#### 

|  |
| --- |
| * Kapitola 9: Úvod k technické stránce Bitcoinu   + 9.0 Úvod     - **Aktivita** – Zhlédněte video ,,Jak Bitcoin funguje pod pokličkou”   + 9.1 Verejné a soukromé klíče: Zabezpečení skrze kryptografii     - 9.1.1 Kryptografické verejné/soukromé klíče     - 9.1.2 Vysvětlení hashovací funkce     - **Aktivita** - Generujte SHA 256 hashovací funkci   + 9.2 UTXO Model   + 9.3 Bližší pohled na Bitcoinové uzly a těžaře     - 9.3.1 Co to je Bitcoinový uzel a jak si ho nastavit doma?     - **Aktivita** – Zhlédněte video o Bitcoinových uzlech     - 9.3.2 Co to je těžební stroj a jak těžba funguje?   + 9.4 Co to je Mempool     - **Aktivita** - Mempool   + 9.5 Jak fungují Bitcoinové transakce od začátku až do konce     - **Aktivita** – Bitcoinové transakce v praxi |

#### 

#### 

#### 

# Kapitola 9: Úvod k technické stránce Bitcoinu

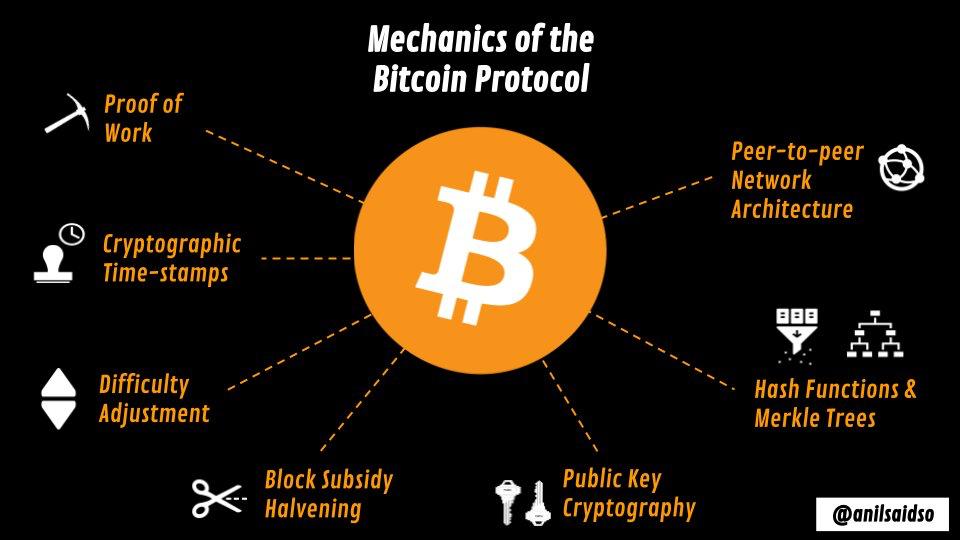
# ,,Bitcoin není neregulovaný. Místo toho, aby byl regulován vládní byrokracií, je regulován algoritmem. Je tedy nezkorumpovatelný."

Andreas M. Antonopoulos

## 9.0 Úvod

V této kapitole se blíže podíváme na technologii, která umožňuje zcela decentralizované fungování Bitcoinové sítě. Zjednodušeně si vysvětlíme, co se děje při odesílání transakcí, jak se tyto transakce zpracovávají a co dělají těžaři a uzly v síti.

[Image from Chapter 9 Images Folder]



V této kapitole se budeme zabývat některými náročnějšími a technickými koncepty. Důležité je si uvědomit, že mnoho lidí například nerozumí ani tomu, jak dnes funguje internet, a přesto ho denně používají k posílání e-mailů, kontaktování přátel na sociálních sítích a dokonce i k placení účtů. Naučit se technickou stránku fungování Bitcoinu je dlouhá cesta, kterou nemusí chtít podniknout každý, i když se rozhodne používat ho jako peníze. I když vám doporučujeme, abyste se o technických aspektech Bitcoinu učili dál, v této kapitole se zaměříme na základní klíčové pojmy.

|  |
| --- |
| [ORANGE NOTE BOX]  Chcete-li se hlouběji seznámit s technickými aspekty fungování Bitcoinu, v zadní části této učebnice naleznete zdroje. Na našich webových stránkách se také můžete zaregistrovat do kurzu Bitcoin Diploma - Technical Edition, abychom vás kontaktovali, jakmile bude tento odbornější kurz dostupný. |

Pojďme se podívat na video, které ukazuje, jak Bitcoinová síť funguje.

**Aktivita** - Zhlédněte ,,Jak Bitcoin funguje pod pokličkou” [[QR-CODE](https://www.youtube.com/watch?v=Lx9zgZCMqXE)]

## Jak jste viděli ve videu, Bitcoinová síť je zjednodušeně řečeno účetní kniha nebo záznam transakcí, který je uložen na mnoha počítačích, které nazýváme uzly. Bitcoinová účetní kniha je pseudonymní, což znamená, že neobsahuje osobní údaje, pouze informace o transakcích a adresách. V účetní knize jsou uvedeny všechny bitcoiny a jejich pohyby od spuštění sítě 3. ledna 2009.

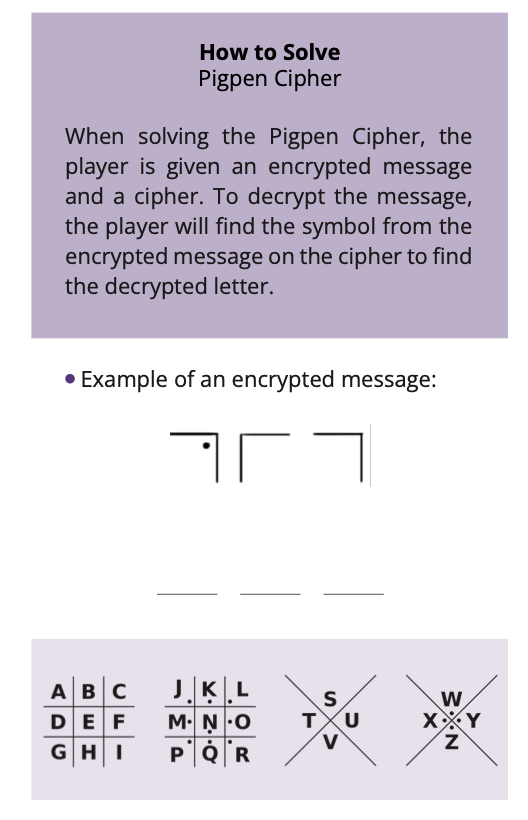
## Dále se podrobněji podíváme na technologii, která umožňuje, aby byl tento systém funkční...

## 9.1 Verejné a soukromé klíče: Zabezpečení skrze kryptografii

"Bitcoin nám nabízí závazný slib: tento program bude vykonávat přesně to, co bylo stanoveno ve zdrojovém kódu."

Andreas Antonopoulos

**9.1.1 Kryptografické verejné/soukromé klíče**

Kryptografie je způsob utajení informací jejich zašifrováním v kódu.

[Images from BD 2023 page 86-88

Jak vyřešit Pigpen šifru

Při řešení Pigpen šifry dostane hráč zašifrovanou zprávu a šifru. Aby hráč dešifroval zprávu, musí najít symbol ze zašifrované zprávy na šifře a najít tak dešifrované písmeno

* Příklad zašifrované zprávy.

]

Šifrování je proces, při kterém se informace převezme a převede do speciálního kódu, tak aby ji nikdo, kdo nemá správnou dešifrovací metodu, nemohl přečíst. Je to podobné jako při zamykání trezoru, který může otevřít pouze osoba se správným klíčem nebo kombinací.

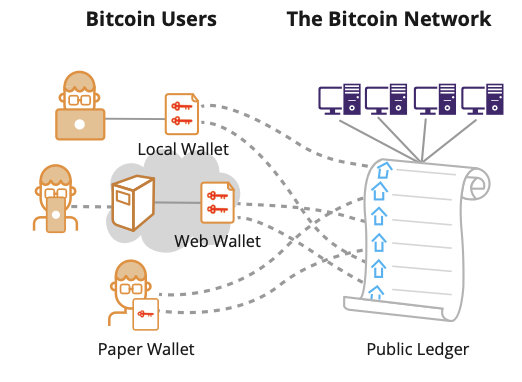
Dešifrování je oproti tomu proces, kdy se zašifrované informace vezmou a znovu se stanou čitelnými, podobně jako když odemknete trezor a můžete si informace uvnitř přečíst.

Řekněme například, že Jan chce poslat Adamovi tajnou zprávu, kterou nemá nikdo jiný číst. Dohodnou se, že před odesláním zprávy použijí k jejímu zamaskování Pigpen šifrovací metodu. Zprávu mohou dešifrovat pouze ti, kteří šifru znají, takže pro kohokoliv jiného je nečitelná. Ačkoli tato metoda není dnes považována za bezpečnou, ilustruje princip šifrování pomocí soukromého klíče pro odesílání zpráv.

Jak tedy funguje kryptografie při Bitcoinových transakcích?

V tradiční kryptografii soukromých klíčů by Jan a Adam museli nejprve vzájemně nasdílet tajný klíč, například heslo nebo Pigpenovu šifru. Jan by pak tento klíč použil k zašifrování své zprávy před odesláním Adamovi. Adam, který také zná tajný klíč, by pak použil stejný klíč k dešifrování zprávy a jejímu přečtení.

Pokud by však klíč vlastnil někdo jiný a zprávu zachytil, mohl by ji taky zašifrovat a přečíst.



[Image from BD 2023 page 26-37]

Kryptografie s veřejnými klíči, která se používá v Bitcoinových transakcích, tento problém řeší. Díky kryptografii s veřejným klíčem si Jan a Adam nemusí navzájem sdělovat heslo ani způsob šifrování. Místo toho má každý z nich dva různé klíče: veřejný klíč (který může bezpečně sdílet s kýmkoli) a soukromý klíč (musí zůstat soukromý).

V tomto případě, když chce Jan poslat zprávu Adamovi, může před odesláním zprávy použít Adamův veřejný klíč k zašifrování své vlastní zprávy. Když Adam zprávu obdrží, může ji dešifrovat pouze on pomocí svého soukromého klíče. Kdokoli jiný, i kdyby zprávu zachytil, by ji nemohl přečíst. Šance na krádež klíče je také mnohem menší, protože ani Jan ani Adam si nemusí tento klíč navzájem sdělovat.

Hlavní výhodou kryptografie s veřejnými klíči oproti kryptografii se soukromými klíči je tedy to, že umožňuje bezpečnou komunikaci, aniž by odesílatel a příjemce museli nejprve sdílet tajný klíč (nebo jinou šifrovací metodu), který by mohla zachytit třetí strana.

