Modul 2

Stavební kameny blockchainu a mechanismus blockchainu

Co-funded by the European Union

Financováno Evropskou unií. Názory vyjádřené jsou názory autora a neodráží nutně oficiální stanovisko Evropské unie či Evropské výkonné agentury pro vzdělávání a kulturu (EACEA). Evropská unie ani EACEA za vyjádřené názory nenese odpovědnost.

Popis modulu

Modul „Stavební kameny blockchainu a mechanismus blockchainu“ zahrnuje principy tvorby blockchainu (co je blok a co je řetězec), základní rysy tradičního, decentralizovaného a distribuovaného pojetí databází a vlastnosti a požadavky kryptografických a hashovacích funkcí, které má jako výsledek. V modulu je také zahrnuto vysvětlení rozdílu mezi proof of work a proof of state a hlavní výhody blockchainu.

Výsledky studia

Absolventi modulu získají základní teoretické znalosti v oblasti tvorby blockchainu a požadavků na kryptografické a hashovací funkce. Znalosti jsou fixovány případovou studií ověřenou kvízem.

Výsledky jsou:

- Modul se studijním materiálem
- Případová studie
- Interaktivní aktivita
- Kvíz

obsahuje

BLOCK CHAIN FOR AGRI FOOD EDU

Co-funded by the European Union

Financováno Evropskou unií. Názory vyjádřené jsou názory autora a neodráží nutně oficiální stanovisko Evropské unie či Evropské výkonné agentury pro vzdělávání a kulturu (EACEA). Evropská unie ani EACEA za vyjádřené názory nenese odpovědnost.

obsahuje

BLOCK CHAIN FOR AGRI FOOD EDU

Co-funded by the European Union

Financováno Evropskou unií. Názory vyjádřené jsou názory autora a neodráží nutně oficiální stanovisko Evropské unie či Evropské výkonné agentury pro vzdělávání a kulturu (EACEA). Evropská unie ani EACEA za vyjádřené názory nenese odpovědnost.

contents

BLOCK CHAIN FOR AGRI FOOD EDU

Co-funded by the European Union

Financováno Evropskou unií. Názory vyjádřené jsou názory autora a neodráží nutně oficiální stanovisko Evropské unie či Evropské výkonné agentury pro vzdělávání a kulturu (EACEA). Evropská unie ani EACEA za vyjádřené názory nenese odpovědnost.

01

ÚVOD K MODULU 2

STAVEBNÍ KAMENY BLOCKCHAINU A MECHANISMUS BLOCKCHAINU

Úvod

Co je technologie blockchain?

Technologie blockchain je pokročilý databázový mechanismus, který umožňuje transparentní sdílení informací v rámci obchodní sítě. Blockchain databáze ukládá data v blocích, které jsou vzájemně propojeny v řetězci.

Data jsou chronologicky konzistentní, protože nemůžete odstranit nebo upravit řetězec bez konsensu ze sítě. Díky tomu můžete pomocí technologie blockchain vytvořit neměnnou nebo neměnnou účetní knihu pro sledování objednávek, plateb, účtů a dalších transakcí.

Systém má vestavěné mechanismy, které zabraňují neoprávněným transakcím a vytvářejí konzistenci ve sdíleném pohledu na tyto transakce.

Úvod

Stavební kameny blockchainu a mechanismus blockchainu

Stavební bloky blockchainu a mechanismus blockchainu jsou klíčové pojmy v oblasti digitálního ekosystému a kryptoměn.

Blockchain je technologie, která umožňuje zaznamenat transakce a události v decentralizovaném a imutabilním systému.

Základními stavebními kameny blockchainu jsou následující prvky:

- Bloky
- Distribuovaná účetní kniha/Distribuované záznamy
- Kryptografie
- Mechanismus konsensu
- Imutabilita

Úvod

Stavební kameny blockchainu a mechanismus blockchainu

BLOKY

Blockchain je tvořen řetězcem bloků, kde každý blok obsahuje seznam transakcí a jedinečný identifikátor (hash) předchozího bloku. Tím je zajištěna integrita dat.

DISTRIBUOVANÉ ZÁZNAMY

Blockchain je uložen na tisících počítačů (uzlů) po celém světě. Každý uzel má kopii celého blockchainu, což zvyšuje jeho odolnost proti výpadkům a útokům.

Úvod

Stavební kameny blockchainu a mechanismus blockchainu

KRYPTOGRAFIE

Asymetrická kryptografie se používá k zabezpečení transakcí. Každý účastník má soukromý a veřejný klíč, které umožňují ověřování a podepisování transakcí.

MECHANISMUS SHODY

Blockchain vyžaduje, aby uzly dosáhly konsensu o platných transakcích. Toho je obvykle dosaženo pomocí různých konsensuálních algoritmů, jako je Proof of Work (PoW) nebo Proof of Stake (PoS).

IMUTABILITA

Jakmile jsou data uložena v blockchainu, nelze je snadno změnit. To zajišťuje důvěru a transparentnost.

Úvod

Stavební kameny blockchainu a mechanismus blockchainu

- Mechanismus blockchainu zajišťuje integritu dat a zajišťuje, že transakce jsou nezpochybnitelné.
- Blockchain má široké uplatnění mimo kryptoměny, včetně financí, dodavatelského řetězce, zdravotnictví a mnoha dalších odvětví.
- Jeho budoucnost závisí na schopnosti komunit a podniků inovovat a využívat jeho potenciál k řešení skutečných problémů a posunu digitálního světa.

02

ZÁKLADNÍ KOMPONENTY: BLOKY, KRYPTOGRAFICKÝ HASH, DECENTRALIZACE

Základní komponenty: bloky, kryptografický hash, decentralizace

Jak funguje blockchain?

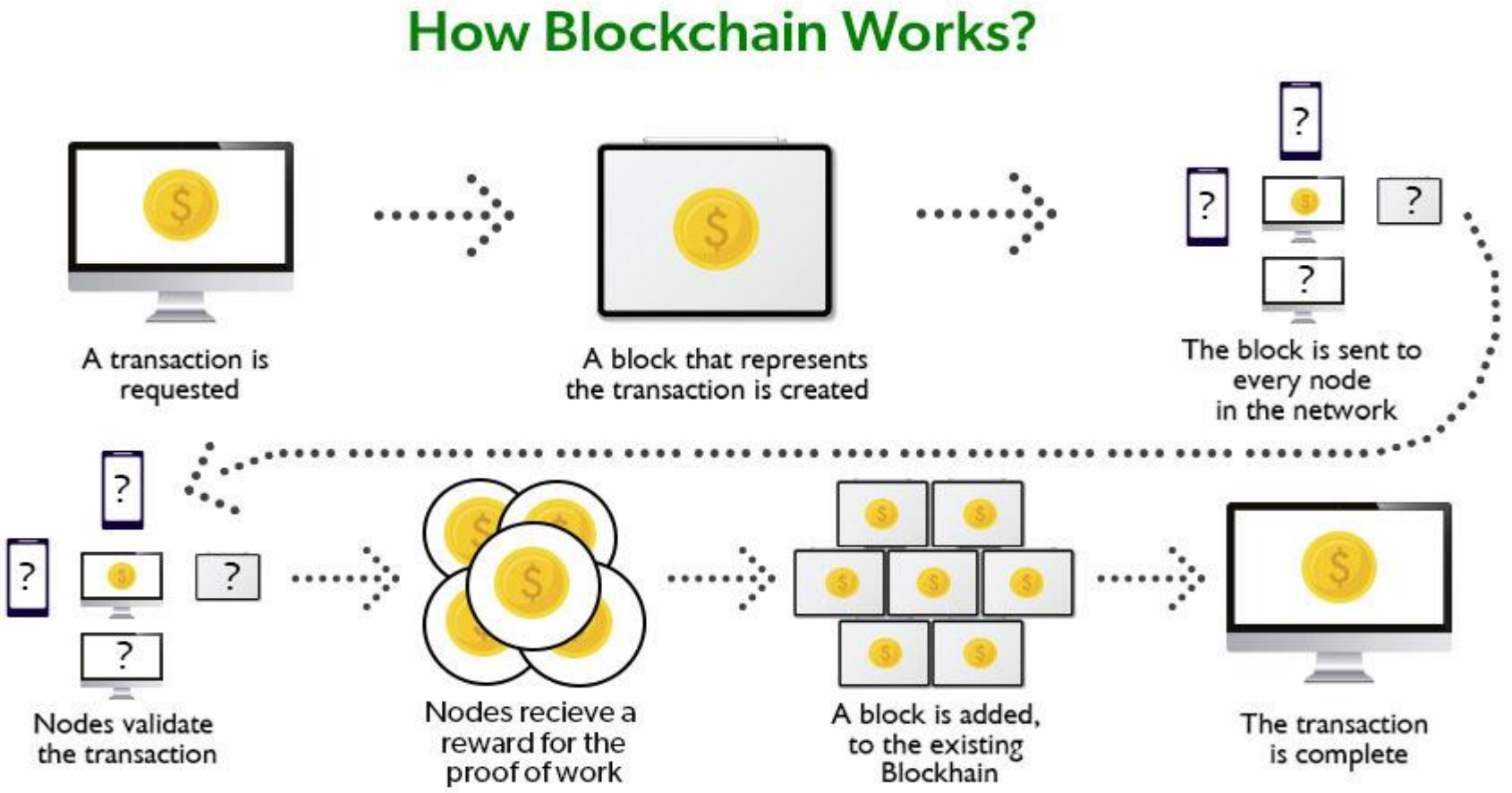
- Každá transakce nebo datový záznam, známý jako „blok“, je bezpečně propojen s předchozím pomocí kryptografického hashování, čímž vzniká nepřetržitý řetězec informací odolný vůči manipulaci .
- Jelikož neexistuje způsob, jak změnit blok, jediná potřebná důvěra je v do době, kdy uživatel nebo program zadává data. Tento aspekt snižuje potřebu důvěryhodných třetích stran, což jsou obvykle auditoři nebo jiní lidé, kteří však zvyšují náklady a dělají chyby.

