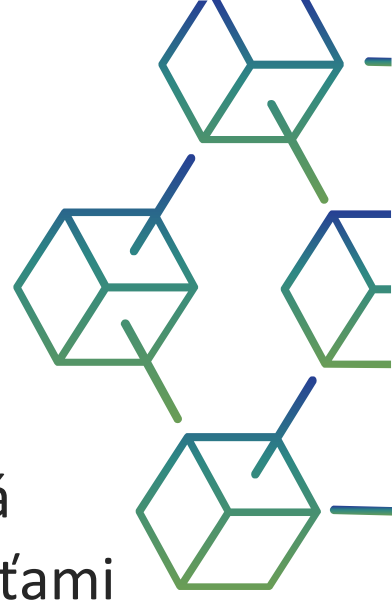
Modul 2

Stavebné bloky blockchainu a mechanizmus blockchainu

Co-funded by the European Union

Financované Európskou úniou. Vyjadrené názory a postoje sú názormi a vyhláseniami autora(-ov) a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie alebo Európskej výkonnej agentúry pre vzdelávanie a kultúru (EACEA). Európska únia ani EACEA za ne nepreberajú žiadnu zodpovednosť.

Popis modulu



Modul "Stavebné bloky blockchainu a mechanizmus blockchainu" sa zaoberá princípmi tvorby blockchainu (čo je blok a čo reťazec), základnými vlastnosťami tradičných, decentralizovaných a distribuovaných databázových konceptov a vlastnosťami a požiadavkami kryptografických a hashovacích funkcií, ktoré z toho vyplývajú. Modul obsahuje aj vysvetlenie rozdielu medzi dôkazom práce a dôkazom stavu a hlavné výhody blockchainu.

Výsledky štúdie

Absolventi modulu získajú základné teoretické znalosti o návrhu blockchainu a požiadavkách na kryptografické a hashovacie funkcie. Znalosti si zafixuje na prípadovej štúdii overenej kvízom.

Výsledky sú nasledovné:

- Modul so študijným materiálom
- Prípadová štúdia
- Interaktívna činnosť
- Kvíz

Obsahuje

BLOCK CHAIN FOR AGRI FOOD EDU

Co-funded by the European Union

Financované Európskou úniou. Vyjadrené názory a postoje sú názormi a vyhláseniami autora(-ov) a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie alebo Európskej výkonnej agentúry pre vzdelávanie a kultúru (EACEA). Európska únia ani EACEA za ne nepreberajú žiadnu zodpovednosť.

Obsahuje

BLOCKCHAIN FOR AGRI FOOD EDU

Co-funded by the European Union

Financované Európskou úniou. Vyjadrené názory a postoje sú názormi a vyhláseniami autora(-ov) a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie alebo Európskej výkonnej agentúry pre vzdelávanie a kultúru (EACEA). Európska únia ani EACEA za ne nepreberajú žiadnu zodpovednosť.

obsah

BLOCKCHAIN FOR AGRI FOOD EDU

Co-funded by the European Union

Financované Európskou úniou. Vyjadrené názory a postoje sú názormi a vyhláseniami autora(-ov) a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie alebo Európskej výkonnej agentúry pre vzdelávanie a kultúru (EACEA). Európska únia ani EACEA za ne nepreberajú žiadnu zodpovednosť.

01

ÚVOD K MODUL 2

STAVEBNÉ BLOKY BLOCKCHAINU A MECHANIZMUS BLOCKCHAINU

Domov

Čo je technológia blockchain?

Technológia blockchain je pokročilý databázový mechanizmus, ktorý umožňuje transparentné zdieľanie informácií v rámci obchodnej siete. Databáza blockchain ukladá údaje v blokoch, ktoré sú navzájom prepojené v reťazci.

Údaje sú chronologicky konzistentné, pretože reťazec nemôžete odstrániť ani upraviť bez súhlasu siete. Výsledkom je, že technológiu blockchain môžete použiť na vytvorenie nemennej alebo nemennej účtovnej knihy na sledovanie objednávok, platieb, účtov a iných transakcií.

Systém má zabudované mechanizmy, ktoré zabraňujú neoprávneným transakciám a vytvárajú konzistenciu v spoločnom zobrazení týchto transakcií.

Domov

Stavebné bloky blockchainu a mechanizmus blockchainu

Stavebné bloky blockchainu a mechanizmus blockchainu sú kľúčovými pojmami digitálneho ekosystému a kryptomien.

Blockchain je technológia, ktorá umožňuje zaznamenávať transakcie a udalosti v decentralizovanom a nemennom systéme.

Základnými stavebnými prvkami blockchainu sú tieto prvky:

- Bloky
- Distribuovaná účtovná kniha / Distribuované záznamy
- Kryptografia
- Mechanizmus konsenzu
- Imutabilita

Domov

Stavebné bloky blockchainu a mechanizmus blockchainu

BLOKY

Blockchain sa skladá z reťazca blokov, pričom každý blok obsahuje zoznam transakcií a jedinečný identifikátor (hash) predchádzajúceho bloku. Tým sa zabezpečuje integrita údajov.

DISTRIBUOVANÉ ZÁZNAMY

Blockchain je uložený na tisícoch počítačov (uzlov) po celom svete. Každý uzol má kópiu celého blockchainu, čo zvyšuje jeho odolnosť voči výpadkom a útokom.

Domov

Stavebné bloky blockchainu a mechanizmus blockchainu

KRYPTOGRAFIA

Na zabezpečenie transakcií sa používa asymetrická kryptografia. Každý účastník má súkromný a verejný kľúč, ktoré umožňujú overovanie a podpisovanie transakcií.

MECHANIZMUS PÁROVANIA

Blockchain vyžaduje, aby uzly dosiahli konsenzus o platných transakciách. To sa zvyčajne dosahuje pomocou rôznych konsenzuálnych algoritmov, ako sú Proof of Work (PoW) alebo Proof of Stake (PoS).

NEZÁVISLOSŤ

Po uložení údajov do blockchainu ich nemožno jednoducho zmeniť. Tým sa zabezpečuje dôvera a transparentnosť.

Domov

Stavebné bloky blockchainu a mechanizmus blockchainu

- Mechanizmus blockchain zabezpečuje integritu údajov a zaručuje nespochybniteľnosť transakcií.
- Blockchain má širokú škálu aplikácií aj mimo kryptomien, vrátane financií, dodávateľského reťazca, zdravotníctva a mnohých ďalších odvetví.
- Jeho budúcnosť závisí od schopnosti komunít a podnikov inovovať a využívať jeho potenciál na riešenie skutočných problémov a zmenu digitálneho sveta.

02

ZÁKLADNÉ KOMPONENTY: BLOKY, KRYPTOGRAFICKÝ HASH, DECENTRALIZÁCIA

Základné komponenty: bloky, kryptografický hash, decentralizácia

Ako funguje blockchain?

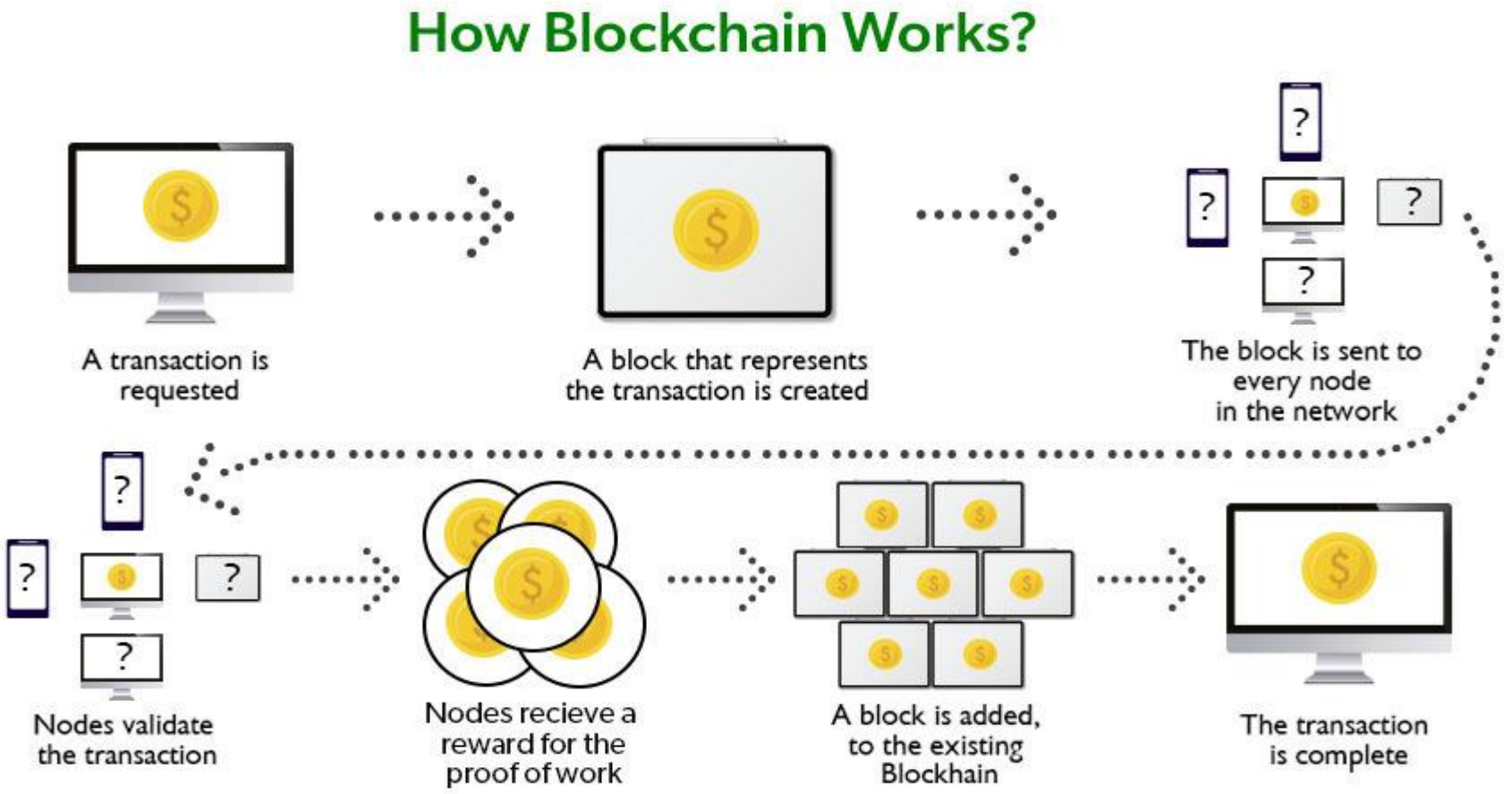
- Každá transakcia alebo dátový záznam, známy ako "blok", je bezpečne prepojený s predchádzajúcim záznamom pomocou kryptografického hashovania, čím sa vytvorí súvislý reťazec informácií odolných voči manipulácii.
- Keďže blok nie je možné zmeniť, jediná dôvera je potrebná v čase, keď používateľ alebo program zadáva údaje. Tento aspekt znižuje potrebu dôveryhodných tretích strán, ktorými sú zvyčajne audítori alebo iné osoby, ale zvyšujú náklady a robia chyby.