V Bitcoinu se k odesílání šifrovaných zpráv nepoužívá kryptografie s veřejným klíčem. Místo toho se používá k vytváření jedinečných digitálních podpisů, díky nimž jsou bitcoinové transakce neměnné. Digitální podpis je způsob, jak prokázat pravost bitcoinové transakce, v jistém smyslu podobný tomu, když napíšete svůj podpis na fyzický dokument.

[Image from BD 2023 page 26-37]

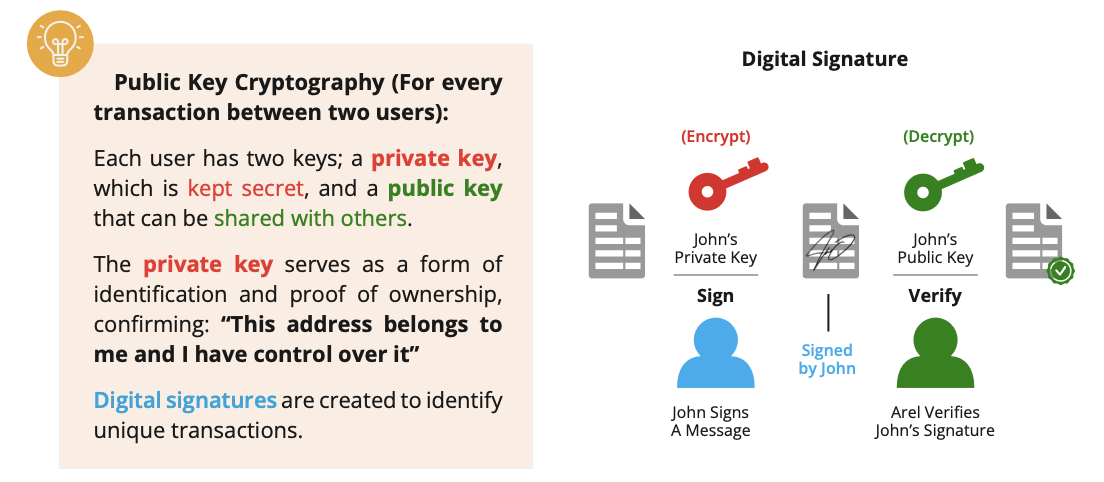
[TEXT BOX]

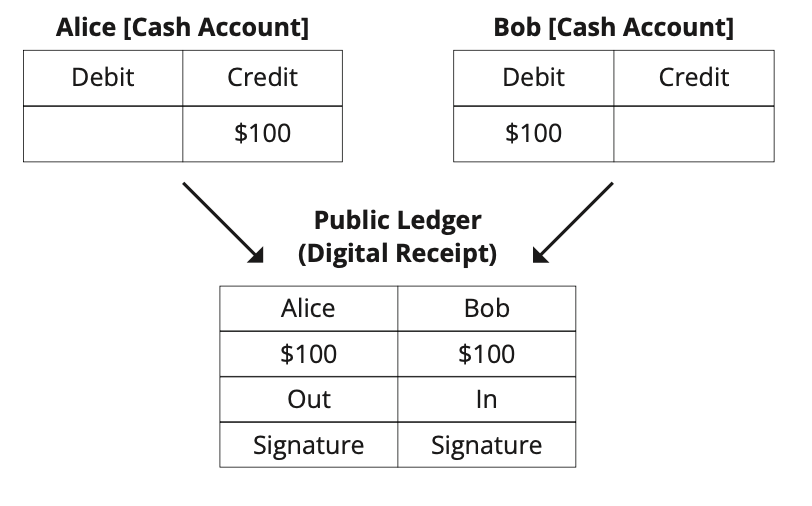
Kryptografie veřejných klíčů (pro transakce mezi dvěma uživateli):  
  
Každý uživatel má dva klíče, soukromý klíč, který je uchováván v tajnosti, a veřejný klíč, který může sdílet s ostatními.

Soukromý klíč slouží jako forma identifikace a důkaz vlastnictví, který potvrzuje, že „tato adresa patří mně a mám nad ní úplnou kontrolu“.

Digitální podpisy se vytvářejí za účelem identifikace jedinečných transakcí.

[END TEXT BOX]



[Image from BD 2023 page 26-37]

* Bitcoinové transakce zahrnují převod určitého množství bitcoinů přímo na adresu jiné osoby.
* Šifrování se používá k zajištění toho, aby pouze skutečný držitel bitcoinu měl kontrolu nad tím, zda může své peníze poslat někomu jinému. Zajišťuje, aby byl majetek střežen před zneužitím jinými aktéry.
* Jako dodatečné ochranné opatření má každá transakce, kterou odešlete v bitcoinu, automaticky UNIKÁTNÍ podpis. Tento jedinečný podpis je vybaven technologií prokazující neoprávněnou manipulaci, která pomáhá síti ověřit, že bitcoin odeslal skutečný vlastník, a ne někdo jiný.

[Image from BD 2023 page 26-37]



Jak to jednoduše funguje při odesílání bitcoinových transakcích:

1. Vytvoření transakce: Uživatel zadá údaje, jako je adresa příjemce a částka v bitcoinech, která má být odeslána.
2. Generování digitálního podpisu: Odesílatel vygeneruje jedinečný digitální podpis pomocí svého soukromého klíče. Tento podpis je jedinečný kryptografický kód, který ověřuje platnost transakce.
3. Vysílání transakce: Podepsaná transakce se vyšle do bitcoinové sítě, čímž se vyjádří záměr převést vlastnictví bitcoinu z odesílatele na příjemce.
4. Ověření v síti: Uzly v Bitcoinové síti přijmou transakci a použijí veřejný klíč příjemce k dešifrování a ověření úplnosti transakce. Současně použijí veřejný klíč odesílatele k ověření digitálního podpisu.
5. Potvrzení v Bitcoinové síti: Pokud je ověření úspěšné, transakce se přidá do účetní knihy, která slouží jako bezpečný a transparentní záznam všech transakcí. Po potvrzení je vlastnictví bitcoinu oficiálně převedeno z odesílatele na příjemce.

Když to shrneme, digitální podpis vytvořený pomocí soukromého klíče odesílatele slouží jako kryptografický důkaz pravosti a vlastnictví. Zároveň tak umožňuje v decentralizované síti potvrdit a zaznamenat transakce do účetní knihy.

**9.1.2 Vysvětlení hashovací funkce**

Nenechte se prosím zastrašit technickými termíny a matematickými pojmy. Chápeme, že ne každý je blázen do matematiky, ale možná sami sebe překvapíte a zjistíte, že i ty nejsložitější myšlenky lze s trochou snahy pochopit celkem jednoduše.

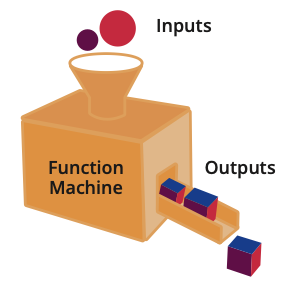
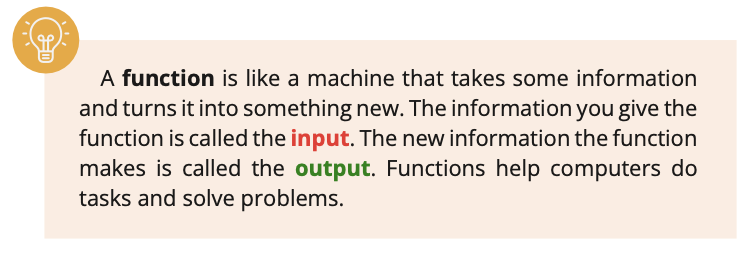
Co to je funkce?

[Image from BD 2023 page 124-128]

[TEXT BOX]

Funkce je jako stroj, který vezme nějakou informaci a přemění ji na něco nového. Informace, které funkci předáte, se nazývají vstup. Nová informace, kterou funkce vytvoří, se nazývá výstup. Funkce pomáhají počítačům plnit úkoly a řešit problémy.

[END TEXT BOX]



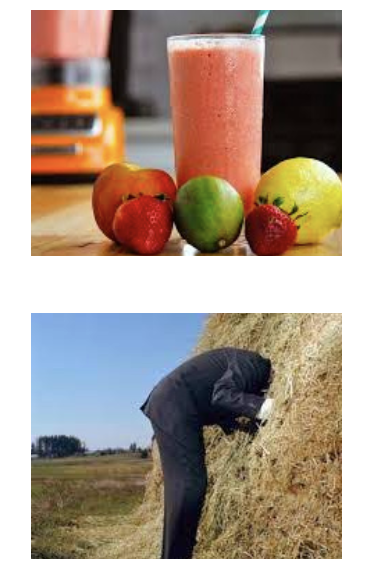
[Image from BD 2023 page 124-128]

Představte si to jako recept na přípravu salátu. Recept (nebo funkce) vám říká, jaké ingredience použít a jak je smíchat dohromady, abyste salát připravili. Můžete do něj vložit různé přísady, ale výsledkem receptu bude vždy salát. Funkce lze použít k usnadnění a zefektivnění práce.

Tento recept je tedy funkcí, která na vstupu přijme ingredience a na výstupu vytvoří míchaný salát.

V Bitcoinu se funkce používají k provádění transakcí. Už víme, že Bitcoinové transakce jsou v podstatě převody hodnoty (peněz) z jedné adresy na druhou. K provedení transakce se používá řada kryptografických funkcí, které transakci ověřují a aktualizují stav Bitcoinové účetní knihy.

Mezi funkce používané při bitcoinových transakcích patří ověřování pravosti vstupů transakce, kontrola, zda má odesílatel dostatek finančních prostředků, a aktualizace zůstatků na příslušných adresách. Jakmile je transakce ověřena a přidána do bloku v účetní knize, stává se součástí trvalého záznamu všech transakcí v síti.

[Image from BD 2023 page 124-128]

Co to je jednosměrná funkce?

Jednosměrná funkce používá sadu instrukcí ke zpracování informací a mění je v něco nového, podobně jako recept na smoothie mění ingredience v nápoj. Ale stejně jako nemůžete rozmixovat smoothie a získat zpět původní ingredience, nemůžete ani obrátit jednosměrnou funkci a získat zpět původní informace.

[Image from BD 2023 page 124-128]

Kryptografie s veřejnými klíči, je založena na použití jednosměrných funkcí, které znesnadňují určení soukromého klíče z veřejného klíče. Teoreticky není úplně „nemožné“ zjistit soukromý klíč z veřejného klíče, ale je to nesmírně obtížné a splnění tohoto úkolu by vyžadovalo nesmírné množství času a výpočetního výkonu.

