EKONOMICKÁ UNIVERZITA V BRATISLAVE
FAKULTA HOSPODÁRSKEJ INFORMATIKY
Evidenčné číslo:103002/I/2020/360971078407482 92

MOŽNOSTI VYUŽITIA TECHNOLÓGIE BLOCKCHAIN PRI ZOSTAVOVANÍ A OVEROVANÍ ÚČTOVNEJ ZÁVIERKY

Diplomová práca

2020 **Bc. Patrícia Šišoláková**

EKONOMICKÁ UNIVERZITA V BRATISLAVE
FAKULTA HOSPODÁRSKEJ INFORMATIKY

MOŽNOSTI VYUŽITIA TECHNOLÓGIE BLOCKCHAIN PRI ZOSTAVOVANÍ A OVEROVANÍ ÚČTOVNEJ ZÁVIERKY

Diplomová práca

Študijný program:	Účtovníctvo a audítorstvo
Študijný odbor:	Ekonómia a manažment
Vedúci práce:	prof. Ing. Miloš Tumpach, PhD.
Školiace pracovisko:	Katedra účtovníctva a audítorstva

Bratislava 2020 **Bc. Patrícia Šišoláková**

Ekonomická univerzita v Bratislave
Fakulta hospodárskej informatiky

3609710784074829 2

ZADANIE ZÁVEREČNEJ PRÁCE

Meno a priezvisko študenta:	Bc. Patrícia Šišoláková
Študijný program:	účtovníctvo a audítorstvo (Jednoodborové štúdium, inžiniersky II. st., denná forma)
Študijný odbor:	ekonómia a manažment
Typ záverečnej práce:	Inžinierska záverečná práca
Jazyk záverečnej práce:	slovenský
Sekundárny jazyk:	anglický

Názov: Možnosti využitia technologie blockchain pri zostavovaní a overovaní účtovnej závierky

Anotácia: Technológia blockchain predstavuje systém umožňujúci validáciu dát s využitím distribuovaných databáz. Hoci sa v odbornej verejnosti spája predovšetým s kryptomenami, jej využittie je ďaleko širšie. V rámci účtovníctva sa môže uplatňovať predovšetkým tam, kde je potrebné zabezpečiť konfirmáciu existencie transakcií, zostatku majetku a záväzkov a súčasne tam, kde je potrebné zabezpečiť integritu účtovných záznamov.

Vedúci:	prof. Ing. Miloš Tumpach, PhD.
Katedra:	KÚA FHI - Katedra účtovníctva a audítorstva FHI

Dátum zadania: 17.10.2018

Dátum schválenia: 21.10.2018

prof. Ing. Miloš Tumpach, PhD.
vedúci katedry

ABSTRAKT

ŠIŠOLÁKOVÁ, Patrícia: *Možnosti využitia technológie blockchain pri zostavovaní a overovaní účtovnej závierky*. – Ekonomická univerzita v Bratislave. Fakulta hospodárskej informatiky; katedra účtovníctva a audítorstva. – Vedúci záverečnej práce: prof. Ing. Miloš Tumpach, PhD. – Bratislava: FHI EU, 2020, 57 s.

Cieľom záverečnej práce je zhodnotiť problematiku technológie blockchain a identifikovať nedostatky súčasne využívaných postupov, ktoré ponúkajú priestor pre zlepšenie práve jej aplikáciou. Rovnako je cieľom navrhnúť možnosti uplatnenia tejto technológie v oblasti účtovníctva a audítorstva. Práca sa skladá z troch častí, teoretickej, metodickej a aplikačnej. Záverečná práca obsahuje osem obrázkov, desať schém a jednu tabuľku. Teoretická časť sa venuje technickým poznatkom, ktoré sú nevyhnutné pre porozumenie fungovania technológie a následnú identifikáciu jej všeobecných výhod a možností riešenia existujúcich nedostatkov súčasných technológií a postupov. Rovnako je obsahom zhodnotenie aktuálneho stavu v rámci oblasti účtovníctva a audítorstva, ktorému sa venujeme v závere prvej časti. Metodickú časť tvorí opis zvolených metód a postupov na dosiahnutie cieľa práce. Aplikačná časť záverečnej práce je tvorená sumarizáciou výhod tejto technológie pre oblasť účtovníctva a audítorstva, a ich následnou aplikáciou na konkrétne príklady. Táto časť nám poskytla podklad a potvrdila tým opodstatnenosť tvrdenia zhodnoteného v závere.

Kľúčové slová: blockchain, účtovníctvo, databáza, šifrovanie

ABSTRACT

ŠIŠOLÁKOVÁ, Patrícia: *Applicability of the blockchain technology for the compilation and audit of the financial statements.* - University of Economics in Bratislava. Faculty of Economic Informatics; Department of Accounting and Auditing. - Advisor: prof. Ing. Miloš Tumpach, PhD. - Bratislava: FHI EU, 2020, 57 p.

The aim of the diploma thesis is to evaluate blockchain technology and identify deficiencies of currently used methods, which could be solved and improved through application of the blockchain. The another aim of diploma thesis is to suggest the application possibilities of this technology in accounting and auditing industry. The thesis consists of three parts, theoretical, methodological and application. The diploma thesis contains eight pictures, ten diagrams and one table. The theoretical part deals with the technical knowledge that is necessary to understand the functioning of the technology and the subsequent identification of its general advantages and possibilities of solving the existing deficiencies of current technologies and processes. The thesis also includes an evaluation of the current state in the accounting and auditing industry, which we discuss in the end of the first part. The methodical part consists of a description of selected methods and procedures to achieve the aim of the thesis. The application part of the diploma thesis consists of summarizing the benefits of this technology in accounting and auditing industry, and their subsequent application to specific examples. This part provided us with a material, that confirmed the validity of the statement evaluated in the conclusion.

Keywords: blockchain, accounting, ledger, hashing, transaction

Zoznam obrázkov

Obrázok 1 Architektúry distribuovaných systémov 14
Obrázok 2 Proces hashingu vstupných dát v aplikácií blockchain 20
Obrázok 3 Digitálny podpis 31
Obrázok 4 Fungovanie smart kontraktov 40
Obrázok 5 Porovnanie tradičnej zmluvy a smart kontraktu 41
Obrázok 6 Verifikácia zabezpečujúca integritu dát v blockchain-data štruktúre 46
Obrázok 7 Verifikácia dát eliminujúca potrebu konfirmácie údajov 47
Obrázok 8 Mechanizmus konsenzu zabezpečujúci správnosť údajov 50

Zoznam schém

Schéma 1 Princíp prepojenia v distribuovanom systéme blockchain 17
Schéma 2 Druhy hash hodnôt podľa použitej hash funkcie 21
Schéma 3 Štruktúra bloku 22
Schéma 4 Pridávanie transakcii do štruktúry blockchain-data 23
Schéma 5 Pridávanie transakcií do štruktúry blockchain-data - Krok 1 23
Schéma 6 Pridávanie transakcií do štruktúry blockchain-data - Krok 2 24
Schéma 7 Pridávanie transakcií do štruktúry blockchain-data - Krok 3 24
Schéma 8 Zdieľanie dát v rámci plnohodnotných uzlov 25
Schéma 9 Zdieľanie dát v rámci odľahčených uzlov 26
Schéma 10 Porušenie blockchain-data štruktúry 26

Zoznam tabuliek

Tabuľka 1 Porovnanie auditu teraz a po zavedení technológie blockchain 52

Obsah

ÚVOD 9

1 SÚČASNÝ STAV RIEŠENEJ PROBLEMATIKY DOMA A V ZAHRANIČÍ 11

1.1 LEGISLATÍVNY RÁMEC VYUŽITIA BLOCKCHAINU V EÚ A SR 11

1.2 TECHNOLÓGIA BLOCKCHAIN 14

1.2.1 Blockchain ako distribuovaný systém typu peer-to-peer 14

1.2.2 Princíp prepojenia uzlov v distribuovanom systéme blockchain 17

1.2.3 Spôsob kódovania dát v technológií blockchain 18

1.2.4 Štruktúra blokov v rámci technológie blockchain 21

1.2.5 Pridávanie transakcií do štruktúry blockchain-data 23

1.2.6 Zdieľanie dát v blockchaine 25

1.2.7 Uchovávanie dát a zmeny v transakciách 26

1.2.8 Verifikácia transakcií prostredníctvom mechanizmu konsenzov 28

1.2.9 Proces autorizácie transakcií 30

1.3 VYUŽITIE TECHNOLÓGIE BLOCKCHAIN V ÚČTOVNÍCTVE A AUDÍTORSTVE 31

1.3.1 Kľúčové vlastnosti blockchainu pre oblasť účtovníctva a audítorstva 33

1.3.2 Vplyv metódy blockchain na finančný sektor 34

1.3.3 Potenciál využitia technológie blockchain pre účtovníctvo 35

1.3.4 Súčasné a potenciálne blockchain aplikácie 37

1.3.4.1 Vnútrobankové zosúlaďovanie dát 37

1.3.4.2 Blockchainová aplikácia katastra nehnuteľností 38

1.3.4.3 Blochainová aplikácia Smart kontrakty 39

1.3.5 Potenciál technológie blockchain v oblasti audítorstva 42

2 CIEĽ PRÁCE, METODIKA PRÁCE A METÓDY SKÚMANIA 43

3 VÝSLEDKY PRÁCE A DISKUSIA 45

3.1 VÝHODY TECHNOLÓGIE BLOCKCHAIN PRE OBLASŤ ÚČTOVNÍCTVA A AUDÍTORSTVA 45

3.1.1 Integrita záznamov 45

3.1.2 Zníženie potreby konfirmácií existencie transakcií, zostatku majetku a záväzkov 47

3.1.3 Odstránenie potreby existencie správcovskej centrálnej entity 48

3.1.4 Eliminácia príležitostí na nezákonné a nemorálne konanie podvody, korupcia, sprenevera majetku, daňové úniky 49
3.1.5 Posilnenie istoty správnosti, jednotnosti a bezpečnosti histórie transakcií 50
3.1.6 Eliminácia potreby fyzickej papierovej formy uchovávania dát a zníženie nákladov a úspora času 51
3.2 PERSPEKTÍVY AUDITU Z POHĽADU VYUŽITIA TECHNOLÓGIE BLOCKCHAIN 52
ZÁVER 53
POUŽITÁ LITERATÚRA 55

Úvod

V posledných rokoch môžeme sledovať rapídny nárast nových prelomových inovácií v oblasti technológií. Spomedzi všetkých nových riešení digitalizácie transakcií je dnes najsľubnejším dostupným technológia blockchain, ktorá má potenciál pretvoriť súčasné hospodárstvo. Finančný sektor by zavedením tejto technológie s najväčšou pravdepodobnosťou prešiel revolučnou zmenou. Blockchain fungujúci na princípe zdieľaného konsenzu predstavuje skutočnú inováciu mnohých systémov a procesov uchovávania a zabezpečovania dát používaných v súčasnosti. Z dlhodobého hľadiska môže ovplyvniť globálny ekonomický systém, zmenu štruktúry trhu, skúsenosti zákazníkov a vlastnosti produktu. Napriek tomu, že táto technológia vzbudila pozornosť mnohých najväčších finančných inštitúcií, možnosti implementácie do praxe sú stále v experimentálnej fáze.

Blockchain predstavuje distribuovanú bázu údajov poskytujúcu nemenný, spoľahlivý a zdieľaný pohľad na transakcie ako napríklad prevody peňažných prostriedkov, záznamy o majetku alebo rôzne iné záznamy. Báza je distribuovaná medzi všetky zapojené uzly v prostredí, ktoré nemusí byť úplne dôveryhodné. Jedinečné vlastnosti tejto technológie umožňujú inštitúciám pracovať oveľa rýchlejšie, lacnejšie, s nižšou chybovosťou, s menším rizikom, s nižšou kapitálovou požiadavkou a menšou zraniteľnosťou voči kybernetickým útokom.

Aktuálne je využívanie decentralizovaného zdieľania dát v účtovníctve a audítorstve v porovnaní s inými odvetviami ešte len v začiatkoch. Jedným z hlavných dôvodov sú výnimočne vysoké nároky na regulačné požiadavky týkajúce sa zabezpečenia správnosti a integrity záznamov. Technológia blockchain je vybudovaná tak, aby každá zmena, skresľovanie alebo manipulácia s dátami bola nemožná alebo neprimerane nákladná. Na dosiahnutie tohto cieľa využíva vnútorné mechanizmy vzájomnej kontroly a konsenzov. Medzi ďalšie prednosti technológie patrí pravidelné automatické auditovanie rozsiahlej databázy údajov, ktoré v súčasnosti prebieha manuálne a je náročné na prácu.

Cieľom diplomovej práce je zhodnotenie technológie blockchain, ktorá predstavuje systém umožňujúci validáciu dát s využitím distribuovaných databáz. V odbornej verejnosti je táto technológia spájaná najmä s kryptomenami, má však ďaleko širšie uplatnenie. V účtovníctve má predovšetkým využitie v oblastiach, kde je potrebné

zabezpečiť konfirmácie existencie transakcií, zostatku majetku a záväzkov a integritu záznamov.

Diplomová práca je rozdelená do troch kapitol. Prvá kapitola opisuje súčasný stav využívania metódy blockchain doma a v zahraničí. Zamerali sme sa na princípy fungovania blockchainu, vďaka ktorým dokáže reagovať na súčasné trendy v znižovaní nákladov a zrýchľovania transakcií. V závere prvej kapitoly sú uvedené možnosti využitia technológie blockchain v oblasti účtovníctva a audítorstva a jej implementáciu s cieľom zjednodušiť a zefektívniť procesy pri zostavovaní a overovaní účtovnej závierky. Druhá kapitola sa venuje cieľu diplomovej práce a použitým metódam skúmania. Záverečná kapitola je aplikačnou časťou práce, v ktorej uvádzame súhrn výhod implementácie technológie blockchain v rôznych oblastiach účtovníctva a audítorstva. Na jednotlivých príkladoch znázorňujeme uchovávanie dát a uskutočňovanie účtovných transakcií prostredníctvom blockchain aplikácie. Súčasťou tejto kapitoly je aj porovnanie momentálne používaných audítorských postupov a ich priebehu v prípade využitia blockchainu.

K výskumu možností a potenciálu technológie blockchain prispievajú aj spoločnosti z rôznych odvetví či už účtovníctva, audítorstva, zdravotníctva, prostredníctvom štúdií venujúcich sa hlavným prínosom pri zavedení technológie blockchain do praxe.

1 Súčasný stav riešenej problematiky doma a v zahraničí

Blockchain je technológia ukladania údajov, ktorá uchováva dáta s digitálnou hodnotou. Každá nová transakcia je uložená do bloku, ktorý sa pridáva k reťazcu už existujúcich záznamov. Typický blockchain duplikuje údaje v otvorenej sieti, takže všetky strany zúčastnené v blockchain sledujú aktualizácie súčasne a všetky aktualizácie sa overujú prostredníctvom verejného overovacieho procesu, ktorý zaisťuje presnosť bez potreby ústredného orgánu, napríklad banky.

Podľa Institute of Chartered Accountants in England and Wales (2020) nastalo vo vývoji technológie blockchain doposiaľ (2020) šesť významných medzníkov. V roku 1991 v článku o digitálnych pečiatkach opísali Haber a Stornetta prvýkrát kryptograficky zabezpečený reťazec blokov. Peck (2012) opisuje ďalší posun vo vývoji technológie blockchain, ktorým bolo navrhnutie mechanizmu pre decentralizovanú digitálnu menu nazvanú „bit gold“ uskutočnené Nickom Szabom v roku 1998. Tá však nikdy nebola implementovaná, ale považuje sa za predchodcu architektúry bitcoin. Následne v roku 2000 opísal svoju teóriu kryptograficky zabezpečených reťazcov a nápadov na implementáciu Konst. Vývojári pracujúci pod pseudonymom Satoshi Nakamoto vydali v roku 2008 diskusný materiál *Bitcoin: A Peer-to-Peer Electronic Cash System* s teoretickým návrhom modelu blockchain. O rok na to (2009) bola prvýkrát implementovaná blockchain verejná báza pre transakcie s kryptomenami, uskutočňované prostredníctvom Satoshiho softvéru Blockchain 1.0. V roku 2014 vzniklo konzorcium R3, spájajúce viac ako štyridsať významných finančných spoločností, vďaka ktorému sa zrodil Blockchain 2.0. Tento rok bol prelomovým, pretože išlo o implementáciu technológie blockchain mimo digitálnu menu. Vznikla otvorená programová platforma Ethereum blockchain, ktorá umožnila fungovanie smart contractov. (Hosp, J. 2019).

Vychádzajúc z údajov zverejnených na stránke www.101blockchains.com viedlo úspešné uplatnenie blockchainu aj mimo kryptomien k vypracovaniu blockchain protokolu, ktorý rozširuje možnosti využitia. Od roku 2018 bolo na základe tohto protokolu spustených niekoľko projektov vyvíjajúcich nové aplikácie. Viaceré z nich sú spomenuté v podkapitole 1.3.4.

1.1 Legislatívny rámec využitia blockchainu v EÚ a SR

Blockchain technológia poskytuje možnosť mnohým distribuovaným softvérovým aplikáciám ukladať a sprístupňovať dáta metódou poskytujúcou vysokú

dôveryhodnosť, integritu a dostupnosť dát. Stále má však niekoľko nedostatkov, ktoré bránia v jednoduchom zavedení tejto technológie vo všetkých odvetviach. Ide najmä absenciu nadnárodnej aj národnej právnej úpravy vyvolávajúcej otázky v oblasti daní, obchodno-právnych vzťahov, ochrany spotrebiteľa.