Základné komponenty: bloky, kryptografický hash, decentralizácia

Blockchain sa skladá z programov nazývaných skripty, ktoré vykonávajú úlohy, ktoré by ste bežne vykonávali v databáze: zadávanie informácií, prístup k nim a ich ukladanie. Je to distribuovaný blockchain, čo znamená, že na mnohých počítačoch je uložených viacero kópií a všetky sa musia zhodovať, aby boli platné.

V blockchaine sa zhromažďujú informácie o **transakciách** a ukladajú sa do bloku, podobne ako bunky v tabuľke obsahujúce informácie. Po vyplnení informácie prejdú **šifrovacím algoritmom,** ktorý vytvorí hexadecimálne číslo nazývané **hash**.

Základné komponenty: bloky, kryptografický hash, decentralizácia



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

Základné komponenty: bloky, kryptografický hash, decentralizácia

Proces transakcie v blockchaine možno zhrnúť takto:

1. Uľahčenie transakcie
2. Overovanie transakcií
3. Vytvorenie nového bloku
4. Algoritmus konsenzu
5. Pridanie nového bloku do blockchainu
6. Ukončenie transakcie

Základné komponenty: bloky, kryptografický hash, decentralizácia

Hash sa potom vloží do hlavičky ďalšieho bloku a zašifruje sa spolu s ostatnými informáciami v bloku. Tým sa vytvorí séria blokov, ktoré sú navzájom prepojené.

Transakcie prebiehajú podľa špecifického procesu v závislosti od blockchainu, na ktorom sa uskutočňujú. Napríklad v bitcoinovom blockchaine, ak iniciujete transakciu pomocou svojej kryptomenovej peňaženky - aplikácie, ktorá poskytuje rozhranie k blockchainu - spustí sa sled udalostí.

Základné komponenty: bloky, kryptografický hash, decentralizácia

1. **Uľahčenie transakcie:** nová transakcia vstupuje do siete blockchain. Všetky informácie, ktoré je potrebné preniesť, sa dvakrát zašifrujú pomocou verejných a súkromných kľúčov.
2. **Overenie transakcie:** transakcia sa následne prenesie do siete peer-to-peer počítačov rozmiestnených po celom svete. Všetky uzly v sieti skontrolujú platnosť transakcie, napríklad či je k dispozícii dostatočný zostatok na vykonanie transakcie.
3. **Vytvorenie nového bloku:** V typickej blockchainovej sieti je veľa uzlov a mnoho transakcií sa overuje naraz. Keď je transakcia overená a vyhlásená za legitímnu, pridá sa do mempoolu. Všetky overené transakcie na konkrétnom uzle tvoria mempool a takéto viaceré mempooly tvoria blok.

Základné komponenty: bloky, kryptografický hash, decentralizácia

6. **Algoritmus konsenzu:** uzly, ktoré tvoria blok, sa pokúsia pridať blok do siete blockchain, aby bol trvalý. Ak však každý uzol môže takto pridávať bloky, naruší to fungovanie siete blockchain.
7. **Pridanie nového bloku do blockchainu:** Po získaní hodnoty hash a overení je novovytvorený blok pripravený na pridanie do blockchainu. Každý blok obsahuje hash hodnotu predchádzajúceho bloku, a tak sú bloky kryptograficky prepojené a tvoria blockchain. Nový blok sa pridáva na otvorený koniec blockchainu.
8. **Dokončenie transakcie:** po pridaní bloku do blockchainu je transakcia dokončená a podrobnosti o nej sú trvalo uložené v blockchaine. Ktokoľvek môže získať údaje o transakcii a potvrdiť transakciu.

Porovnanie s tradičnými databázami

Tradičné databázy sú centralizované, meniteľné a optimalizované na vysokorýchlostné spracovanie údajov, zatiaľ čo blockchainy sú decentralizované, nemenné a zamerané na poskytovanie dôvery a transparentnosti prostredníctvom mechanizmov konsenzu. Výber medzi nimi závisí od konkrétnych potrieb danej aplikácie.

- *Centralizácia vs. decentralizácia*
- *Štruktúra údajov*
- *Kontrola prístupu*
- *Mechanizmus konsenzu*
- *Invariantné vs. variabilné údaje*
- *Rýchlosť transakcií a škálovateľnosť*
- *Prípadová štúdia*

Porovnanie s tradičnými databázami

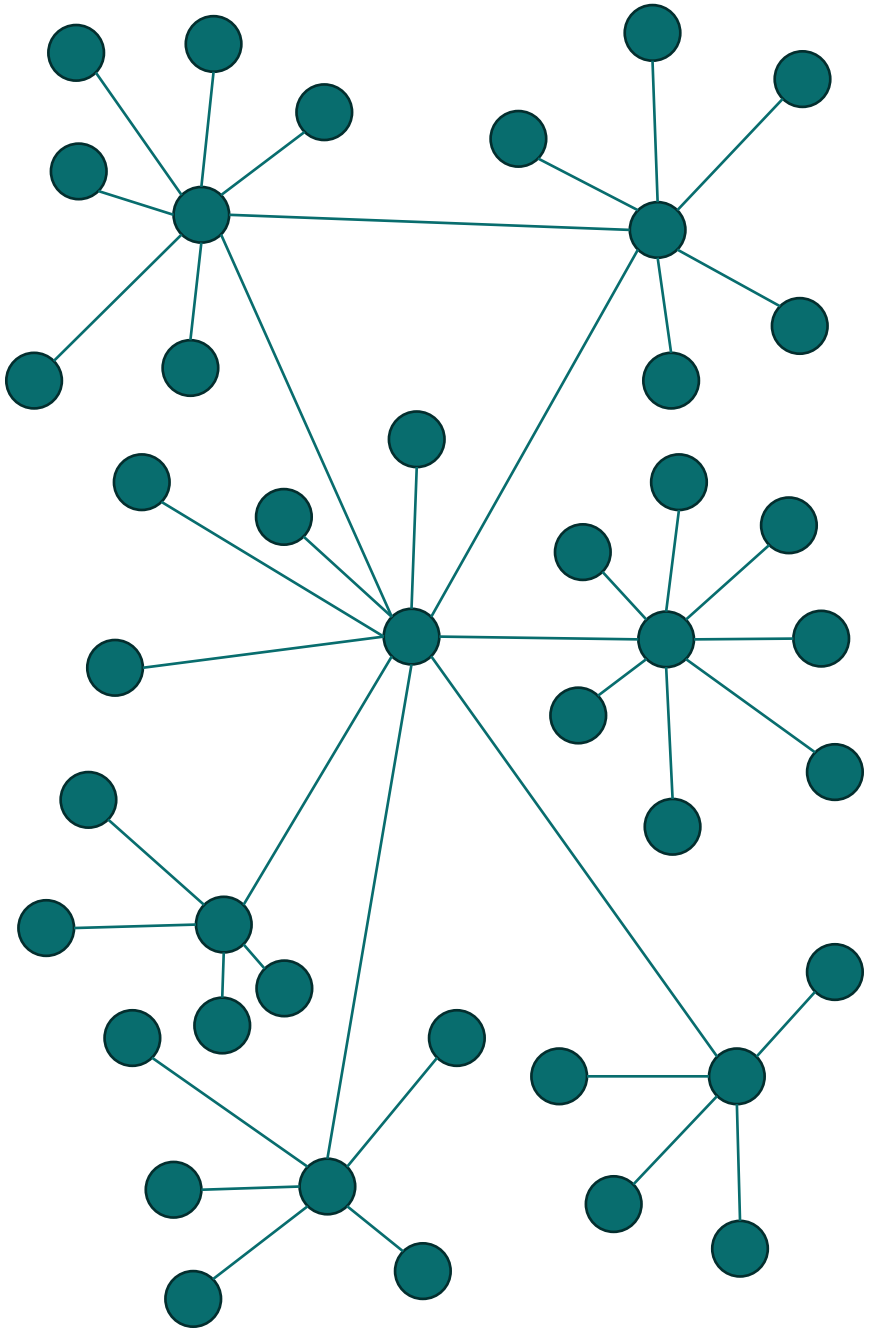
Centralizácia vs. decentralizácia

Tradičné databázy: Tradičné databázy sú centralizované systémy, v ktorých má nad databázou kontrolu jeden subjekt (napr. spoločnosť alebo organizácia). Pri správe a ukladaní údajov sa spoliehajú na centrálny server alebo klaster serverov.