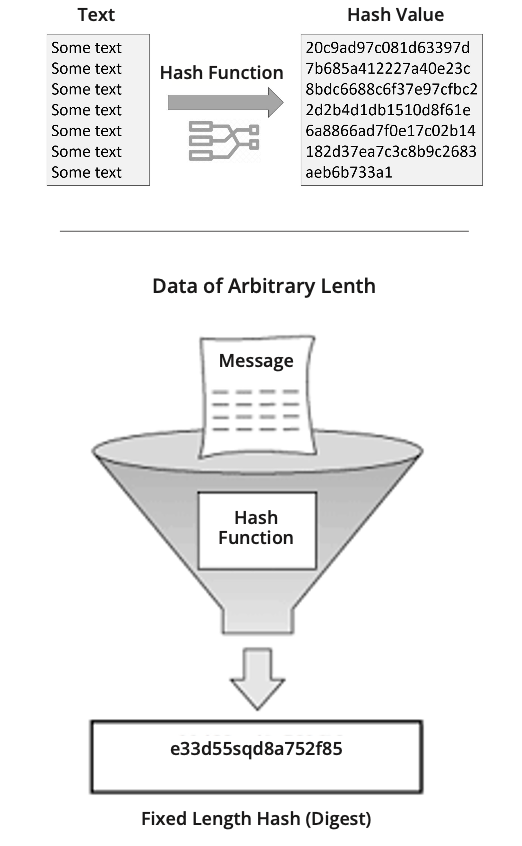
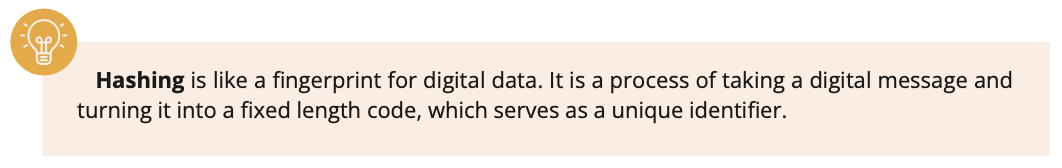
Najít soukromý klíč z veřejného klíče v Bitcoinu je jako hledat jehlu v kupce sena o velikosti fotbalového hřiště. Jehla představuje soukromý klíč a kupka sena všechny možné soukromé klíče. Jinými slovy řečeno, množství soukromých klíčů, které mohou být vygenerovány, je větší než je počet atomů ve vesmíru.

Stejně tak jsou jednosměrné funkce navrženy způsobem, aby byly nevratné a nebylo možné je dešifrovat.

[Image from BD 2023 page 124-128]

Co je to hashovací funkce?

[TEXT BOX]



Hashování je jako otisk prstu pro digitální data. Je to proces, při kterém se digitální zpráva převede na kód pevné délky, který slouží jako jedinečný identifikátor.

[END TEXT BOX]

Stejně jako otisk prstu umožňuje identifikovat osobu, hash může identifikovat digitální zprávu. Hashe se používají v mnoha aplikacích, včetně bitcoinových transakcí.

Jak se hashování používá v Bitcoinových transakcích?

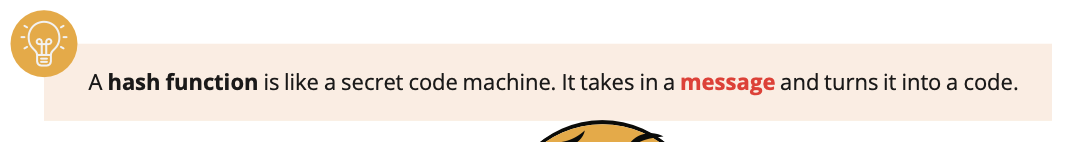
V Bitcoinu je každá transakce před přidáním do bloku v účetní knize hashována. Hash slouží jako podpis transakce a ověřuje, že transakce je platná a nebylo s ní manipulováno. Pokud se někdo pokusí změnit byť jen jediné písmeno v transakci, hash bude úplně jiný a upozorní na změnu ostatní.

**Úloha hashování při zajišťování bezpečnosti**

Hashování je pro bezpečnost Bitcoinové sítě zásadní. Pomocí hashů k identifikaci transakcí může síť odhalit jakýkoli pokus o změnu nebo manipulaci s transakcemi. To pomáhá předcházet podvodům a zajišťuje, že všechny transakce jsou v účetní knize zaznamenány přesně a neměnným způsobem.

Hashovací funkce je typ jednosměrné funkce, která přijímá vstup (označovaný jako „zpráva“ nebo „data“) a převádí jej na číselnou reprezentaci označovanou jako „hash“. Výstupní hash je jedinečný pro vstupní data, takže i malá změna vstupních dat vede k úplně jinému výsledku.

[TEXT BOX]



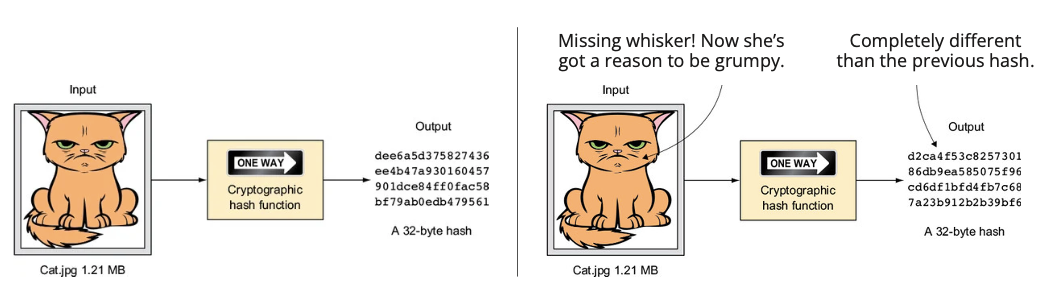
Hashovací funkce je jako stroj na vytváření tajných kódů. Přijme zprávu a přemění ji na kód.

[END TEXT BOX]

[Image from BD 2023 page 124-128]

Kód vypadá pro jednu a tutéž zprávu vždy stejně. Pokud zprávu jen trochu změníte, kód bude zcela jiný. To pomáhá počítačům zapamatovat si věci a kontrolovat, zda se něco nezměnilo.

**Aktivita** - Generujte SHA 256 hashovací funkci →

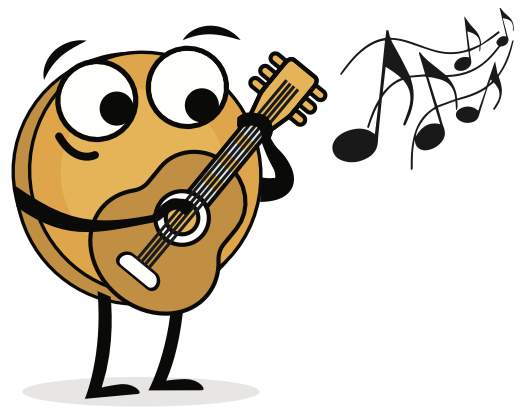


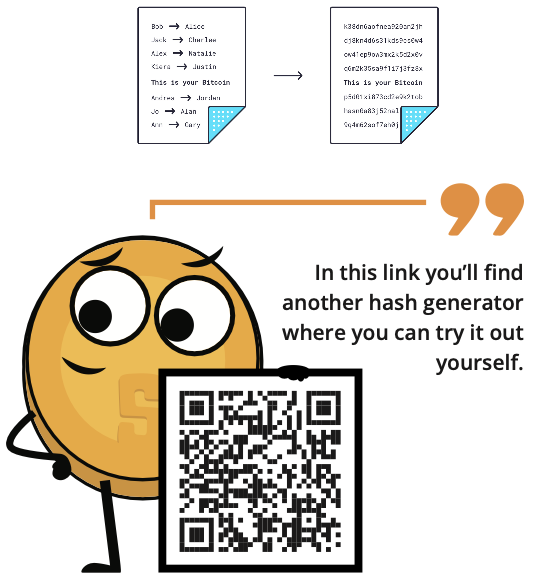
Výstup neboli hash má vždy stejnou délku bez ohledu na to, jak dlouhá byla původní informace.

Bitcoin používá několik specifických typů hashovacích funkcí nazvaných SHA-256 a RIPEMD160.

* Níže uvádíme několik příkladů: Všimněte si, že malá změna (kurzíva) druhého vstupu zcela změní výstup ve srovnání s prvním vstupem.
* Třetí vstup je obrovský soubor, přesto má výstup stále stejnou pevnou délku jako ostatní dva.



[Image from BD 2023 page 124-128]

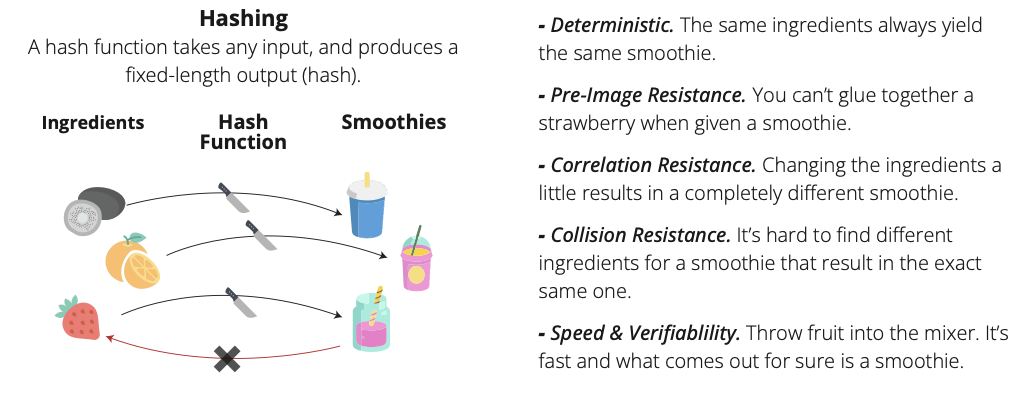
Hashování si lze také představit jako hudební noty, které zachycují refrém hudební skladby. Stejně jako jsou noty jedinečnou reprezentací melodie, je hodnota hashe jedinečnou reprezentací kusu dat. Porovnáním notového zápisu hudební skladby se skutečným provedením může hudebník určit, zda je představení přesné. Podobně lze porovnáním hodnoty hashe přijatých dat s původní hodnotou hashe určit, zda byla data během přenosu změněna.

Stejně jako nepatrná odchylka v hudebním výkonu může způsobit, že melodie bude znít jinak, i sebemenší změna původních dat povede k jiné hodnotě hashe. Díky tomu je hashování mocným nástrojem pro zajištění integrity a pravosti Bitcoinové transakce.

