# Jak funguje Blockchain

## Hashovací funkce

Hashovací funkce jsou jádrem blockchainu, všech kryptoměn, elektronických podpisů, databází a veškeré bezpečnosti v IT.

Představte si automat na kávu. Pokud do něj hodíte stejný počet mincí a zmáčknete stejná tlačíka, automat vám vždy vydá stejnou kávu. To to by byl příklad **deterministické funkce** - jednoduše na stejná vstupní data bude vrácen stejný výsledek.

Nedeterministickou funkcí by tedy mohl být například hrací automat. Ten na stejnou akci a stejně zmáčknutá tlačítka vždy vrátí jiný výsledek.

Toto je velmi důležité pochopit, protože hashovací funkce jsou funkce deterministické. Stejně jako automat, do kterého hodíte minci, aby vám dal kafe, hashovací funkce vezmou jakýkoliv vstup (slova, čísla, soubory, nebo třeba tento dokument) a udělají z něj dlouhý řetězec písmen a číslic.

Ukažme si příklad použití algoritmu (nebo chcete-li automatu) SHA-256 jinak také nazýván SHA-2. Pokud do našeho automatu hodíme slovo “cybersecurity” vypadne z něj následující:

“***64a1e1972b663b35a8c06b453ce018251efef00925fb414217f6087f179031b8***”

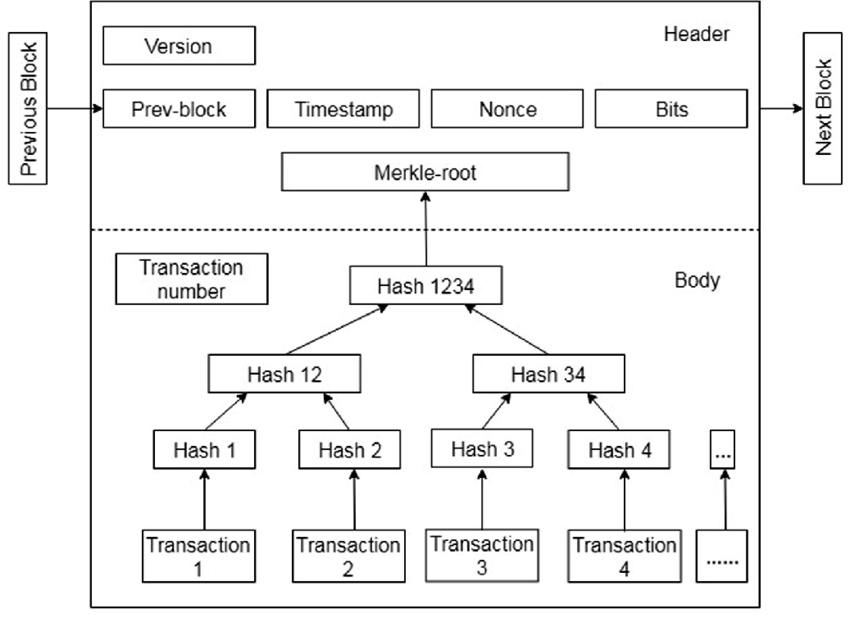
Pokud do automatu SHA256 hodíme znovu stejné slovo, výsledek bude naprosto identický výsledku předešlému, pokud ale pro naše účely změníme byť jedno písmeno, vyměníme poslední písmeno “y” za “i” a napíšeme “cybersecuriti”, bude nyní hash vypadat takto:

“***ea10873056b2ccf2657165136477bc9eca28e4f5b93a1bfea4eba8ede6efbbc6***”

V porovnání s hashem předešlým je výsledek radikálně odlišný. Na základě hashe se již není možné dopátrat vstupu. Nicméně pokud vstup máte, jste schopni vygenerovat hash.

### Blok

* Blok se skládá z hlavičky a těla bloku
* Hlavička
  + Obsahuje hash předchozího bloku, časové razítko, nonci, obtížnost a finální hash
    - **Finální hash = hash (aktuálního bloku) + hash (předchozího bloku)**
* **Tělo**
  + Záznamy všech transakcí v bloku, jejich hash a kombinace hashů do jednoho celkového (*Merklovy kořeny*)



#### Merkelovy stromy

Merklovy stromy jsou založené na hashích a umožnují ověřovat změny nebo udržovat konzistentní stav větších datových struktur.

Populární nástroj Git, kryptoměny bitcoin nebo Ethereum či souborový systém společnosti Apple – všude zde je využíváno Merklových stromů. V kryptoměnách mají Merklovy stromy za úkol udržovat transakce. Takzvaný Merklův kořen je pak součástí každého bloku.