Blockchain: Blockchainy sú decentralizované siete, v ktorých sú údaje distribuované medzi viaceré uzly (počítače) v sieti. Neexistuje žiadna centrálna autorita ani jediný kontrolný bod, vďaka čomu sú odolné voči cenzúre a manipulácii.

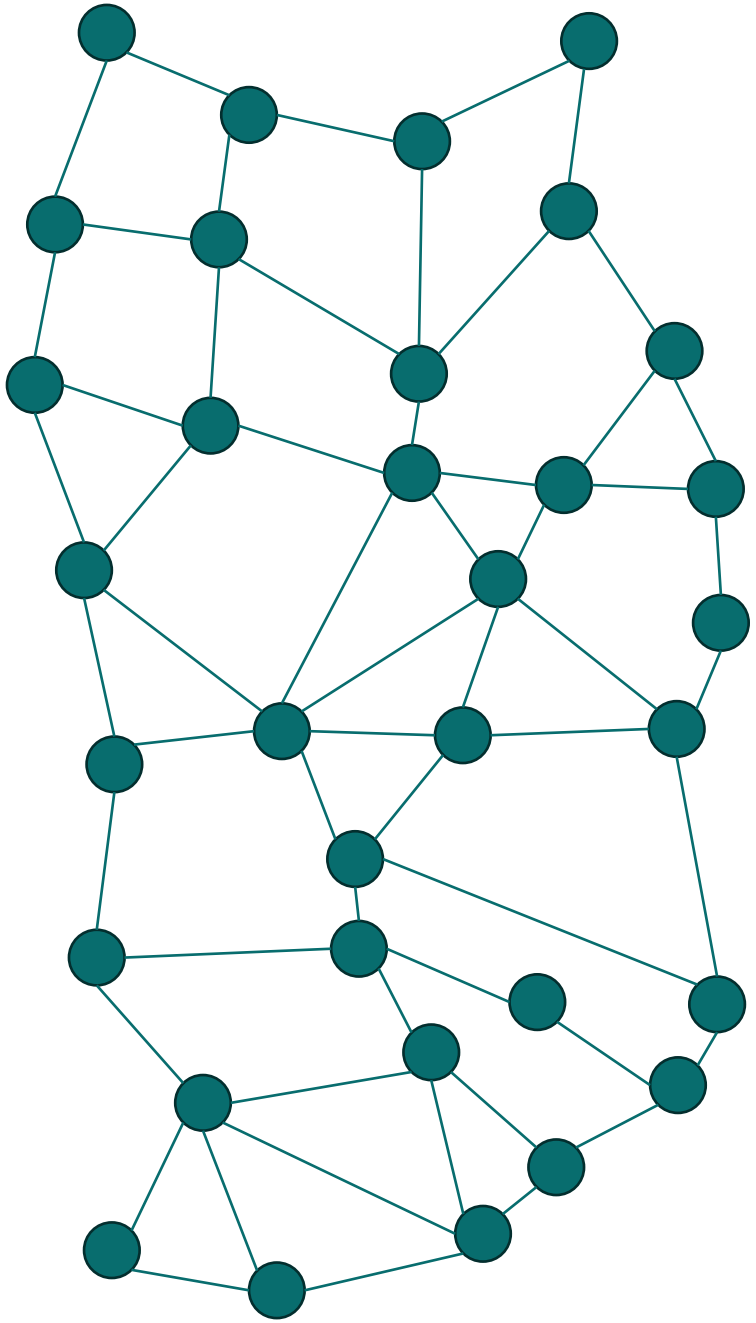
Centralizované

Všetky uzly sú prepojené pod jednou autoritou.



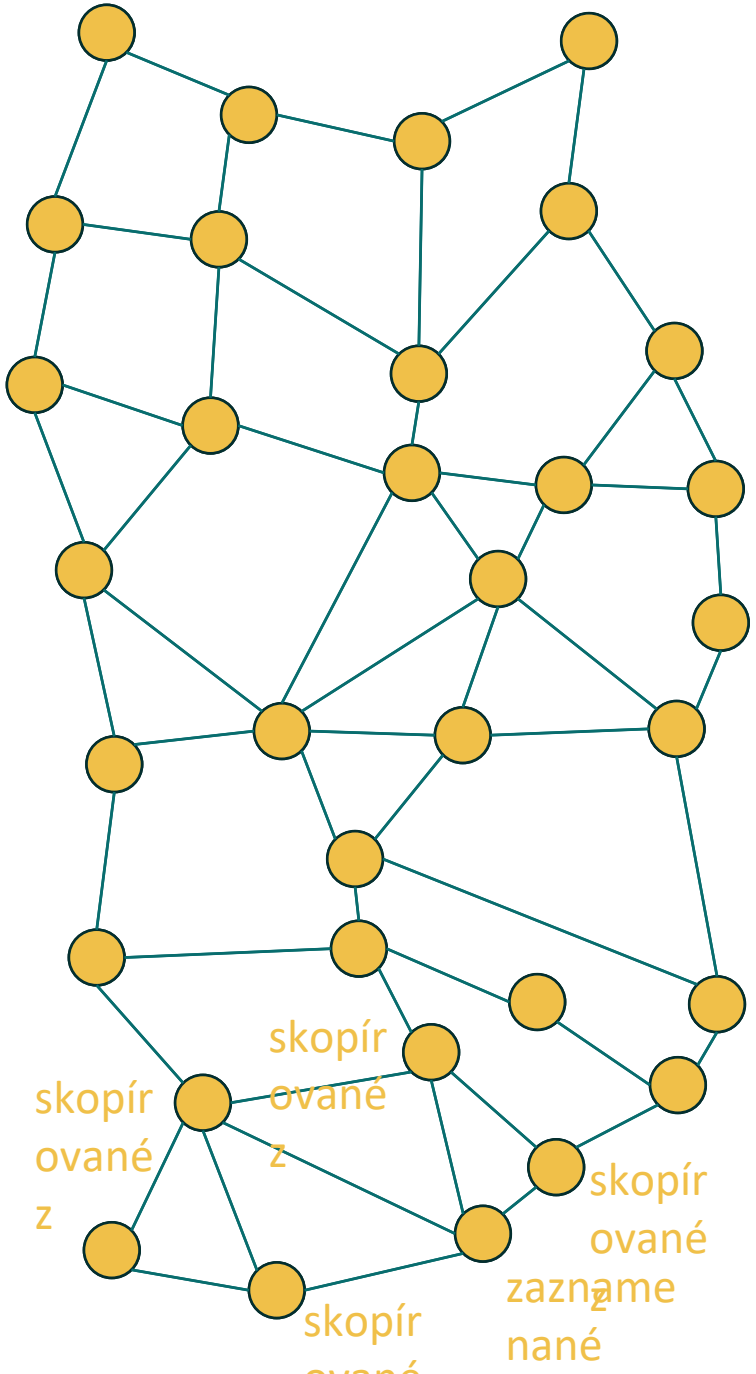
Decentralizované

Uzly nie sú spravované žiadnym autoritatívnym serverom, všetky majú individuálne entity.



Distribuuje

Každý uzol je nezávislý a vzájomne prepojený.



Transakcie v distribuovanej sieti

Transakcia sa zaznamená v uzle a skopíruje sa do neho.

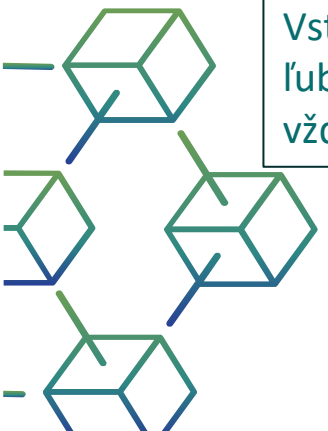
Funkcia Hash

Hašovacia funkcia je matematická funkcia, ktorá konvertuje vstupnú hodnotu na inú komprimovanú hodnotu. Vstup do hašovacej funkcie má ľubovoľnú dĺžku, ale výstup má vždy pevnú dĺžku.

Hashovacie funkcie sú mimoriadne užitočné a vyskytujú sa takmer vo všetkých aplikáciách informačnej bezpečnosti.