[Image from BD 2023 page 124-128]

Proces kódování veřejného klíče pomocí hashování se používá ke zvýšení bezpečnosti informací tím, že se převedou do nečitelného formátu s pevnou délkou. Bitcoin používá k vytváření veřejných adres algoritmy SHA-256 a Ripemd-160. Výsledný výstup slouží jako jedinečný identifikátor veřejného klíče a pomáhá zajistit integritu a bezpečnost transakcí uložených v účetní knize. Tímto způsobem šifrování informací je pro neoprávněné osoby obtížnější získat přístup k datům a manipulovat s nimi.

[Image from BD 2023 page 124-128]



## 9.2 UTXO Model

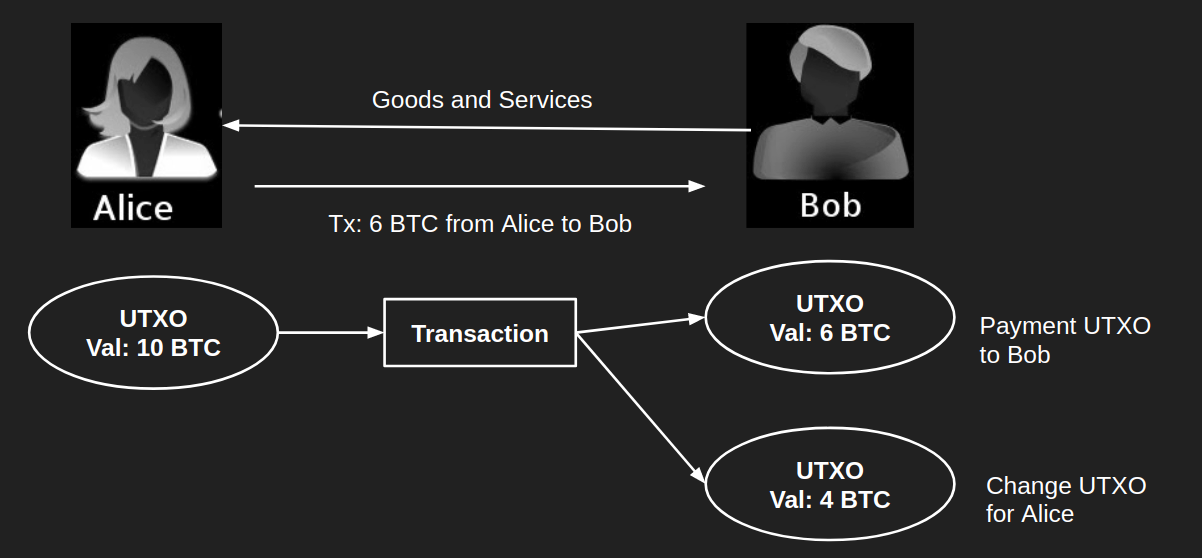
|  |
| --- |
| ORANGE IDEA BOX  UTXO znamená Unspent Transaction Output (Neutracený výstup z transakce) |

Co to jsou UTXO?

V Bitcoinu fungují transakce tak, že větší ,,kus” bitcoinu rozdělíte na menší kousky a tyto menší kousky pošlete ostatním i sobě.

UTXO si můžete představit jako různé velikosti a kousky bitcoinu nebo různě denominované bankovky ve vaší peněžence. Když utratíte UTXO, přetvoří se na nové UTXO pro příjemce a to, co zbyde, se vám pošle zpět v podobě nového UTXO. Je to podobné, jako když si za 10-ti dolarovou bankovku koupíte dva šálky kávy za 6 dolarů. 6 dolarů si kavárna ponechá a 4 dolary vám vrátí v drobných.

[Image from Chapter 9 Images Folder]



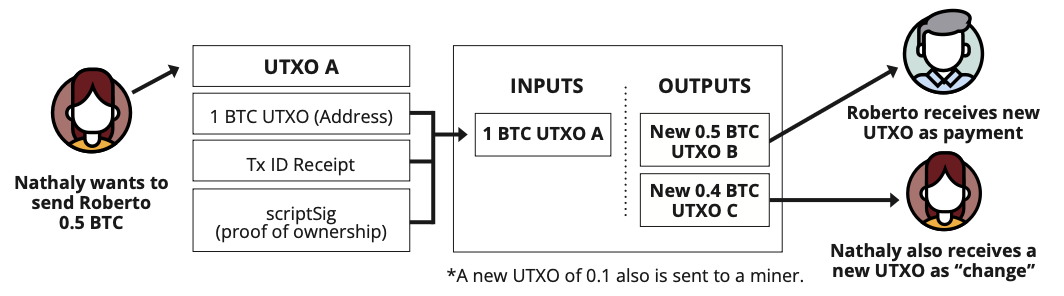
Při odesílání bitcoinů posíláte vždy celou částku jednoho (nebo více) UTXO v Bitcoinové peněžence. Co se stane? Část pošlete příjemci a zbývající částku obdržíte zpět jako drobné na jednu ze svých nových bitcoinových adres. Drobné, které obdržíte zpět, se nazývají neutracený výstup transakce neboli UTXO a lze je použít jako vstup pro novou budoucí transakci.

Zůstatek vaší Bitcoinové peněženky je součtem všech vašich různých UTXO. Součet vašich UTXO je tedy součtem množství bitcoinů, které vlastníte.

|  |
| --- |
| ORANGE IDEA BOX  Je důležité si uvědomit, že byste neměli dávat ostatním vědět o svých UTXO, protože když někdo zná vaše UTXO, může sledovat vaše bitcoinové transakce v síti a nakonec zjistí, kolik peněz vlastníte. |

Závěrem lze říci, že pokaždé, když provedete transakci, použijete jedno nebo více svých stávajících UTXO k utrácení bitcoinů a vytvoří se nová UTXO (pro vás i pro příjemce).

[Image from BD 2023 page 122]

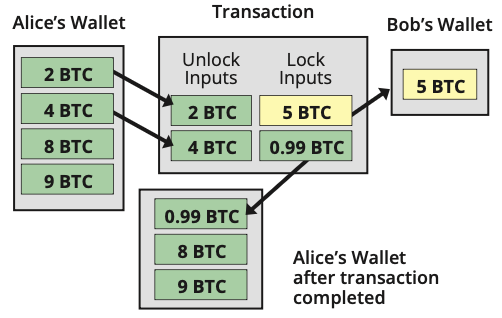


Při transakci se odeslaná částka bitcoinů rozdělí na více výstupů, z nichž každý je spojen s novou bitcoinovou adresou (novým UTXO).

Když někomu posíláte bitcoiny, použijete jednu nebo více UTXO jako zdroj finančních prostředků (vstup). Tyto UTXO se v případě potřeby zkombinují a vytvoří nové výstupy, které patří jak příjemci transakce, tak vám. Tyto nové výstupy neboli UTXO se pak stanou majetkem příjemce i vaším majetkem. Tyto UTXO pak můžete použít jako zdroj prostředků v dalších budoucích transakcích. Tento řetězec UTXO vytváří transparentní a dohledatelnou historii všech bitcoinových transakcí v účetní knize, počínaje úplně prvním blokem (3. ledna 2009).

Ilustrační příklad: pokud chcete poslat 2 bitcoiny, ale máte pouze UTXO v hodnotě 5 bitcoinů, rozdíl 3 bitcoinů vám bude zaslán zpět jako "drobné". Tato změna pro vás představuje nové UTXO a toto nové UTXO můžete utratit v budoucí transakci.

[Image from BD 2023 page 122]

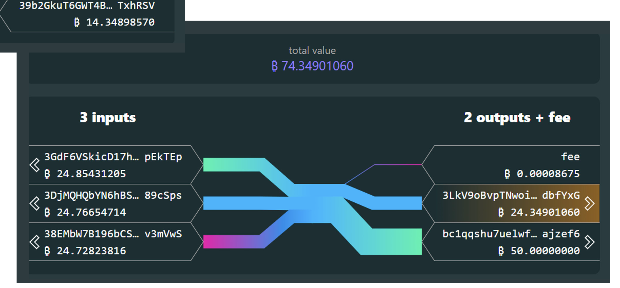
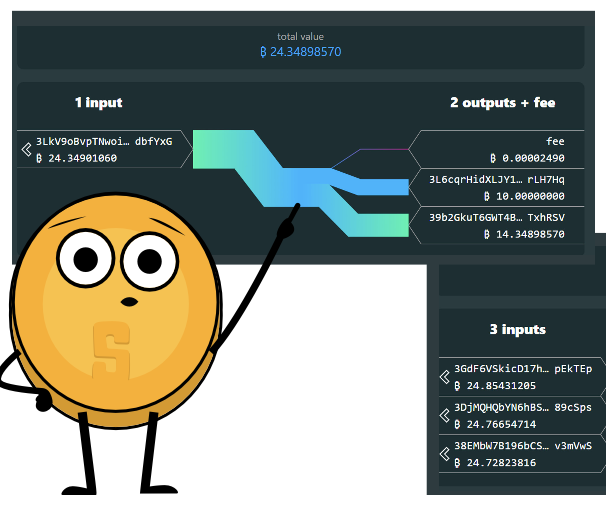
Další příklad:

1. Alice chce poslat Bobovi 5 bitcoinů.
2. Spojí 6 bitcoinů ze dvou svých UTXO.
3. Z těchto UTXO pošle Bobovi 5 bitcoinů, zpět k sobě dostane 0,99 bitcoinu jako drobné a musí zaplatit poplatek za transakci ve výši 0,01 bitcoinu.
4. Po potvrzení je transakce přidána do účetní knihy a aktualizují se všechny uzly, které mají kopii této knihy.

Řekněme, že se Alice pokusí použít jeden ze svých již utracených výstupů k provedení další transakce. Uzly ji automaticky odmítnou, protiže si udržují kopii účetní knihy (a všech jeho transakcí), a tak mohou snadno zkontrolovat zůstatek Aliciných UTXO a ověřit, že transakce není platná.

Níže je reálný snímek obrazovky skutečné transakce, kde je pouze jeden vstup. Počáteční zůstatek však může být v jiném případě součtem více UTXO (více vstupů). Jaké závěry můžete učinit, když se podíváte na dvě níže uvedené transakce? Odpovídají vstupy výstupům? Můžete popsat podrobnosti transakce? Existuje mezi oběma snímky nějaká souvislost? A která transakce proběhla jako první?

[Image from BD 2023 page 123]



## 9.3 Bližší pohled na Bitcoinové uzly a těžaře

V této části se podrobněji podíváme na dvě velmi důležité účastníky Bitcoinové sítě, kteří byli poprvé představeny v kapitole 6. Podíváme se na:

1. Bitcoinové uzly: Jejich hlavním úkolem je uchovávat kopii Bitcoinové účetní knihy, dohlížet na platnost všech transakcí a na to, aby se všichni řídili stejnými pravidly.