Európska únia spočiatku nezaujala pozitívny postoj k využívaniu technológie blockchain ako legitímneho spôsobu fungovania transakcií. Táto technológia je vo svete známa najmä v súvislosti s kryptomenami, ktoré sa stále viac používajú aj na nezákonné činnosti, ako je pranie špinavých peňazí, financovanie terorizmu a iné. Podľa štúdie Houbena a Snyearsa (2018) vypracovanej na žiadosť výboru Európskeho parlamentu TAX3, je hlavným problémom nedostatočná identifikácia používateľov digitálnych aplikácií. To poskytuje priestor na nezákonné konanie a znižuje pravdepodobnosť odhalenia páchateľa. Túto problematiku upravuje *Smernica Európskeho parlamentu a Rady (EÚ) 2018/843 z 30. mája 2018, ktorou sa mení smernica (EÚ) 2015/849 o predchádzaní využívaniu finančného systému na účely prania špinavých peňazí alebo financovania terorizmu a smernice 2009/138/ES a 2013/36/EÚ* označovaná skratkou AMLD. Obsahuje definície virtuálnych mien a subjektov poskytujúcich služby výmeny virtuálnej meny a poskytovateľov úschovy virtuálnej meny podľa požiadaviek týkajúcich sa povinnej starostlivosti o zákazníka a povinnosti nahlasovať podozrivé transakcie finančným spravodajským jednotkám. Získané informácie môžu používať aj daňové orgány na boj proti daňovým podvodom. Blockchain zasahuje svojím využívaním do platobného styku. Túto oblasť upravuje *Smernica Európskeho parlamentu a Rady (EÚ) 2015/2366 z 25. novembra 2015 o platobných službách na vnútornom trhu, ktorou sa menia smernice 2002/65/ES, 2009/110/ES a 2013/36/EÚ a nariadenie (EÚ) č. 1093/2010 a ktorou sa zrušuje smernica 2007/64/ES* známa pod skratkou PSD2. Uplatnenie blockchainu je však omnoho širšie, čo vníma aj Európska únia a preto založila pracovnú skupinu European Blockchain Partnership.

Pri blockchaine je často spomínaný nesúlad s nariadením General Data Protection Reguation (GDPR), ktoré sa stalo platným v roku 2018. Z tohto dôvodu vydalo EU Blockchain Observatory and Forum v októbri 2018 správu názvom Blockchain v súlade s GDPR, ktorá vysvetľuje, že zabezpečenie ochrany osobných údajov sa netýka samotnej technológie blockchain, ale spôsobu jej využívania.

Ďalšou oblasťou regulácie je samotná *decentralized ledger technology* (DLT) v preklade technológia decentralizovanej databázy. Tento termín sa používa na označenie

technológie, medzi ktoré zaraďujeme aj blockchain. DLT umožňuje zdieľanie záznamov na viacerých miestach v tom istom čase v rámci počítačovej siete. Podľa Houbena a Snyearsa (2018) by sa Únia mala riadiť zásadou technologickej neutrality, mala by byť naklonená inováciám a nemala regulovať DLT ako takú, ale mala by sa snažiť odstrániť existujúce prekážky pri implementácii technológie blockchain, aby podporila harmonizáciu právnych predpisov.

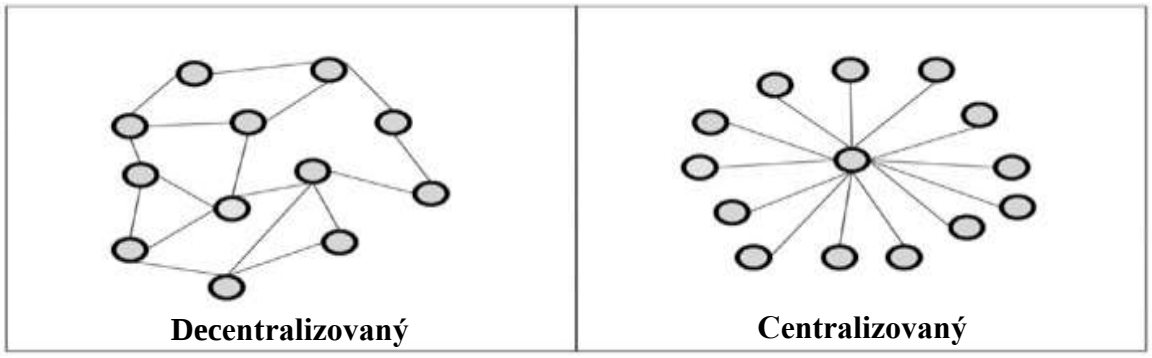
Postoj vlády Slovenskej republiky k distribuovaným technológiám vrátane blockchainu, vystihujú dokumenty schválené uznesením vlády v roku 2019. Ide o *Akčný plán digitálnej transformácie Slovenska na roky 2019-2022*, ktorý priamo nadväzuje na nadrezortnú *Stratégiu digitálnej transformácie Slovenska 2030*. Potreba ich schválenia vychádzala z prebiehajúcej globálnej digitalizácie hospodárstva a odporúčaní a záväzkov európskych politík alebo priamo z dohôd členských štátov. Zvyšujúcim sa využívaním metódy blockchain vo svete vláda deklaruje poskytnutie podpory *Slovenskému centru pre výskum umelej inteligencie* za účelom zabezpečenia základného výskumu, jeho implementácie a prepojenia akademickej, štátnej a podnikateľskej sféry.

Právna úprava platobných služieb v Slovenskej republike ako člena Európskej únie vychádza z aj nadnárodnej legislatívy prostredníctvom povinnosti implementácie. Smernica PSD 2 bola transponovaná do *zákona č. 492/2009 Z. z. o platobných službách a o zmene a doplnení niektorých zákonov*, ktorý upravuje reguláciu v oblasti poskytovania platobných služieb prostredníctvom fintech spoločností, zvyšovania bezpečnosti a vyššej ochrany spotrebiteľa. Jej cieľom je harmonizácia trhu elektronických platieb v rámci celého paneurópskeho priestoru, v súlade s rozvojom digitálnych platieb a inováciami. Z hľadiska bezpečnosti spracovávaných údajov musí blockchain spĺňať aj požiadavky *zákona č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov vychádzajúci z Nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679.* V prípade implementácie technológie blockchain v rámci Slovenskej republiky v oblasti účtovníctva a audítorstva je potrebné, aby boli používané aplikácie v súlade so *zákonom č. 431/2002 Z. z. o účtovníctve,* s postupmi účtovania pre podnikateľov účtujúcich v sústave podvojného účtovníctva, audítorskými štandardmi a ostatnými právnymi rámcami upravujúce túto oblasť.

1.2 Technológia blockchain

Distribuovaný systém zdieľania dát má veľa možností využitia. Jedným zo základných atribútov, ktorými sa tieto systémy líšia je ich architektúra, ktorá definuje akým spôsobom sú jeho zložky usporiadané a navzájom prepojené. Dresher (2017) uvádza, že v súčasnosti sú známe dve hlavné architektúry distribuovaného zdieľania dát, a to centralizovaná a decentralizovaná (Obrázok 1).

Obrázok 1 Architektúry distribuovaných systémov



Na obrázku 1 sú znázornené dve odlišné architektúry distribuovaných systémov. *Body* predstavujú súčasti systému, nazývané uzly a *čiary* predstavujú prepojenia medzi nimi. Podrobnosti o tom, čo sú tieto uzly a aké informácie sa medzi nimi vymieňajú, si vysvetlíme neskôr v podkapitole 1.2.2. Na ľavej strane obrázku 1 je znázornená decentralizovaná architektúra, kde sú uzly navzájom prepojené bez toho, aby mali jeden centrálny prvok. Treba si všimnúť, že žiaden z uzlov v sieti nie je *priamo* spojený s každým uzlom, ale všetky sú navzájom prepojené *nepriamo*. Pravá strana obrázku 1 zobrazuje centralizovanú architektúru, pri ktorej má každý uzol iba jedno priame spojenie, a to s centrálnym komponentom. Tieto uzly nemajú medzi sebou iné priame spojenie. Vzájomne sú prepojené iba nepriamo, prostredníctvom centrálneho komponentu.

1.2.1 Blockchain ako distribuovaný systém typu peer-to-peer

Blockchain technológia predstavuje distribuovaný systém typu peer-to-peer umožňujúci ukladať, uchovávať a sprístupňovať dáta, spôsobom zaručujúcim vysokú mieru dostupnosti, dôvernosti a integrity. Siete typu peer-to-peer sú s malou odchýlkou ekvivalentom distribuovaných decentralizovaných systémov. Skladajú sa z jednotlivých uzlov, ktorými sú počítače. Tie sprístupňujú svoje výpočtové zdroje, napríklad výkon a úložnú kapacitu ďalším uzlom bez toho, aby mali centrálny koordinačný bod. Ako uvádza Drescher (2017), systém peer-to-peer využívajúci internet ako prostriedok komunikácie

je charakterizovaný nasledujúcimi skutočnosťami. Každý počítač je označený jedinečnou identifikačnou adresou. Používateľ sa môže kedykoľvek odpojiť a znova pripojiť do siete. Počítač nezávisle vedie zoznam rovnocenných uzlov, s ktorými komunikuje. Komunikácia medzi uzlami je založená na správach, ktoré sa odosielajú z jedného uzla do druhého prostredníctvom internetu.

Oram (2001) uvádza, že uzly v sieti peer-to-peer sú si rovné, pokiaľ ide o ich práva a úlohy v systéme. Okrem toho sú všetci dodávateľmi a zároveň aj spotrebiteľmi zdrojov. Tieto systémy majú veľký potenciál pretvoriť celé hospodárstvo na základe jednoduchej myšlienky, ktorou je nahradiť sprostredkovateľa interakciami typu peer-to-peer. Nakoľko základnou vlastnosťou tejto technológie je práve absencia centrálnej entity, pri vývoji sa vychádzalo z požiadaviek, aby systém dokázal fungovať aj v prípade, ak nebude známy počet uzlov, ich dôveryhodnosť ani miera spoľahlivosti. Zároveň musí byť schopný zabezpečiť správu *vlastníctva*. Na základe toho Drescher (2017) identifikoval sedem oblastí, ktoré musia byť vyriešené v rámci blockchainu: opis *vlastníctva, ochrana vlastníctva, ukladanie údajov o transakciách, príprava bázy údajov na distribúciu v nedôveryhodnom prostredí, distribúcia báz, možnosť pridávania nových transakcií do bázy a identifikácia správnosti bázy*.

Vlastníctvo je podľa §123 Občianskeho zákonníka všeobecne definované ako právo vlastníka, mať predmet vlastníctva v držbe, využívať ho, alebo s ním nakladať (zákon č. 40/1964 Zb.) Môže ísť napríklad o vlastníctvo nehnuteľností, dopravných prostriedkov alebo duševné vlastníctvo. Vlastníctvo, ktoré vymedzuje slovenský právny systém, nepredstavuje *vlastníctvo* z pohľadu blockchainu. Daisyme (2019) ho opisuje ako prevod existujúcich hmotných aj nehmotných aktív do zrkadlových digitálnych hodnôt , ku ktorým sú pridávané ďalšie doplňujúce údaje kedy, v akom čase, od koho, prípadne za koľko sa prevádzali. Tieto digitálne záznamy tvoria úplnú overiteľnú históriu vlastníctva. Podobne, aj účtovníctvo vedie údaje o aktívach v symbolických záznamoch. Hlavným rozdiel blockchainu oproti účtovníctvu je, že účtovníctvo vedie len poslednú informáciu o súčasnom vlastníkovi.

Ďalšou dôležitou oblasťou blockchainu je *ochrana vlastníctva*. Drescher (2017) uvádza, že potrebujeme spôsob, ktorým zabránime neoprávneným používateľom v prístupe k majetku iných. V skutočnom živote dokážeme ľahko zabrániť ostatným používať naše vozidlo alebo vstúpiť do domu. Kryptografia ponúka spôsob ochrany transakcií na individuálnej úrovni, podobne ako zamknuté dvere chránia naše súkromné auto alebo

dom. Ochrana vlastníctva má tri hlavné prvky, ktorými sú identifikácia vlastníka, overenie totožnosti vlastníka a obmedzenie prístupu neoprávneným osobám. Tieto hlavné prvky fungujú na koncepcií hash hodnôt, ktorým sa budeme venovať osobitne v podkapitole 1.2.3.

Najlepší spôsob zaznamenania prevodu vlastníctva je transakcia teda digitálny prevod. Tá predstavuje v rámci blockchainu proces prevodu digitálneho práva z jedného vlastníka na druhého. Z hľadiska identifikácie vlastníkov, je podľa Dreschera (2017) dôležité, aby táto technológia umožňovala uchovávať *kompletnú históriu transakcií*. Napríklad si predstavme, že by sa v reálnom živote objavili dve identické knihy od rôznych autorov. Skutočný autor by oproti falšovateľovi vedel predložiť celý vývoj práce prostredníctvom pracovných verzií z rôznych časov, zahŕňajúce zmeny, chyby a úpravy diela. Vďaka tomu by ľahko dokázal, že pravým vlastníkom je on. Na rovnakom princípe je zabezpečené preukázanie pravosti vlastníka aj v blockchaine. Údaje o pôvode a zmenách vlastníkov sú ukladané do jednotlivých blokov vytvárajúcich históriu formou decentralizovanej databázy označovanej ako *štruktúra blockchain-data*. Procesu tvorby blokov sa detailne venuje podkapitola 1.2.4.

Technológia blockchain funguje ako *open source*, čo znamená, že ide o voľne dostupné zdrojové kódy s možnosťou ďalšej distribúcie. Tým, že umožňuje pripojiť sa do siete ľubovoľnému používateľovi, *prostredie* v ktorom sú kópie dát zdieľané *sa stáva nedôveryhodným* (Parisi, 2019). Nakoľko je zodpovednosť za kontrolu prenesená na všetky uzly bez existencie centrálneho bodu koordinácie, je potrebné zabrániť falšovaniu alebo manipulácii s údajmi. Z tohto dôvodu sú zdieľané identické kópie blockchain-data štruktúry na všetkých uzloch pripojených do systému. V praxi to znamená, že ak by nastal vyššie spomínaný prípad s dvoma rovnakými dielami od rôznych autorov, pravosť autora by potvrdili všetci ostatní používatelia, vďaka zaslaným identickým kópiám záznamov o vývoji diela.

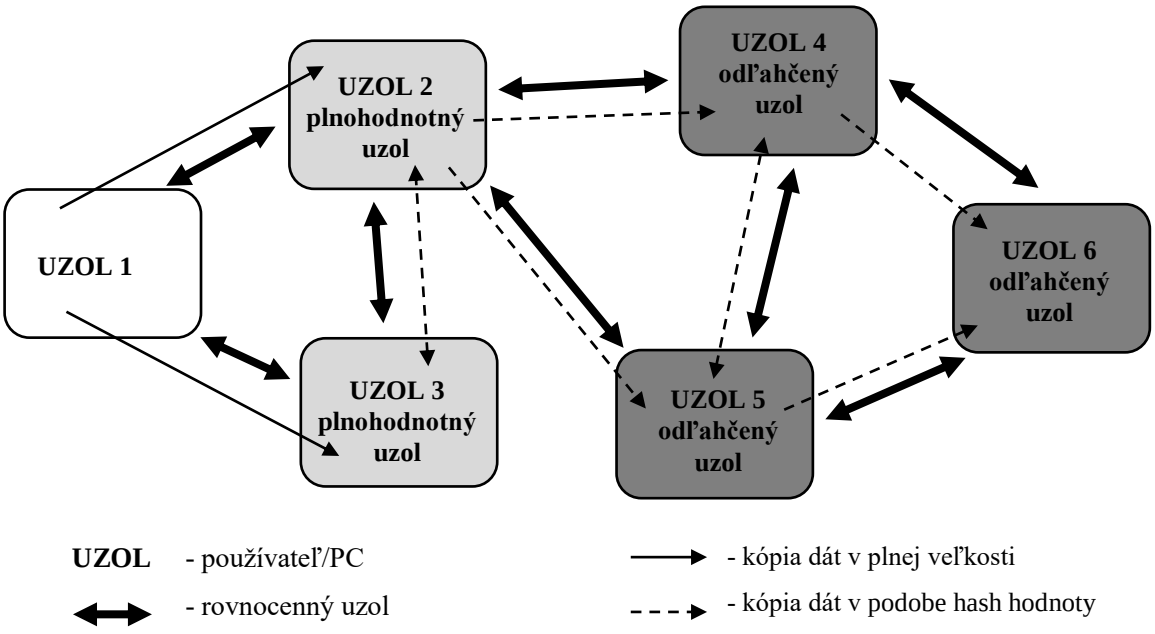
Nakoľko blockchain *umožňuje pridávať nové transakcie* je potrebné zaistiť, aby boli do bázy pridané iba tie, ktoré sú správne, platné a autorizované. Parisi (2019) uvádza, že technológia to zabezpečuje tým, že každý uzol siete môže pridávať nové transakcie, ale zároveň je aj supervízorom všetkých pripojených uzlov. Umožnením pridávania nových transakcií všetkým uzlom sa môže stať, že boli distribuované rozdielne dáta a história transakcií u jednotlivých uzlov by sa tak líšila, čo predstavuje vážnu hrozbu narušenia integrity systému. Preto je dôležité nájsť spôsob ako *identifikovať správnu históriu*

transakcií. Drescher (2019) uvádza, že vzhľadom na povahu čisto distribuovaného systému typu peer-to-peer nie je možné vzniku rôznych histórií transakcií zabrániť. Tento problém rieši zadefinovaním kritéria, ktoré spočíva v tom, že každý uzol v systéme sám rozhodne, ktorá z histórií transakcií je tá pravdivá. Za správnu sa označí tá, na ktorej sa väčšina uzlov nezávisle zhodla a následne sa ostatné histórie podľa nej aktualizujú.