Jedinečná výstupná funkcia hashovania

DÁTA	HAŠOVACIA FUNKCIA	HASH
Stavebné bloky blockchainu.	Funkcia Hash SHA1	d355724c886c15a6272e5a8e6f416438535ca0be
stavebné bloky blockchainu.	Funkcia Hash SHA1	54b05cb173b979447e87e3d4af19a41a774f631c
Hašovacia funkcia je matematická funkcia, ktorá konvertuje vstupnú hodnotu na inú komprimovanú hodnotu. Vstup do hašovacej funkcie má ľubovoľnú dĺžku, ale výstup má vždy pevnú dĺžku.	Funkcia Hash SHA1	63dd04188931586e47c899271ccdcd681b0cc357

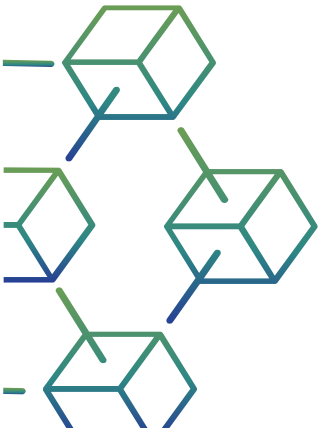


SHA1 v súčasnosti nestačí

Stavebné bloky blockchainu.

hašovacia
funkcia
SHA3-512

33322d615333e9faa2109c35997cf144876cc75ba76059454b28c81d2fa1c286a68679a00afb
baa71e9170ffc3bdaf6fbef5035a31b4f40a354502dd985368d4

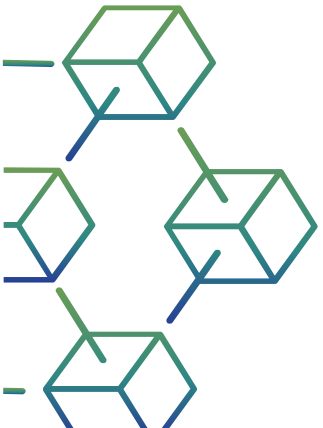


Odolnosť proti zobrazeniu

Táto vlastnosť znamená, že by malo byť výpočtovo náročné obrátiť hašovaciu funkciu.

Inými slovami, ak hašovacia funkcia h vytvorila hašovaciu hodnotu z, potom by malo byť ťažké nájsť akúkoľvek vstupnú hodnotu x, ktorá by sa rovnala hodnote z.

Táto vlastnosť chráni pred útočníkom, ktorý má len hodnotu hash a snaží sa nájsť vstup.



Odolnosť voči kolízii

Táto vlastnosť znamená, že by malo byť ťažké nájsť dva rôzne vstupy akejkoľvek dĺžky, ktoré vedú k rovnakému hash. Táto vlastnosť sa označuje aj ako bezkolízna hašovacia funkcia.

Inými slovami, pre hašovaciu funkciu h je ťažké nájsť akékoľvek dva rôzne vstupy x a y tak, aby h(x) = h(y).

Keďže hašovacia funkcia je kompresná hašovacia funkcia s pevnou dĺžkou, nie je možné, aby hašovacia funkcia nemala žiadne kolízie. Táto bezkolízna vlastnosť len potvrdzuje, že tieto kolízie by sa mali ťažko nájsť.

Vďaka tejto vlastnosti je pre útočníka veľmi ťažké nájsť dve vstupné hodnoty s rovnakým hashom.

Ak je hašovacia funkcia odolná voči kolíziám, je odolná aj voči druhému predobrazu.

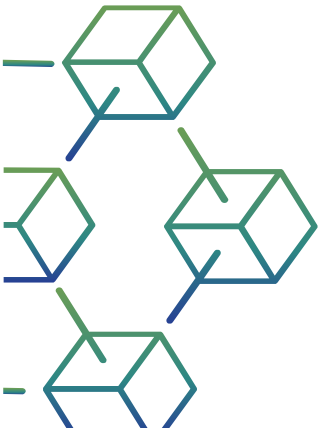
Zdroj: https://www.tutorialspoint.com/cryptography/cryptography_hash_functions.htm

Druhá odolnosť pred zobrazením

Táto vlastnosť znamená, že pri danom vstupe a jeho hash by malo byť ťažké nájsť iný vstup s rovnakým hashom.

Inými slovami, ak hašovacia funkcia h pre vstup x vytvára hašovaciu hodnotu h(x), potom by malo byť ťažké nájsť akýkoľvek iný vstup y taký, aby h(y) = h(x).

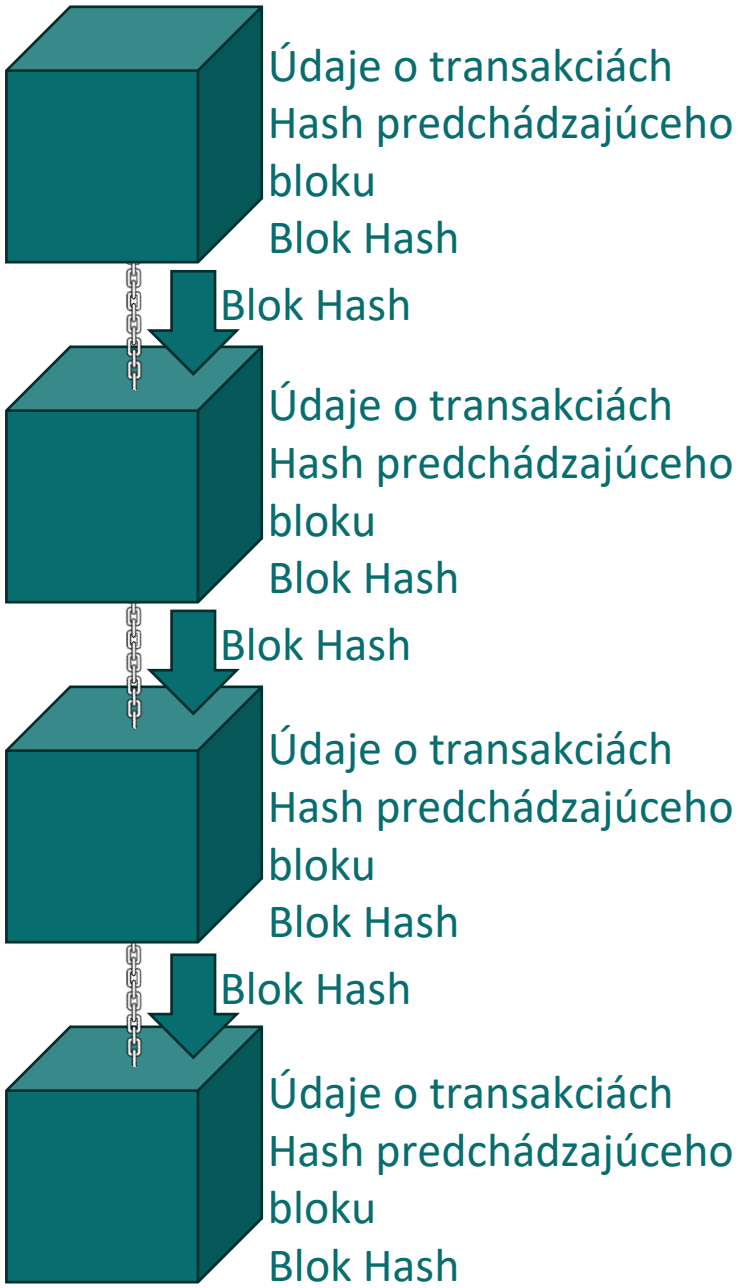
Táto vlastnosť hashovacej funkcie chráni pred útočníkom, ktorý má vstupnú hodnotu a jej hash a chce namiesto pôvodnej vstupnej hodnoty nahradiť inú hodnotu ako legitímnu.



