šéf, namísto toho jsou těžaři, uzly, uživatelé, vývojáři a ti všichni plní své role autonomně a ve vzájemné spolupráci.

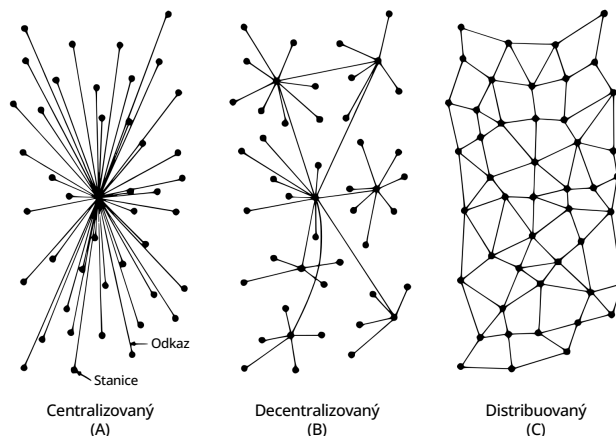
Decentralizovaná účetní kniha spravovaná uzly zaručuje transparentnost, zatímco mechanismus proof-of-work zajišťuje bezpečnost a brání centralizaci těžby. Uživatelé pocítují finanční suverenitu a nezávislost na kontrole fiat systému. Vývojáři, kteří se řídí metodou konsensu, zajišťují, aby se protokol přizpůsoboval měnícím se potřebám člověka. Bitcoinové projekty svým vlastním jedinečným způsobem přispívají k širšímu poslání kolektivní svobody.



# Úvod do Bitcoinu

Jak vidíte, každý účastník hraje zásadní roli při formování adopce Bitcoinu a posilování lidských práv. Každý účastník tohoto decentralizovaného systému přispívá k vyšší odolnosti a životnosti bitcoinu, čímž vytváří ekosystém bez hranic a bez nutnosti důvěry.

Shrnuto a podtrženo, decentralizace v Bitcoinu rezonuje jako důkaz vize Satoshiho Nakamota a obrovského nadšení globální komunity, která usiluje o svobodu a posílení lidských práv.



## Aktivita ve třídě - Vytváření konsensu v síti peer-to-peer



### Cíl

Pochopit, jak se dosahuje konsensu ve skupině, seznámit se s kryptografií na Bitcoinu.



### Materiály

Zpráva s šifrovanými a nezašifrovanými instrukcemi pro akce („zaútočit“ nebo „neútočit“).

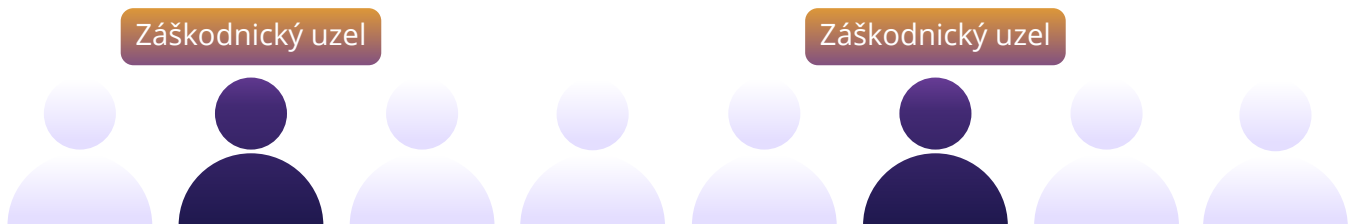


### Příprava na aktivitu

Učitel před hodinou vybere skupinu 3 nebo 4 studentů, kteří budou v následující aktivitě „záškodnickými uzly“. Těmto záškodnickým uzlům zadá učitel jako domácí úkol v předchozí hodině kryptografickou hádanku.

### Postup cvičení:

- 1 Učitel vybere "iniciátora", který obdrží zprávu na papírku s nápisem "ÚTOK" a sérii čísel, které jsou následující "4-16-14-21-1-21-21-1-3-11-", a to jednomu studentovi ze skupiny.
- 2 Studenti vytvoří kruh ve vymezeném prostoru a zajistí, aby vybraní studenti, kteří budou škodlivými uzly, nestáli vedle sebe, čímž se zvýší efektivita celé lekce.