1.2.2 Princíp prepojenia uzlov v distribuovanom systéme blockchain

Hlavný princíp prepojenia uzlov a rozposielania dát v distribuovanej sieti s cieľom lepšie porozumieť vlastnostiam a výhodám technológie blockchain, opisovaných v nasledujúcich kapitolách znázorňuje Schéma 1. Pri jej spracovaní sme vychádzali z informácií uvedených v štúdií Ernst&Young z roku 2018. Každý uzol predstavuje konkrétneho používateľa, ktorý sa dobrovoľne pripojí do príslušnej aplikácie blockchain prostredníctvom počítača. Následne systém automaticky a nezávisle priradí novému užívateľovi zoznam rovnocenných uzlov. Rozdielom medzi rovnocenným spojením uzlov a nepriamym spojením je vo veľkosti zdieľaných dát pridávaných do siete, napríklad novej transakcie. Uzol, ktorý je rovnocenným predstavuje takzvaný full node *(plnohodnotný uzol)* a uzly prepojené nepriamo sú nazývané. lightweight node *(odľahčený uzol)*. Detailnejšie je problematika rozobraná v podkapitole 1.2.6.

Schéma 1 Princíp prepojenia v distribuovanom systéme blockchain



V schéme 1 je prepojenie rovnocenných uzlov znázornené obojstrannými hrubými šípkami. Povedzme, že v sieti je celkovo pripojených sto uzlov. Každý má napríklad šesť rovnocenných uzlov a s ostatnými je prepojený nepriamo, prostredníctvom rovnocenných spojení ostatných uzlov. Dostávame sa k hlavnej podstate toho ako sa dajú dáta zdieľať s každým uzlom bez toho, aby zaberali obrovské množstvo pamäte.

Uzol 1, ktorý má uložené informácie o transakcii v plnej veľkosti, pridá novú transakciu do siete. Pre uzol 1 predstavujú rovnocenné plnohodnotné uzly 2 a 3, ktorým je zasielaná kópia pridanej transakcie v plnej veľkosti. Jeho plnohodnotné uzly vedú vlastný zoznam svojich rovnocenných uzlov, ktoré predstavujú pre uzol 1 odľahčené uzly. To znamená, že do ich počítača sa pridaná transakcia uloží už v odľahčenej veľkosti. Rovnako sa ich transakcie ukladajú v uzle 1. Každý uzol je súčasne aj plnohodnotným aj odľahčeným v závislosti od toho, ktorý uzol pridáva do siete transakciu. Vďaka hash hodnotám je možné, aby každý uzol dostal kópiu pridanej transakcie a zároveň aby nezaberala veľa pamäte. Táto požiadavka je dôležitá, ak si predstavíme, že v systéme by sa mali ukladať záznamy o všetkých transakciách. Hash hodnotám sa budeme podrobne venovať v nasledujúcej podkapitole.

1.2.3 Spôsob kódovania dát v technológií blockchain

V distribuovanom systéme peer-to-peer sa pracuje s veľkým počtom transakčných údajov. Preto je potrebné ich jednoznačne identifikovať a porovnať čo najpresnejšie a najrýchlejšie. Parisi (2019) považuje za jeden zo základných pilierov technológie blockchain kryptografickú *hash funkciu*, ktorá zabezpečuje výpočet hash hodnôt. Hashing predstavuje koncepciu identifikácie dát. Zjednodušene môžeme *hash hodnotu* označiť za jedinečný digitálny odtlačok prislúchajúci konkrétnym dátam alebo súboru dát. Laicky ho môžeme prirovnať k odtlačkom prstov, ktoré sú rovnako jedinečné, nezameniteľné a použiteľné na identifikáciu konkrétnej osoby. Bez autorizácie nie je možné iba na základe informácie o dátume a mieste narodenia, mene, výške, hmotnosti či dosiahnutom vzdelaní odvodiť odtlačok prsta. Opačne to však možné je.

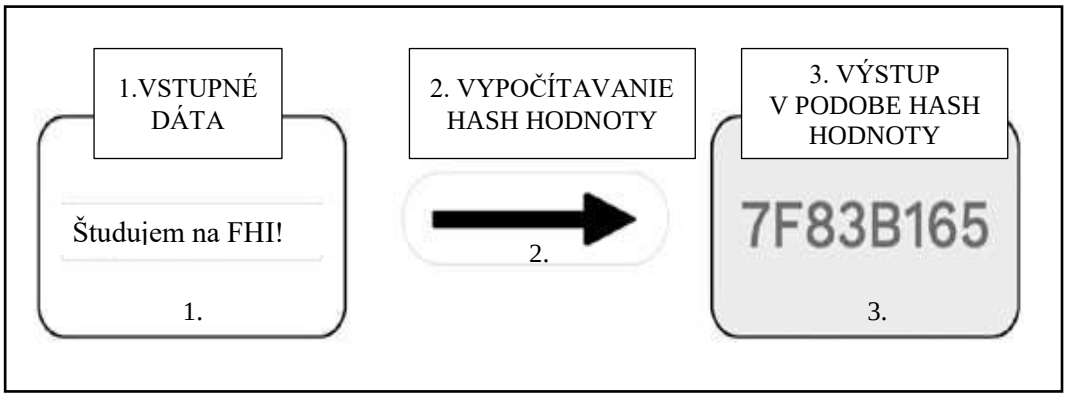
Mailund (2019) opisuje hash funkcie ako malé počítačové algoritmy, ktoré transformujú akýkoľvek druh digitálnych dát na konečný počet čísel bez ohľadu na veľkosť vstupných údajov. Existuje mnoho rôznych hash funkcií, ktoré sa okrem iného líšia v závislosti od dĺžky hash hodnoty, ktorú produkujú. Kryptografické hash funkcie majú

nasledujúce vlastnosti: *rýchlosť*, *deterministickosť*, *pseudonáhodnosť*, *jednosmernosť* a *odolnosť proti kolízii*. Týmto vlastnostiam sa podrobnejšie venuje nasledujúci text.

Rýchlosť je vlastnosť, ktorá je schopná vypočítať hash hodnoty pre rôzne druhy údajov a vo veľmi krátkom čase. V rámci technológie blockchain je táto vlastnosť zabezpečená tým, že systém nekóduje chybové správy. *Deterministickosť* znamená, že hash funkcia poskytuje rovnaké hash hodnoty pre rovnaké vstupné údaje. Všetky odlišnosti v hash hodnotách musia byť spôsobené výlučne nezrovnalosťami vo vstupných údajoch a nie chybovosťou hash funkcie. Prirovnajme si túto funkciu k elektrickej rúre. Ak do rúry vložíme cesto na koláč, po upečení z nej zákonite vyberieme koláč. V prípade, že by sme z nej po upečení vybrali napríklad mäso, táto nezrovnalosť nebola spôsobená chybovosťou elektrickej rúry, ale odlišnou vstupnou surovinou. Byť *pseudonáhodný* znamená, že vygenerovaná hash hodnota sa pri zmene vstupných údajov nepredvídateľne zmení. Aj v prípade, že sa zmenia iba minimálne, výsledná hash hodnota sa bude neporovnateľne líšiť od pôvodnej. Inak povedané, hash hodnota vstupných údajov musí byť vždy prekvapením a nemalo by byť možné predpovedať aká bude hash hodnota na základe vstupných údajov. To v skutočnosti znamená že, ak by bolo heslo do počítača 45678 v šifrovanej podobe je to napríklad hodnota 768A9872CFD8278. Ak by sme v hesle zmenili len jedno číslo na 45679 hash hodnota by sa zásadne zmenila napríklad na hodnotu AFC5425A98709BB. *Jednosmernosť* funkcie znemožňuje identifikovať vstupné údaje na základe výstupnej hash hodnoty. Funkciu nie je možné použiť opačne. To znamená, že hash hodnoty vám nič nehovoria o obsahu vstupných údajov, rovnako ako odtlačok prstu nič nehovorí o osobe, ktorej prst patrí. O jednosmerných funkciách môžeme povedať, že sú nezvratné. Hash funkcia sa nazýva *odolná proti kolízii*, ak je veľmi ťažké nájsť dve alebo viac odlišných dát, pre ktoré poskytuje rovnakú hash hodnotu. Inak povedané, ak je minimálna šanca získať identickú hash hodnotu pre rôzne dáta, potom je hash funkcia odolná proti kolízii. V tomto prípade môžeme považovať hash hodnoty vytvorené pomocou hash funkcie za jedinečné a použiteľné na identifikáciu údajov. Ak by sme získali rovnaké hodnoty hash pre rôzne časti údajov, narazili by sme na kolíziu. Hash kolízia je digitálny ekvivalent toho, že majú dvaja ľudia rovnaké odtlačky prstov. Aby boli hodnoty hash použiteľné ako digitálne odtlačky, je nevyhnutná odolnosť proti kolíziám. Podrobné vysvetlenie ako interne fungujú hash funkcie, aby boli odolné proti kolízii, je nad rámec mojej práce, ale existencia rôznych hashovacích algoritmov je práve výsledkom

vynaloženia veľkého úsilie na zníženie rizika vzniku kolízií hash. Zjednodušený proces hashingu je znázornený na Obrázok 2.

Obrázok 2 Proces hashingu vstupných dát v aplikácií blockchain



Zdroj: Spracované podľa DRESCHER, (2017)

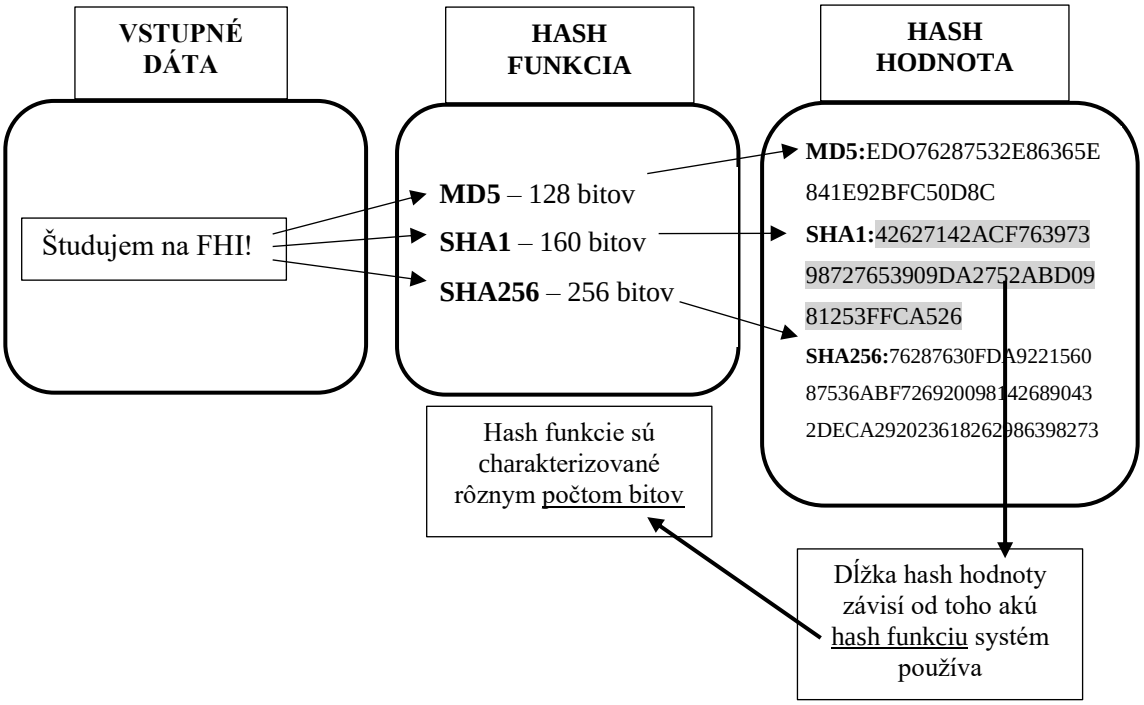
Na obrázku 2 je vidieť proces vytvárania hash hodnoty. Bunka č. 1 obsahuje slová, dáta, ktoré sú predmetom šifrovania. Šípka v bunke č. 2 znázorňuje proces transformácie dát na hash hodnotu a bunka č. 3 zobrazuje už skrátenú hash hodnotu zodpovedajúcu daným vstupným dátam. Hash funkcie pracujú v hexadecimálnej sústave, ktorá obsahuje číslice 0 - 9 a písmená A až F. V praxi sa používajú rôzne hash funkcie, od ktorých závisí dĺžka danej hash hodnoty.

Jednotlivé blockchain aplikácie vždy fungujú na jednej hash funkcii, ktorá generuje hash hodnoty. Tieto funkcie sú charakterizované rôznym počtom bitov, ktorú má výstupná hash hodnota dosahovať. Pre lepšie porozumenie Mailund (2019) uvádza niekoľko druhov hash funkcií:

- MD 5 – generuje 128-bitové hash hodnoty,
- SHA 1 – generuje160-bitové hash hodnoty,
- SHA 256 – generuje 256-bitové hash hodnoty, táto funkcia sa v súčasnosti používa pri bitcoin,
- Keccak-256 – generuje rovnako 256-bitové hash a je využívaná Ethereom, na ktorom fungujú smart contracts.

Čím je počet bitov vyšší, tým viac číslic a písmen z hexadecimálnej sústavy daná hash hodnota obsahuje. Zvyšuje sa tým bezpečnosť a odolnosť systému proti kolízií, ktoré sú hlavnými požiadavkami blockchain systémov. Rozdiel v generovaných hash hodnotách podľa použitej hash funkcie je znázornený v Schéma 2.

Schéma 2 Druhy hash hodnôt podľa použitej hash funkcie



Zdroj: Spracované podľa: DRESCHER, (2017)

Z grafického znázornenia v schéme 2 je viditeľné, ako sa líši dĺžka hash hodnoty v závislosti od hash funkcie, ktorú daná blockchain aplikácia používa. Čím je požadovaný počet bitov vyšší, tým je aplikácia bezpečnejšia, pretože sa priamo úmerne zvyšuje odolnosť hash funkcie proti kolízií. Dôvod je jednoduchý. Čím viac číslic a písmen použije funkcia v hash hodnote, tým viac kombinácií má systém k dispozícií. Vďaka tomu je minimalizovaná pravdepodobnosť vygenerovania rovnakej hash hodnoty pre dve rozličné vstupné dáta. Hashing dát sa v rámci technológie blockchain využíva na vytváranie digitálnych odtlačkov transakčných dát a ukladanie transakcií spôsobom citlivým na zmeny.

1.2.4 Štruktúra blokov v rámci technológie blockchain

Názov blockchain predstavuje spojenie dvoch anglických slov block - blok a chain - reťaz. Blockchain, v slovenskom preklade teda reťaz blokov, vyjadruje štruktúru ukladania dát. Parisi (2019) vysvetľuje, že jednotlivé údaje sú vkladané do samostatných blokov a prostredníctvom odkazov na predchádzajúci blok, vytvárajú reťaz. Vďaka tomu sa dá jednoducho a presne určiť, ktoré údaje historicky predchádzajú danému bloku.