Tím, že je tato práce rozdělena mezi mnoho lidí po celém světě, zůstává Bitcoin odolný proti potenciálním útokům. Tyto uzly pomáhají udržovat systém důvěryhodný a věrný jeho decentralizované myšlence, kdy žádná osoba ani skupina nemá příliš velkou moc.

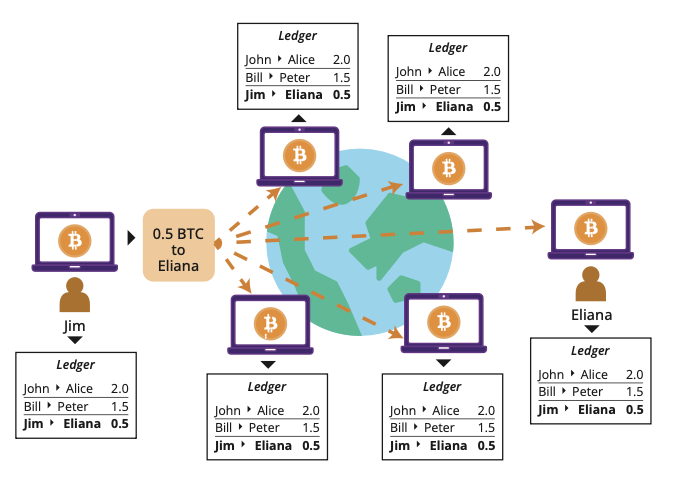
1. Těžaři bitcoinů: architekti bezpečnosti, kteří pomocí výkonných počítačů a elektřiny kontrolují/potvrzují transakce a zároveň zajišťují, aby vše bylo bezpečné. Díky této práci je účetní kniha neboli blockchain odolný vůči všem subjektům, které by se snažily síť napadnout.

Společně pracují uzly a těžaři bitcoinu jako tým, aby udržovali decentralizovaný, bezpečný a odolný systém - nový způsob nakládání s penězi, na který se mohou spolehnout lidé na celém světě. Prozkoumejme tyto role podrobněji, abychom pochopili, jak přispívají k tomuto inovativnímu systému.

**9.3.1** Co to je Bitcoinový uzel a jak si ho nastavit doma?

Image from BD 2023 page 93]

Bitcoinový uzel může znít jako příliš technická záležitost, ale je to jen kus softwaru, který provozuje kopii bitcoinové účetní knihy. Když spustíte svůj vlastní bitcoinový uzel, získáte možnost podílet se na tvorbě pravidel bitcoinové sítě.

Představte si to: pokud se skupina lidí pokusí změnit fungování Bitcoinu, například změnou celkového množství bitcoinů, máte možnost se k tomu vyjádřit. Můžete se rozhodnout, že svůj uzel na nový systém nezměníte, což je jako hlasovat o prosazení pravidel sítě, která podporujete.

Představme si Bitcoinový uzel jako digitálního dopravního policistu s několika nezbytnými úkoly:

1. Strážci platnosti: Bitcoinový uzel uchovává digitální kopii blockchainu, což je něco jako sdílená účetní kniha všech bitcoinových transakcí. Stejný záznam uchovává tisíce uzlů po celém světě.
2. Komunikační uzel: Uzly se vzájemně propojují a vytvářejí rozsáhlou komunikační síť. Sdílejí informace, zejména transakce čekající na přidání do blockchainu, uložené v digitální databázi zvané „mempool“.
3. Kontrolor kvality: Každý přidaný údaj do blockchainu prochází kontrolou. Uzly zajišťují platnost transakcí a odmítají všechny, kteří nesplňují pravidla Bitcoinové sítě.
4. Informátor blockchainu: ostatní aplikace, jako jsou například peněženky, mohou požádat uzel o informace v blockchainu, například o bitcoinových zůstatcích. Uzly slouží jako informační uzly.
5. Přijetí nových uzlů: Když se chce připojit nový uzel, stávající uzly mu velkoryse poskytnou kopii blockchainu. Nový uzel nezávisle kontroluje platnost každé transakce, což klade důraz na systém bez důvěry.

**Aktivita** – Zhlédněte video o Bitcoinových uzlech: <https://youtu.be/xc_TxlByxeY>

Jednou z možností, jak spustit vlastní uzel, je stáhnout si software Bitcoin Core a dát mu nějaký čas na stažení celého blockchainu. Jakmile je připraven, můžete jej nechat zapnutý a přibližně každých 10 minut přibudou nové bloky s transakcemi. Váš uzel zkontroluje jejich platnost a přidá je do vaší lokální kopie blockchainu.

|  |
| --- |
| [RESOURCE QR CODE LINK] Zdroj: Bitcoin Core Software - <https://bitcoincore.org/en/download/> |

Provozování uzlu poskytuje suverenitu a nezávislost. Nespoléháte se na ostatní, je to váš vlastní dopravní policista. Na rozdíl od vaší bitcoinové peněženky, která postrádá kopii blockchainu, uzel zajišťuje soběstačnost. Namísto toho, abyste důvěřovali ostatním ohledně svých bitcoinů (a stavu bitcoinové sítě), vaše peněženka komunikuje s vaším osobním uzlem, díky čemuž je vaše digitální působnost bezpečnější a důvěryhodnější.

**9.3.2** Co to je těžební stroj a jak těžba funguje?

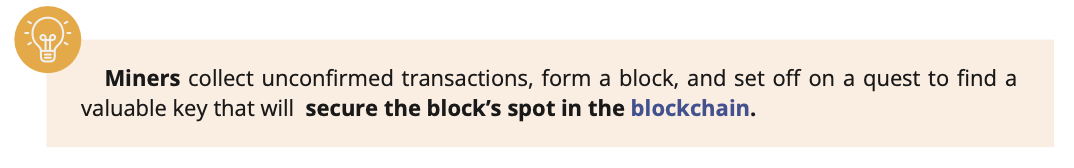
„Účelem těžby není vytváření nových bitcoinů. To je motivační systém.

Těžba je mechanismus, díky němuž je bezpečnost Bitcoinu decentralizovaná.“

Andreas M. Antonopoulos

Představte si těžaře jako digitální účetní. Stejně jako firmy platí účetním za vedení finančních záznamů, těžaři dostávají zaplaceno v bitcoinech za ověřování a přidávání transakcí do blockchainu, čímž zajišťují bezpečnost a hladký chod sítě. Tento úkol vyžaduje enormní výpočetní výkon, takže specializované vybavení a velké množství spotřebované energie.

[TEXT BOX]



Těžaři shromažďují nepotvrzené transakce, vytvářejí bloky a vynakládají elektrickou energii na hledání předem daného čísla, které doplní a zajistí tak místo bloku v blockchainu.

[END TEXT BOX]

Těžaři se předhánějí v přidávání dalších bloků do blockchainu. Vytouženou cenou je „platný hash bloku“, který je důmyslně ukrytý mezi miliardami dalších a odemknout ho může pouze specifický klíč přidělený sítí.

Představte si obrovskou kupku sena plnou milionů klíčů, z nichž každý představuje jedinečný hash bloku. Síť vybrala jeden konkrétní klíč, který odemkne cennou odměnu. Těžaři se prohrabávají kupkou sena, testují každý klíč v zámku, ale pouze jeden šťastlivec objeví dokonalou shodu.

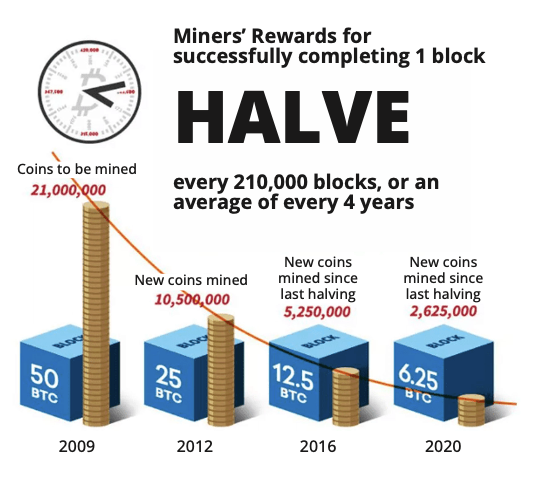
Jakmile těžař najde správný hash bloku, sdílí jej se sítí spolu s vytvořeným blokem nových transakcí. Ostatní těžaři toto řešení ověří, aby se ujistili, že je správné. Pokud vše souhlasí, je blok přidán do blockchainu, čímž se vytváří bezpečná a veřejná účetní kniha.

Těžaři získávají odměny za své úsilí dvěma způsoby:

1. Odměna v bloku
2. Transakční oplatky

Odměny za bloky jsou nové bitcoiny uvolněné do oběhu s každým blokem přidaným do blockchainu. Transakční poplatky jsou malé částky, které uživatelé bitcoinů platí za to, že jejich transakce jsou zpracovávány rychleji a těžař je upřednostňuje. Těžaři si mohou vybrat, které transakce zahrnou do těženého bloku, přičemž obvykle upřednostňují transakce s vyššími transakčními poplatky.

[Image from BD 2023 page 139]

Halving Bitcoinu

Je nezbytnou součástí bitcoinového světa, která pomáhá udržet jeho vzácnost a hodnotu v čase. Jak víte, existuje pevná nabídka celkem 21 000 000 bitcoinů. Tato zásoba není plně k dispozici ode dne spuštění Bitcoinu. Místo toho se tato zásoba v ekosystému uvolňuje postupně.

Satoshi Nakamoto chytře navrhl systém blokových odměn, který umožňuje distribuci nových bitcoinů bez centrální autority. V počáteční fázi dostávali těžaři za každý vytěžený blok sladkou odměnu 50 bitcoinů, což je motivovalo k investicím do výkonného vybavení a elektřiny pro těžební operace.

Aby byla síť stabilní a bylo možné řídit přírůstek nových bitcoinů, snižuje se odměna za blok každých 210 000 bloků na polovinu (cca každé 4 roky). Tato událost, česky nazývaná „půlení“, snižuje počet nových bitcoinů vstupujících do oběhu a nadále motivuje těžaře k ochraně sítě a udržování její decentralizace. Historicky vedly události halvingu k výraznému nárůstu cen na trhu, a to v důsledku snížené nabídky nových bitcoinů, které se dostávají do oběhu.

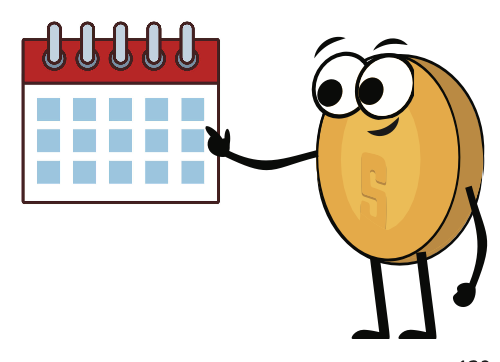
[TEXT BOX]



Nabídka kolující v oběhu označuje celkové množství dostupných jednotek. U Bitcoinu je celková nabídka v oběhu počet mincí, které byly vytěženy a jsou v daném okamžiku v oběhu, bez mincí, které jsou navždy ztraceny.