- 3 Jakmile skupina vytvoří kruh, iniciátor předá poznámku jednotlivci na pravé straně kruhu.
- 4 Poté, co si všichni zprávu přečtou, dá iniciátor skupině pokyn slovem "Ted" a skupina na zprávu současně zareaguje. Pokud zpráva zní "ÚTOK", všichni účastníci udělají krok vpřed.
- 5 Po počáteční reakci zůstanou někteří studenti (ti, kteří obdrželi zašifrovanou zprávu a správně ji interpretovali) v klidu, zatímco ostatní se budou řídit původním pokynem, což odhalí absenci shody.

### Závěr:

Pobavte se o tom, proč nebylo dosaženo shody, a přibližte si koncept „problému byzantských generálů“, jak souvisí s nutností dosáhnout společného cíle, a později diskutujte o tom, jak Bitcoin nabízí řešení tohoto problému.

# Úvod do Bitcoinu

## 6.2 Bitcoin jako kvalitní digitální peníze

### 6.2.1 Úvod

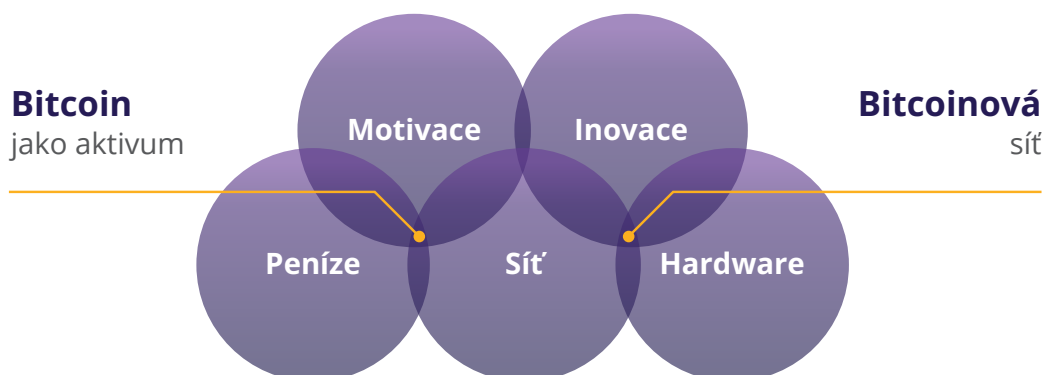
#### Aktivita:

Podívejte se na krátké video „Co je Bitcoin?“



Bitcoin jsou stručně řečeno peníze. Nejedná se o investici, ale spíše o bezpečný a účinný způsob, kam si dlouhodobě uložit své těžce vydělané peníze.

To, že máte bitcoin, neznamená, že z vás budou boháči, protože vám nepřinese výnos v podobě dalších bitcoinů. Jeho hodnota měřená vůči fiat měně sice dlouhodobě stoupá, ale to jen díky jeho vzrůstající adopci a devalvaci fiat měn.



Bitcoin je nová forma peněz. Je to "internet peněz", což znamená, že se k němu může připojit kdokoli a okamžitě si s ostatními může předávat hodnotu. I ty nejizolovanější a nejchudší komunity na světě mají konečně přístup k peněžnímu systému. Podobně jako může každý, kdo má telefon a připojení k internetu, používat vyhledávač, umožňuje Bitcoin každému, kdo má telefon (lze i bez internetu), přístup k novému globálnímu peněžnímu systému.



**Rychlejší  
a levnější  
platby**

Posílejte peníze po celém světě během několika minut a to s velmi nízkými poplatky.



**Zapojení do  
finančního  
systému**

2,5 miliardy lidí bez bankovního účtu může mít nyní přístup k digitálním transakcím pomocí svého telefonu nebo počítače.