Schéma 3 Štruktúra bloku

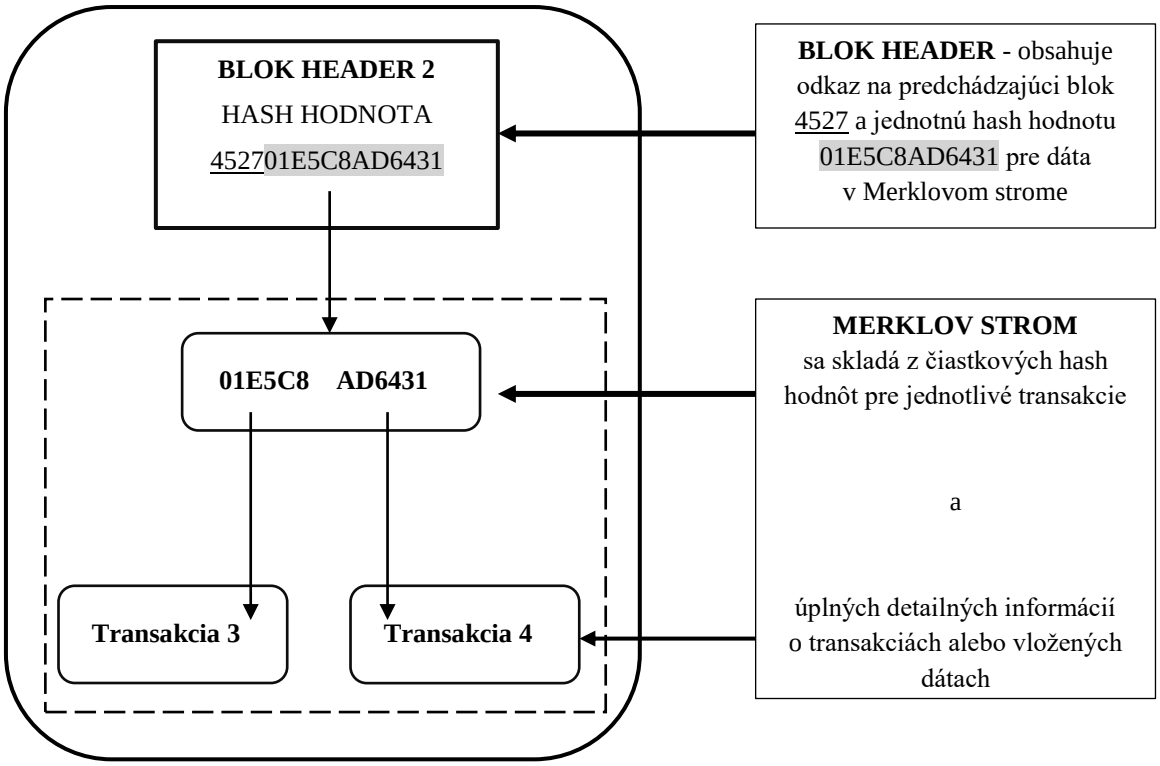


Schéma 3 graficky znázorňuje štruktúru bloku, ktorú je dôležité objasniť pre porozumenie ako sa pridáva transakcia do bloku, ako je porušená štruktúra bloku v prípade zmien a rozdielov v spôsobe zdieľania dát opisovaných v nasledujúcich podkapitolách. *Blok* sa delí na dve časti. V hornej sa nachádza takzvaný *blok header*, ktorý je nosičom zašifrovaných informácií. Obsahuje odkaz na predchádzajúci blok (v našom prípade 4527) a hash hodnotu, ktorá predstavuje novo pridané dáta nachádzajúce sa v spodnej časti. Táto časť obsahuje detailné údaje ohľadom transakcií a nazýva sa Merkle tree, v preklade *Merklov strom*. Pomenovaný je podľa tvorcu Ralpha Merkle a tvaru pripomínajúceho obrátený strom. Tento druh usporiadania je vhodný na zoskupenie mnohých rôznych častí údajov súčasne a ich sprístupnenie prostredníctvom jedinej referenčnej hash hodnoty. Aby sa dosiahla štruktúra Merklovho stromu, je potrebné začať zadaním dvoch transakčných údajov reprezentujúce v políčka v spodnej časti bloku. Najprv sa vytvoria hash odkazy pre tieto jednotlivé údaje o transakciách (Transakcia 3 a 4), ktoré tvoria dvojicu. Následne sa vytvorí jeden spoločný hash odkaz, ktorý sa nazýva koreň Merklovho stromu a nachádza sa spolu s odkazom na predchádzajúci blok v hornej časti bloku, v blok header.

1.2.5 Pridávanie transakcií do štruktúry blockchain-data

V predchádzajúcej podkapitole je objasnené, že databáza v blockchaine je tvorená dvomi hlavnými súčasťami, a to usporiadaným reťazcom blok headerov a Merklových stromov obsahujúcich údaje o transakciách. Táto dátová štruktúra nazývajúca sa *blockchain-data* bola navrhnutá s cieľom bezpečného ukladania údajov o transakciách a zdieľania dát spôsobom umožňujúcim úsporu pamäte. Nasledovný text je spracovaný podľa Dreschera (2017) a je venovaný postupom ako sa správne pridávajú nové transakcie do existujúcej databázy. Pre ich lepšie porozumenie sú v nasledujúcich schémach znázornené jednotlivé kroky.

Schéma 4 Pridávanie transakcii do štruktúry blockchain-data

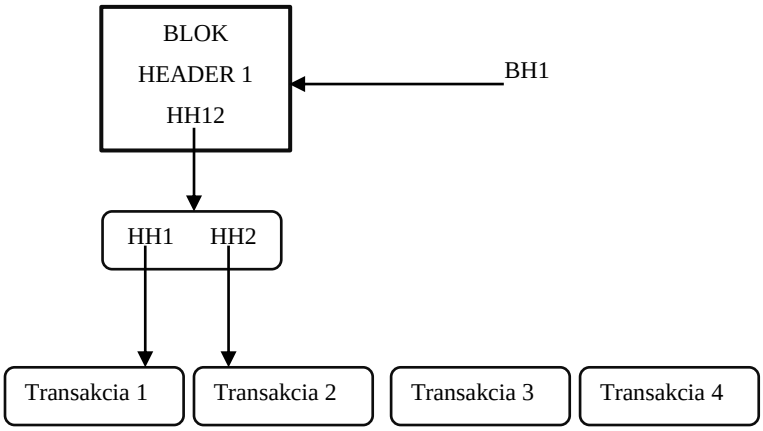
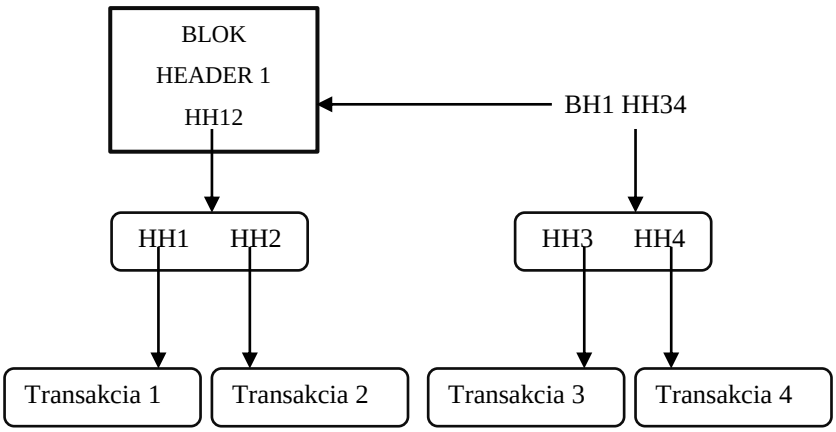


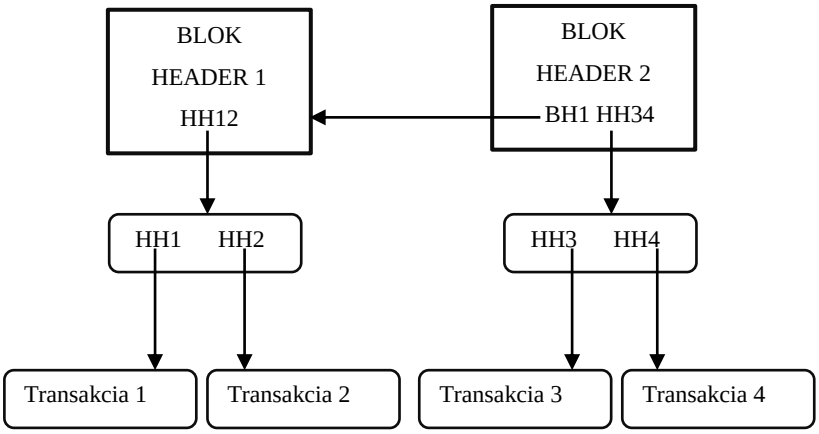
Schéma 4 zobrazuje počiatočný stav štruktúry blockchain-data, ktorá zatiaľ pozostáva iba z jedného bloku. Existujúca štruktúra má zatiaľ uložené iba transakcie 1 a 2. Transakcie 3 a 4 ešte nie sú pridané do štruktúry. Pre ich pridanie je potrebné vykonať nasledujúce kroky graficky zobrazené v schémach 5,6,7.

Schéma 5 Pridávanie transakcií do štruktúry blockchain-data - Krok 1



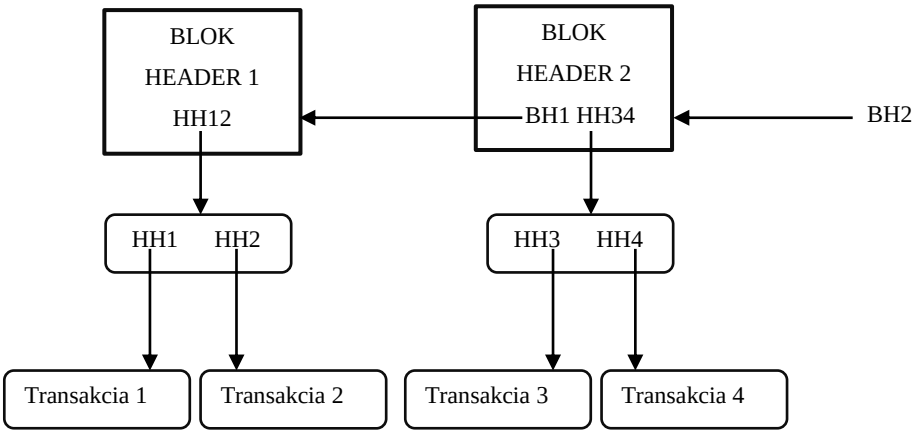
V prvom kroku sa vytvorí nový Merklov strom, obsahujúci všetky detailné údaje o nových transakciách, ktoré majú byť pridané do štruktúry.

Schéma 6 Pridávanie transakcií do štruktúry blockchain-data - Krok 2



V druhom kroku v Schéma 6 je vytvorený nový blok header 2, ktorý obsahuje *hash odkaz* BH1 odkazujúci na predchádzajúci blok. Zároveň sa v ňom nachádza aj koreň Merklovho stromu predstavujúci hash hodnotu HH34, ktorá nesie informáciu o nových transakciách 3 a 4.

Schéma 7 Pridávanie transakcií do štruktúry blockchain-data - Krok 3

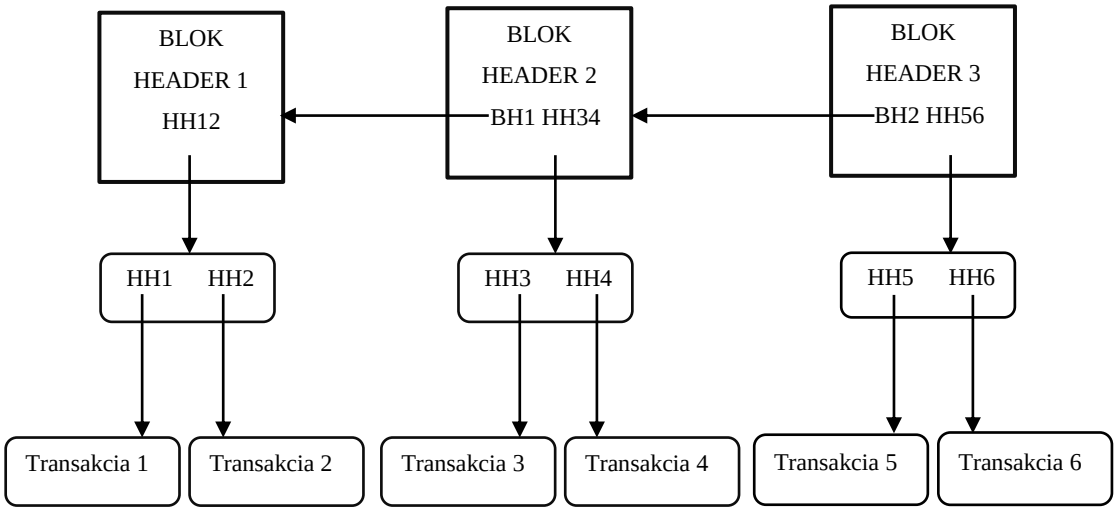


Ako zobrazuje Schéma 7, na záver sa vytvorí nový hash odkaz BH2 odkazujúci na novo vytvorený blok header 2 druhého pridaného bloku. Tento odkaz označíme ako nový *head* celej aktualizovanej štruktúry blockchain-data, ktorý predstavuje odkaz na posledné pridané údaje v reťazci. V našom prípade je označený ako BH2. V tomto momente je nová transakcia úspešne pridaná a rozposlaná všetkým počítačom, spôsobom, ktorý sme si vysvetlili v Schéma 1.

1.2.6 Zdieľanie dát v blockchaine

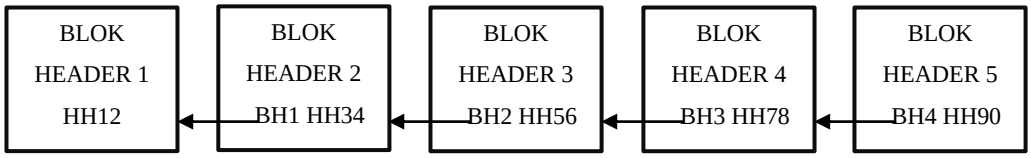
Podľa Parisi (2019) môžeme na technológiu blockchain pozerať z rôznych uhlov pohľadu, buď ako na distribuovanú aplikáciu, databázu, infraštruktúru alebo komunikačnú sieť. Práve pohľad na blockchain ako na komunikačnú sieť predstavuje pojem opisujúci fungovanie blockchainu aj v priestore. Historicky bol blockchain navrhnutý ako peer-to-peer sieť rovnocenných uzlov. V súčasnosti využívaný princíp prepojenia a spôsob komunikácie uzlov v rámci technológie blockchain znázorňuje sSchéma 1. Schéma 3 ilustruje časti, z ktorých sa bloky skladajú a v Schéma 8 aSchéma 9 sú zobrazené dva rozdielne druhy zdieľaných blockchain-data štruktúr. Tie sa líšia v závislosti od toho, či ide o štruktúru uchovávanú u plnohodnotného alebo odľahčeného uzlu. V tejto časti si ukážeme ako je zabezpečené, aby mal každú uzol rovnakú kópiu blockchain data štruktúry, ale zároveň nebolo potrebné obrovské množstvo pamäte. Pri predstave, že by napríklad všetky banky nahradila technológia blockchain vieme, že by išlo o presun obrovského množstva transakcií a údajov. Pri takom množstve je z hľadiska veľkosti pamäte nepredstaviteľné, aby mal každý uzol uloženú úplnú kópiu dát.

Schéma 8 Zdieľanie dát v rámci plnohodnotných uzlov



Na Schéma 8 vidíme ako vyzerá blockchain-data štruktúra ukladaná na plnohodnotných uzloch. Ide o identickú kópiu štruktúry vkladajúceho uzlu, ktorá zahŕňa časť blok headerov aj Merklovho stromu. Z hľadiska veľkosti zaberá štruktúra rovnakú pamäť ako štruktúra, ktorú má uloženú v počítači vkladajúci uzol.

Schéma 9 Zdieľanie dát v rámci odľahčených uzlov



V rámci odľahčených uzlov je uchovávaná blockchain-data štruktúra len vo forme reťaze blok headerov. Vďaka tejto odľahčenej blockchain-data štruktúre vo forme hash hodnôt, majú všetky uzly v sieti rovnocennú kópiu a prístup k dátam, ale zároveň nezaberajú enormné množstvo pamäte.

1.2.7 Uchovávanie dát a zmeny v transakciách

Myšlienka odkazovania na predchádzajúce uložené údaje založená na ich hash hodnotách má dôležitú úlohu. Je ňou zabezpečenie ukladania údajov spôsobom citlivým na zmeny, čo znamená, že je veľmi rýchlo a ľahko zistiteľné, či došlo k úprave už uložených údajov. Blockchain môžeme prirovnať k prepojenému zoznamu. Vytvára sa spôsobom, že hash hodnota pre každý nový pripojený blok údajov, obsahuje aj časť hash odkazu predchádzajúceho bloku dát. Tento druh štruktúry je vhodný na ukladanie a spájanie údajov, ktoré nie sú úplne dostupné v jednom časovom okamihu, ale namiesto toho prichádzajú postupne krok za krokom.