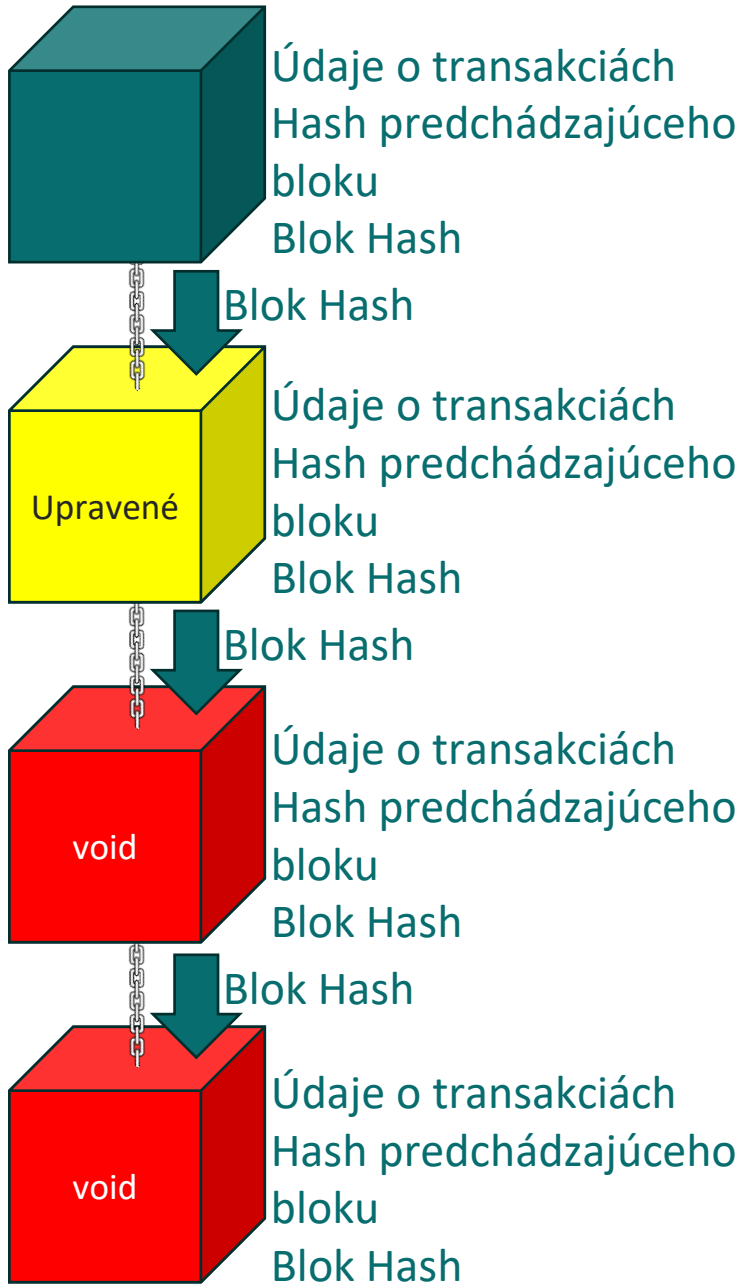
Blockchain

Blok = dáta + hash predchádzajúceho bloku + hash

Reťaz = reťaz medzi blokmi

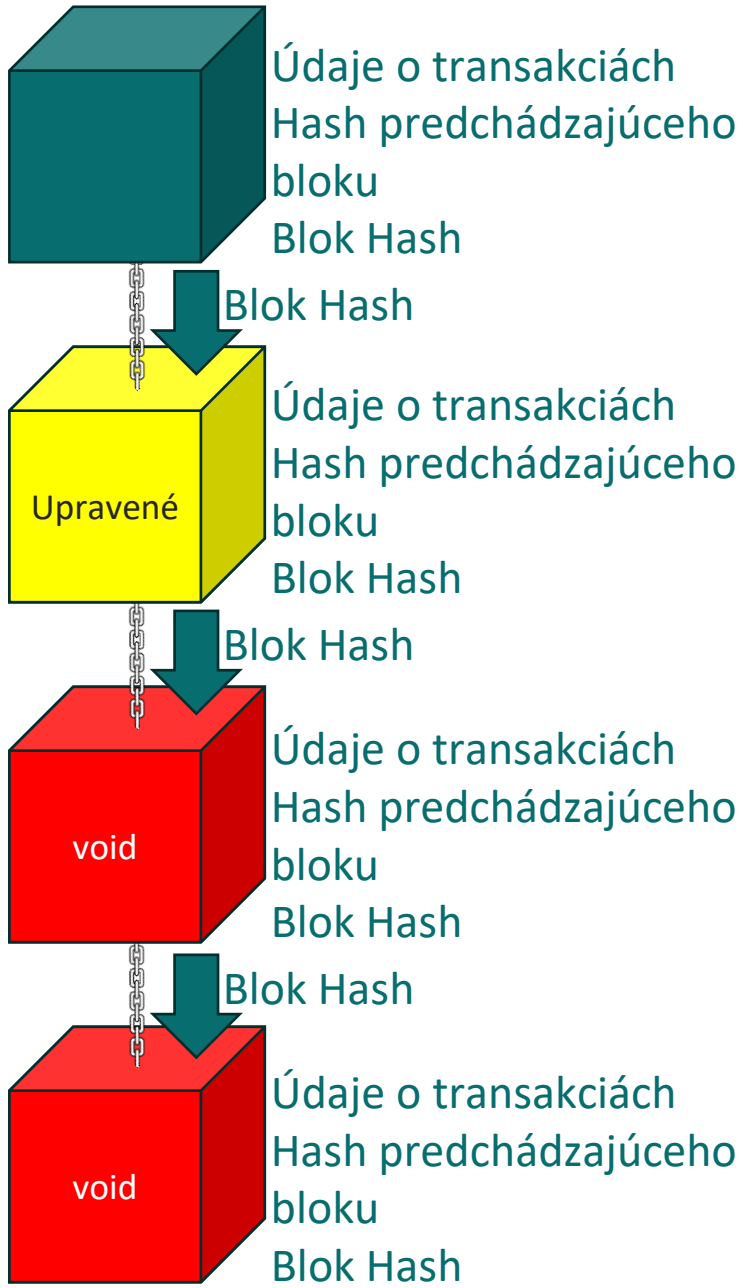


Všetky transakcie sa zaznamenávajú v "blokoch".



Ak sa zmení jeden blok (jedna transakcia v jednom bloku).

Hodnota hašovacej funkcie je iná



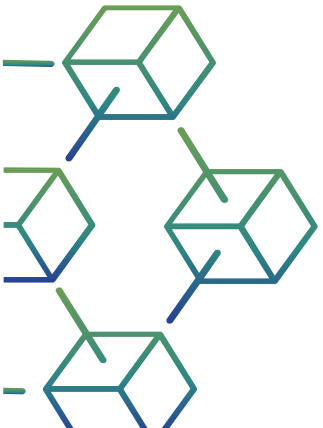
Ak chce hacker zmeniť jeden blok (údaje v jednom bloku), musí zmeniť všetky ostatné bloky a všetky kópie blokov v distribuovanej sieti.

Takmer nemožné (potrebuje obrovský výpočtový výkon, elektrinu atď.)

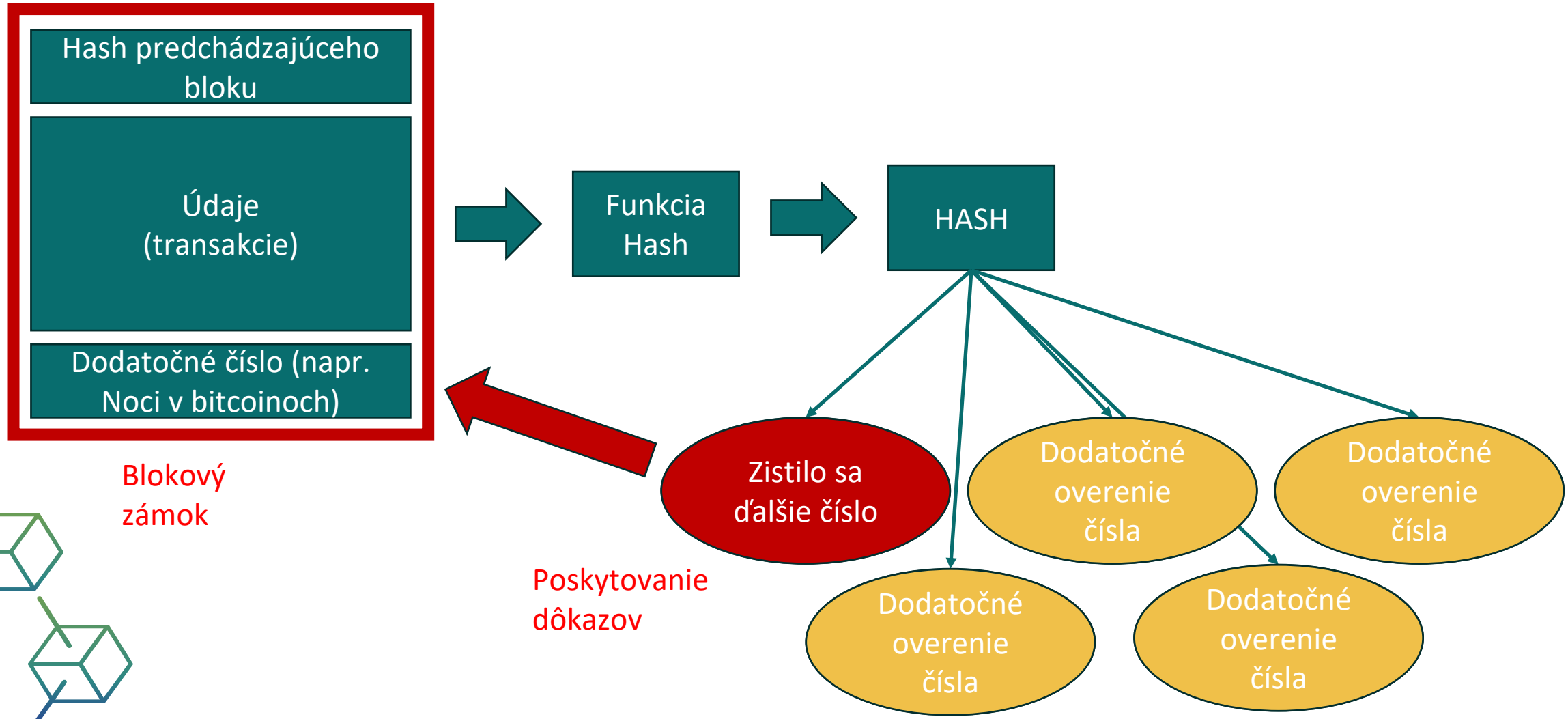
Dôkaz o práci

Dôkaz práce (PoW) je forma kryptografického dôkazu, pri ktorej jedna strana (prover) dokazuje ostatným stranám (verifikátorom), že bolo vynaložené určité množstvo špecifického výpočtového úsilia.