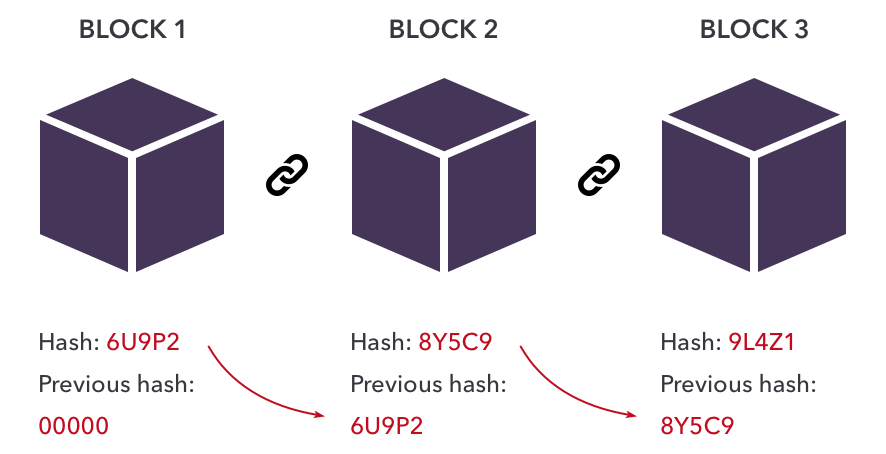
Merklovy stromy umožnují oddělit transakce od hlavičky bloku, zajišťují integritu a je to laciný způsob jak přepočítat, ověřit nebo vyhledat hash pro transakci. Následující obrázek je příkladem toho, jak vypadá takový Merklův strom.

Uvažujeme-li, že Hash A až Hash D je hash transakcí, pak jednotlivé hashe můžete spojit dohromady a zahashováním vznikne úplně nový hash. Tento proces bude pokračovat do té doby, dokud nezbyde poslední hash — Merklův kořen (anglicky “Merkl Root”).

Pokud v uvedeném obrázku do sítě přibude transakce C a D, vznikne nový Hash C a Hash D, výsledkem je pak Hash CD, který společně s Hashem AB vytvoří nový kořen. Všimněte si, že Hash AB se již znovu počítat nemusel.

Pokud by se ale jakýkoliv z hashů změnil, i kořen stromu by byl změněn a jelikož je kořen zahrnutý v hlavičce bloku, není možné s transakcemi jakkoliv manipulovat pokud byl blok vytěžen.

Na obrázku níže lze vidět návaznost jednotlivých bloků navzájem – Block 3 má svou hash (9L4Z1) odvozenou z finální hashe Blocku 2 (8Y5C9), která je odvozena z finální hashe Blocku 1 (6U9P2). Změnou jakýchkoliv dat v Blocku 3 by došlo k chybě, jelikož by neseděly hashe ve všech následujících blocích.

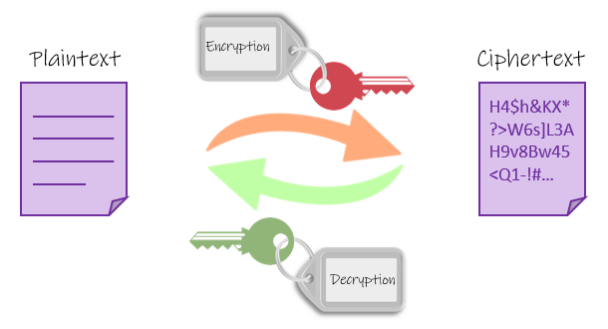


## Podpisy a ověřování transakcí

## Veřejný a soukromý klíč

HTTPS nebo kryptoměnová peněženka by bez tohoto vynálezu nemohly fungovat. Na rozdíl od symetrické kryptografie, kde využíváme zvoleného hesla, asymetrické kryptografie používá hesla dvě. Ani jedno z nich není námi určené, tedy místo slova “heslo” použijeme slovo “klíč”.

Vygenerované klíče budou dva – **veřejný a soukromý** (privátní). Veřejným klíčem můžete obsah zašifrovat, ale pouze soukromým klíčem můžete obsah dešifrovat.



Veřejný klíč si představte jako adresu vašeho domu. Když vám někdo bude chtít odeslat balíček, vy mu napíšete adresu (veřejný klíč) a on vám poštou (bitcoinová síť) zašle balíček (bitcoiny). Až z práce přijdete domů a balíček si budete chtít vzít ze schránky, budete potřebovat klíč od domu, případně od schránky (soukromý neboli privátní klíč).