Schéma 10 Porušenie blockchain-data štruktúry

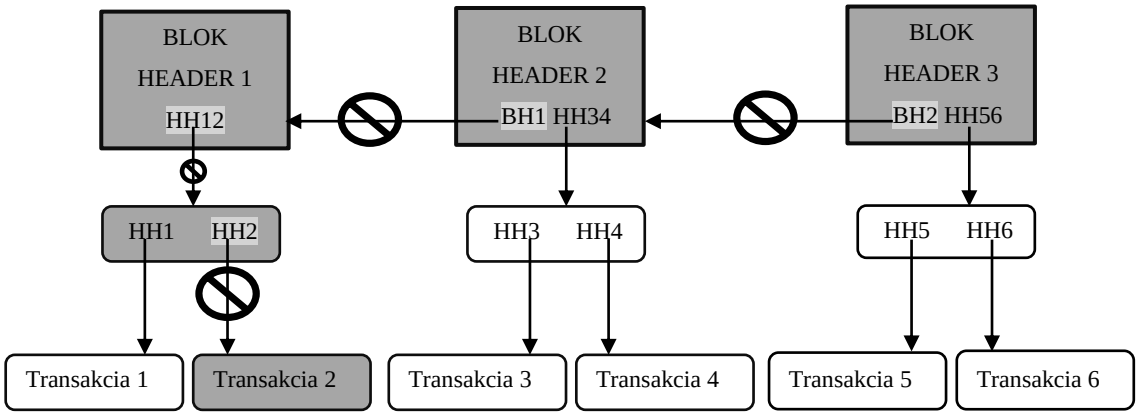


Schéma 10 znázorňuje, čo sa stane, ak zmeníme transakciu 2. Táto transakcia je jednou z častí tvoriacich Merklov strom. Okrem nej pozostáva z koreňa HH12 a z čiastkových hash hodnôt HH1 a HH2. Zmenou niektorých vlastností transakcie 2

napríklad množstva tovaru, ktoré sa prevádza alebo zmena čísla účtu prijímajúceho platbu, sa zmení aj jeho jedinečný odtlačok, respektíve jeho kryptografická hodnota hash. Výsledkom zmeny je, že hash hodnota HH2, ktorá odkazovala na pôvodné údaje o transakcii, je neplatná. V momente, keď systém zaznamená vstup do bloku, spúšťa sa proces verifikácie dát. Systém vyšle správu do všetkých uzlov v sieti, aby preverili a zaslali mu správu späť, či evidujú rovnaké údaje ako sú uložené v jeho počítači. Plnohodnotné uzly preverujú celú štruktúru vrátane Merklových stromov a odľahčené uzly preverujú hash hodnoty v blok headeroch. Vďaka procesu verifikácie systém odhalí, že údaje ktoré pôvodne uvádzal sa medzičasom zmenili, pretože nekorešpondujú s kópiami údajov v ostatných uzloch. Zmena v transakcii 2 spôsobila neplatnosť celej štruktúry blockchain-data na všetkých uzloch. Pre upresnenie, bloky ktoré predchádzajú bloku v ktorom nastala zmena sú stále platné. Vďaka tomu je možné exaktne zistiť, ktoré údaje boli menené. Dôvodom prečo sú však neplatné nasledujúce bloky je to, že zmenou transakcie 2 systém vygeneroval jej novú hash hodnotu v Merklovom strome čím, bola zmenená aj hash hodnota HH12 predstavujúca koreň Merklovho stromu. Tým, že je neplatný koreň, je neplatný aj blok header 1. Vieme, že každý nasledujúci block header, obsahuje odkaz na predchádzajúci blok. Tým pádom, keď je neplatný blok header 1 aj odkaz naň obsiahnutý v blok header 2 je neplatný, čím je porušený celý block header 2, aj keď nenastali žiadne zmeny v bloku 2. Keď sa pozrieme na schému vidíme rovnaký dopad porušenia platnosti aj blok headeru 3. V prípade každej minimálnej zmeny v histórií je porušená a neplatná celá nasledujúca blockchain-data štruktúra. Tento proces predstavuje *funkciu vysokej citlivosti systému na zmeny,* vďaka čomu nám technológia blockchain poskytuje istotu nemennosti histórie transakcií. Drescher (2017) uvádza, že hlavnou myšlienkou na zabezpečenie tejto funkcie je urobiť každú zmenu *neprimerane nákladnou*. To znamená, že náklady sú tak vysoké, že je oveľa ľahšie a lacnejšie držať sa pravdy. Aby bola táto funkcionalita zabezpečená, musí spĺňať tri podmienky. Prvou z nich je, že ukladá históriu transakčných údajov spôsobom, aby aj *najmenšia manipulácia s obsahom bola výrazne viditeľná.* Nie je možné tajne a potichu manipulovať s dátami, ktoré sú súčasťou štruktúry blockchain-data a dúfať, že si to nikto nevšimne. Aj najmenšia zmena sa uskutoční s obrovským „hlukom“ spôsobeným prerušením hash odkazov, ktoré sa stanú neplatnými v dôsledku zmeny údajov, na ktoré sa odvolávajú. Druhou požiadavkou je, aby si každá manipulácia alebo zásah do histórie transakcií vyžadovali prepísanie veľkej časti štruktúry. Blockchain pri zmene údajov uplatňuje radikálny prístup – všetko alebo nič. Zmeny sa

dotknú celej štruktúry údajov počnúc bodom, ktorý spôsobuje zmenu, až po hlavičku štruktúry. Poslednou podmienkou je výpočtová náročnosť prepisovania údajov v histórií. Obrovské výpočtové náklady sú vyvolané generovaním nových hash hodnôt, ktoré boli porušené. Práve finančná náročnosť má odradiť potenciálneho páchateľa od manipulácie s históriou transakcií

1.2.8 Verifikácia transakcií prostredníctvom mechanizmu konsenzov

Dôvera v rámci obchodných vzťahov je v dnešnej dobe sústredená na tretie strany, ktoré sprostredkúvajú transakcie, eliminujú riziko poškodenia jednej zo strán a ručia za autenticitu a pravosť údajov. Na druhej strane však práve tretie strany predstavujú riziko bezpečnosti úschovy a pravosti údajov, vyššie náklady a časovú náročnosť na overovanie údajov. Najväčšou výhodou technológie blockchain je práve možnosť eliminácie tretích strán z transakčného procesu. Nakoľko je odstránená centrálna zodpovednosť a každý pripojený používateľ v sieti môže vkladať dáta, je potrebné, aby boli všetky transakcie neustále kontrolované a auditované všetkými uzlami.

Welfare (2019) tvrdí, že väčšina aplikácií blockchain funguje na spoločných princípoch. Jednou z možností, čím sa môžu aplikácie odlišovať, je práve spôsob verifikácie pridávaných transakcií. Rozhodnutie, ktoré transakcie sú legitímne a pridajú sa do blockchain-data štruktúry, zabezpečuje technológia blockchain pomocou rôznych mechanizmov konsenzu. Mechanizmy konsenzu sú protokoly, ktoré zaisťujú, že všetky uzly pripojené do blockchain, sú navzájom synchronizované a dohodnú sa, ktoré transakcie sú legitímne a následne pridané do blockchain data štruktúry. Tieto mechanizmy konsenzu sú rozhodujúce pre správne fungovanie blockchain. Zabezpečujú, aby mal každý používateľ rovnakú reťaz blokov tzn. rovnakú blockchain-data štruktúru. Bez dobrých mechanizmov konsenzu je blockchain vystavený riziku rôznych útokov. Existuje niekoľko spôsobov ako dosiahnuť konsenzus.

Medzi najpoužívanejšie mechanizmy patrí podľa Hospa (2019) *proof-of-work* a *proof-of-stake*. V nasledujúcom texte si v krátkosti objasníme to, ako funguje mechanizmus konsenzu proof-of-work, využívaný technológiou blockchain. Ten bol prvý krát použitý pri bitcoine, následne prijali tento mechanizmus aj mnohé iné kryptomeny. V rámci bitcoin aplikácií sa nachádzajú v sieti aj uzly – *validátori* , ktoré zabezpečujú výpočtový výkonov. Ich počítače majú za úlohu riešiť zložité matematické hádanky, ktoré vyžadujú veľa výpočtovej sily. Z tohto dôvodu neprebieha proces generovania odpovede

u každého používateľa. V momente ako niekto zadá transakciu do systému, počítače validátorov začnú riešiť matematické problémy, ktorými sa dostanú k odpovedi vo forme *hash hodnoty a nonce hodnoty*. Nonce hodnota je v rámci bitcoin aplikácií využívaná ako vyšší stupeň zabezpečenia jedinečnosti generovaných hodnôt. Ide o reťazec čísiel, ktorý tvorí jedinečnú dvojicu číselných údajov pre generované hash hodnoty. Prvý, kto vyrieši hádanku vytvorí blok a pridá ho do blockchain data štruktúry. Ostatní validátori, ktorí vyriešili hádanku neskôr musia dostať rovnaké hodnoty, čím potvrdia jej správnosť. V tomto bode je blok schválený a transakcia je uznaná za legitímnu. Validátor, ktorý ako prvý poskytne odpoveď na matematický problém získava odmenu vo forme bitcoinov, v prípade aplikácie pre tútokryptomenu. Tieto matematické problémy majú zaujímavé vlastnosti (Berg – Davidson – Potts, 2019). V prvom rade sú asymetrické, čo znamená, že nájdenie odpovede vyžaduje veľa času, ale je ľahké overiť, či je odpoveď správna. Druhou vlastnosťou je, že jediný spôsob, ako vyriešiť tieto problémy je uhádnuť odpoveď. Nie je možné vyriešiť problémy rýchlejšie inak než metódu pokus a omyl. To znamená, že ak chce niekto nájsť odpoveď na matematický problém rýchlejšie, bude potrebovať viac výpočtovej sily, ktorá môže byť veľmi nákladná. Treťou vlastnosťou je obtiažnosť týchto hádaniek sa mení v závislosti ako rýchlo sa ťažia bloky. Aby sa zachovala stála ponuka nových bitcoinov, musia sa v určitom časovom rámci vytvoriť bloky. Ak sa bloky vytvárajú príliš rýchlo, hádanky sa stávajú ťažšími a ak sa vytvárajú príliš pomaly, hádanky sú ľahšie.

Ďalším distribuovaným mechanizmom konsenzu, ktorý uvádza Hosp (2019) je spomínaný *proof-of-stake*, ktorý rovnako slúži na potvrdzovanie transakcií. Rovnako ako pri proof-of-work ide o algoritmus, no líši sa v procese dosiahnutia konsenzu. Rozdielom je, že pri proof-of-work sa vytvárajú nové bloky prostredníctvom validátorov a v rámci mechanizmu proof-of-stake sú všetky bloky vytvorené hneď na začiatku a ich počet je nemenný. Z tohto dôvodu hovoríme o validačných uzloch ako o takzvaných falšovateľoch a nie validátoroch. V sieti blockchain využívajúcej proof-of-stake nedostávajú validačné uzly odmenu za vyťaženie nového bloku, ale sú odmeňované prostredníctvom transakčných poplatkov, ktoré si účtujú za potvrdzovanie transakcií Výhodou mechanizmu proof-of-stake oproti proof-of-work je, že falšovatelia nepotrebujú na validáciu transakcií využívať tak obrovský počítačový výkon. Dôvodom je, že uzol, ktorý bude validovať transakciu je vyberaný náhodne a jedinými faktormi ovplyvňujúcimi jeho šancu, sú aktuálna zložitosť siete a jeho celkový počet vlastnených digitálnych mincí. Na tento algoritmus dosahovania distribuovaného konsenzu v súčasnosti (2020) plánuje prejsť aj

digitálna mena Ethereum, ktorá je druhou najhodnotnejšou kryptomenou hneď po bitcoine. Kľúčový dôvod, pre ktorý jej developeri uvažujú nad touto zmenou je, že mechanizmus proof-of-stake potrebuje na potvrdenie transakcií menšie množstvo spotrebovanej energie. Stále je teda zabezpečené dosiahnutie distribuovaného konsenzu, respektíve overenie transakcií bez potreby tretích strán, ale pri výrazne lacnejších energetických nákladoch než pri proof-of -work.

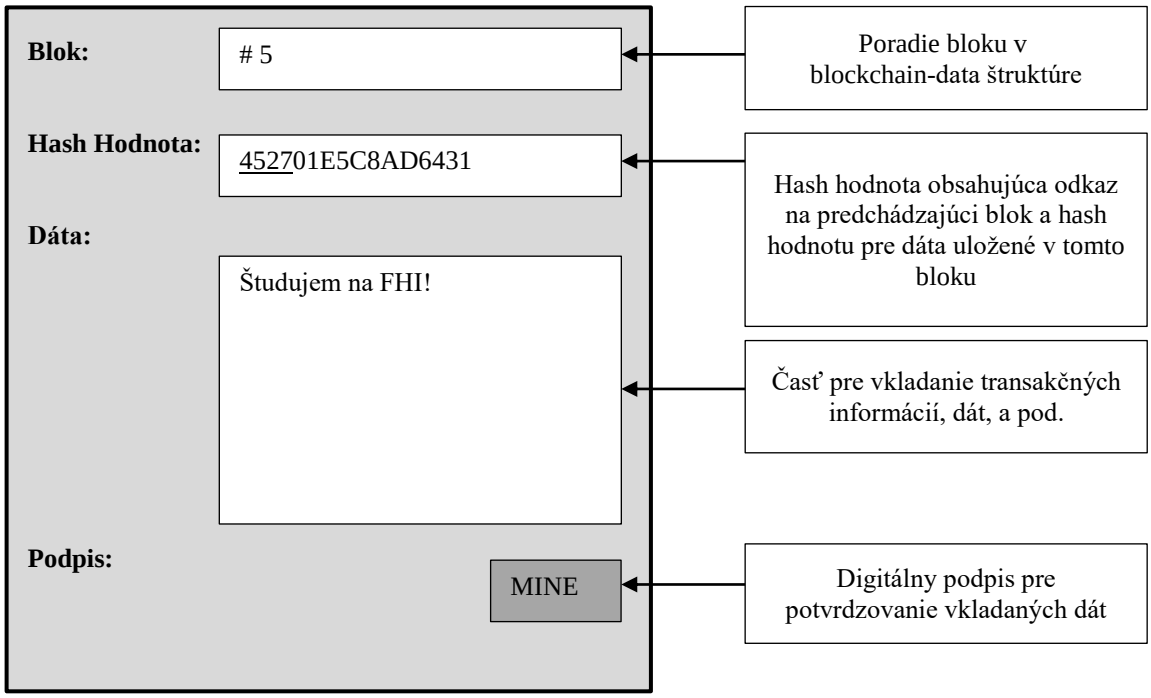
1.2.9 Proces autorizácie transakcií

Drescher (2017) konštatuje, že digitálny podpis predstavuje matematickú kombináciu, ktorá zabezpečuje pravosť digitálnych správ alebo dokumentov. Vďaka platnému digitálnemu podpisu sú zabezpečené tri funkcie. *Overenie*, pretože príjemca sa na základe neho domnieva, že správu vytvoril oprávnený odosielateľ, ďalej *nenávratnosť,* pretože odosielateľ nemôže poprieť odoslanie správy a zároveň *integritu,* pretože podpisom je zabezpečené, že sa správa pri prenose nezmení. Digitálne podpisy sa často používajú na implementáciu elektronických podpisov, čo predstavuje širší pojem, ktorý sa vzťahuje na všetky elektronické údaje, ktoré musia byť podpísané, ale nie všetky elektronické podpisy využívajú digitálne podpisy. Digitálne podpisy používajú asymetrickú kryptografiu, ktorá funguje prostredníctvom verejných a súkromných kľúčov. V prípade asymetrického šifrovania platí, že súkromnú časť podpisu na dešifrovanie pozná iba podpisujúci a verejnú časť na šifrovanie pozná každý. Blockchain musí v prípade zabezpečovania transakcií spĺňať aj ďalšiu dôležitú úlohu a tou je, že musí umožniť, aby mohol prevádzať svoj majetok na iné účty iba zákonný vlastník. Práve na to využíva spomínané digitálne podpisy, ktoré sú aj v rámci blockchainu považované za najbezpečnejšiu kryptografickú metódu, ktorá umožňuje zaistiť bezpečnosť zdieľaných údajov. Okrem zaisťovania hodnovernosti správ a integrity údajov poskytujú digitálne podpisy aj spôsob overenia vlastníka. Vďaka tomu môže príjemca v prípade vzniku sporu digitálne podpísané údaje predložiť tretej strane ako dôkaz.

V tejto časti si objasníme ako sa používajú digitálne podpisy v systéme blockchain na autorizáciu transakcií. V papierovej forme slúžia na vyjadrenie súhlasu s obsahom dokumentu ručné podpisy. Dôvodom, prečo akceptujeme vlastnoručný podpis ako dôkaz súhlasu, je jedinečnosť rukopisu každej osoby. Krok autorizácie je rozhodujúci pre bezpečnosť jednotlivých transakcií v blockchain. Súhlas s obsahom transakcie v rámci blockchain prejavuje užívateľ digitálnym podpisom. Majiteľ účtu, ktorý chce previesť

majetok musí prejsť nasledujúcimi krokmi. Najskôr zadá transakciu so všetkými potrebnými informáciami, ako sú čísla príslušných účtov, prevádzaná suma, splatnosť a podobne. Následne systém vytvorí kryptografickú hash hodnotu pre transakčné dáta a ako posledné majiteľ transakciu potvrdí svojim digitálnym podpisom. Vykonaním všetkých krokov je transakcia pridaná do štruktúry blockchain-data, ktorá sa rovnako zaktualizuje u každého uzlu. Nasledujúci obrázok ilustruje autorizáciu transakcií v blockchain aplikácií.

Obrázok 3 Digitálny podpis



Názov poľa *mine* sa používa v existujúcej blockchain aplikácií pre bitcoin. Kliknutím na pole minie užívateľ potvrdí, že súhlasí s obsahom transakcie a následne sa začne celý proces verifikácie proof-of-work u validátorov.

1.3 Využitie technológie blockchain v účtovníctve a audítorstve

Tapscott a Tapscott (2016) uvádzajú, že blockchain je dômyselne jednoduchá a revolučná technológia, ktorá umožňuje, aby boli transakcie anonymné a zároveň bezpečné. Aj napriek tomu, že je blockchain označovaný za najznámejšiu technológia, na ktorej fungujú bitcoin a iné digitálne meny, má veľký potenciál na uplatnenie aj mimo mien. Dokáže zaznamenať prakticky všetko, čo je nositeľom informácií a má pre človeka hodnotu. Napríklad rodné listy, poistné zmluvy, evidenciu vlastníkov pozemkov a dokonca aj volebné hlasy.

Vďaka všeobecným výhodám blockchainu, sa vytvára priestor aj na jeho využitie v účtovníctve a audítorstve. Má potenciál zvýšiť efektívnosť účtovania transakcií a aktív, ktoré prebiehajú na úrovni medzinárodného účtovníctva. Prostredníctvom prenosu dôvery a zodpovednosti za pravosť a autenticitu dát z centrálnych subjektov na všetky uzly v sieti zyšuje potrebnú istotu v súvislosti s právami, povinnosťami a pôvodom majetku. Odľahčením účtovníctva od týchto funkcií, by mohlo rozšíriť svoj rozsah pôsobnosti na zaznamenávanie viacerých druhov činností ako predtým napríklad by mohlo poskytovať podrobnejšie informácie o hospodárskej realite zaznamenávaných transakcií.