Základní komponenty: bloky, kryptografický hash, decentralizace

Blockchain se skládá z programů nazývaných skripty, které provádějí úkoly, které byste obvykle dělali v databázi: Zadávání informací, přístup k nim a jejich ukládání a ukládání. Je distribuován blockchain, což znamená, že na mnoha počítačích je uloženo více kopií a všechny se musí shodovat, aby byl platný.

Blockchain shromažďuje informace o **transakcích** a vkládá je do bloku, jako je buňka v tabulce obsahující informace. Jakmile se zaplní, informace projdou **šifrovacím algoritmem**, který vytvoří hexadecimální číslo zvané **hash**.

Základní komponenty: bloky, kryptografický hash, decentralizace



Obrázek 1 Jak funguje blockchain (Zdroj: https://www.geeksforgeeks.org/how-does-the-blockchain-work/)

Základní komponenty: bloky, kryptografický hash, decentralizace

Transakční proces v blockchainu lze shrnout následovně:

1. Usnadnění transakce
2. Ověření transakce
3. Vytvoření nového bloku
4. Algoritmus konsensu
5. Přidání nového bloku do blockchainu
6. Dokončení transakce

Základní komponenty: bloky, kryptografický hash, decentralizace

Hash je pak vložen do následující hlavičky bloku a zašifrován s ostatními informacemi v bloku. To vytváří řadu bloků, které jsou spojeny dohromady.

Transakce probíhají podle specifického procesu v závislosti na blockchainu, na kterém probíhají. Například na blockchainu bitcoinu, pokud zahájíte transakci pomocí vaší kryptoměnové peněženky – aplikace, která poskytuje rozhraní pro blockchain – spustí se sled událostí.

Základní komponenty: bloky, kryptografický hash, decentralizace

1. **Usnadnění transakce:** Do blockchainové sítě vstupuje nová transakce. Všechny informace, které je třeba přenést, jsou dvojitě šifrovány pomocí veřejných a soukromých klíčů.
2. **Ověření transakce:** Transakce je poté přenesena do sítě peer-to-peer počítačů distribuovaných po celém světě. Všechny uzly v síti zkontrolují platnost transakce, například zda je k dispozici dostatečný zůstatek pro provedení transakce.
3. **Vytvoření nového bloku:** V typické blockchainové síti existuje mnoho uzlů a mnoho transakcí se ověřuje najednou. Jakmile je transakce ověřena a prohlášena za legitimní, bude přidána do mempoolu. Všechny ověřené transakce na konkrétním uzlu tvoří mempool a takové více mempoolů tvoří blok.

Základní komponenty: bloky, kryptografický hash, decentralizace

6. **Algoritmus konsensu:** Uzly, které tvoří blok, se pokusí přidat blok do blockchainové sítě, aby byl trvalý. Ale pokud je každému uzlu povoleno přidávat bloky tímto způsobem, naruší to fungování blockchainové sítě.
7. **Přidání nového bloku do blockchainu:** Poté, co nově vytvořený blok získá svou hash hodnotu a je ověřen, je nyní připraven k přidání do blockchainu. V každém bloku je hash hodnota předchozího bloku, a tak jsou bloky navzájem kryptograficky propojeny, aby vytvořily blockchain. Na otevřený konec blockchainu se přidá nový blok.
8. **Dokončení transakce:** Jakmile je blok přidán do blockchainu, transakce je dokončena a podrobnosti o této transakci jsou trvale uloženy v blockchainu. Kdokoli může získat podrobnosti transakce a potvrdit transakci.

Srovnání s tradičními databázemi

Tradiční databáze jsou centralizované, proměnlivé a optimalizované pro vysokorychlostní zpracování dat, zatímco blockchainy jsou decentralizované, neměnné a zaměřené na poskytování důvěry a transparentnosti prostřednictvím mechanismů konsenzu. Volba mezi těmito dvěma závisí na konkrétních potřebách dané aplikace.

- *Centralizace vs. decentralizace*
- *Datová struktura*
- *Řízení přístupu*
- *Mechanismus konsensu*
- *Neměnná vs. proměnlivá data*
- *Rychlost transakce a škálovatelnost*
- *Případová studie*

Srovnání s tradičními databázemi

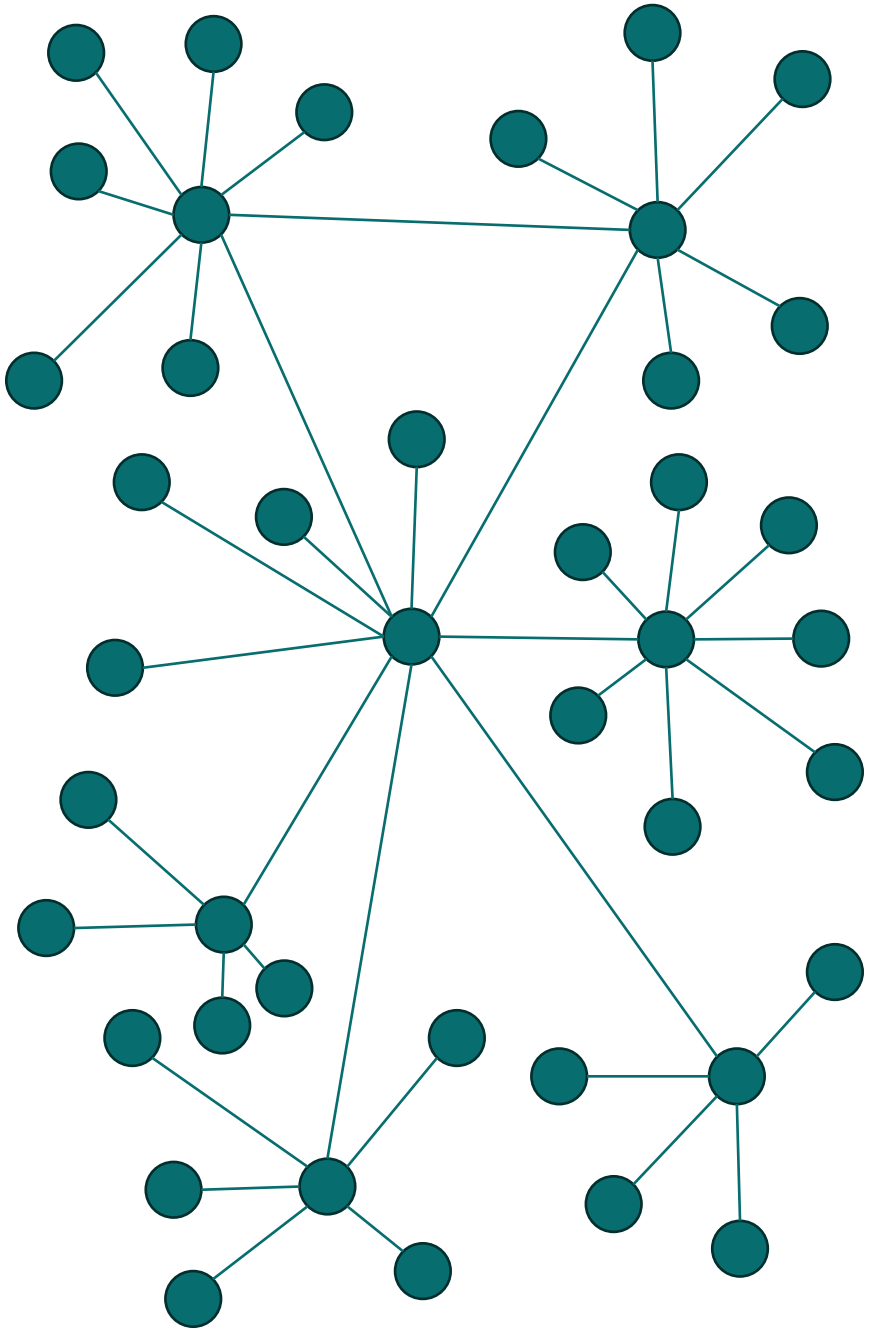
Centralizace vs. Decentralizace

Tradiční databáze: Tradiční databáze jsou centralizované systémy, kde má nad databází kontrolu jeden subjekt (např. společnost nebo organizace). Spoléhají na centrální server nebo shluk serverů pro správu a ukládání dat.