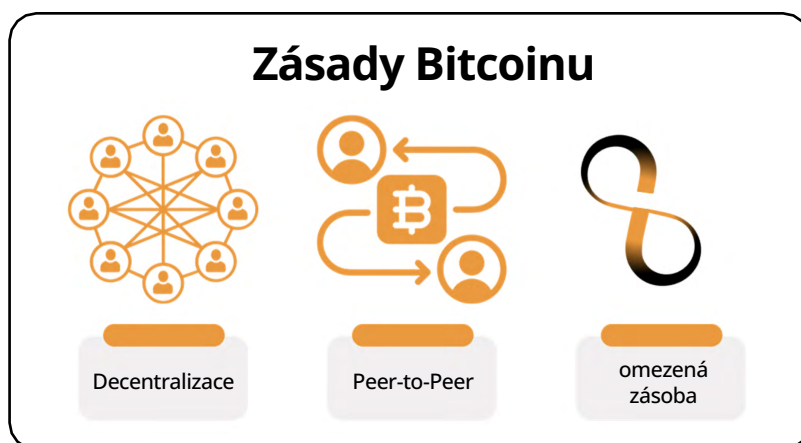
**Zvýšená  
ochrana  
soulkromí**

Bitcoinové transakce jsou veřejné, ale vaše identita nikoli.

Bitcoin je kompletně digitální a zároveň bez hranic. Nezáleží na tom, kde se nacházíte, protože se nachází v počítačích a chytrých telefonech lidí po celém světě. Spousta uživatelů po celém světě provozuje software bitcoinu a vlastní kopii jeho účetní knihy.

Tento software a záznam všech transakcí má velmi malou šanci, že zmizí, protože existuje nespočet jeho kopií. K jeho vypnutí by bylo nutné vypnout internet po celém světě, a to navždy. Tento scénář je velmi nepravděpodobný.

A nakonec, bitcoin je vzácný, což znamená, že množství bitcoinových mincí, které mohou existovat, je absolutně omezené. Nikdo nemůže bitcoin padělat. Dokonce ani nejmocnější vlády a finanční instituce.



## 6.2.2 Vlastnosti Bitcoinu

### Evoluce zdravých peněz

Jak jste se dozvěděli v kapitole 2, životní cyklus kvalitních peněz prochází třemi fázemi, než dojde k jejich obecnému přijetí ve společnosti: A to od uchovatele hodnoty přes prostředek směny až po účetní jednotku.

První stádium peněz, které je uchovatel hodnoty, nastává, když si platidlo začne získávat důvěru jako stabilní (nebo zhodnocující se) aktivum v čase. Lidé, kteří tuto skutečnost včas rozpoznají, se snaží chránit své bohatství uložením peněz v této podobě, a to zejména v době geopolitické a makroekonomické nejistoty.

Některé mediálně známé subjekty označují bitcoin za formu "digitálního zlata". Je to proto, že Bitcoin se v uplynulém desetiletí prosadil jako bezpečný uchovatel hodnoty. Každým dnem začíná stále více lidí vnímat bitcoin jako pojistku proti inflaci, podobně jako to v historii dokázalo zlato.

Další fází je posílení důvěry ohledně stability měny. To je okamžik, kdy měna začíná být prostředkem směny a usnadňuje transakce v každodenním životě lidí. V této fázi začíná být široce přijímána pro směnu zboží a služeb.