Za hlavné výhody blockchainu pre oblasť účtovníctva a audítorstva považuje Hacioglu (2019) to, že nové transakcie majú pôvod u jedného používateľa, ale sú rozposielané prostredníctvom siete do identických kópií databáz bez potreby centrálneho správcu. Ďalšou je, že všetky transakcie a záznamy sú trvalé a nemožno s nimi manipulovať alebo ich odstrániť. Taktiež považuje za veľkú výhodu, že mnoho blockchainov je programovateľných. To umožňuje pridávanie ďalších funkcionalít napríklad automatizáciu nových transakcií, kontrolu stavu transakcií. Na tomto princípe fungujú napríklad smart kontrakty.

Aj keď existujú nepochybne niektoré technologické a právne problémy, ktoré treba predtým vyriešiť, blockchain sa dá v plnej miere začleniť do finančných účtovných systémov vo svete. Jedinečná kombinácia technických a obchodných znalostí v rámci účtovníckej profesie je obzvlášť vhodná na pomoc pri navrhovaní prostredia a riešení, na ktorých bude blockchain fungovať. Blockchain je spojením ekonomického obchodného modelu a šikovnej podpornej technológie. Účtovníci v spolupráci s IT odborníkmi môžu výrazne pomôcť pri tvorbe štandardov, ktoré posunú blockchain vpred. Blockchain predstavuje základnú zmenu v spôsobe vytvárania, vedenia a aktualizácie finančných záznamov. Hlavná výhoda blockchain technológie spočíva v používaní komplexného systému overovania prostredníctvom mechanizmu konsenzov. Vďaka nim je možné zabezpečiť aj bez centrálneho správcu, aby sa dostala ku všetkým používateľom jediná dohodnutá verzia pravdy ako súčasť trvalého záznamu. Technológia blockchain vytvára univerzálnu databázu, kde je každý jednotlivý záznam zdieľaný identicky a natrvalo s každým účastníkom.

1.3.1 Kľúčové vlastnosti blockchainu pre oblasť účtovníctva a audítorstva

Blockchain je neobvyklým druhom technológie v oblasti nastupujúcich inovatívnych trendov, pretože ide o online administratívne riešenie prevodu vlastníctva, a zaznamenávania údajov. Inými slovami, je to platforma, na ktorej môžu fungovať niektoré oblasti účtovníctvo a podnikanie ako sú napríklad automatizácia transakcií, uchovávanie dát a zabezpečovanie integrity a spoľahlivosti údajov. Technickým podrobnostiam ako blockchain funguje a čo ho robí odolným proti útokom a krádeži sa venuje podkapitola 1.2.

Vlastnosti technológie blockchain zhrnul The Institute of Chartered Accountants in England and Wales, (2018) do takzvaných *„3P" – propagácia, permanentnosť a programovateľnosť.* Predstavujú tri kľúčové pojmy odlišujúce blockchain od dnešných známych databáz, ktoré sú vlastnené a prevádzkované jednou centrálnou správcovskou entitou. *Propagácia* je definovaná existenciou mnohých identických kópií databáz v blockchaine. V systéme nie je žiadna hlavná databáza, ktorá by bola nadradená ostatným. Všetci účastníci siete majú prístup k úplnej, ekvivalentnej báze a ku jej všetkým kópiám v systéme. Vieme, že všetci účastníci sú si z hľadiska kontroly rovní takže žiaden účastník nepredstavuje nadradenú autoritu. Nové transakcie sa dajú zaúčtovať rýchlo a okamžite, sú distribuované do databáz všetkých účastníkov, ktoré sa následne aktualizujú. Tým, že má každý používateľ svoju vlastnú kópiu databázy, pravdivosť a správnosť údajov je stanovovaná na základe konsenzov. Uložené a distribuované transakcie nemožno editovať bez súhlasu väčšiny, čo znamená, že záznamy blockchainu sú *permanentné.* Celá báza údajov je uchovávaná u každého účastníka a môže byť kedykoľvek skontrolovaná a overená. Niektoré blockchain aplikácie umožňujú pridávanie ďalších funkcionalít, čím hovoríme o systéme, že je *programovateľný*. Vďaka ďalším pridaným programovým kódom môžu byť automaticky tvorené účtovné zápisy, uskutočňované transakcie alebo prevody vlastníckych práv.

To, či je blockchain v praxi použiteľný, bude záležať od toho, či sú jeho kvality a funkcie žiaducou alternatívou za súčasné metódy. Na rozdiel od internetu, v ktorom sa údaje iba zdieľajú, blockchain umožňuje aj prevod vlastníctva z jedného používateľa na druhého. Aplikácie blockchain sa sústredia na nákladové a časové úspory, odstránenie centrálnych správcovských jednotiek zo systému, ale zároveň zabezpečujú istotu , nakoľko ide o systém postavený na konsenzoch. Zdieľaním identických databáz, by bola na trhu s mnohými obchodujúcimi entitami odstránená potreba zosúlaďovania rozličných údajov.

Distribúciou dát medzi všetkých používateľov sa rovnako minimalizujú výpadky dostupnosti k dátam a náklady na poplatky ústredným orgánom za spravovanie údajov a záruky integrity databázy. Jednou z hlavných výhod je, že každý zainteresovaný používateľ môže sledovať všetky predchádzajúce transakcie, čo zabezpečuje úplnú transparentnosť a plní funkciu samokontroly.

1.3.2 Vplyv metódy blockchain na finančný sektor

Finančné inštitúcie používajú dátové sklady pre vlády, ľudí a rôzne tretie strany. Z tohto dôvodu je veľmi dôležité, aby sa tieto údaje uchovávali čo najbezpečnejšie. Upadhyay (2019) uvádza, že dnešné rozsiahle databázy sú dôležitou súčasťou každodenného fungovania hospodárstva. Tieto databázy však potrebujú permanentnú kontrolu a zálohovanie, pretože je vysoký predpoklad, že sa niečo pokazí. Problémom súčasných databáz je, že boli vytvorené za účelom ukladania dát a nie ich pravidelnej aktualizácie. Aj napriek tomu, že niektoré transakčné databázy sú na tom výkonnostne dobre, stále sú neporovnateľné s funkcionalitou blockchainu alebo jeho odľahčených verzií uzatvoreného transakčného systému.

Z koncepčného hľadiska je blockchain krok vpred. Z bodu, kde dôveryhodnosť databázy závisí od centrálnej entity, ktorá ju spravuje, sa presúva dôveryhodnosť do rúk všetkých zainteresovaných používateľov systému. Vďaka týmto funkciám fungujú aj smart kontrakty, ktorých celoplošné zavedenie by mohlo zásadne zmeniť a uľahčiť fungovanie zmluvných vzťahov. Za predpokladu, že sa prekonajú všetky technologické a právne prekážky, blockchain je naozaj budúcnosť v oblasti podnikania, financií a obchodu. Medzi skupinami, ktoré medzi sebou často obchodujú, by súkromné blockchain aplikácie mohli nahradiť tretie strany ako sú napríklad banky, zúčtovacie a právne služby. So schopnosťou priamej interakcie v rámci jednej bázy údajov, ktorá by si nikdy nevyžadovala zosúladenie, by podniky mohli ušetriť značné finančné prostriedky. Rovnako odstránenie neistoty prispieva k zefektívneniu ekonomiky a zvýšením dôveryhodnosti údajov uľahčuje rozhodovanie. Upadhyay (2019) ďalej vidí zaujímavé uplatnenie technológie blockchain aj v rámci správcovských orgánov akým je napríklad daňový úrad, ktorý by mal prístup do potrebných databáz len na prezeranie, čím by bol schopný kontrolovať a monitorovať transakcie v reálnom čase. Tento druh poznatkov, by mohol viesť k zníženiu nákladov a zvýšeniu efektívnosti regulačných a kontrolných činností súvisiacich s dodržiavaním

predpisov. Trvalosť záznamov v blockchain-data štruktúrach eliminuje priestor na finančné a daňové podvody, čím taktiež zvyšuje dôveryhodnosť záznamov.

1.3.3 Potenciál *využitia technológie blockchain pre účtovníctvo*

Podľa Holbrooka (2020) môžeme blockchain chápať aj ako účtovnú technológiu. Umožňuje prevod vlastníctva a vedenie presných a úplných finančných informácií v databáze. Účtovníctvo sa vo všeobecnosti venuje kvantifikácií, zaznamenávaniu a analýze finančných informácií. Hlavnú časť tvorí sledovanie pohľadávok a záväzkov viažucich sa k majetku alebo plánovanie toho, ako najlepšie alokovať finančné zdroje. Pre účtovníkov predstavuje použitie technológie blockchain správu majetku a existujúcich záväzkov spoločnosti, čo môže výrazne zlepšiť ich efektivitu. Popri ďalších trendoch automatizácie a digitalizácie, by mohol blockchain vďaka svojim funkciám prevziať časť účtovníctva, ktorá sa venuje transakciám. Blockchain by mohol pomôcť účtovníkom získať lepší prehľad o voľných finančných zdrojoch a záväzkoch svojej spoločnosti. Predstavuje relevantnú náhradu za mechanické účtovnícke a zosúlaďovacie práce. Mohlo by sa zdať, že by tým bola ohrozená práca účtovníkov. V oblastiach, ktoré dokážu byť zabezpečené automatickým systémom a nevyžadujú si ľudský faktor, by ich síce nahradili, ale zároveň im dávajú viac času a priestoru na dôležitejšie oblasti, kde je ľudský faktor nevyhnutný. Predstavovalo by to možnosť lepšej organizácie práce a využitia ľudských zdrojov. Účtovníci sa môžu sústrediť na hodnotenie reálnej finančnej situácie podniku interpretáciou záznamov blockchain, priraďovaním záznamov k hospodárskej realite a jej hodnotením. Napríklad blockchain vie identifikovať majetok, ale jeho spätne získateľná hodnota a ekonomická hodnota sú stále diskutabilné. Rovnako aj v oblasti hĺbkového prieskumu pri fúziách, akvizíciách, poradenstve a v diskutabilných oblastiach účtovníctva, ktoré si vyžadujú posúdenie účtovníkom. Taktiež vlastnícke právo k majetku sa dá overiť pomocou blockchainových záznamov, ale jeho stav, umiestnenie a reálnu hodnotu je potrebné overiť a odsúhlasiť účtovníkom. Ďalšou výhodou technológie blockchain je eliminácia potreby zosúlaďovania údajov a zabezpečenie istoty v súvislosti s históriou transakcií. Vďaka tomu by blockchain zvýšil spoľahlivosť účtovníctva zvýšiť v oblastiach, ktoré sú v súčasnosti považované za nespoľahlivé, ako napríklad pravdivosť a relevantnosť údajov, ktoré spoločnosti prezentujú. Aplikácie blockchain umožňujú väčšiu transparentnosť ako tradičné databázy. Veľké využitie, by mali vo verejnom sektore, v prípadoch, kde je veľký priestor na korupciu alebo zneužitie majetku. Napríklad výdavky

na dotácie, by sa mohli poskytovať prostredníctvom blockchainu, vďaka čomu by bolo možné ľahko a presne identifikovať konečného príjemcu.

Transakcie medzi spoločnosťami v súčasnosti vedú podľa Holbrooka (2020) k pomyselnému „štvornásobnému vedeniu účtovníctva“. Každá spoločnosť spraví svoj podvojný zápis a teoreticky ide o dve skupiny zápisov pre rovnakú hodnotu. Tento model by mohol byť podstatne zmenený technológiou blockchain, znížením bariér okolo interného účtovníctva každej spoločnosti a zadávania údajov priamo do blockchain-data štruktúry. Na rozdiel od účtovníctva, by sa takto zabezpečilo, aby sa transakcia zaznamenala verne, overiteľne, pravdivo a identicky každou stranou. Na začiatok by sa mohol využiť na obchodovanie v rámci skupiny a postupne sa rozrastať pripájaním ďalších entít, až by sa časom vytvorilo takzvané „univerzálne účtovníctvo“. V zásade bude musieť byť každá blockchain aplikácia navrhnutá len do miery obmedzení súkromia, ktoré poskytuje technológia blockchain. Kým údaje týkajúce sa pôvodu alebo vlastníctva majetku môžu byť v každej transakcii šifrované, potom musia byť predchádzajúce transakcie verejné, aby potvrdili správnosť transakcie. Nájdenie spôsobu, ako vyvážiť konkurenčné výhody decentralizácie a súkromia a bezpečnosti je súčasnou oblasťou výskumu medzi špecialistami na blockchain.

Otázka ako identifikovať osobu pripojenú v sieti sa prakticky rieši od vzniku internetu. V začiatkoch bolo postačujúcim riešením kombinácia používateľského mena a hesla, ktorá sa napokon využíva vo veľkej miere dodnes. Technologický vývoj v oblasti informačných technológií priniesol množstvo pozitívnych riešení, ktoré nám zjednodušili život, no rovnako so sebou priniesol aj poznatky ako tieto systémy napadnúť. Preto sme momentálne v štádiu, kedy je pre druh aplikácií uchovávajúce citlivé osobné údaje tento spôsob zabezpečenia nedostatočný. Brayman (2019) uvádza, že mnoho inštitúcií používa zložité identifikačné procesy napríklad *Know Your Customer- Poznaj svojho zákazníka*, ktorých cieľom je preveriť totožnosť klientov a ich finančnú minulosť. Tieto procesy sú nákladné, zdĺhavé a nesú so sebou riziko, pretože sa spoliehajú na tretiu stranu. Servery týchto tretích strán zhromažďujú citlivé dáta, čím predstavujú cieľ pre hackerov. Prostredníctvom šifrovania dát, ktoré blockchain využíva, sa dajú osobné údaje jednotlivcov uchovávať bezpečne, trvalo a bez možnosti manipulácie. Rovnako by sa zmenila centrálna zodpovednosť za správu dát na decentralizovanú zodpovednosť všetkých používateľov, čím by sa eliminoval priestor pre hackerské útoky. Na podobnom princípe by sa mohla zdieľať napríklad aj databáza práv duševného vlastníctva pre zjednodušenie

procesu identifikácie vlastníkov, podávania žiadostí a úhrad za poskytnuté práva a licencie a ďalšie obdobné databázy.

1.3.4 Súčasné a potenciálne blockchain aplikácie

Welfare (2019) rozdelil blockchain aplikácie do niekoľkých kategórií v závislosti od základných funkcií technológie, na ktoré sa najviac zameriavajú. Niektoré aplikácie sú postavené na automatickej synchronizácii databáz, čím zjednodušujú zosúlaďovanie údajov a zároveň zabezpečujú transakčnú istotu. Niektoré sa viac sústredia na možnosť odstránenia sprostredkovateľskej inštitúcie zo systému, čím sa znižujú náklady a subjektívnosť, zatiaľ čo umožňujú prístup ďalším účastníkom. Iné sú spojením oboch a používajú blockchain ako platformu umožňujúcu automatizáciu a zvyšovanie istoty v rámci zmluvných dohôd a transakcií.

1.3.4.1 Vnútrobankové zosúlaďovanie dát

Blockchain je navrhnutý tak, aby bol užitočný v systémoch, ktoré si vyžadujú zosúlaďovanie údajov medzi stranami. Holbrook (2020) konštatuje, že mnoho hlavných aktérov v bankovníctve podporujú konzorcium R3, ktoré skúma použitie distribuovanej bázy podobnej blockchain na medzibankové zosúlaďovania a iné finančné operácie. V súčasnosti sa ročne vynakladajú milióny na zosúladenie údajov medzi bankami. Ak by sa však našlo riešenie v podobe distribuovanej databázy, ktoré je schopné zvládnuť objem transakcií medzi bankami, potom by bolo možné náklady značne znížiť. Tento druh aplikácie by bol súkromnou databázou, kde by si mohli prezerať záznamy a podieľať sa na vytváraní nových, výlučne iba pozvané strany. Umožnilo by sa tým to, aby sa v rámci medzibankových finančných transakcií vytvoril jediný autoritatívny záznam, ktorý by mohli overiť všetky strany. Značne by sa tým znížila potreba úsilia, ktoré sa v súčasnosti vynakladá na zosúladenie údajov s protistranami a vytvoril by sa efektívnejší bankový systém. Pri súčasnej kapacite a rýchlosti blockchainu však nie je možné, aby sa projekt konzorcia R3 skutočne premenil na distribuovanú aplikáciu databázy pre finančný sektor. Avšak za predpokladu, že sa tieto významné prekážky podarí odstrániť, bankový sektor je potencionálne veľmi vplyvná oblasť pre uplatnenie blockchainu.