Blockchain: Blockchainy jsou decentralizované sítě, kde jsou data distribuována přes více uzlů (počítačů) v síti. Neexistuje žádný ústřední orgán ani jediný kontrolní bod, což je činí odolnými vůči cenzuře a manipulaci.

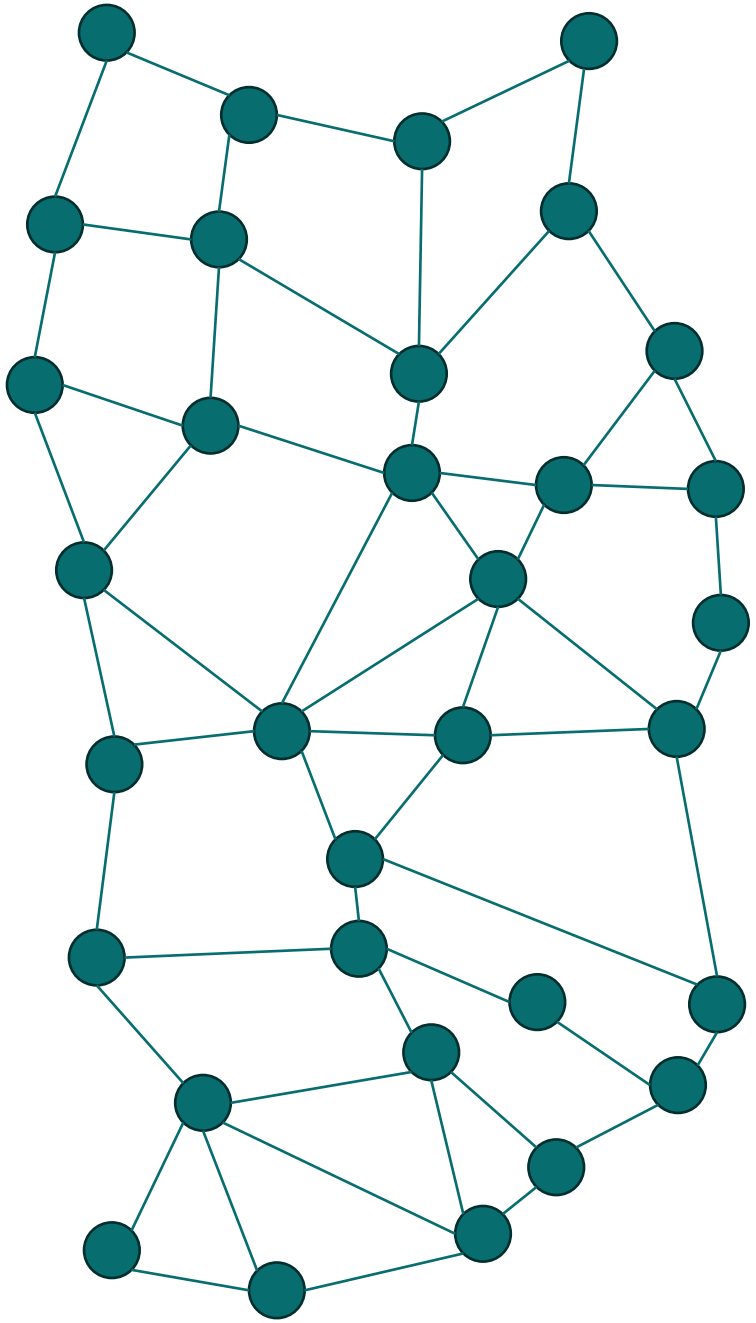
Centralizované

Všechny uzly jsou propojeny pod jedinou autoritou.



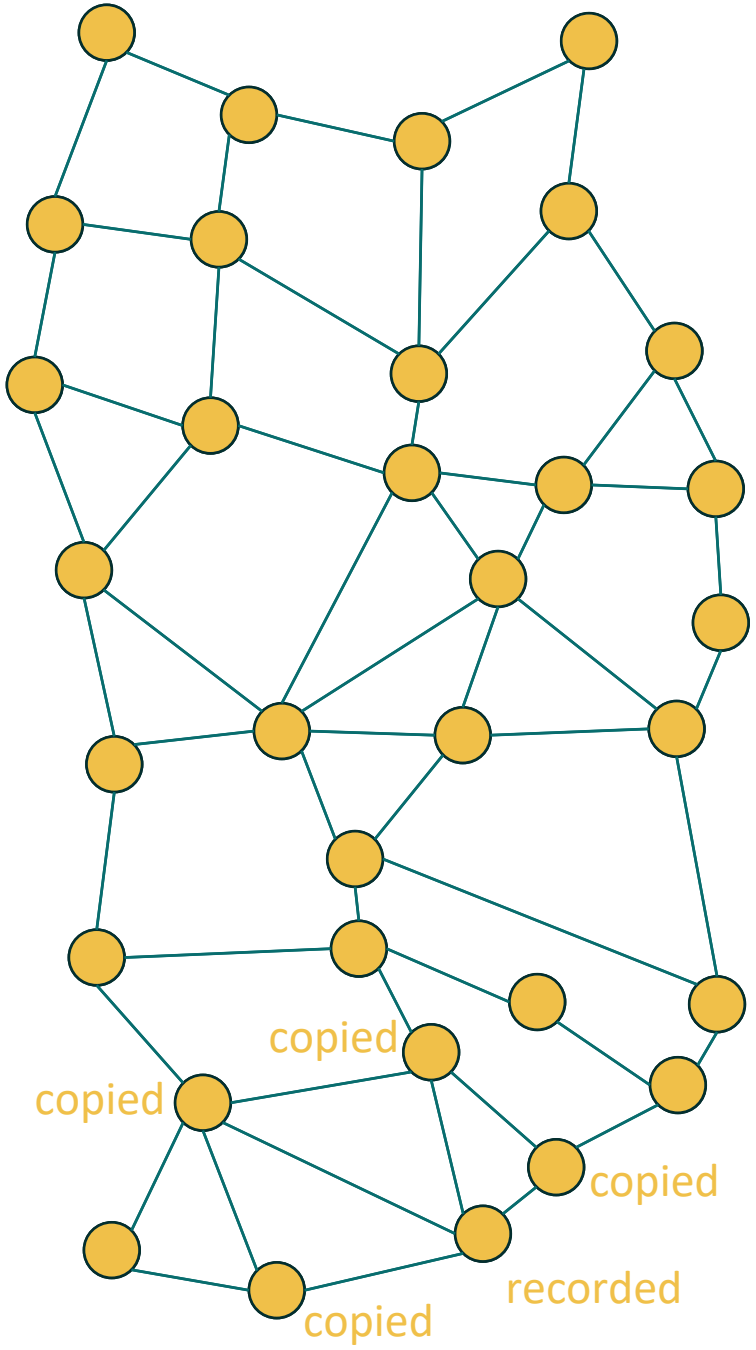
Decentralizované

Uzly neřídí žádný server autority, všechny mají individuální entity.



Distribuovaný

Každý uzel je nezávislý a vzájemně propojený.



Transakce v distribuované síti

Transakce je zaznamenána v uzlu a zkopírována do sebe.

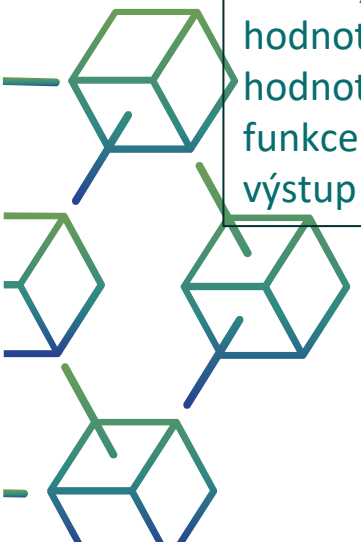
Hashovací funkce

Hašovací funkce je matematická funkce, která převádí vstupní hodnotu na jinou komprimovanou hodnotu. Vstup do hashovací funkce má libovolnou délku, ale výstup má vždy pevnou délku.

Hashovací funkce jsou mimořádně užitečné a objevují se téměř ve všech aplikacích pro zabezpečení informací.