Dôkazy potom môžu tieto výdavky potvrdiť s minimálnym úsilím z ich strany.



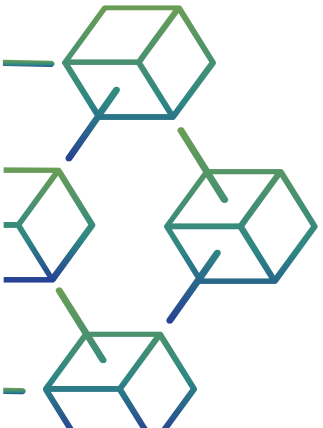
Dôkaz o práci



Dôkaz o podiele

Protokoly PoS (Proof-of-stake) sú triedou konsenzuálnych mechanizmov pre blockchainy, ktoré fungujú tak, že vyberajú overovateľov v pomere k sume držanej v príslušnej kryptomene.

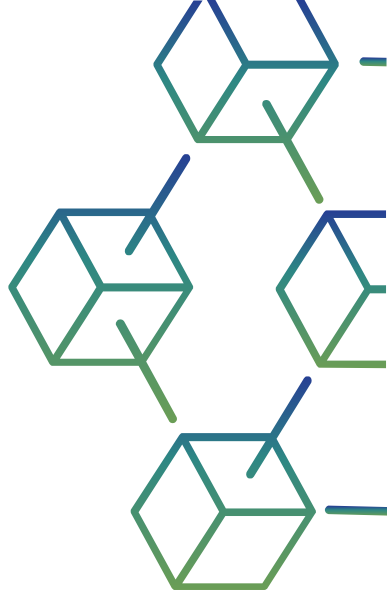
Týmto spôsobom sa predchádza výpočtovým nákladom schém proof-of-work (POW).



3 úrovne blockchainu

1. Blockchain 1.0: Vznik moderného blockchainu
2. Blockchain 2.0: inteligentné zmluvy
3. Blockchain 3:0: Decentralizované aplikácie na podnikovej úrovni

Porovnanie s tradičnými databázami



Štruktúra údajov

Tradičné databázy: Tradičné databázy používajú tabuľky na štruktúrovanú organizáciu údajov, zvyčajne podľa vopred definovanej schémy.

Blockchain: Blockchain používa štruktúru záznamov, v ktorej sú údaje usporiadané do blokov a každý blok obsahuje zoznam transakcií alebo záznamov údajov. Štruktúra je zvyčajne menej rigidná, čo umožňuje väčšiu flexibilitu typov a formátov údajov.

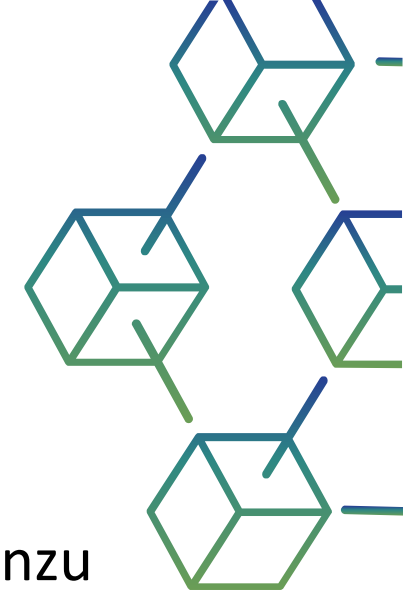
Porovnanie s tradičnými databázami

Kontrola prístupu

Tradičná databáza: riadenie prístupu riadi centralizovaná autorita a oprávnenia možno udeliť alebo odobrať rôznym používateľom alebo rolám.

Blockchain: kontrola prístupu je často riadená kryptografickými kľúčmi. Používatelia majú kontrolu nad svojimi súkromnými kľúčmi, čo im umožňuje komunikovať s blockchainom bez toho, aby sa spoliehali na centrálnu autoritu. Verejné blockchainy sú zvyčajne bez oprávnení, zatiaľ čo súkromné blockchainy môžu mať rôzne úrovne kontroly prístupu.

Porovnanie s tradičnými databázami

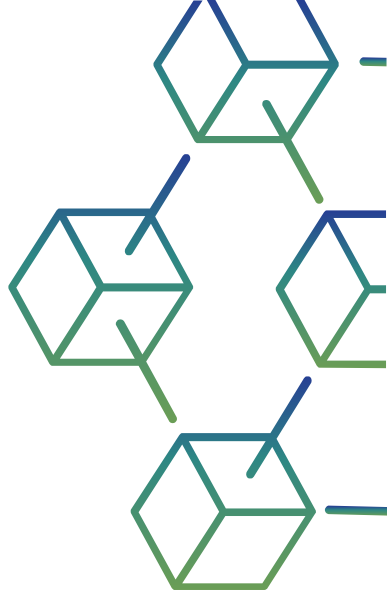


Mechanizmus konsenzu

Tradičné databázy: Tradičné databázy sa nespoliehajú na mechanizmus konsenzu viacerých strán. Predpokladajú, že údaje uložené v databáze sú presné.

Blockchain: Blockchain používa mechanizmy konsenzu (napr. Proof of Work, Proof of Stake) na overovanie a zosúlaďovanie stavu záznamov. Tým sa zabezpečí, že všetci účastníci siete majú spoločný a dohodnutý pohľad na údaje.

Porovnanie s tradičnými databázami



Invariantné vs. variabilné údaje

Tradičné databázy: údaje v tradičných databázach môžu upravovať alebo vymazávať oprávnení používatelia s potrebnými oprávneniami.

Blockchain: keď sú údaje zaznamenané v blockchaine, sú zvyčajne nemenné a odolné voči zmenám. Táto nemennosť je základnou vlastnosťou technológie blockchain.

Porovnanie s tradičnými databázami

Rýchlosť transakcií a škálovateľnosť

Tradičné databázy: Tradičné databázy sú často optimalizované na vysokú rýchlosť transakcií a dajú sa ľahko škálovať pridaním ďalších serverov alebo zdrojov.

Blockchain: Verejné blockchainy, najmä tie, ktoré používajú Proof of Work, môžu mať nižšiu rýchlosť spracovania transakcií a problémy so škálovateľnosťou. Vyvíjajú sa však rôzne riešenia a technológie na zlepšenie škálovateľnosti blockchainu.

Porovnanie s tradičnými databázami

Prípadové štúdie

Tradičné databázy: Tradičné databázy sú vhodné pre aplikácie, ktoré vyžadujú vysokú priepustnosť, nízku latenciu a centralizovanú správu, ako sú bankové systémy a platformy elektronického obchodu.

Blockchain: Blockchain je najvhodnejší pre aplikácie vyžadujúce decentralizáciu, dôveru, transparentnosť a bezpečnosť, ako sú napríklad kryptomeny, sledovanie dodávateľského reťazca, hlasovacie systémy a inteligentné zmluvy.

03

Aké sú kľúčové komponenty technológie blockchain?

Aké sú kľúčové komponenty technológie blockchain?

Architektúra blockchainu má tieto hlavné komponenty:

1. **Distribuované záznamy**
2. **Inteligentné zmluvy**
3. **Kryptografia s verejným kľúčom**

Aké sú kľúčové komponenty technológie blockchain?

1. Distribuované záznamy

Distribuované záznamy sú zdieľané databázy v sieti blockchain, v ktorých sa ukladajú transakcie, napríklad zdieľaný súbor, ktorý môže upravovať ktokoľvek z tímu. Vo väčšine zdieľaných textových editorov môže ktokoľvek s právami na editáciu vymazať celý súbor. Technológie distribuovaných záznamov však majú prísne pravidlá o tom, kto a ako môže upravovať. Po nahratí záznamov ich nemožno vymazať.

Aké sú kľúčové komponenty technológie blockchain?

2. Inteligentné zmluvy

Spoločnosti používajú inteligentné zmluvy na vlastnú správu obchodných zmlúv bez potreby pomoci tretej strany. Ide o programy uložené v systéme blockchain, ktoré sa automaticky spúšťajú po splnení vopred definovaných podmienok. Vykonávajú kontroly typu "ak - potom", takže transakcie sa môžu dokončiť s istotou. Napríklad logistická spoločnosť môže mať inteligentnú zmluvu, ktorá automaticky vykoná platbu, keď tovar dorazí do prístavu.

Aké sú kľúčové komponenty technológie blockchain?

3. Kryptografia s verejným kľúčom

Kryptografia s verejným kľúčom je bezpečnostný prvok na jednoznačnú identifikáciu účastníkov siete blockchain. Tento mechanizmus generuje dve sady kľúčov pre členov siete. Jeden kľúč je verejný kľúč, ktorý zdieľajú všetci v sieti. Druhý je súkromný kľúč, ktorý je jedinečný pre každého člena. Súkromný a verejný kľúč spolupracujú pri odomykaní údajov v účtovnej knihe.

Aké sú kľúčové komponenty technológie blockchain?