1.3.4.2 Blockchainová aplikácia katastra nehnuteľností

Asi najlepším príkladom aplikácie, v ktorom by blockchain mohol byť užitočný na bezpečné uchovávanie dát o pôvode a prevodoch vlastníctva majetku je kataster nehnuteľností. V rámci tejto myšlienky bolo vypracovaných niekoľko pilotných štúdií a konceptov, ale väčšina z nich nedosiahla doposiaľ úplnú funkčnosť alebo neprešla celkovým testovaním. Jedným z prípadov nevydareného pilotného projektu bol pozemkový register v Hondurase, ktorý nemá v súčasnosti žiadny register vlastníctva pôdy a čelí problémom s korupciou a spreneverou majetku. Naopak podľa prípadovej štúdie McMurrena, Younga a Verhulsta (2018) Švédsko po dvoch rokoch testovania demo verzie katastra nehnuteľností fungujúceho prostredníctvom technológie blockchain, vykonalo prvú transakciu prevodu vlastníctva v marci 2018. Za najväčšiu výhodu považujú, že čas od podpísania kúpnej zmluvy až po právoplatné nadobudnutie vlastníckeho práva druhým vlastníkom sa znížil z niekoľkých mesiacov na pár hodín. Otvorená viditeľnosť blockchainu ako verejného registra nie je pre pozemkový register prekážkou. V rámci potreby zabezpečiť overiteľnosť transakcií a transparentnosť je prípustné, aby účastníci videli, kto vlastní a predáva pôdu. Hacioglu (2019) opisuje, že blockchainová aplikácia katastra, by sa musela začať *tokenizáciou* predmetných pozemkových aktív, ktorá predstavuje proces premietnutia reálnej peňažnej hodnoty každého pozemku do legálnej ekvivalentnej digitálnej hodnoty uloženej na v štruktúre blockchain-data. Nasledovalo by zabezpečenie toho, aby súčasní vlastníci mali pridelené správne množstvo príslušných tokenov, podľa ich vlastníctva. Nakoľko je vlastníctvo hlavou spravovanou veličinou je nie je potrebné ho iba zaznamenávať, ale rovnako musia tieto záznamy zostať previazané s realitou, a preto musí register spoľahlivo odrážať existenciu a stav aktív v reálnom svete. Zároveň musia existovať aj právne mechanizmy na uplatňovanie vlastníckych práv pokiaľ záznamy blockchain indikujú existenciu vlastníctva, a to aj voči stranám, ktoré nie sú súčasťou blockchain alebo nepovažujú blockchain za relevantný legitímny zdroj. Za predpokladu, že by sa dali tieto bariéry prekonať, vytváraním overiteľných a trvalých záznamov by sa mohla technológia blockchain použiť ako kataster nehnuteľností a následne zaznamenávať všetky predaje pozemkov, nehnuteľností a súvisiacich transakcií. Okrem toho, distribuovaná povaha databázy by zabezpečovala, že ani výpadok alebo zlyhanie servera by nikdy neovplyvnili dostupnosť služby. Náklady na uskutočňovanie transakcií prostredníctvom blockchainu, ako sú nákupy a predaje pozemkov

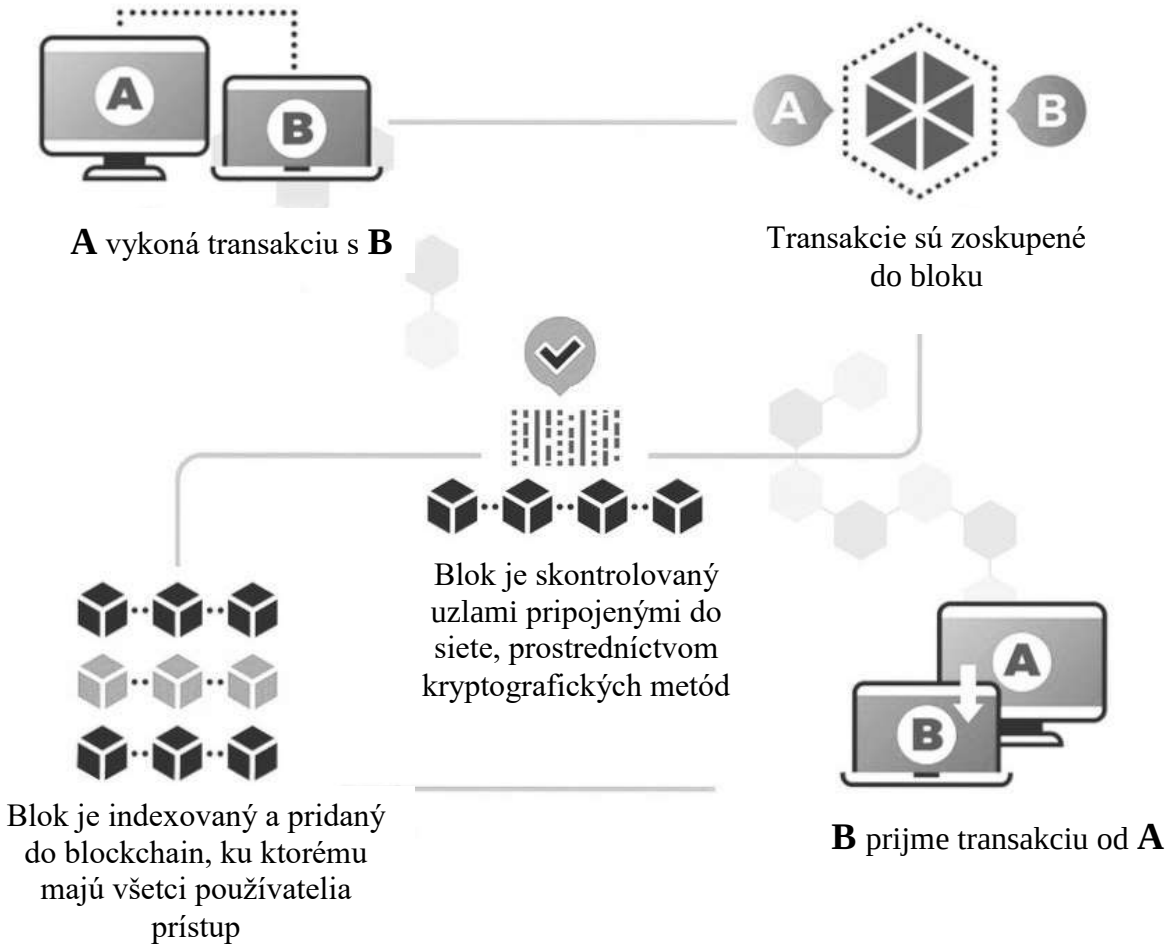
a nehnuteľností, môžu byť relatívne vysoké no pre tento druh nízko objemových operácií s vysokou hodnotou komodity, by mohol blockchain konkurovať súčasným mechanizmom.

1.3.4.3 Blochainová aplikácia Smart kontrakty

Zaujímavou vlastnosťou blockchainu je, že niektoré z blockchain aplikácií, ako napríklad Ethereum, môžu v rámci nich obsahovať ešte iný spustiteľný počítačový program. Peck (2012) uvádza, že smart kontrakt definoval v roku 1994 Szabo ako automatizovaný transakčný protokol, ktorý vykonáva podmienky kontraktu, čiže zmluvy. Ide o kód, ktorý je nastavený tak, aby automaticky pridal do systému určitý druh transakcie, akonáhle sú splnené zadefinované podmienky, respektíve nastali potrebné udalosti. Kód, ktorý tvorí smart kontrakt, je nastaviteľný, takže si strany môžu vopred dohodnúť podmienky, za akých obchod prebehne.

Welfare (2019) tvrdí, že vo finančnej sfére existuje v súčasnosti viacero príkladov automatizovaných zmlúv. Od mechanicky jednoduchších, ako sú predajné automaty až po bankový platobný príkaz či inkaso. Myšlienka smart kontraktov spočíva v možnosti vykonania všetkých druhov transakcií automaticky a jednoducho, rovnako ako nákup v automate, bez potreby platiť alebo spoliehať sa na centrálnu entitu pri určovaní zmluvných podmienok. Technológia blockchain ponúka mnoho príležitostí na využitie vo finančnej oblasti. Pri smart kontraktoch sa dajú podmienky zmluvy definovať priamo do blockchain a je možné si ich dohodnúť vopred, rovnako ako pri tradičnej zmluve. Ak sú podmienky splnené, smart kontrakt disponuje príslušnými právami a automaticky vykoná definované úkony, napríklad uvoľniť peňažné prostriedky z účtu, zinkasovať platbu na účet, vykonať investíciu alebo čokoľvek iné. Okrem odstránenia sprostredkovateľskej strany, je jednou z hlavných výhod smart kontratov v porovnaní s tradičnými zmluvami zníženie rizika nedodržania podmienok jednej zo strán. Ak dôjde k porušeniu zmluvy pri tradičnej forme zmluvy, má túto úlohu na starosti súd, aby donútil nápravu u strany, ktorá porušila podmienky. Avšak, pri smart kontraktoch je zabezpečené dodržanie dohodnutých podmienok vyplývajúcich zo zmluvy preventívne. Fungujú na dohodnutých podmienkach, ktorým sa zaviazali obe strany, bez možnosti zmeny. Smart kontrakty sú jednoznačné, zakaždým je vykonaný po splnení podmienok úkon, ktorý bol definovaný.

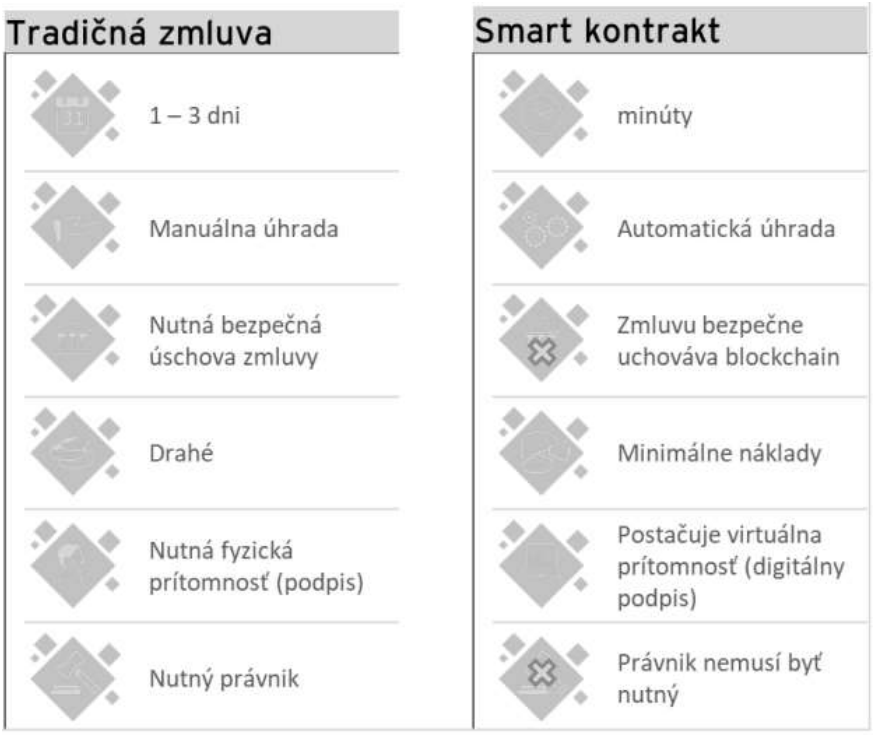
Obrázok 4 Fungovanie smart kontraktov



Zdroj: *Spracované podľa WELFARE,* (2019)

Na celoplošné zavedenie smart kontraktov do súčasného hospodárstva je potrebné vyriešiť isté problémy. Aj keď by bola z procesu obchodných transakcií odstránená tretia strana, stále potrebujeme z hľadiska zabezpečenia objektivity dôveryhodného profesionála. V tomto prípade nezávislého, nestranného a kvalifikovaného programátora, ktorý naprogramuje aplikáciu bez zámeru zvýhodnenia jednej strany, podvodu alebo iného nezákonného konania. V opačnom prípade, by išlo len o presunutie inštitucionálnej dôvery a nákladov z právnikov na programátorov, ktorí ho kódujú a neexistovala, by žiadna skutočná výhoda oproti súčasným zmluvám.

Obrázok 5 Porovnanie tradičnej zmluvy a smart kontraktu



Zdroj: *Spracované podľa WELFARE,* (2019)

Welfare (2019) uvádza, že niektoré projekty, ako napríklad Legalese sa snažia vytvoriť počítačový jazyk na zmluvy, vďaka ktorému by sa dali ľahko preložiť do bežného jazyka, avšak v súčasnosti sme ďaleko od tejto reality. Aj napriek tomu, že smart kontrakty fungujú preventívne, nikdy nevieme zabezpečiť sto percentnú istotu dodržania podmienok. Práve preto je potrebné aby súdy uznali, že operácie v rámci smart kontraktov sú legitímnymi spôsobmi, ako previesť vlastníctvo alebo finančnú hodnotu medzi stranami a zabezpečili vymožiteľnosť zmluvných podmienok v prípade porušenia. Rovnako je potrebné vyriešiť dodatočné úpravy zmluvných podmienok. Možnosť upraviť podmienky, už po uzavretí smart contractu a odstrániť tým nekalý zámer jednej strany, v prípade, že jedna zo strán využíva smart kontrakt iným spôsobom, ako by si druhá strana predstavovala. Tieto problémy nie sú len teoretické. Príkladom je projekt „The DAO“ investičný nástroj vytvorený pre blockchain Ethereum. Spoločnosť prišla o veľkú časť svojich finančných prostriedkov kvôli hackerovi, ktorý našiel medzeru v zle naprogramovanej inteligentnej zmluve. Systém oneskorene aktualizoval zostatok na smart kontrakte DAO, čo umožnilo viackrát požiadať o vrátenie finančných prostriedkov vo forme ETH. Problémom bolo, že pri vytvorení smart kontraktu DAO programátori nezohľadnili možnosť tejto rekurzívnej požiadavky a skutočnosť, že smart kontrakt najskôr

odoslal prostriedky ETH až následne aktualizoval interný tokenový zostatok. Práve kauza ohľadom projektu DAO poukázala na jeho veľký nedostatok v zabezpečení

1.3.5 Potenciál technológie blockchain v oblasti audítorstva

Blockchain by mal výborné využitie v externom audite. Auditom sa nerozumie len overovanie údajov, medzi akými stranami a v akej peňažnej sume sa transakcia uskutočnila. Overuje sa aj to, ako bola transakcia zaznamenaná a klasifikovaná. Blockchain v kombinácií s vhodnou analytickou evidenciou údajov, by poskytoval audítorom potrebnú istotu o správnosti zaúčtovania transakcií. Ak by boli všetky operácie týkajúce sa peňažných prostriedkov zaznamenávané a zaznamenávané na blockchain, znížila by sa potreba vykonávania konfirmácií transakcií a zostatkov. Tieto kroky by znamenali zásadnú zmenu v spôsobe práce audítorov. Podľa The Institute of Chartered Accountants in England and Wales, (2018) uplatnením blockchain riešení, by audítorom odpadla veľká časť mechanickej práce. Vďaka tomu, by sa mohli počas zákazky venovať hlavne rizikovejším oblastiam účtovnej závierky, ktoré si vyžadujú ľudský faktor. V účtovníctve existujú oblasti ako sú napríklad rezervy, opravné položky, odpisy, ktoré nie sú striktne upravené a vo veľkej miere závisí ich výška od rozhodnutia účtovnej jednotky. Práve tie umožňujú ovplyvňovať výšku a charakter výsledku hospodárenia. Aby mohol audítor overiť a posúdiť správnosť účtovnej závierky potrebuje poznať celkový kontext uzávierkových hodnôt, ktorý nie je všeobecne dostupný verejnosti. Zavedením blockchain, by sa zvýšila istota správneho zaznamenávania transakcií a audítor sa môže venovať práve spomínaným rizikovým oblastiam, ktoré si vyžadujú kvalifikované posúdenie odborníkom.

2 Cieľ práce, metodika práce a metódy skúmania

Hlavným cieľom diplomovej práce-je zhodnotiť súčasné možnosti využitia metódy blockchain v oblasti účtovníctva a audítorstva, ktorá ponúka priestor na jej implementáciu. Zistiť existujúce problémy pri jej zavádzaní do praxe a v neposlednom rade identifikovať výhody, na základe ktorých by mohla byť vhodnou alternatívou pre momentálne využívané metódy.

Pre splnenie cieľa sme v prvom kroku analyzovali existujúci stav právnej úpravy na národnej a nadnárodnej úrovni, vďaka ktorej by sa eliminovali rizikové faktory v oblasti bezpečnosti uchovávaných údajov a poskytla podpora širšieho využitia tejto technológie vo finančnom sektore aj mimo neho. Napriek veľkému potenciálu tejto technológie je práve nedostatočná legislatíva jednou z prekážok pri jednoduchom zavádzaní. Aj právny rámec Slovenskej republiky je v tejto oblasti vo väčšine tvorený prostredníctvom implementácií smerníc vydaných Európskym parlamentom a Radou EÚ.

Ďalším krokom k naplneniu nášho cieľa bolo zvládnutie technickej stránky technológie blockchain. Opísali sme spôsob fungovania distribuovaných sieti typu peer-to-peer, ktorou blockchain je, a dospeli ku kľúčovým vlastnostiam a funkciám, ktoré ho robia výnimočným a odlišným oproti momentálne používaným technológiám. Keďže ide o náročnú a obsiahlu technickú problematiku, selekciou nadobudnutých poznatkov sme identifikovali a následne rozobrali základné okruhy potrebné na porozumenie tejto technológie bežnému čitateľovi. V tejto časti boli zdrojom informácií okrem literatúry aj dostupné demo verzie aplikácií blockchain. Konkrétne sme využívali vizuálnu demo verziu Blockchain 101, podpornú študijnú aplikáciu hash puzzle a rovnako aj, už existujúce používané aplikácie fungujúce na princípoch blockchain, napríklad BitcoinCore.

Vďaka analýze dostupných štúdií ohľadom prínosu metódy blockchain pre oblasť účtovníctva a audítorstva vypracovaných členmi sme následne identifikovali možnosti uplatnenia tejto technológie pre túto oblasť. Blockchain, ktorý poskytuje možnosť trvalého a bezpečného uchovávania digitálnych dát tak ponúka spôsob ako nahradiť sprostredkovateľské inštitúcie, centrálne registre a v istej mieste aj dozorné orgány, čím by sa prispelo k zvýšeniu dôveryhodnosti informácií, úspore času a rovnako aj úspore nákladov. Sumarizáciou všeobecných výhod blockchainu a komparáciou tradičných používaných metód v účtovníctve a audítorstve a technológie blockchain sme dospeli k súboru hlavných výhod.