Unikátní výstup hashovací funkce

DATA	HASHOVACÍ FUNKCE	HASH
Stavební kameny blockchainu.	Hashovací funkce SHA1	d355724c886c15a6272e5a8e6f416438535ca0be
stavební kameny blockchainu.	Hashovací funkce SHA1	54b05cb173b979447e87e3d4af19a41a774f631c
Hašovací funkce je matematická funkce, která převádí vstupní hodnotu na jinou komprimovanou hodnotu. Vstup do hashovací funkce má libovolnou délku, ale výstup má vždy pevnou délku.	Hashovací funkce SHA1	63dd04188931586e47c899271ccdcd681b0cc357

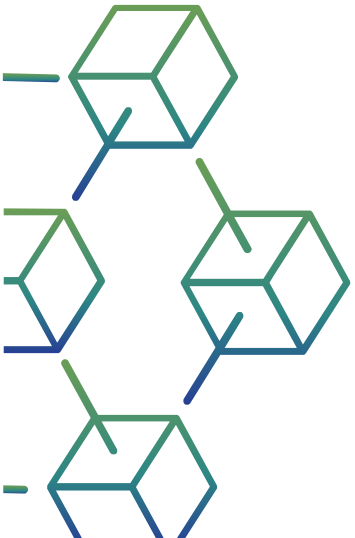


SHA1 v této době nestačí

Stavební kameny blockchainu.

hashovací funkce
SHA3-512

33322d615333e9faa2109c35997cf144876cc75ba76059454b28c81d2fa1c286a68679a00afb
baa71e9170ffc3bdaf6fbef5035a31b4f40a354502dd985368d4

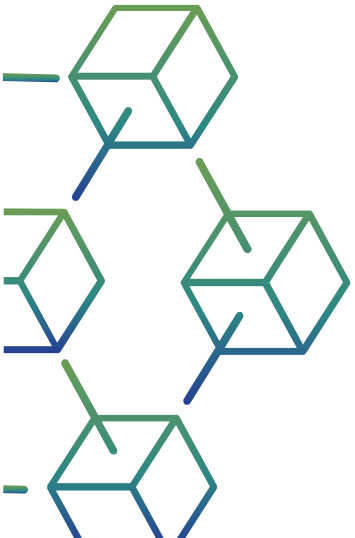


Odolnost před zobrazením

Tato vlastnost znamená, že by mělo být výpočetně obtížné zvrátit hashovací funkci.

Jinými slovy, pokud hašovací funkce h vytvořila hashovací hodnotu z, pak by mělo být obtížné najít jakoukoli vstupní hodnotu x, která se hashuje na z.

Tato vlastnost chrání před útočníkem, který má pouze hodnotu hash a snaží se najít vstup.



Odolnost proti kolizi

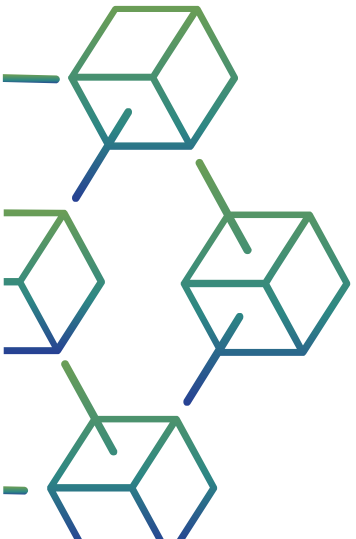
Tato vlastnost znamená, že by mělo být obtížné najít dva různé vstupy jakékoli délky, které vedou ke stejnému hash. Tato vlastnost se také označuje jako hašovací funkce bez kolize.

Jinými slovy, pro hashovací funkci h je těžké najít nějaké dva různé vstupy x a y takové, že h(x) = h(y).

Protože hashovací funkce je kompresní funkce s pevnou délkou hash, je nemožné, aby hashovací funkce neměla kolize. Tato vlastnost bez kolizí jen potvrzuje, že tyto kolize by měly být těžko k nalezení.

Tato vlastnost útočníkovi velmi ztěžuje nalezení dvou vstupních hodnot se stejným hashem.

Také, pokud je hašovací funkce odolná proti kolizi, je odolná vůči druhému předobrazu.



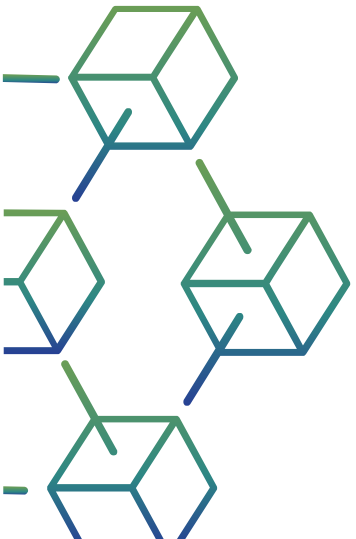
Source: https://www.tutorialspoint.com/cryptography/cryptography_hash_functions.htm

Druhá předobrazová odolnost

Tato vlastnost znamená, že daný vstup a jeho hash by mělo být těžké najít jiný vstup se stejným hashem.

Jinými slovy, pokud hašovací funkce h pro vstup x produkuje hašovací hodnotu h(x), pak by mělo být obtížné najít jakoukoli jinou vstupní hodnotu y, aby h(y) = h(x).

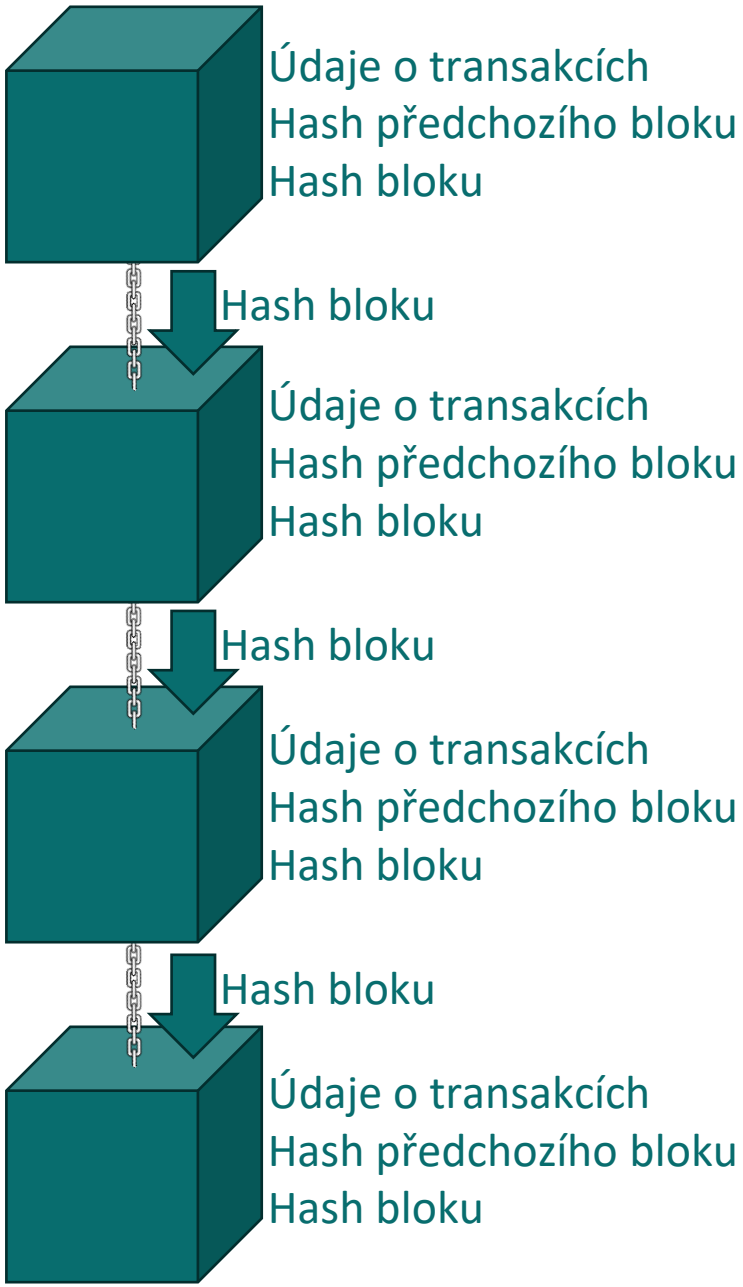
Tato vlastnost hashovací funkce chrání před útočníkem, který má vstupní hodnotu a její hash a chce nahradit jinou hodnotu jako legitimní hodnotu místo původní vstupní hodnoty.