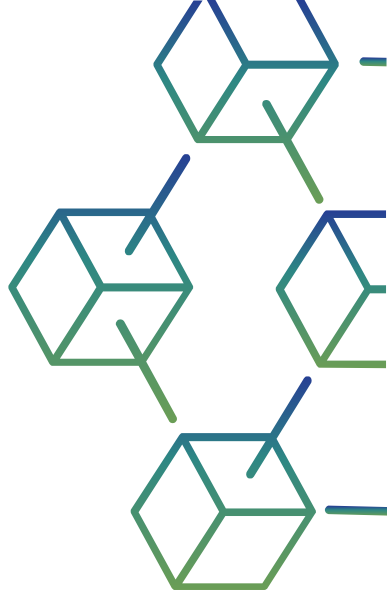
3. Kryptografia s verejným kľúčom

Napríklad John a Jill sú dvaja členovia siete. John zaznamená transakciu, ktorá je zašifrovaná jeho súkromným kľúčom. Jill ju môže dešifrovať pomocou svojho verejného kľúča. Týmto spôsobom je Jill presvedčená, že transakciu uskutočnil John. Jillin verejný kľúč by nefungoval, keby bol Johnov súkromný kľúč zmanipulovaný.

04

Aké sú výhody technológie blockchain?

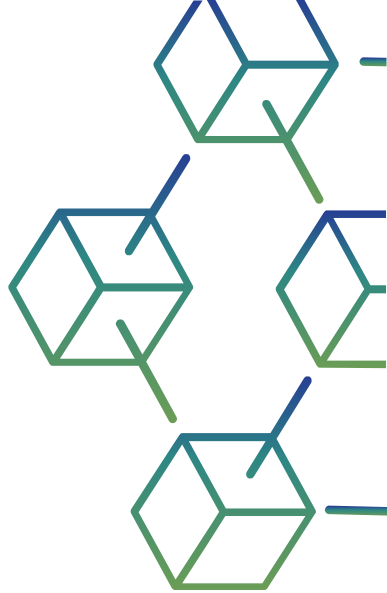
Aké sú výhody technológie blockchain?



Technológia blockchain prináša mnoho výhod pri správe transakcií s aktívami. Niektoré z nich sú uvedené v nasledujúcich podkapitolách:

1. **Pokročilé zabezpečenie**
2. **Zvýšená účinnosť**
3. **Rýchlejší audit**

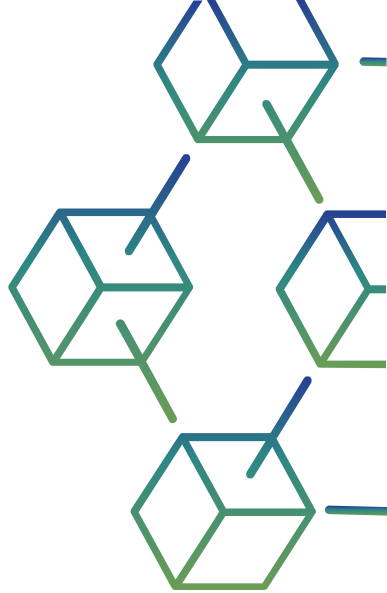
Aké sú výhody technológie blockchain?



1. Pokročilé zabezpečenie

Systémy blockchain poskytujú vysokú úroveň bezpečnosti a dôvery, ktorú si moderné digitálne transakcie vyžadujú. Vždy existuje obava, že niekto bude manipulovať s podkladovým softvérom, aby pre seba vygeneroval falošné peniaze. Blockchain však využíva tri princípy: kryptografiu, decentralizáciu a konsenzus na vytvorenie vysoko bezpečného základného softvérového systému, ktorý je takmer nemožné zmanipulovať. Neexistuje jediný bod zlyhania a žiadny používateľ nemôže zmeniť záznamy o transakciách.

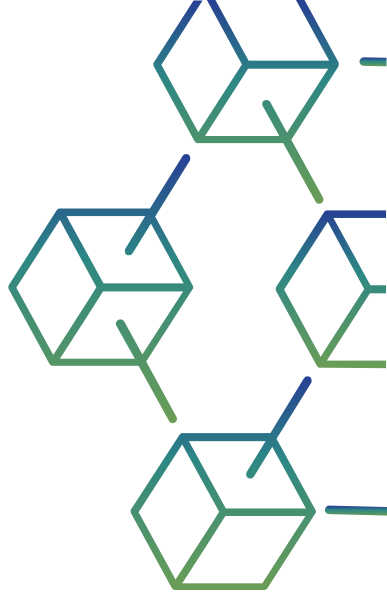
Aké sú výhody technológie blockchain?



2. Zlepšenie účinnosti

Transakcie medzi podnikmi môžu zabrať veľa času a spôsobiť prevádzkové prekážky, najmä ak sú do nich zapojené regulačné orgány tretích strán. Transparentnosť a inteligentné zmluvy na blockchaine takéto obchodné transakcie urýchľujú a zefektívňujú.

Aké sú výhody technológie blockchain?



3. Rýchlejší audit

Podniky musia byť schopné bezpečne vytvárať, vymieňať, archivovať a rekonštruovať elektronické transakcie auditovateľným spôsobom. Záznamy v blockchaine sú chronologicky nemenné, čo znamená, že všetky záznamy sú vždy zoradené podľa času. Vďaka tejto transparentnosti údajov je spracovanie auditu oveľa rýchlejšie.

05

Aký je rozdiel medzi databázou a blockchainom?

Aký je rozdiel medzi databázou a blockchainom?

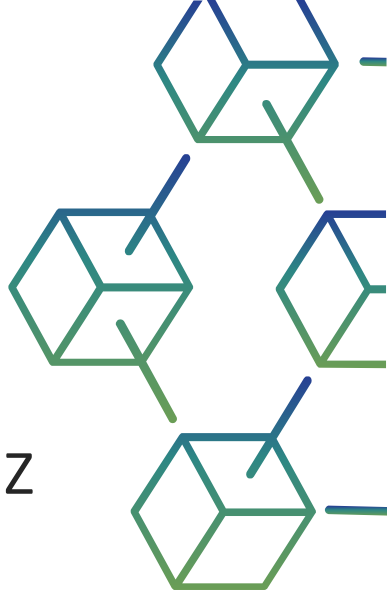
Blockchain je špeciálny typ systému správy databáz, ktorý má viac funkcií ako bežná databáza. Nasledujúci zoznam opisuje niektoré dôležité rozdiely medzi tradičnou databázou a blockchainom:

- Blokové reťazce decentralizujú kontrolu bez toho, aby narušili dôveru v existujúce údaje. To nie je možné v iných databázových systémoch.
- Spoločnosti zapojené do transakcie nemôžu zdieľať celú svoju databázu. V blockchainových sieťach má však každá spoločnosť svoju vlastnú kópiu účtovnej knihy a systém automaticky udržiava konzistenciu medzi týmito dvoma účtovnými knihami.
- Hoci vo väčšine databázových systémov môžete údaje upravovať alebo mazať, v blockchaine môžete údaje iba vkladať.

06

V čom sa blockchain líši od cloudu?

V čom sa blockchain líši od cloudu?



Pojem cloud označuje počítačové služby, ku ktorým možno pristupovať online. Z cloudu môžete pristupovať k softvéru ako službe (SaaS), produktu ako službe (PaaS) a infraštruktúre ako službe (IaaS).

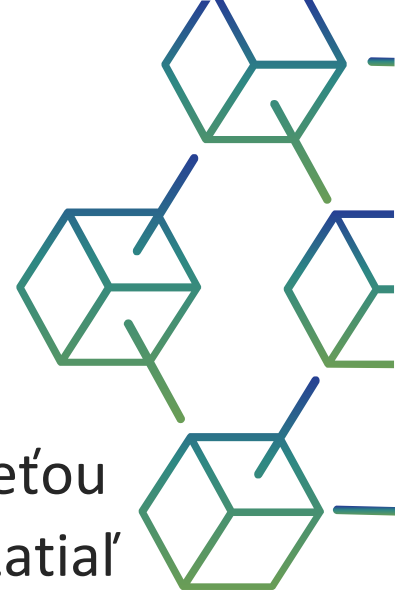
Poskytovatelia cloudu spravujú svoj hardvér a infraštruktúru a poskytujú vám prístup k týmto výpočtovým zdrojom prostredníctvom internetu. Poskytujú oveľa viac zdrojov ako len správu databáz.

Ak sa chcete pripojiť k verejnej sieti blockchain, musíte poskytnúť svoje hardvérové prostriedky na uloženie kópie účtovnej knihy. Na tento účel môžete použiť aj server z cloudu. Niektorí poskytovatelia cloudových služieb ponúkajú aj kompletný blockchain ako službu (BaaS) z cloudu.

07

Čo je blockchain ako služba?

Čo je blockchain ako služba?



Blockchain ako služba (BaaS) je spravovaná služba blockchainu poskytovaná treťou stranou v cloude. Môžete vyvíjať blockchainové aplikácie a digitálne služby, zatiaľ čo poskytovateľ cloudu dodáva infraštruktúru a nástroje na vytvorenie blockchainu.

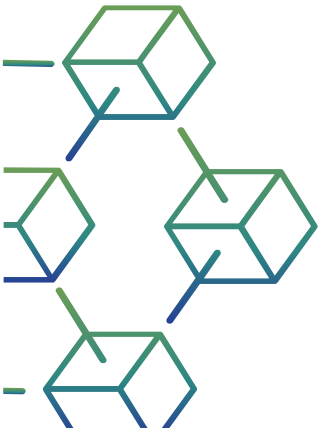
Stačí len prispôsobiť existujúcu technológiu blockchain, aby bolo prijatie blockchainu rýchlejšie a efektívnejšie.