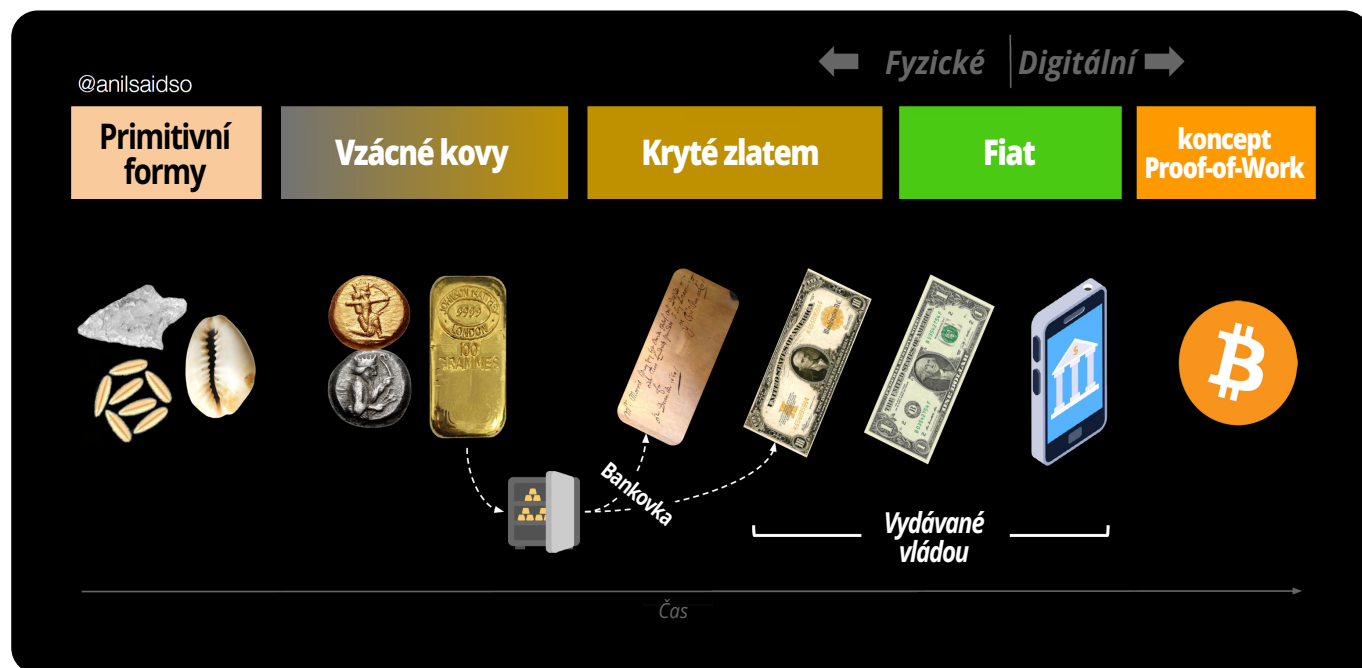
Bitcoin pomalu směřuje k tomu, aby se stal prostředkem směny. S rostoucí mírou přijetí ze strany obchodníků a vývojem protokolu se transakce s bitcoinem stávají efektivnějšími a běžnějšími v každodenním obchodování. Jedním z příkladů je Salvador, kde je bitcoin oficiálně uznán jako zákonné platidlo. Každým dnem začíná stále více běžných občanů a podniků používat bitcoin jako prostředek směny.

# Úvod do Bitcoinu



V závěrečné fázi získává platidlo status účetní jednotky, která slouží jako společné měřítko pro oceňování zboží a služeb. V této fázi se stává základním měřítkem, podle kterého se poměřují všechny ostatní hodnoty.

Cesta k tomu, aby se Bitcoin stal účetní jednotkou, je dlouhý proces. Svět v současnosti měří zboží a služby pouze ve fiat měnách, a proto Bitcoin potřebuje širší přijetí a integraci do různých finančních systémů. Nicméně tento předpoklad je již na dobré cestě, protože podniky i jednotlivci začínají uvažovat o denominaci zboží a služeb přímo v bitcoinu.



Jak je vidět, Bitcoin je v tomto evolučním cyklu zdravých peněz na dobré cestě. Až se Bitcoin plně začlení do globálního finančního systému, mohl by se stát standardní zúčtovací jednotkou a změnit tak celý globální monetární systém.

### Vlastnosti peněz

Jak jste se dozvěděli v kapitole 2, lidstvo postupem času přišlo na to, že skutečné kvalitní peníze musí mít určité vlastnosti, aby byly efektivní. Těmito vlastnostmi jsou odolnost, dělitelnost, přenositelnost, přijatelnost, vzácnost a zaměnitelnost.

Podívejme se, zda Bitcoin v tomto testu obstojí.