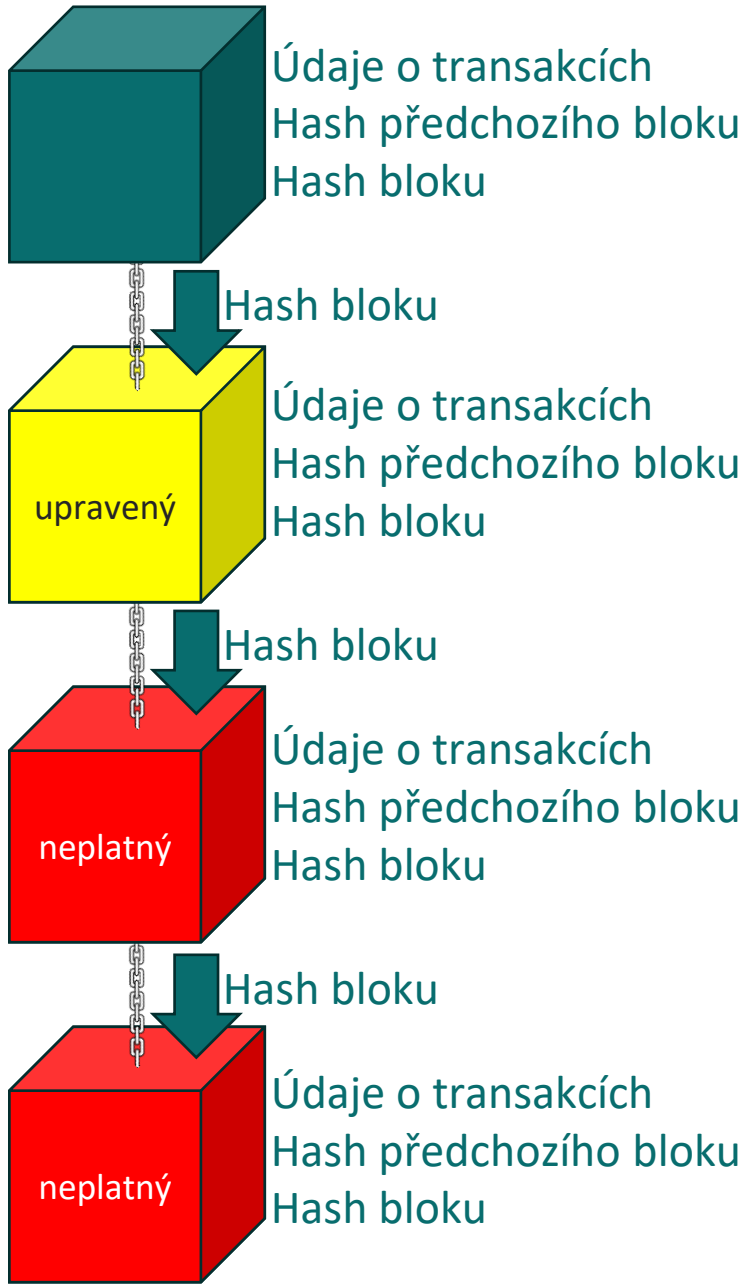
Blockchain

Blok = data + hash předchozího bloku + hash

Řetěz = řetěz mezi bloky

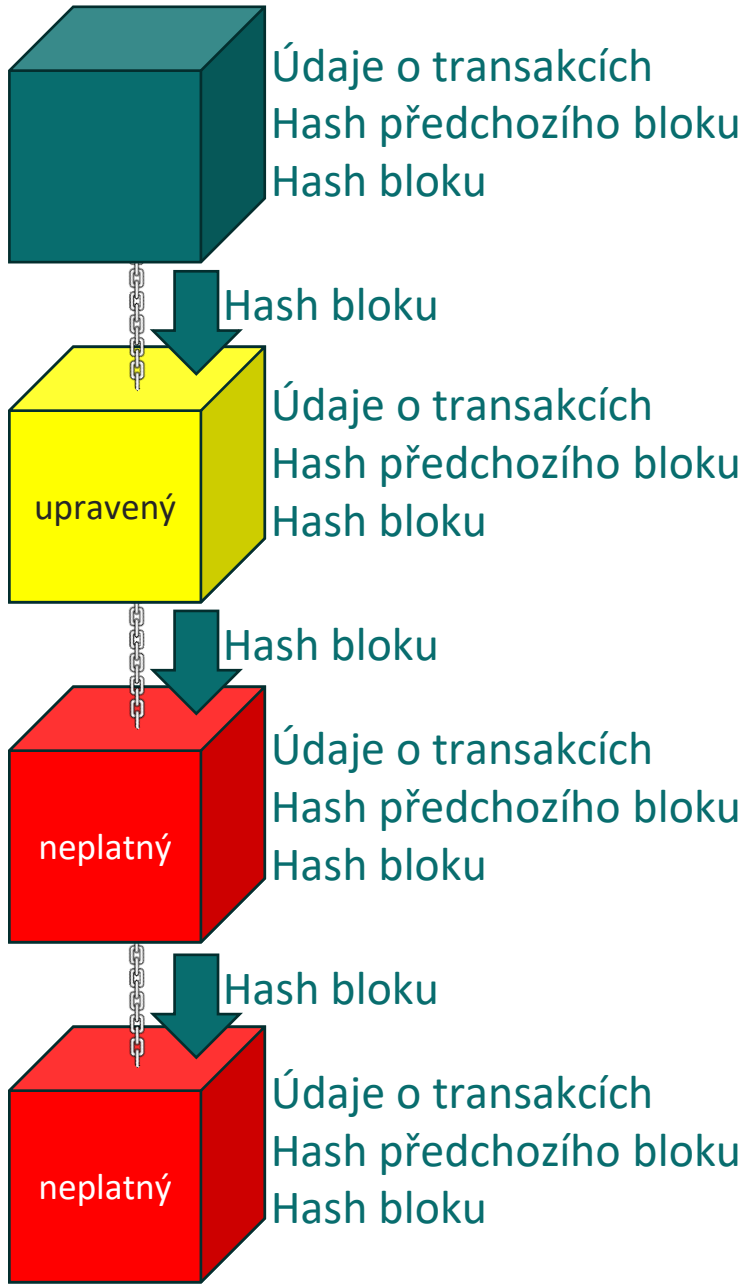


Všechny transakce jsou zaznamenány v „blocích“



Pokud je upraven jeden blok (jedna transakce v jednom bloku).

Hodnota hashovací funkce je různá



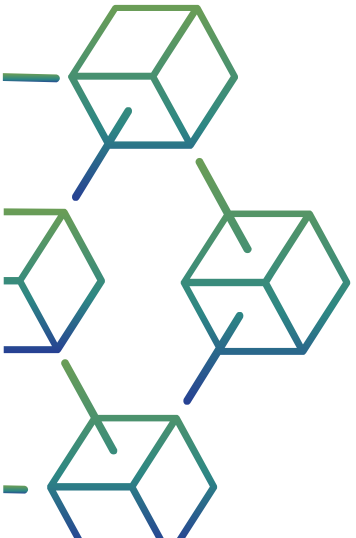
Pokud chce hacker upravit jeden blok (data v jednom bloku), musí upravit všechny další bloky a všechny kopie bloků v distribuované síti

Téměř nemožné(potřebuje obrovský výpočetní výkon, elektřinu atd.)