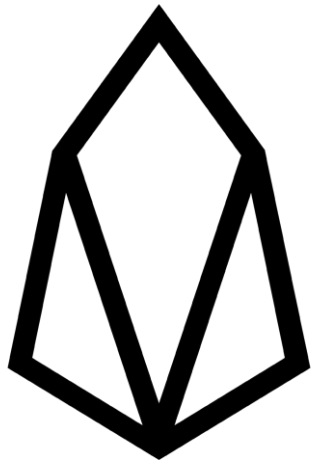
08

Prípadová štúdia

Kryptomena - prvý široko používaný blockchain

- Moderné kryptomeny využívajú blockchain
  - Bitcoin
  - Litecoin
  - Ethereum
  - XRP
  - EOS
  - NEO
  - Hviezdne
  - Monero
  - Dash
  - ...



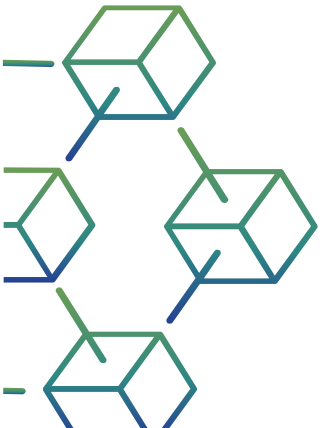


09

Záver

Záver

Technológia blockchain je pokročilý databázový mechanizmus, ktorý umožňuje transparentné zdieľanie informácií v rámci obchodnej siete. Blockchain sa skladá z reťazca blokov, pričom každý blok obsahuje zoznam transakcií a jedinečný identifikátor (hash) predchádzajúceho bloku. Tým sa zabezpečuje integrita údajov. Blokové reťazce sú decentralizované siete, v ktorých sú údaje distribuované medzi viaceré uzly (počítače) v sieti. Neexistuje žiadna centrálna autorita ani jediný kontrolný bod, vďaka čomu sú odolné voči cenzúre a manipulácii. Blockchain je uložený na tisícoch počítačov (uzlov) po celom svete. Každý uzol má kópiu celého blockchainu, vďaka čomu je odolnejší voči výpadkom a útokom.



Video

- Ako funguje blockchain - jednoducho vysvetlené [6:00]
- Blockchain za 7 minút [7:03]
- Vysvetlenie blockchainu [10:23]
- Čo je blockchain? (Animované + príklady) [8:27]
- Vysvetlenie technológie Blockchain (2 hodinový kurz) [1:54:53]
- Základy blockchainu a kryptografie [1:17:37]

Odkazy

- Princípy, typ a aplikácia BlockChainu a prečo by vás to malo zaujímať?
- Zásady návrhu pre blockchain
- Princípy blockchainov
- Zásady úspešného nasadenia blockchainu
- Základné zabezpečenie blockchainu
- Dizajn blockchainu - preskúmajte princípy blockchainu
- Technológia blockchain: princípy a použitie v lekárskom zobrazovaní

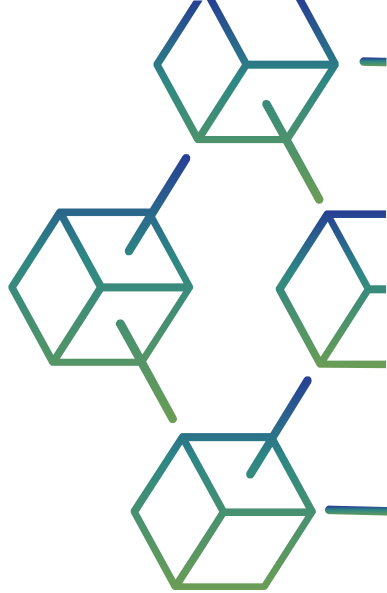
10

Interaktívna vzdelávacia aktivita

Vytvorenie 5 blokov v rámci blockchainu

1. Použite online nástroj na porovnávanie https://emn178.github.io/online-tools/sha256.html
2. Pomocou SHA256 vytvorte hash 5 blokov - obsah nájdete na ďalšom slajde

Vytvorenie 5 blokov v rámci blockchainu



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

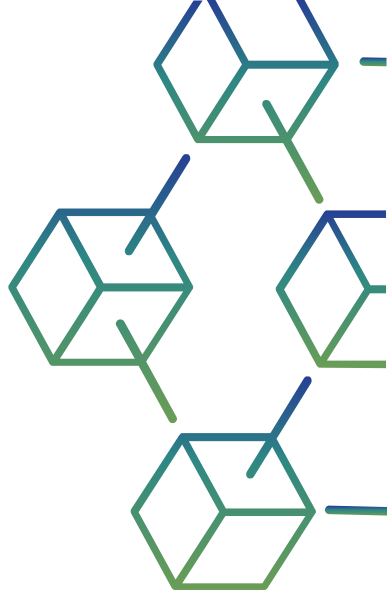
2. Obsah druhého bloku:
   2023-01-01T10:35:28+1,Steve Johnson,Richard McCay,100.00,EUR
   použite hash z hashovacej funkcie prvého bloku

3. Obsah 3. bloku:
   2023-01-01T10:35:33+1,Charles Tann,Elisabeth Bronson,100.00,EUR
   použite hash z hashovacej funkcie bloku 2

4. Obsah 4. bloku:
   2023-01-01T10:35:59+1,Roger Blackburn,Lisa Tann,50.00,EUR
   použite hash z hashovacej funkcie bloku 3

5. Obsah 5. bloku :
   2023-01-01T10:36:01+1,Richard Moss,Edward Morris,85.00,EUR
   použite hash z hashovacej funkcie bloku 4

Vyskúšajte to:



1. Urobte rovnaké malé zmeny v druhom bloku a porovnajte nové hashe
2. Použitie inej hashovacej funkcie - horné menu - Hash
    1. SHA1
    2. SHA2-512
    3. SHA3
    4. ...
3. Použite obsah bloku pre funkciu has

11

Kvíz

Kvíz

1. Aká je kľúčová požiadavka na bezpečnú hašovaciu funkciu:
    a) Odolnosť voči kolízii
    b) Prebytočnosť
    c) Predvídateľnosť
    d) Linearita

Kvíz

2. Čo je charakteristické pre centralizovanú databázovú architektúru?
   a) Jednotný kontrolný bod a autorita
   b) Distribuované ukladanie údajov medzi viacerými uzlami
   c) Autonómne rozhodovanie každého uzla
   d) Vysoká odolnosť voči cenzúre a manipulácii

Kvíz

3. Aká je kľúčová vlastnosť decentralizovanej databázy?
   a) Viac "centrálnych" uzlov
   b) Jednotný kontrolný bod a autorita
   c) Centralizované rozhodovanie určeného uzla
   d) Nízka redundancia a odolnosť voči poruchám

Kvíz

4. Čo je charakteristickým znakom distribuovaného databázového systému?
   a) Údaje sú uložené vo viacerých uzloch siete
   b) Centralizovaná kontrola a autorita nad celou databázou
   c) Nedostatok redundancie na zvýšenie výkonu
   d) Obmedzená škálovateľnosť kvôli architektúre s jedným uzlom

Kvíz

5. Čo najlepšie opisuje hash v kontexte informatiky a kryptografie?

   a) Výstup s pevnou veľkosťou generovaný hašovacou funkciou, ktorý predstavuje jedinečný digitálny podpis vstupných údajov.

   b) Reťazec s premenlivou dĺžkou, ktorý sa používa na ukladanie údajov v databázach

   c) Programová konštrukcia na optimalizáciu vyhľadávania údajov v algoritmoch

   d) Metóda šifrovania v reálnom čase na zabezpečenie komunikačných kanálov

Kvíz

6. Ktorý komponent je zodpovedný za udržiavanie chronologického a nemenného záznamu transakcií v blockchaine?

   a) Blok

   b) Uzol

   c) Inteligentné zmluvy

   d) Algoritmus konsenzu

Kvíz

7. **Aký je hlavný rozdiel medzi blockchainom a tradičnou databázou?**

   a) Blockchain ponúka decentralizovanú a distribuovanú správu, zatiaľ čo tradičné databázy sú zvyčajne centralizované.

   b) Tradičné databázy poskytujú rýchlejšie spracovanie transakcií v porovnaní s pomalšou povahou blockchainu

   c) Blockchain sa spolieha na jediný kontrolný bod, zatiaľ čo tradičné databázy využívajú na kontrolu distribuovanú sieť.

   d) Tradičné databázy sú zo svojej podstaty odolné voči manipulácii, zatiaľ čo blockchain je náchylnejší na manipuláciu s údajmi.

Kvíz

8. Kde bola technológia blockchain prvýkrát implementovaná?
    a) Financie a kryptomena
    b) Zdravotná starostlivosť a lekárske záznamy
    c) Sociálne médiá a siete
    d) Elektronický obchod a online maloobchod

https://blockchainforagrifood.eu/

Ďakujem

Priestor na otázky

BLOCK CHAIN FOR AGRI FOOD EDU

Co-funded by the European Union

Financované Európskou úniou. Vyjadrené názory a postoje sú názormi a vyhláseniami autora(-ov) a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie alebo Európskej výkonnej agentúry pre vzdelávanie a kultúru (EACEA). Európska únia ani EACEA za ne nepreberajú žiadnu zodpovednosť.