[END TEXT BOX]

[Image from BD 2023 page 139]

Během každé události půlení dostávají těžaři menší odměnu v bitcoinu, což snižuje míru emise nových mincí. V důsledku toho a s nárůstem celkového výpočetního výkonu, se obtížnost těžby zvyšuje, aby se udržel čas vytěžení bloku stále jednou za 10 minut v průměru. To nám zajišťuje, že nové bloky jsou do blockchainu přidávány stabilním tempem. Snížení odměn za těžbu nemusí nutně znamenat, že těžaři mají menší zisk, protože cena bitcoinu v čase může růst a těžaři také získávají transakční poplatky za ověřování transakcí a jejich přidávání do blockchainu. To může kompenzovat snížení odměn za těžbu v průběhu let.

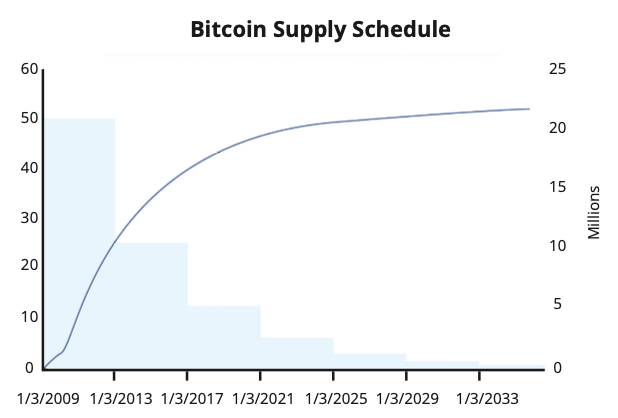
Události půlení jsou předem naprogramovány v protokolu Bitcoinu, takže je jejich distribuce předvídatelná a transparentní.

[Image from BD 2023 page 139-141]

[TEXT BOX]

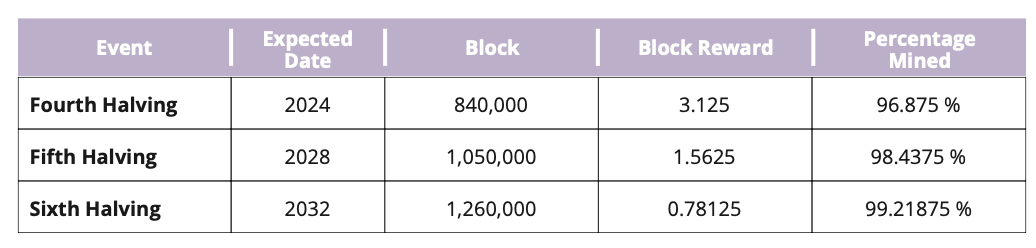
Distribuce bitcoinů je předem stanovený a veřejný plán uvolňování nových mincí do oběhu, jehož cílem je udržet vzácnost bitcoinu v čase.

[END TEXT BOX]

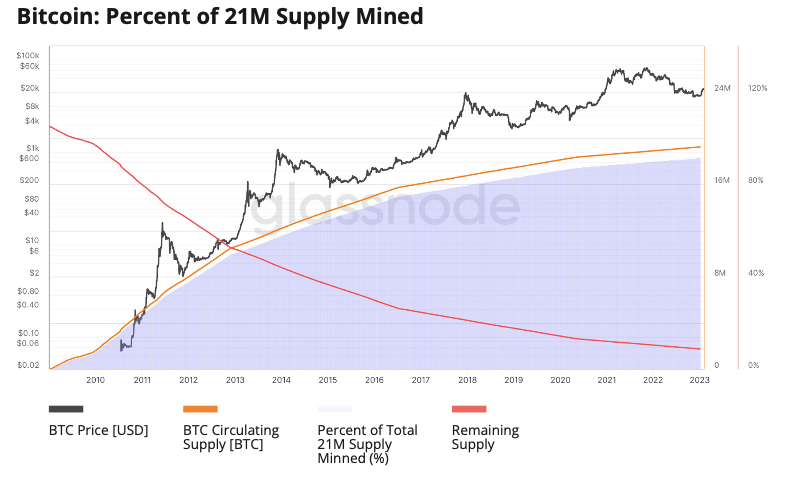


V následující tabulce jsou uvedeny podrobnosti o nadcházejících událostech půlení bitcoinů, včetně očekávaného data příští události půlení, čísla bloku, ve kterém k události půlení dojde, odměny za vytěžený blok během této události půlení a procenta celkové nabídky, které bude vytěženo.

Image from BD 2023 page 139-141]



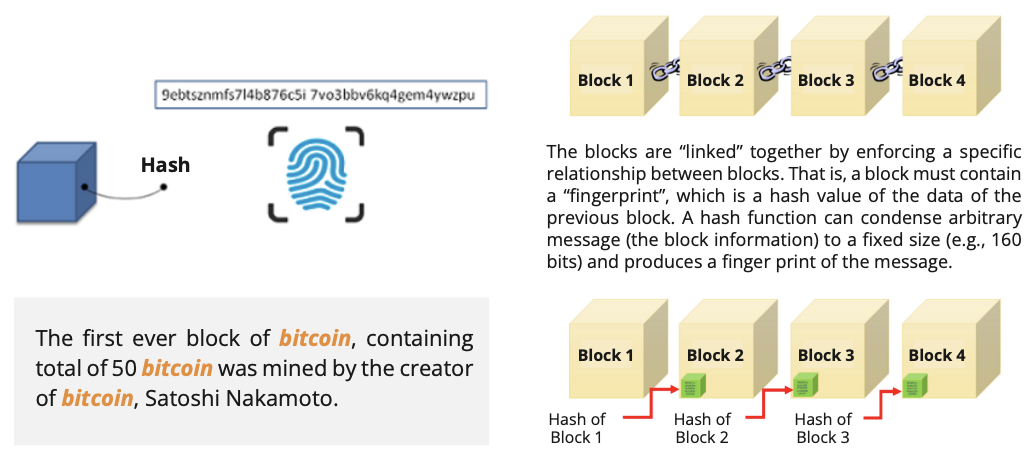
V průběhu let se bude zvyšovat nabídka bitcoinů v oběhu a také procento celkové nabídky, které bylo vytěženo. A to do té doby, dokud nebude dosaženo celkové nabídky 21 000 000 bitcoinů. Snížená nabídka v kombinaci s rostoucí poptávkou tak může zvýšit cenu bitcoinu (měřeno v dolarech). To přináší výhody prvním uživatelům a také motivuje těžaře, aby pokračovali v zabezpečování sítě a přispívali svým výpočetním výkonem a finančními prostředky.



Co to je platný hash v bitcoinovém bloku?

Platný hash je v něco jako speciální kód, který se těžaři snaží najít. Je to jedinečné číslo, které pomáhá sledovat každý blok v blockchainu, v němž jsou uloženy informace o transakcích. Bloky na sebe navazují v řetězci od prvního („genesis block“) po nejnovější, čímž vzniká veřejný záznam všech transakcí. Tento hash bloku je klíčový, protože spojuje každý blok s tím předchozím, což komukoli usnadňuje kontrolu historie transakcí. Je to něco jako otisk prstu každého bloku, který zajišťuje správnost a bezpečnost informací. Hash bloku slouží jako způsob, jak potvrdit, že data v bloku nebyla změněna.

[Image from BD 2023 page 139-141]

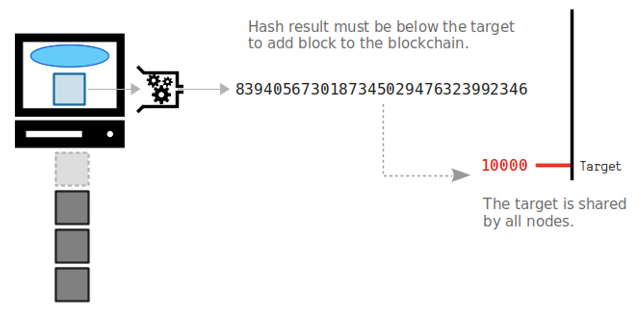


[TEXT BOX]

Satoshi Nakamoto, tvůrce bitcoinu, vytěžil úplně první blok, který obsahoval celkem 50 bitcoinů. [END TEXT BOX]

Závod o vytěžení bloku

Těžaři soutěží o to, kdo odhalí hash bloku, který se shoduje s cílem (speciálním číslem) stanoveným sítí. Těžař, který jako první úspěšně odhalí správný hash bloku, získá možnost přidat tento blok do blockchainu a přiřadit mu odpovídající hash ID. Toto řešení slouží jako ověření pravosti bloku.

[Image from BD 2023 page 142-144]

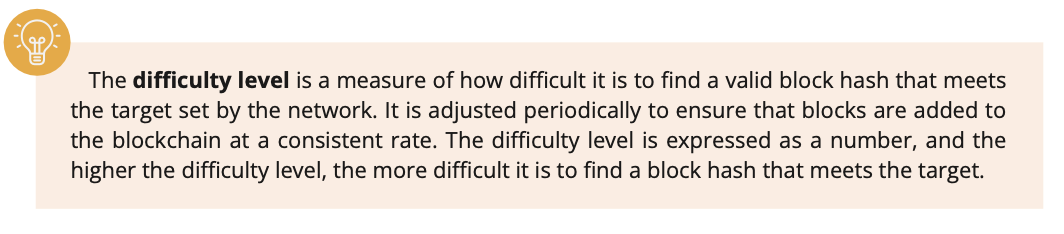
Těžbu lze přirovnat k závodu, jehož cílem je co nejrychleji dorazit do cíle. To, jak obtížné je najít hash bloku, se pravidelně upravuje a zajišťuje, aby byl každý blok vytěžen jednou za cca 10 minut (podle toho, jak těžaři připojují a odpojují své stroje). Tento mechanismus se nazývá „automatická úprava obtížnosti“.

Řekněme, že cílové číslo stanovené sítí Bitcoin je 1000. Těžaři by museli využít svůj výpočetní výkon a energii k hledání hashe bloku (konkrétního čísla), který je nižší než 1000. Těžař, který jako první najde hash bloku nižší než 1000, přidá nový blok do blockchainu a je odměněn bitcoiny.

[TEXT BOX]

Úroveň obtížnosti při těžbě bitcoinů je měřítkem toho, jak obtížné je najít platný hash bloku, který splňuje cíl stanovený sítí. Upravuje se každých 2016 bloků (zhruba každé dva týdny), aby se zajistilo, že bloky budou do blockchainu přidávány konzistentní rychlostí. Úroveň obtížnosti je vyjádřena číslem a čím vyšší je, tím obtížnější je najít platný hash bloku.