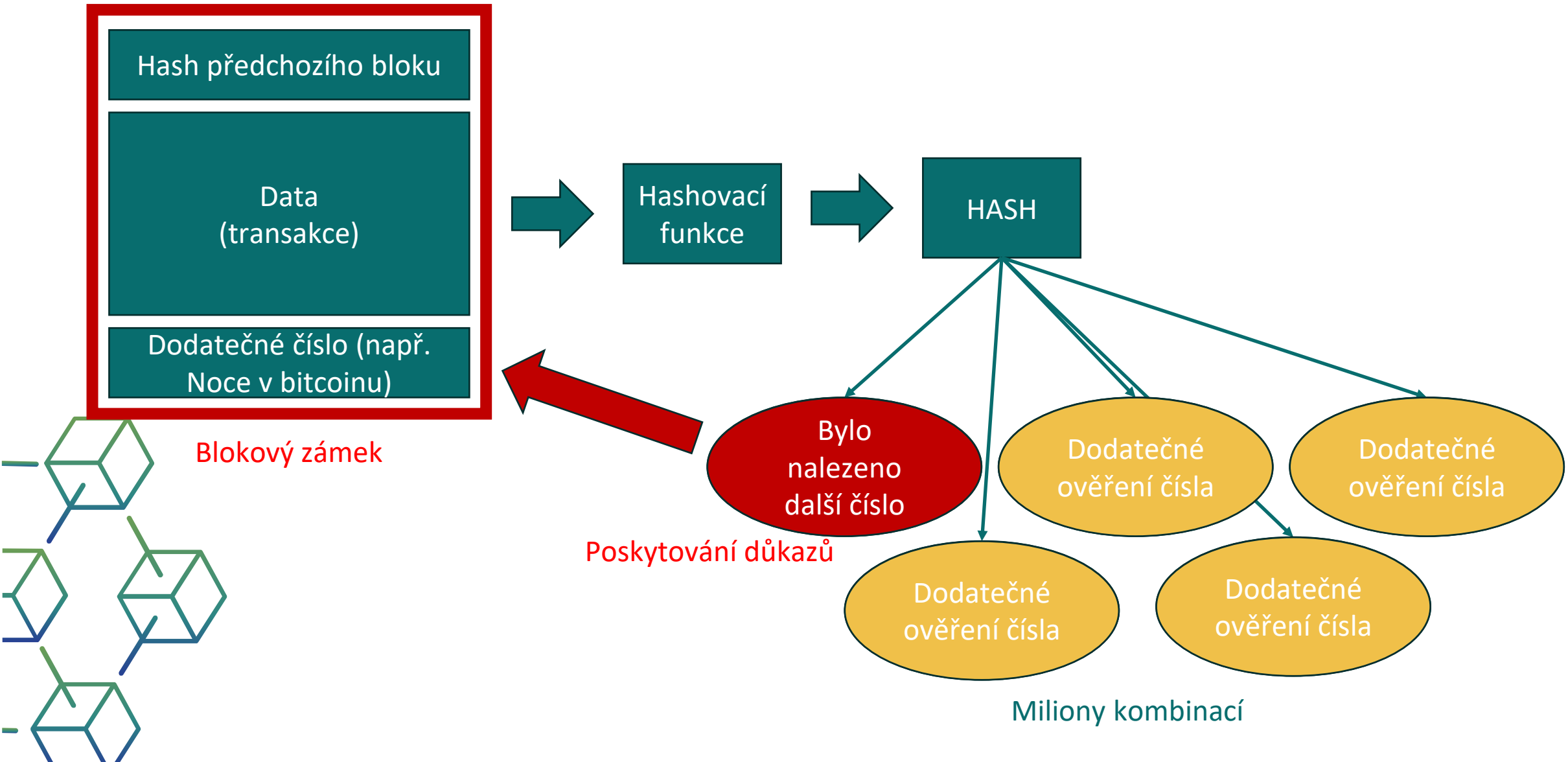
Proof of Work

Proof of Work (PoW) je forma kryptografického důkazu, ve kterém jedna strana (dokazatel) dokazuje ostatním (ověřovatelům), že bylo vynaloženo určité množství specifického výpočetního úsilí.

Dokazatelé mohou následně tyto výdaje potvrdit s minimálním úsilím z jejich strany.



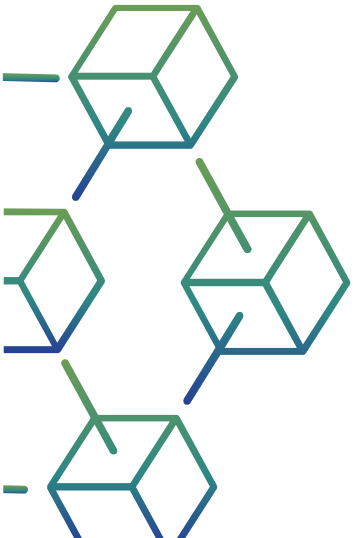
Proof of Work



Proof of stake

Protokoly Proof-of-stake (PoS) jsou třídou konsenzuálních mechanismů pro blockchainy, které fungují tak, že vybírají validátory v poměru k jejich množství držených v přidružené kryptoměně.

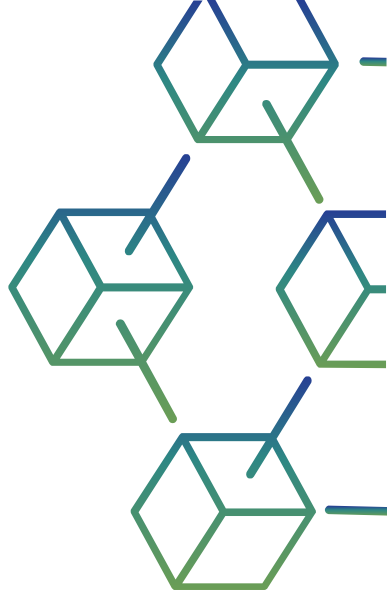
To se provádí proto, aby se předešlo výpočetním nákladům schémat proof-of-work (POW).



3 úrovně blockchainu

1. Blockchain 1.0: Původ moderního blockchainu
2. Blockchain 2.0: Chytré smlouvy
3. Blockchain 3:0: Decentralizovaná aplikace na podnikové úrovni

Srovnání s tradičními databázemi

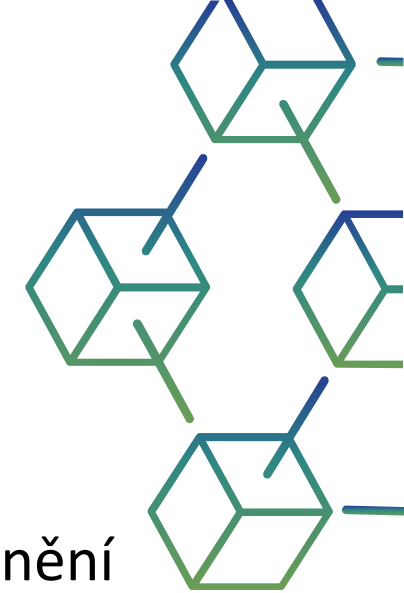


Datová struktura

Tradiční databáze: Tradiční databáze používají tabulky k uspořádání dat strukturovaným způsobem, obvykle podle předem definovaného schématu.

Blockchain: Blockchain používá strukturu záznamů, kde jsou data organizována do bloků a každý blok obsahuje seznam transakcí nebo datových záznamů. Struktura je obvykle méně pevná, což umožňuje větší flexibilitu v typech dat a formátech.

Srovnání s tradičními databázemi

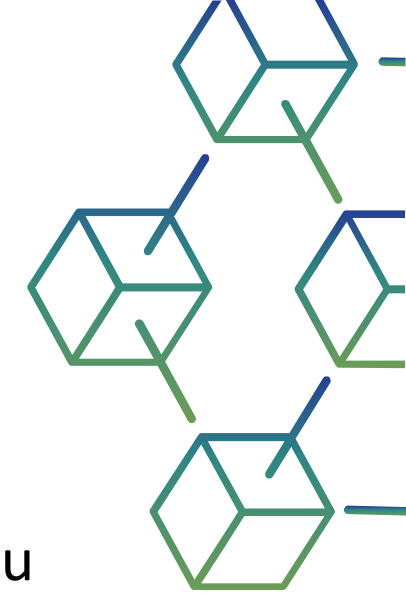


Řízení přístupu

Tradiční databáze: Řízení přístupu je řízeno centralizovanou autoritou a oprávnění lze udělovat nebo odebírat různým uživatelům nebo rolím.

Blockchain: Řízení přístupu je často řízeno pomocí kryptografických klíčů. Uživatelé mají kontrolu nad svými soukromými klíči, což jim umožňuje komunikovat s blockchainem, aniž by se spoléhali na centrální autoritu. Veřejné blockchainy jsou obvykle bez oprávnění, zatímco soukromé blockchainy mohou mít různé úrovně řízení přístupu.

Srovnání s tradičními databázemi

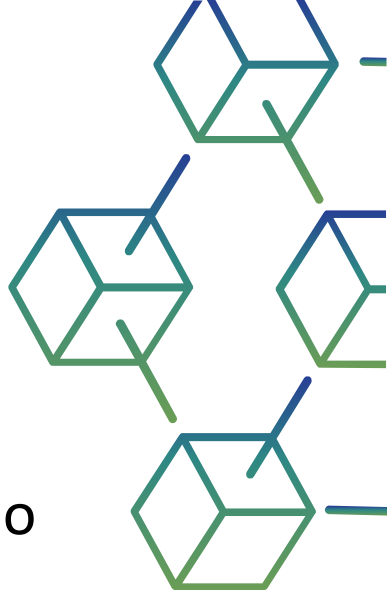


Mechanismus konsensu

Tradiční databáze: Tradiční databáze se nespoléhají na mechanismus konsensu mezi více stranami. Předpokládají, že data uložená v databázi jsou přesná.

Blockchain: Blockchain používá mechanismy konsenzu (např. Proof of Work, Proof of Stake) k ověření a odsouhlasení stavu záznamů. To zajišťuje, že všichni účastníci v síti mají sdílený a odsouhlasený pohled na data.

Srovnání s tradičními databázemi



Neměnná vs. proměnlivá data

Tradiční databáze: Data v tradičních databázích mohou být upravována nebo mazána oprávněnými uživateli s potřebnými oprávněními.

Blockchain: Jakmile jsou data zaznamenána na blockchain, jsou obvykle neměnná a odolná vůči změnám. Tato neměnnost je základním rysem technologie blockchain.