**Odolnost:** Bitcoin je čistě v digitální podobě, a proto je zcela odolný.

**Dělitelnost:** Pro srovnání: fiat měnu jako je dolar lze dělit na centy (100 centů = 1 dolar). Bitcoin lze rozdělit na tzv. satsoshi neboli sat (100 000 000 sats = 1 bitcoin). A vzhledem k digitálnímu charakteru bitcoinu jej lze v budoucnu dělit ještě více, bude-li to lidstvo potřebovat. Bitcoin je v současné době nejvíce dělitelným peněžním aktivem na světě.

**Přenositelnost:** V dubnu 2020 bylo převedeno 1,1 miliardy dolarů za pár minut, a to za pouhých 68 centů. Žádný jiný způsob placení nedokáže přesunout tolik peněz s tak nízkými náklady, tak rychle a to pouze v rámci sítě samostatně. Právě to dělá z bitcoinu nejsnáze přenositelnou formu peněz na světě.

**Přijatelnost:** Bitcoin je stále v počátečním stádiu své existence jako prostředek směny, a proto je v porovnání s fiat měnami jeho akceptovatelnost v současné době nízká.

**Vzácnost:** Bitcoinů bude vždy existovat pouze 21 milionů. Podle pravidel konsenzu je nemožné, aby se toto množství někdy zvýšilo, což znamená, že počet mincí je nejen vzácný, ale je zároveň nejvzácnějším peněžním aktivem na světě.

**Zaměnitelnost:** Každá jednotka bitcoinu je stejná jako jakákoli jiná jednotka a lze ji směňovat a obchodovat s ní prostřednictvím protokolu na základě stejného druhu. To z nich činí stoprocentně zastupitelnou měnu.

# Úvod do Bitcoinu

## Bitcoin vs Zlato vs Dolar

Vlastnosti peněz	Zlato	Fiat	Bitcoin
Odolnost	Vysoká	Střední	Vysoká
Přenositelnost	Střední	Vysoká	Vysoká
Dělitelnost	Střední	Střední	Vysoká
Zaměnitelnost	Vysoká	Vysoká	Vysoká
Vzácnost	Střední	Nízká	Vysoká
Ověřitelnost	Střední	Střední	Vysoká
Prověřenost v čase	Vysoká	Střední	Nízká
Odolnost vůči cenzuře	Střední	Střední	Vysoká
Programovatelnost	Nízká	Střední	Vysoká

"Bitcoin vs Zlato vs Dolar" Bitcoin Magazine, <https://bitcoinmagazine.com>

Bitcoin je druh „chytrých“ peněz, které jsou programovatelné, nelze je odcizit a mají všechny vlastnosti, díky nimž jsou skvělé pro spoření a snadno použitelné pro obchodníky, kteří chtějí rychlé transakce.






Protože se jedná o transparentní digitální účetní knihu, může být Bitcoin mimořádně efektivní v takových věcech, jako je odhalování podvodných praktik a zjišťování rizik v určitých online službách. Bitcoin má všechny dobré vlastnosti zlata, jako je jeho omezené množství, ale má také výhody oproti fiat měnám, protože jej můžete jednoduše rozdělit a přenášet. Stručně řečeno, od obou aktiv si bere ty jejich nejlepší vlastnosti a to bez jejich omezení a nevýhod.

Co myslíte? Bitcoin sice zatím není široce rozšířen a adoptován, ale mohl být zdravými penězi?



## Aktivita: Diskuse ve třídě - Jsou Bitcoin kvalitní peníze?

Nyní, když jsme se Bitcoinem zabývali podrobněji, podívejme se znovu na naši srovnávací tabulku peněz z kapitoly 2 a zhodnoťme, jak si Bitcoin stojí v porovnání s ostatními formami peněz:

Vlastnosti kvalitních peněz	 Krávy	 Cigarety	 Diamanty	 Eura	 Bitcoin
Odolnost					
Přenositelnost					
Zaměnitelnost					
Akceptovatelnost					
Vzácnost					
Dělitelnost					
Celkem					

### 6.2.3 Přijetí osobní odpovědnosti

Výsledkem je distribuovaný systém bez jediného centrálního bodu selhání. Uživatelé drží kryptografické klíče ke svým vlastním penězům a provádějí transakce přímo mezi sebou formou P2P v síti, která kontroluje, zda nedochází k dvojímu utrácení stejných mincí.