[END TEXT BOX]



Vezměme si například dva různé hashe:

* Hash 1: 0000A1mINgF0RbL0cK5wItHth3hAy5tAcK

Úroveň obtížnosti: 1

* Hash 2: 00000000A1mINgF0RbL0cK5wItHth3hAy5tAcK

Úroveň obtížnosti: 2

V tomto příkladu má hash 2 vyšší úroveň obtížnosti než hash 1, protože je delší a má na začátku více nul. Pro těžaře by bylo těžší najít Hash 2, protože jejich počítače by musely vynaložit více práce.

[TEXT BOX]

Nalezením platného hashe bloku těžař prokáže, že vykonal práci potřebnou k přidání nového bloku do blockchainu, a za své úsilí dostane odměnu v bitcoinech plus transakční poplatky. Důkaz o vykonané práci (Proof of Work - PoW) je metoda, kterou bitcoinová síť používá k ověřování transakcí a přidávání nových bloků do blockchainu.

[END TEXT BOX]

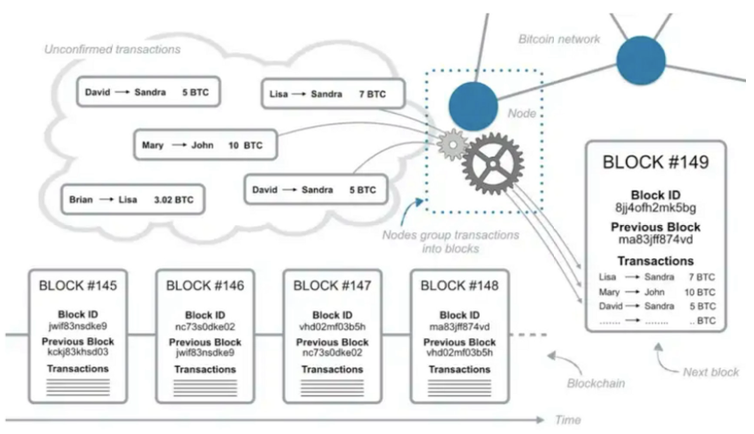


PoW udržuje Bitcoin v bezpečí tím, že znesnadňuje převzetí kontroly nad sítí někým, kdo má nekalé úmysly.

Stručně řečeno, úkoly těžařů spočívají v:

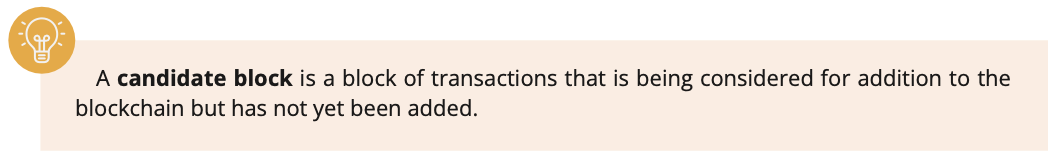
1. Spojování transakcí do bloků: Zatímco uzly ověřují nově vytvořené transakce, které čekají v „mempoolu“, těžaři z nich vyberou podmnožinu, kterou zahrnou do svého kandidátského bloku.
2. Proof of Work (důkaz o vykonané práce): Těžaři mezi sebou závodí v hledání platného hashe bloku.
3. Vysílání platných bloků: Po nalezení platného hashe bloku se nový blok zveřejní a aktualizuje v síti.
4. Získávaní odměny: Nakonec vítěz obdrží nově vytvořené bitcoiny a transakční poplatky za úspěšné přidání bloku do blockchainu.

[Image from BD 2023 page 142-144]



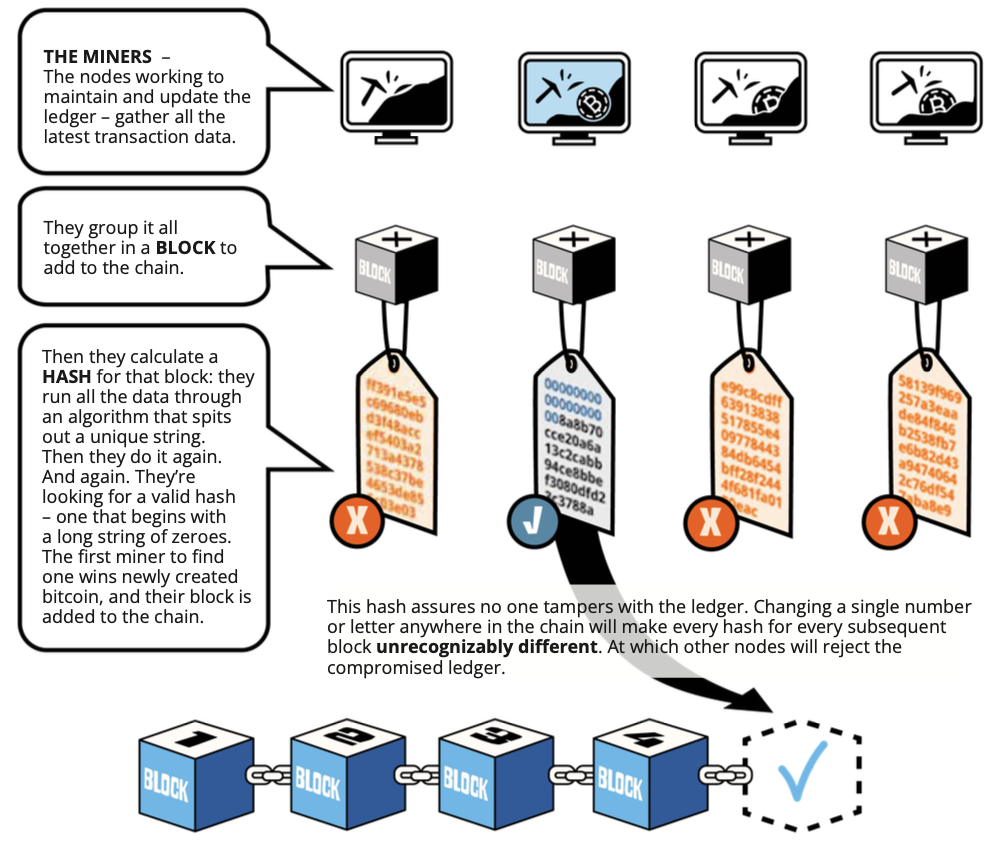
Na vytváření nových bloků může pracovat více těžařů současně. Těžař, který jako první objeví hash bloku splňující cíl stanovený sítí, jej oznámí síti a ostatní těžaři pak zkontrolují transakce v kandidátském bloku tohoto těžaře, aby se ujistili, že jsou platné. Pokud jsou transakce skutečně platné, je blok přidán do blockchainu. Ostatní bloky vytvořené ostatními těžaři v té době přidány nejsou a jsou vyřazeny. Tento proces pomáhá udržovat konsensus v síti a zabraňuje dvojímu utrácení stejných mincí.

[TEXT BOX]

Kandidátský blok je soubor transakcí, o jejichž přidání do blockchainu se uvažuje, ale dosud nebyly přidány.

[END TEXT BOX]

[Image from BD 2023 page 155]

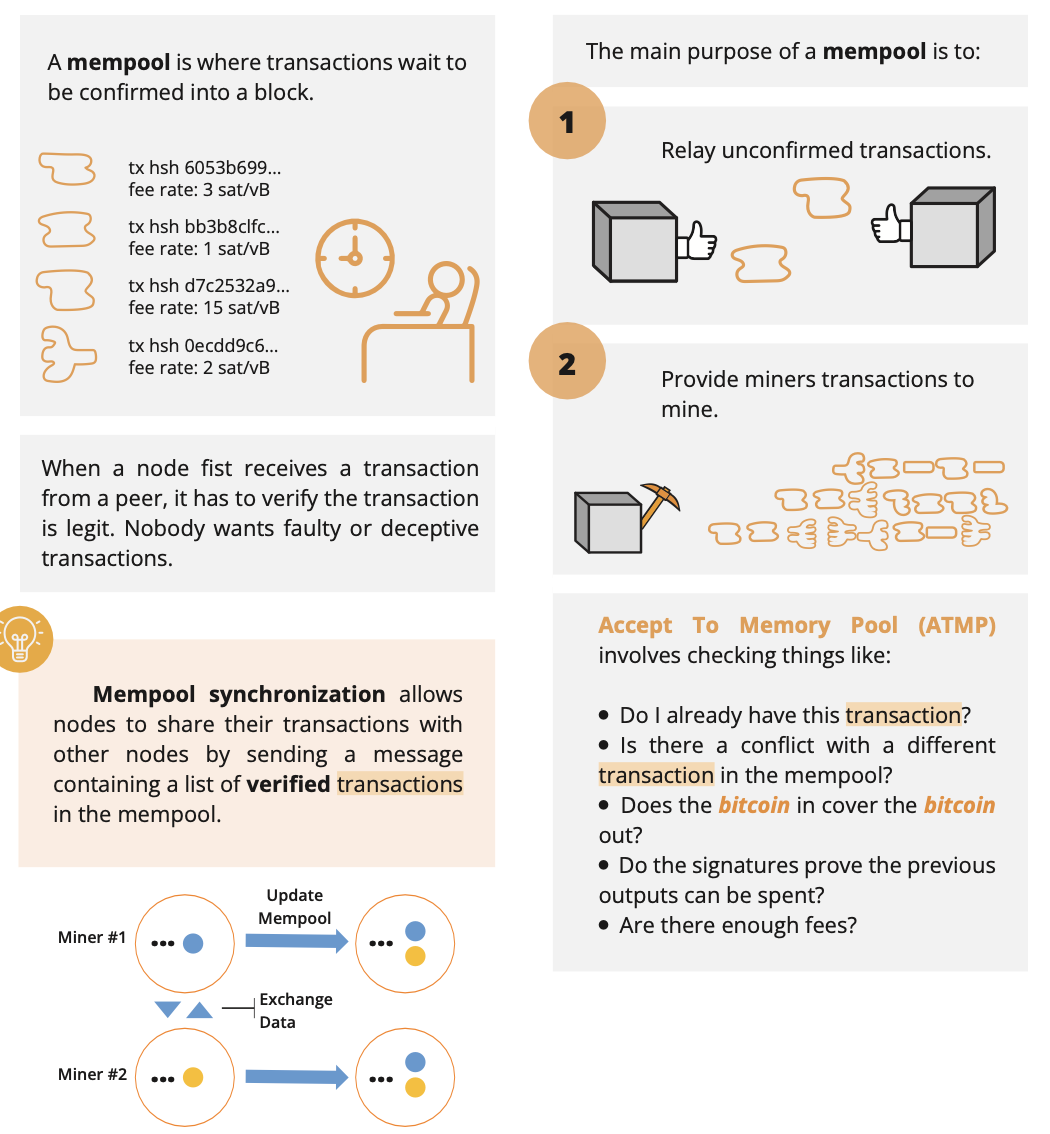


## 9.4 Co je to Mempool?

„Mempool“ neboli Memory Pool je něco jako ,,čekárna pro transakce v bitcoinové síti”. Když provedete transakci, je nejprve vysílána do Mempoolu, než je ověřena, vybrána a přidána do blockchainu.