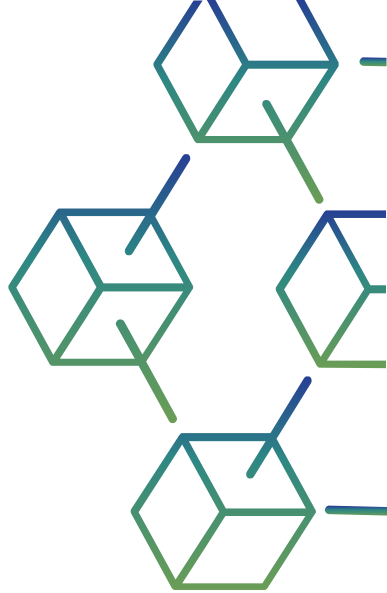
Srovnání s tradičními databázemi

Rychlost transakce a škálovatelnost

Tradiční databáze: Tradiční databáze jsou často optimalizovány pro vysoké rychlosti transakcí a lze je snadno škálovat přidáním dalších serverů nebo zdrojů.

Blockchain: Veřejné blockchainy, zejména ty, které používají Proof of Work, mohou mít pomalejší rychlost zpracování transakcí a problémy se škálovatelností. Pro zlepšení škálovatelnosti blockchainu se však vyvíjejí různá řešení a technologie.

Srovnání s tradičními databázemi



Případové studie

Tradiční databáze: Tradiční databáze se dobře hodí pro aplikace, které vyžadují vysokou propustnost, nízkou latenci a centralizované řízení, jako jsou bankovní systémy a platformy elektronického obchodování.

Blockchain: Blockchain se nejlépe hodí pro aplikace vyžadující decentralizaci, důvěru, transparentnost a zabezpečení, jako jsou kryptoměny, sledování dodavatelského řetězce, hlasovací systémy a chytré smlouvy.

03

Jaké jsou klíčové součásti technologie blockchain?

Jaké jsou klíčové součásti technologie blockchain?

Blockchain architektura má následující hlavní komponenty:

1. **Distribuované záznamy**
2. **Chytré smlouvy**
3. **Kryptografie veřejného klíče**

Jaké jsou klíčové součásti technologie blockchain?

1. Distribuované záznamy

Distribuované záznamy jsou sdílené databáze v blockchainové síti, které ukládají transakce, jako je například sdílený soubor, který může upravovat každý v týmu. Ve většině sdílených textových editorů může kdokoli s právy k úpravám smazat celý soubor. Technologie distribuovaných záznamů však mají přísná pravidla o tom, kdo a jak může upravovat. Záznamy po nahrání nelze smazat.

Jaké jsou klíčové součásti technologie blockchain?

2. Chytré smlouvy

Společnosti používají chytré smlouvy k samostatné správě obchodních smluv bez potřeby asistující třetí strany. Jsou to programy uložené v blockchainovém systému, které se spouštějí automaticky při splnění předem stanovených podmínek. Provádějí kontroly if-then, takže transakce mohou být dokončeny s jistotou. Například logistická společnost může mít inteligentní smlouvu, která automaticky provede platbu, jakmile zboží dorazí do přístavu.

Jaké jsou klíčové součásti technologie blockchain?

3. Kryptografie veřejného klíče

Kryptografie veřejného klíče je bezpečnostní funkce k jedinečné identifikaci účastníků v blockchainové síti. Tento mechanismus generuje dvě sady klíčů pro členy sítě. Jeden klíč je veřejný klíč, který je společný pro všechny v síti. Druhým je soukromý klíč, který je jedinečný pro každého člena. Soukromý a veřejný klíč spolupracují na odemknutí dat v hlavní knize.

Jaké jsou klíčové součásti technologie blockchain?

3. Kryptografie veřejného klíče

Například John a Jill jsou dva členové sítě. John zaznamená transakci, která je zašifrována jeho soukromým klíčem. Jill to může dešifrovat svým veřejným klíčem. Tímto způsobem je Jill přesvědčená, že transakci provedl John. Jillin veřejný klíč by nefungoval, kdyby byl Johnův soukromý klíč zmanipulován.

04

Jaké jsou výhody technologie blockchain?

Jaké jsou výhody technologie blockchain?

Technologie blockchain přináší mnoho výhod pro správu transakcí aktiv. Některé z nich uvádíme v následujících podsekcích:

1. **Pokročilé zabezpečení**
2. **Zlepšená účinnost**
3. **Rychlejší auditování**

Jaké jsou výhody technologie blockchain?

1. Pokročilé zabezpečení

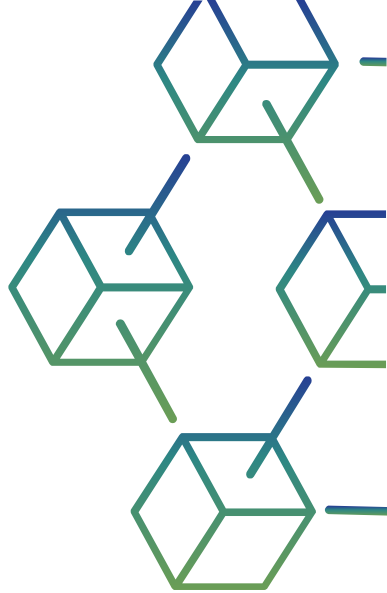
Blockchainové systémy poskytují vysokou úroveň zabezpečení a důvěry, kterou moderní digitální transakce vyžadují. Vždy tu je strach, že někdo bude manipulovat se základním softwarem, aby pro sebe vygeneroval falešné peníze. Blockchain však využívá tři principy kryptografie, decentralizace a konsensu k vytvoření vysoce bezpečného základního softwarového systému, se kterým je téměř nemožné manipulovat. Neexistuje jediný bod selhání a jediný uživatel nemůže změnit záznamy transakcí.

Jaké jsou výhody technologie blockchain?

2. Zlepšená účinnost

Transakce mezi podniky mohou zabrat spoustu času a vytvářet provozní úzká místa, zejména pokud jsou zapojeny regulační orgány třetích stran. Transparentnost a chytré smlouvy v blockchainu takové obchodní transakce urychlují a zefektivňují.

Jaké jsou výhody technologie blockchain?



3. Rychlejší auditování

Podniky musí být schopny bezpečně generovat, vyměňovat, archivovat a rekonstruovat elektronické transakce auditovatelným způsobem. Blockchainové záznamy jsou chronologicky neměnné, což znamená, že všechny záznamy jsou vždy seřazeny podle času. Díky této transparentnosti dat je zpracování auditu mnohem rychlejší.

05

Jaký je rozdíl mezi databází a blockchainem?

Jaký je rozdíl mezi databází a blockchainem?

Blockchain je speciální typ systému správy databází, který má více funkcí než běžná databáze. V následujícím seznamu popisujeme některé významné rozdíly mezi tradiční databází a blockchainem:

- Blockchainy decentralizují kontrolu bez poškození důvěry ve stávající data. V jiných databázových systémech to není možné.
- Společnosti zapojené do transakce nemohou sdílet celou svou databázi. Ale v blockchainových sítích má každá společnost svou kopii účetní knihy a systém automaticky udržuje konzistenci mezi dvěma účetními knihami.
- Přestože ve většině databázových systémů můžete data upravovat nebo mazat, v blockchainu můžete data pouze vkládat.

06

Jak se blockchain liší od cloudu?

Jak se blockchain liší od cloudu?

Termín cloud označuje počítačové služby, ke kterým lze přistupovat online. Z cloudu můžete přistupovat k softwaru jako službě (SaaS), produktu jako službě (PaaS) a infrastruktuře jako službě (IaaS).

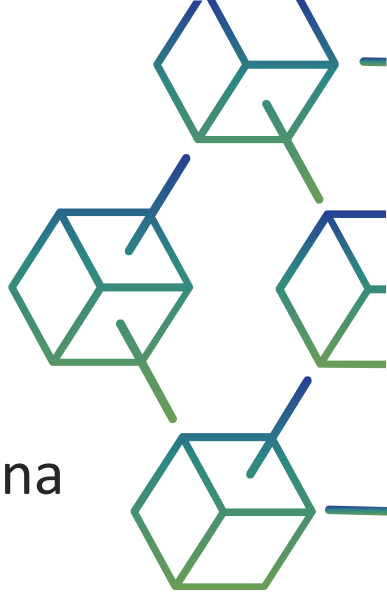
Poskytovatelé cloudu spravují svůj hardware a infrastrukturu a poskytují vám přístup k těmto výpočetním zdrojům přes internet. Poskytují mnohem více zdrojů než jen správu databází.

Pokud se chcete připojit k veřejné blockchainové síti, musíte poskytnout své hardwarové prostředky pro uložení kopie účetní knihy. K tomuto účelu můžete použít i server z cloudu. Někteří poskytovatelé cloudu také nabízejí kompletní Blockchain jako službu (BaaS) z cloudu.

07

Co je blockchain jako služba?

Co je blockchain jako služba?



Blockchain jako služba (BaaS) je spravovaná blockchain služba, kterou třetí strana poskytuje v cloudu. Můžete vyvíjet blockchainové aplikace a digitální služby, zatímco poskytovatel cloudu dodává infrastrukturu a nástroje pro vytváření blockchainu.