**Veřejný klíč není nic tajného**, nemusíte se při jeho přeposílání ničeho bát. Má podobnou funkcionalitu jako již zmiňovaná doručovací adresa nebo číslo bankovního účtu, tedy jde sice o osobní údaje, útočník by však pouze s tímto údajem příliš nezmohl.

**Velice opatrní ale musíte být se svým privátním klíčem**, který představuje pomyslné klíče od vašeho domu!

## Konsensus

Proč je doopravdy těžba potřeba? Co znamená zkratka PoW a PoS a jaký je důvod pro manipulaci obtížnosti?

Většina kryptoměn má jakýsi algoritmus, který umožňuje kolektivní shodu. Mezi nejznámější patří takzvaný “Proof of Work” (PoW), “Proof of Stake” (PoS), “Proof of Elapsed Time” (PoET) a další.

Tyto algoritmy chrání síť a udržují konzistenci. Pokud Alice vlastní pouze 1 BTC a poslala by ho Bobovi a ve stejnou chvíli by zároveň stejný 1 BTC poslala i Jakubovi, a obě transakce by byly propagovány do bitcoinové sítě jiným uzlům, mohlo by dojít k rozdělení sítě.

**Jak se uzly shodnout na tom, co je doopravdy ta správná transakce?** Kdybyste byli centrální autoritou, jak byste rozhodli o takové situaci? Ve světě kryptoměn ale žádná centrální autorita není. Vždy musí existovat algoritmus, který rozhodne. V obou případech je transakce validní a bitcoinová síť musí uznat buď jednu, nebo druhou.

Obsah obrázku text, hodiny, podepsat

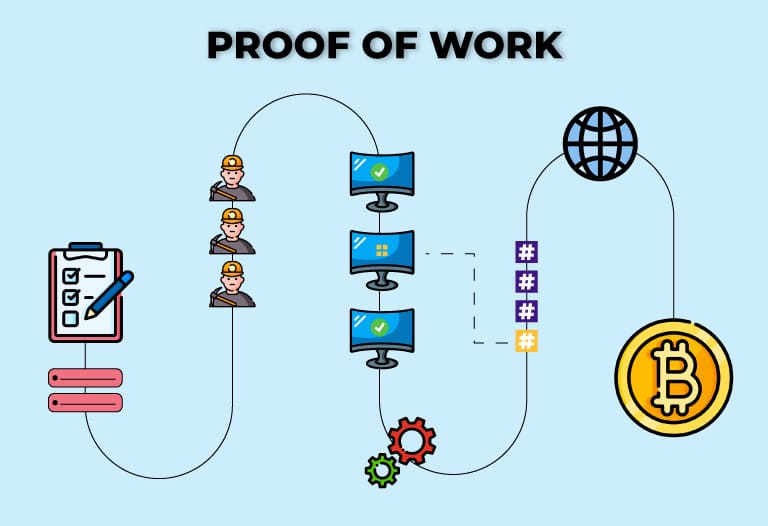
Popis byl vytvořen automaticky

### Proof of Work (PoW)

Tento mechanismus je využíván bitcoinem a původně pochází z projektu Adama Backa – HashCash. Původně měl sloužit jako prevence mailového spamu.

Pokud by bylo nutné pro každý odeslaný e-mail vyřešit moderovaně náročný matematický úkol (u kterého by stoupala náročnost s množstvím odeslaných e-mailů), uživatelé by byli více motivováni rozesílat pouze důležité e-maily. Větší množství e-mailů by tak vyžadovalo větší množství elektřiny a tudíž větší náklady na rozesílání.

Na podobném principu je založen i systém PoW, na kterém funguje bitcoinová síť. Je nezbytně nutné uhodnout moderovaně složitou kryptografickou hádanku pro to, aby jedna stránka v účetní knize (tedy jeden blok) mohla být vytvořena.



Pokud by tomu tak nebylo, počítač s největším výkonem by měl výhodu vytvoření nejdelšího řetězce bloků (měl by nejvíce stránek v účetní knize) a byl tak schopen manipulovat s historií účetní knihy. Moderovaná obtížnost tak zaručuje, že každý blok bude vytěžen přibližně jednou za 10 minut. Zároveň vyrovnává soutěž o každý blok mezi těžaři.