Představte si, že čekáte ve frontě v restauraci. Vaše jméno je přidáno na seznam lidí čekajících na stůl. Když se stůl uvolní, hostitel zavolá vaše jméno a usadí vás. Podobně je bitcoinová transakce přidána do Mempoolu a následně je potvrzena a přidána do blockchainu v momentě, kdy ji těžař zahrne do bloku.

[Image from BD 2023 page 128-130]

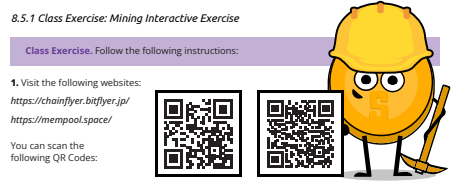


Jak se transakce ověřují a přidávají do Mempoolu?

Když jsou do bitcoinové sítě vysílány nové transakce, uzly je ověřují, aby se ujistily, že jsou platné a že prostředky nebyly již dříve utraceny. Jakmile jsou tyto transakce ověřeny, uzly je přidají do svého Mempoolu. Poté uzly sdílejí transakce s ostatními uzly, aby je mohly překontrolovat. Nakonec, pokud většina uzlů souhlasí, budou transakce zpřístupněny těžařům, aby je vybrali a zařadili do bloku. Existuje však několik důvodů, proč transakce nemusí být po 72 hodinách potvrzena:

1. Nízké transakční poplatky: Transakce s nízkým poplatkem nemusí být zpracovány dostatečně rychle, protože těžaři si do svých bloků vybírají transakce s vyššími poplatky.
2. Přetížení sítě: Pokud je síť přetížená, může dojít ke zpoždění při potvrzování transakcí, i když mají vysoký poplatek.
3. Pokus o dvojí útratu: Pokud se záškodník pokusí o dvojí útratu, bude jeho transakce sítí odmítnuta.
4. Nesprávné nebo neúplné údaje: Pokud transakce obsahuje nesprávné nebo neúplné údaje, může ji síť odmítnout.
5. Špatně vytvořená transakce: Pokud je transakce nesprávně formulovaná, může ji síť odmítnout.

Abyste se vyhnuli odmítnutí transakce, doporučujeme uvést dostatečně vysoký poplatek, který zajistí včasné zpracování transakce, a před odesláním transakce dvakrát zkontrolovat, zda jsou všechny údaje v transakci správné.

[Image from BD 2023 page 152]

**Aktivita - Mempool**

* Naskenujte následující [QR code](https://mempool.space/):

—-------------------------------- Notes only - Below not in 2024 workbook —---------------------------

*Note to designer: please keep the QR code that forwards to mempool.space and REMOVE the other one from the image → → →*

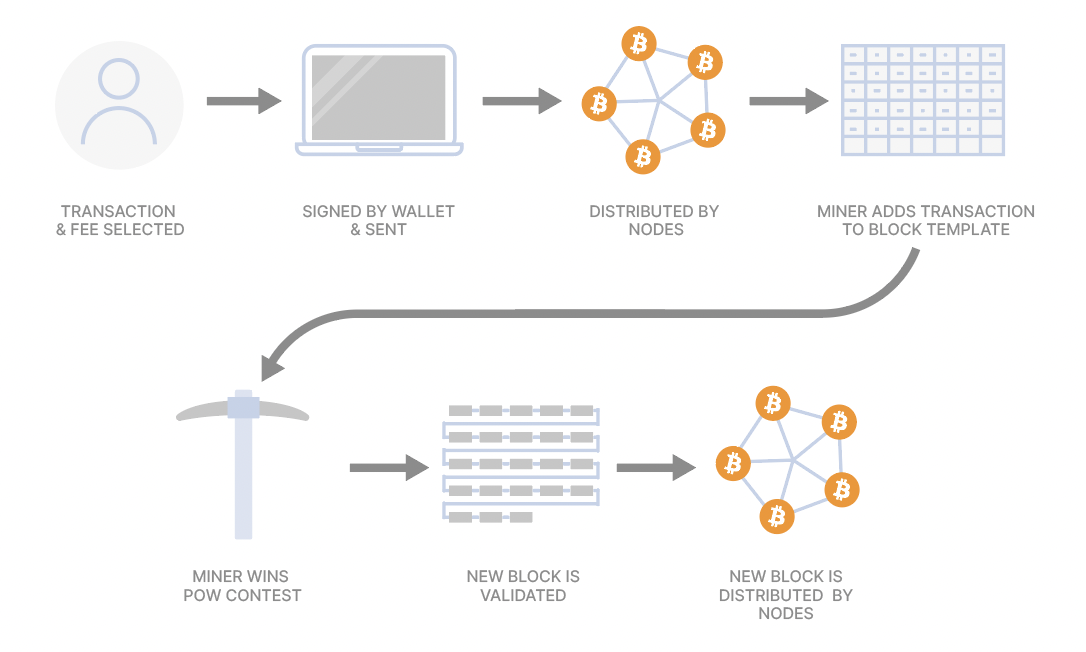
—---------------------------- Notes only - Above not in 2024 workbook —---------------------------------

* Prohlédněte si jednotlivé údaje zobrazené na stránce, včetně nejnovějších bloků, potvrzených transakcí, počtu transakcí, využití paměti a přibližné hodnoty celého bloku. Odpovězte na otázky:
  + Jaký byl poslední vytěžený blok?
  + Kolik transakcí bylo v tomto bloku zahrnuto?
  + Jaká je celková hodnota zobchodovaných bitcoinů?
  + Jaká byla velikost bloku v megabajtech?
  + Kolika nulami začíná ,,nonce" bloku?
  + Kolik bitcoinů těžař celkem vydělal?
  + Jaká byla celková hodnota poplatků, které těžař obdržel za přidání transakcí do sítě?
  + Vyberte jednu z transakcí s nejvyšší hodnotou v bloku. Na kolik bitcoinových adres se tato částka rozdělila?

## 9.5 Jak fungují Bitcoinové transakce od začátku až do konce

* + Adam chce poslat bitcoin Petrovi. Vybere si jedno ze svých UTXO, vytvoří transakci a přidá všechny potřebné údaje, včetně částky bitcoinů, kterou chce poslat, Petrovu adresu a nadprůměrnou výši transakčních poplatků.
  + Poté, co provede závěrečnou kontrolu, zda jsou všechny údaje správné, Adam podepíše transakci svým soukromým klíčem.
  + Adam vyšle transakci do bitcoinové sítě.

[Image from Chapter 9 Images Folder]



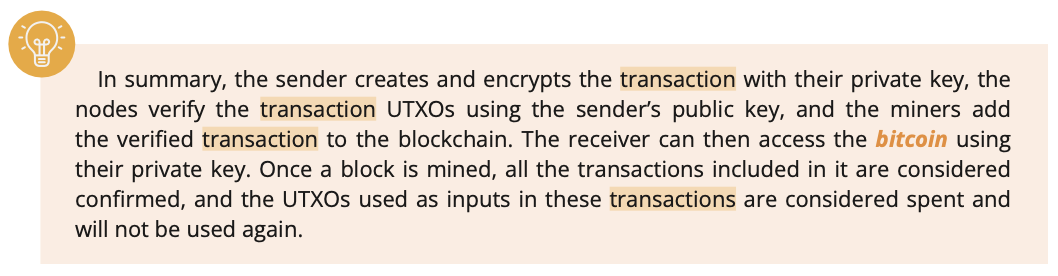
*Od: Stevenot, Ted, “Co je to Bitcoinový uzel a jak funguje?”. Unchained Capital, 17. Ledna 2023, https://unchained.com/blog/what-is-a-bitcoin-node/*

* + Uzly v síti přijmou transakci a ověří její platnost podle pravidel konsensu (například zkontrolují, zda je Adamův podpis platný a zda má dostatek prostředků na provedení transakce).
  + Transakce je označena za platnou a uzly ji rozšíří mezi ostatní uzly v síti a přidají ji do Mempoolu.
  + Protože si Adam vybral dostatečně vysoký poplatek za transakci, téměř všichni těžaři jeho transakci zařadí do svých bloků.
  + Důkaz o vykonané práci: Těžaři závodí a snaží se vytěžit svůj blok nalezením platného hashe bloku. Jeden z těžařů najde hash a pošle svůj blok do sítě.
  + Uzly obdrží nově vytěžený blok a ověří jeho platnost. To zahrnuje ověření všech transakcí v rámci bloku a zajištění splnění požadavku na PoW.
  + Většina uzlů se shodne na tom, že blok je platný, a přidá jej do blockchainu. Petr obdrží potvrzené bitcoiny na svou přijímací adresu.
  + Jak jsou v následující hodině do blockchainu přidávány další bloky, počet potvrzení této danné transakce roste. S rostoucím počtem potvrzení transakce získává Petr větší důvěru v její správnost a nezvratnost.

[TEXT BOX]

Stručně řečeno, odesílatel podepíše transakci svým soukromým klíčem, uzly ověří transakci UTXO a těžaři přidají ověřenou transakci do blockchainu. Příjemce pak má k bitcoinu přístup pomocí svého soukromého klíče. Jakmile je blok vytěžen, jsou všechny transakce v něm obsažené považovány za potvrzené a UTXO použité jako vstupy v těchto transakcích jsou považovány za spotřebované a nemohou být znovu použity.

[END TEXT BOX]



Na závěr této kapitoly jste získali cenné informace o základních principech fungování Bitcoinu. Probrali jsme základní aspekty, od základů peněz až po technickou stránku Bitcoinu. Nyní si všechny tyto koncepty v další kapitole propojíme. Čeká nás kapitola 10, kde se ponoříme do významné otázky: „Proč Bitcoin?“

—-------------------------------- Notes only - Below not in 2024 workbook —---------------------------

* + ***Notes to designer:***
    - **Source images tagged “**[Image from Chapter 9 Images Folder]” from: <https://drive.google.com/drive/folders/1Dbg9PL0OpkJ78PDMFZ5HyKYu31sFDllU?usp=sharing>

—---------------------------- Notes only - Above not in 2024 workbook —---------------------------------

#### 

#### 