**Satoshi Nakamoto**

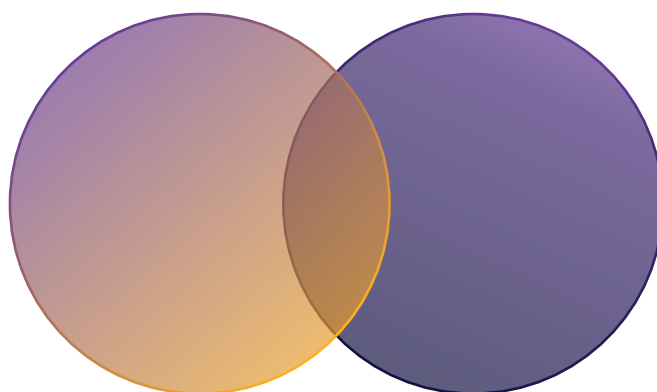
# Úvod do Bitcoinu

V systému fiat měn se lidé spoléhají na vlády, banky a zavedené platební instituce. Šéfové těchto institucí určují pravidla sítě a účastníci (většinou běžní občané) se musí těmito pravidly řídit. Nezáleží na tom, kde žijete, vždy existuje soubor standardních postupů, které vás vedou k tomu, co a jak máte dělat.

Díky tomuto systému jsou lidé zvyklí svěřovat odpovědnost za své finance do rukou jiných. Většina lidí například spoléhá na to, že jim někdo jiný pomůže, a to zejména tehdy, když se něco pokazí (například když ztratí přístup ke svému bankovnímu účtu).

„Bitcoin bude zastaven“

**Pochopení monetární historie**



„Bitcoin se stane zastaralým“

**Pochopení Digitálních sítí**

„Bitcoin už dávno vyhrál“

Monetární systém Bitcoinu je, jak víte, velmi odlišný. Bitcoin funguje specifickým způsobem a vládci byli nahrazeni autonomním systémem pravidel. Neexistuje žádný diktátor nebo vůdce, což také znamená, že vám nikdo nebude diktovat, co máte dělat. Pokud chcete nově objevenou svobodu a suverenitu v podobě Bitcoinu, budete se muset naučit, jak funguje, a začlenit do svého života tuto technologii způsobem, který vám osobně vyhovuje.



Jednotka

1 cent

Vypořádání



Emise



Sat  
0.00000001



S Bitcoinem máte nad svými prostředky plnou kontrolu, ale s touto dodatečnou kontrolou přichází i zvýšená zodpovědnost. Například ztráta přístupu k bitcoinům ztrátou privátních klíčů k digitální peněženke znamená, že jste o své úspory přišli natrvalo. Neexistuje žádná zákaznická linka, na kterou byste mohli zavolat, nebo někdo jiný, na koho byste se mohli obrátit v případě problému. Musíte se o své soukromé klíče starat sami.

Naštěstí se to nestane jedincům, kteří se rozhodnou převzít plnou zodpovědnost za svůj život. Používat Bitcoin není ze své podstaty složité, je to jen nový koncept. Případné nepříjemnosti vznikají proto, že jde o něco neznámého. Pokud jste však ochotni naučit se Bitcoin používat a plně přijmout odpovědnost za ochranu svého bohatství, stává se Bitcoin mocným nástrojem, protože jej máte pod kontrolou a nikdo nemůže vaše bohatství zkonfiskovat.

Klíčem k úspěchu je pochopení fungování Bitcoinu a jeho implementace v souladu s vašimi jedinečnými potřebami a životní filozofií. V další kapitole začneme používat bitcoin tím způsobem, že si založíme libovolnou bitcoinovou peněženku, odešleme a přijmeme první transakce a projdeme si osvědčené bezpečnostní postupy.