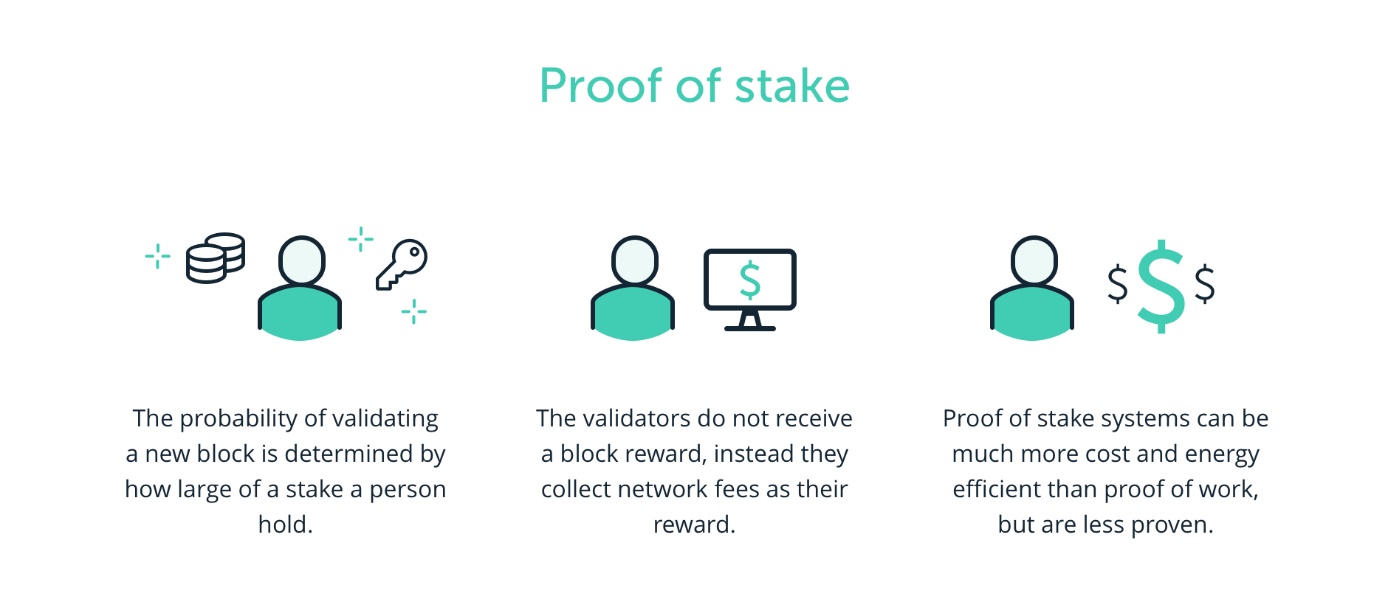
Bitcoin tedy jako první vyřešil takzvaný “double spend problem", který se často vyskytuje v distribuovaných systémech. Pokud nemáte více než 50 % těžařské síly, nemáte ani možnost manipulovat s účetní knihou a opakovat již provedené transakce.

### Proof of Stake (PoS)

Mladším bratrem PoW je PoS. Nápad je podobný, ale terminologie a implementace jsou odlišné. Provozovatelé uzlů mohou být takzvaní “validátoři”. Validátorem se může stát každý, kdo vlastní nějaké mince kryptoměny se systémem PoS. Validátorský uzel nemusíte provozovat sami, ale určitý počet mincí delegujete do takzvaného “stake poolu” (což je v podstatě společný uzel pro více účastníků). Účastníci stakovaní jsou financováni z poplatků za transakce, popřípadě odměňování protokolem z nově vytisknutých mincí. Pokud se tisknou nové coiny, taková kryptoměna je inflační. Do jisté míry se tak neliší oproti klasickým fiat měnám s tím rozdílem, že inflace u kryptoměn bývá přesně definovaná a známá dlouhodobě.

V systému PoS jsou všechny mince tak trochu “vytisknuté”. Na začátku je první blok, který rozdá mince, a pokud to stanovuje protokol, můžou vznikat i nové mince během ověřování transakcí.

Pro ověřování transakcí je náhodně vybrán validátor, který bude mít za úkol stejně jako v systému PoW zkontrolovat transakce a uzavřít blok. Ostatní validátoři pak můžou jednoduše zkontrolovat, zda vybraný validátor provedl úkol správně a hlasovat o tom, zda podváděl, nebo ne. Pokud by došlo k podvodu, uzel by byl potrestán odebráním stakovaných (uzamčených) mincí.



PoS trpí stejně jako PoW takzvaným 51% útokem, který funguje za předpokladu, že vlastníte více než 50 % všech mincí v oběhu. Na rozdíl od PoW tak trochu zvýhodňuje v rozhodování ty, kteří mají větší počet mincí. Pokud bychom však posuzovali toto tvrzení detailněji, zjistili bychom, že úplně takto striktní závislost zde není. Více se o této problematice dočtete v odborných publikacích. Pro účely tohoto ebooku řekněme, že “bohatší uzly” mohou teoreticky v síti rozhodovat větší mírou.