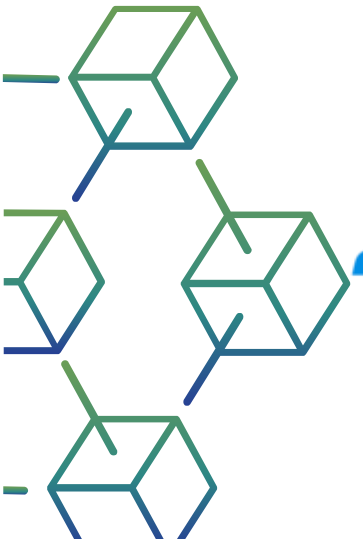
Jediné, co musíte udělat, je přizpůsobit stávající technologii blockchainu, díky které je přijetí blockchainu rychlejší a efektivnější.

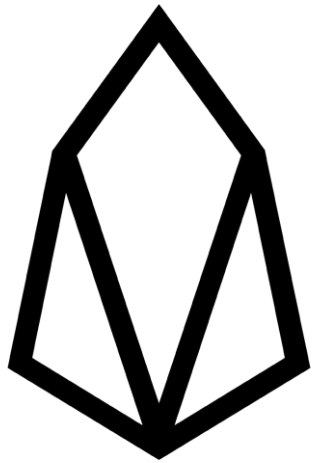
08

Případová studie

Kryptoměna – první široce používaný blockchain

- Moderní kryptoměny využívaly blockchain
  - Bitcoin
  - Litecoin
  - Ethereum
  - XRP
  - EOS
  - NEO
  - Stellar
  - Monero
  - Dash
  - …



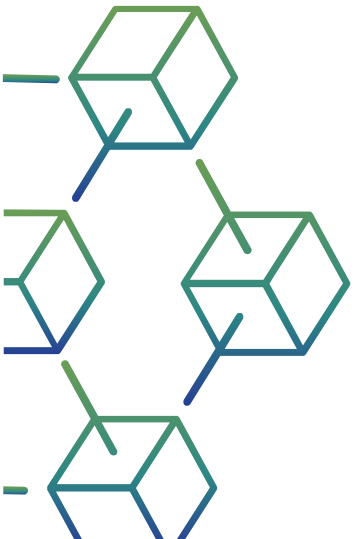


09

Závěr

Závěr

Technologie blockchain je pokročilý databázový mechanismus, který umožňuje transparentní sdílení informací v rámci obchodní sítě. Blockchain je tvořen řetězcem bloků, kde každý blok obsahuje seznam transakcí a jedinečný identifikátor (hash) předchozího bloku. Tím je zajištěna integrita dat. Blockchainy jsou decentralizované sítě, kde jsou data distribuována přes více uzlů (počítačů) v síti. Neexistuje žádný ústřední orgán ani jediný kontrolní bod, což je činí odolnými vůči cenzuře a manipulaci. Blockchain je uložen na tisících počítačů (uzlů) po celém světě. Každý uzel má kopii celého blockchainu, což zvyšuje jeho odolnost proti výpadkům a útokům.



Video

- How does a blockchain work – Simply Explained [6:00]
- Blockchain In 7 minutes [7:03]
- Blockchain Explained [10:23]
- What is a Blockchain? (Animated + Examples) [8:27]
- Blockchain Technology Explained (2 Hour Course) [1:54:53]
- Blockchain Basics & Cryptography [1:17:37]

Odkazy

- BlockChain Principles, Type & Application & Why You Should Care About It?
- Design principles for blockchain
- Principles of Blockchains
- Principles of Successful Blockchain Deployments
- Basic blockchain security
- Blockchain Design – Explore The Blockchain Principles
- Blockchain Technology: Principles and Application in Medical Imaging

10

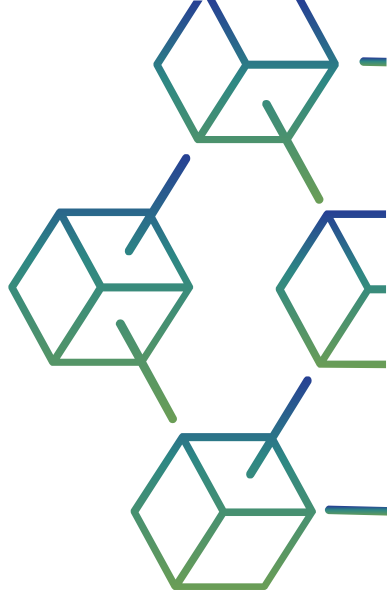
Interaktivní výuková aktivita

Vytvořte 5 bloků pod blockchainem

1. Použijte online nástroj pro hash
   https://emn178.github.io/online-tools/sha256.html

2. Použijte SHA256 a vytvořte hash 5 bloků – obsah je na dalším snímku

Vytvořte 5 bloků pod blockchainem



1. Obsah 1. bloku:
   2023-01-01T10:34:12+1,Jonh Newman,Jane Newman,236.23,EUR
   e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855

2. Obsah druhého bloku:
   2023-01-01T10:35:28+1,Steve Johnson,Richard McCay,100.00,EUR
   použijte hash z hashovací funkce 1. bloku

3. Obsah 3. bloku:
   2023-01-01T10:35:33+1,Charles Tann,Elisabeth Bronson,100.00,EUR
   použijte hash z hashovací funkce 2. bloku

4. Obsah 4. bloku:
   2023-01-01T10:35:59+1,Roger Blackburn,Lisa Tann,50.00,EUR
   použijte hash z hashovací funkce 3. bloku

5. Obsah 5. bloku :
   2023-01-01T10:36:01+1,Richard Moss,Edward Morris,85.00,EUR
   použijte hash z hashovací funkce 4. bloku

Vyzkoušejte:

1. Proveďte stejné malé změny ve 2. bloku a porovnejte nové hashe
2. Použijte jinou hashovací funkci – horní menu – Hash
    1. SHA1
    2. SHA2-512
    3. SHA3
    4. …
3. Použijte svůj obsah bloku pro funkci has

11

Kvíz

Kvíz

1. Jaký je klíčový požadavek na zabezpečenou hashovací funkci:
    a) Odolnost proti kolizi
    b) Nadbytečnost
    c) Předvídatelnost
    d) Linearita

Kvíz

2. Co je charakteristické pro architekturu centralizované databáze?
    a) Jediný kontrolní bod a autorita
    b) Distribuované úložiště dat mezi více uzly
    c) Autonomní rozhodování každého uzlu
    d) Vysoká odolnost vůči cenzuře a manipulaci

Kvíz

3. Co je klíčovou vlastností decentralizované databáze?
    a) Více „centrálních“ uzlů
    b) Jediný kontrolní bod a autorita
    c) Centralizované rozhodování určeným uzlem
    d) Nízká redundance a odolnost proti chybám

Kvíz

4. Jaká je definující charakteristika distribuovaného databázového systému?

   a) Data jsou uložena na více uzlech v síti

   b) Centralizovaná kontrola a autorita nad celou databází

   c) Nedostatek redundance pro zvýšení výkonu

   d) Omezená škálovatelnost díky jednouzlové architektuře

Kvíz

5. Co nejlépe popisuje hash v kontextu informatiky a kryptografie?

   a) Výstup s pevnou velikostí generovaný hašovací funkcí, představující jedinečný digitální podpis vstupních dat

   b) Řetězec proměnné délky používaný pro ukládání dat v databázích

   c) Programovací konstrukt pro optimalizaci získávání dat v algoritmech

   d) Metoda šifrování v reálném čase pro zabezpečení komunikačních kanálů

Kvíz

6. Která složka je zodpovědná za udržování chronologického a neměnného záznamu transakcí v blockchainu?

   a) Blok

   b) Uzel

   c) Chytré smlouvy

   d) Algoritmus konsensu

Kvíz

7. **Jaký je klíčový rozdíl mezi blockchainem a tradiční databází?**

   a) Blockchain nabízí decentralizované a distribuované řízení, zatímco tradiční databáze jsou typicky centralizované

   b) Tradiční databáze poskytují rychlejší zpracování transakcí ve srovnání s pomalejší povahou blockchainu

   c) Blockchain se spoléhá na jediný bod kontroly, zatímco tradiční databáze používají k ovládání distribuovanou síť

   d) Tradiční databáze jsou ze své podstaty odolné vůči manipulaci, zatímco blockchain je náchylnější k manipulaci s daty.

Kvíz

8. Kde byla technologie blockchain poprvé implementována?
    a) Finance a kryptoměna
    b) Zdravotní péče a lékařské záznamy
    c) Sociální média a sítě
    d) E-commerce a online maloobchod

https://blockchainforagrifood.eu/

Děkuji

Prostor na dotazy

BLOCK CHAIN FOR AGRI FOOD EDU

Co-funded by the European Union

Financováno Evropskou unií. Názory vyjádřené jsou názory autora a neodráží nutně oficiální stanovisko Evropské unie či Evropské výkonné agentury pro vzdělávání a kulturu (EACEA). Evropská unie ani EACEA za vyjádřené názory nenese odpovědnost.