Aplikáciou nami identifikovaných výhod na praktické príklady sme podporili opodstatnenosť tvrdení, že technológia blockchain je vhodnou alternatívou tradičných metód uchovávania dát, a že predstavuje reálne aplikovateľný spôsob nahradenia sprostredkovateľských inštitúcií alebo inak centrálne sústredenej dôvery a zodpovednosti. V závere poslednej kapitoly sme porovnaním dokázali, že technológia blockchain so sebou prináša zjednodušenie, zefektívnenie práce a zároveň by výrazne ušetrila momentálne vynakladané náklady, úsilie a čas.

3 Výsledky práce a diskusia

Na základe odbornej literatúry venujúcej sa technológii blockchain, dostupným demo verziám aplikácií blockchain, už existujúcim aplikáciám postavených na technológii blockchain ako sú Smart kontrakty a Bitcoin a štúdií pre oblasť účtovníctva a audítorstva sme dospeli k súhrnu výhod uplatnenia technológie blockchain pre oblasť účtovníctva a audítorstva, ktoré si v tejto časti jednotlivo ukážeme.

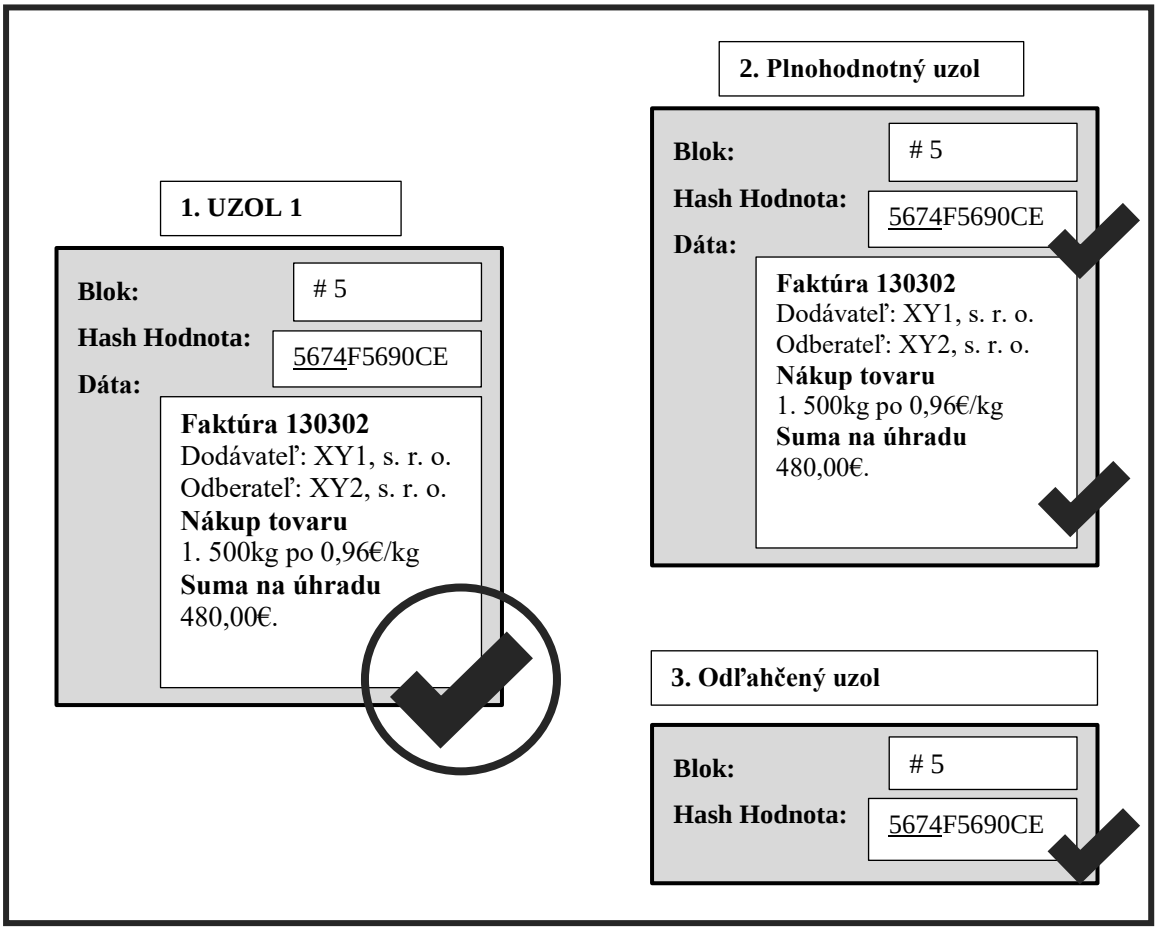
3.1 Výhody technológie blockchain pre oblasť účtovníctva a audítorstva

Už v teoretickej časti sme si overili, že spomínané oblasti účtovníctva a audítorstva poskytujú priestor pre jeho aplikáciu do praxe. Jeho zavedením by prispel k zjednodušeniu a zefektívneniu procesov a taktiež sme identifikovali nasledovné výhody, ktoré poskytuje: zabezpečenie integrity záznamov, zníženie potreby konfirmácií existencie transakcií, zostatku majetku a záväzkov – bežný chod firmy, zakladanie, umorovanie, odstránenie potreby existencie správcovskej centrálnej entity resp. tretej strany. Ďalej by eliminoval príležitosti na nezákonné a nemorálne konanie ako sú podvody, korupcia, sprenevera majetku, daňové úniky. Rovnako by posilnenil istotu v správnosti, jednotnosti a bezpečnosti histórie transakcií, prispel k zníženiu nákladov a úspore času a v neposlednom rade eliminuje potreby fyzickej papierovej formy uchovávania dát, kópií. Uvedeným výhodám sa budeme venovať v nasledujúcich častiach.

3.1.1 Integrita záznamov

Integrita predstavuje nezmenený stav, takže nebol menený, porušený a nebolo doňho nijak zasiahuté. Ako sme si ukázali v podkapitole 1.2.7. technológia blockchain uchováva dáta spôsobom veľmi citlivým na najmenšie zmeny. Nejde o ich úplne zamedzenie, ale je veľmi obtiažne a až neprimerane nákladné vykonať zmeny už zaevidovaných dát. Vďaka tejto vlastnosti blockchain technológia poskytuje istotu, že s uloženými dátami nebolo manipulované. Ak by sa tak stalo, systém by upozornil všetkých používateľov, že došlo k zmene a blockchain-data štruktúra je porušená. Použitie technológie blockchain umožňuje preukázať integritu elektronických dát ľahko, rýchlo a v každom okamihu. Integritu zabezpečujú spomínané hash hodnoty, ktoré sú generované pre každé vkladané údaje do blockchain štruktúry.

Obrázok 6 Verifikácia zabezpečujúca integritu dát v blockchain-data štruktúre

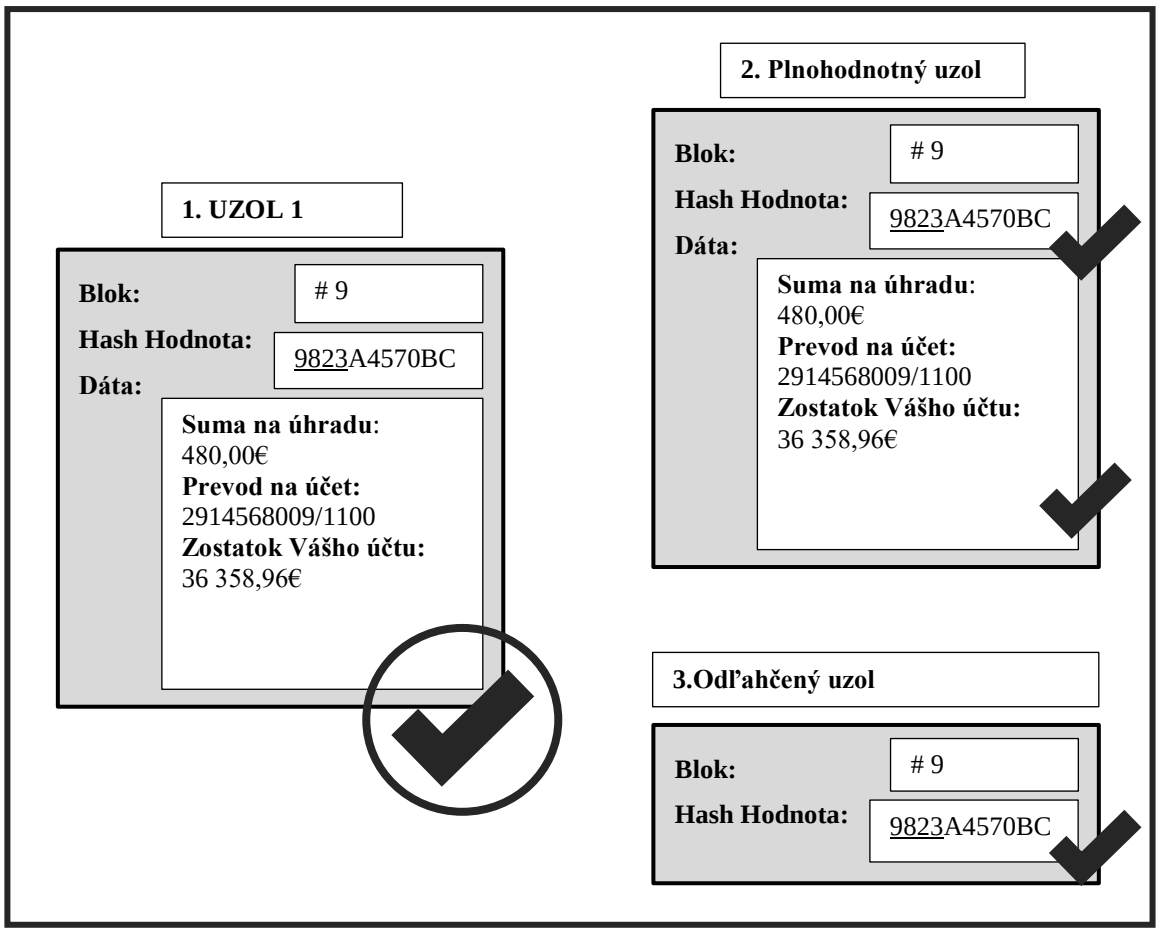


Na obrázku je graficky znázornené ako vyzerá proces verifikácie dát, vďaka ktorému dokáže blockchain technológia zabezpečovať integritu dát. Overovanie vykonáva systém automaticky. Uzly si rozposielajú správy, prostredníctvom ktorých kontrolujú či sa uložené údaje zhodujú. V rámci plnohodnotných uzlov systém skontroluje všetky detailné informácie v našom prípade dodávateľa, odberateľa, množstvo tovaru a sumu na úhradu. Dáta musia byť úplne identické, pretože aj vloženie jednej medzery navyše by vygenerovalo novú hash hodnotu. Uzly komunikujú so svojimi plnohodnotnými uzlami, ktoré následne zasielajú overovacie, správy vlastným plnohodnotným uzlom. Tie predstavujú v prípade tohto overovania odľahčené uzly a preto sa porovnajú údaje už len na úrovni hash hodnôt. Takýmto spôsobom prebehne verifikácia hash hodnôt v celej blockchain sieti. V prípade, že by uzol 1 manipuloval s údajmi, hash hodnoty v ostatných blokoch by boli odlišné a systém by vykazoval neplatnosť štruktúry, ktorú si môžeme predstaviť tak, že by na obrázku boli namiesto znakov správnosti krížiky. Na našom obrázku však vidíme, že systém vykazuje úplnú zhodu vďaka čomu vieme s určitosťou povedať, že údaje sú pravdivé, správne a úplné.

3.1.2 *Zníženie potreby konfirmácií existencie transakcií, zostatku majetku a záväzkov*

V rámci štatutárneho auditu patrí medzi audítorské postupy overovania správnosti účtovnej závierky aj vyžiadanie si konfirmačných listov od externých partnerov napr. na potvrdenie zostatku bankového účtu, existencie transakcie alebo výšky záväzkov alebo pohľadávok. Ak by transakcie prebiehali prostredníctvom technológie blockchain, bola by potreba konfirmácií podstatne eliminovaná ako demonštruje nasledujúci obrázok.

Obrázok 7 Verifikácia dát eliminujúca potrebu konfirmácie údajov

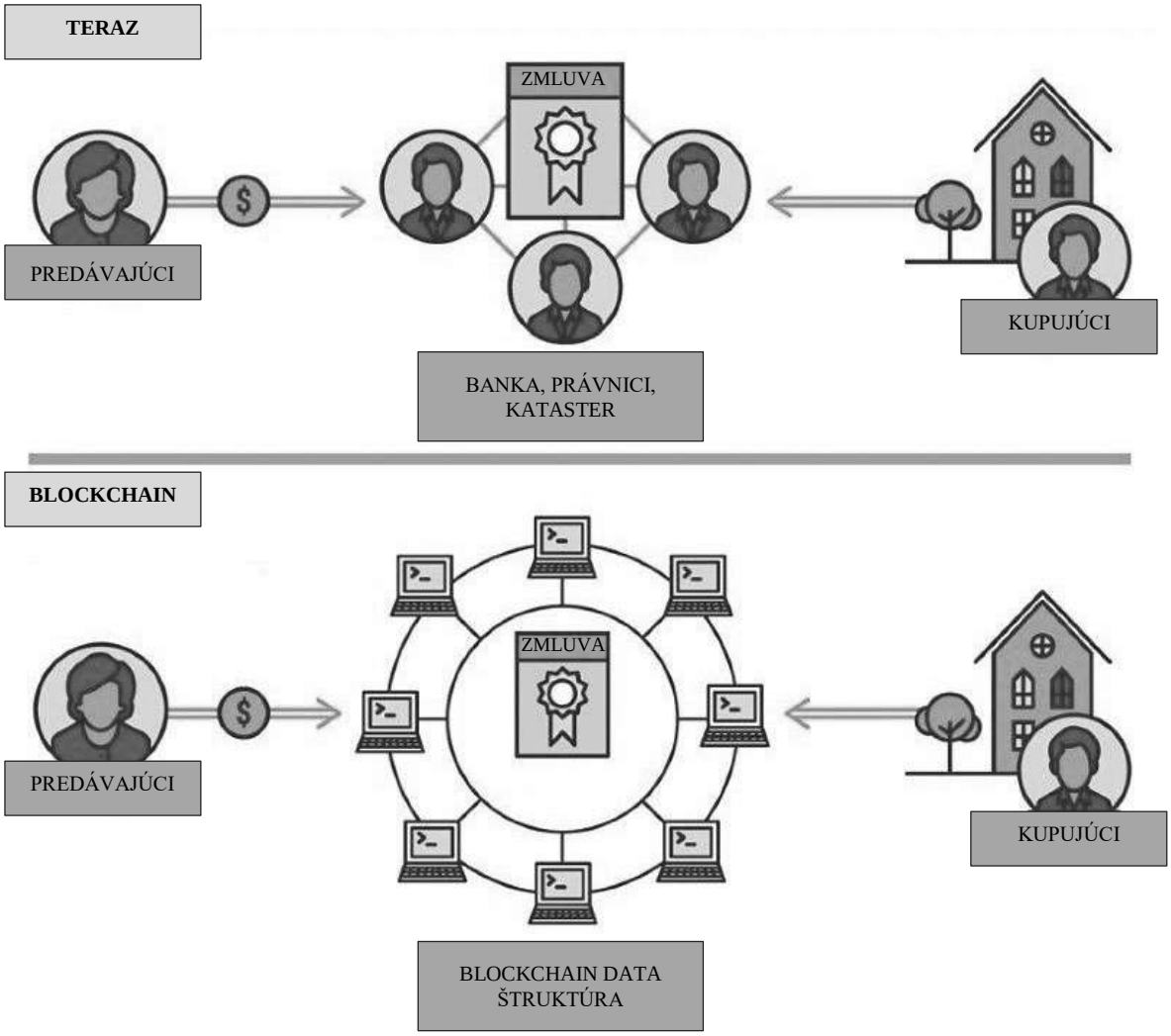


Vidíme, že pre danú transakciu je vygenerovaná určitá hash hodnota, ktorá zabezpečuje, že druhá strana príjme rovnakú sumu aká bola poukázaná na účet. Rozoslaním hash hodnoty uskutočnenej transakcie všetkým uzlom v sieti, je zaručená istota a dôkaznosť existencie transakcie. Ak by napríklad druhá strana chcela poprieť, že jej bola suma uhradená, je to nemožné, pretože každý uzol v sieti má dôkaz, že bola úhrada uskutočnená. Rovnako daná hash hodnota reprezentuje aj výšku zostatku nášho účtu.

V prípade, že štruktúra blockchain-data nevykazuje žiadne známky jej porušenia, pretože korešponduje so všetkými kópiami v systéme, máme istotu, že údaje sú pravdivé a správne. Vďaka týmto vlastnostiam technológie blockchain sa dá eliminovať potreba konfirmácií zostatkov a existencie transakcií od zákazníkov a obchodných partnerov.

3.1.3 Odstránenie potreby existencie správcovskej centrálnej entity

Momentálne sú transakcie medzi jednotlivými stranami zabezpečovaný prostredníctvom centrálnych správcovských entít resp. tretích strán, ktoré predstavujú pilier poskytujúci spoľahlivosť, dôveru a istotu. Najčastejšou treťou stranou pri transakciách sú banky, ale rovnako ide o katastrálne úrady, právnikov, ministerstvá či sprostredkovateľské agentúry. Ďalšou formou správcovskej entity sú centrálne databázy, spravujúce dáta. Napríklad register účtovných závierok, centrálna evidencia zmlúv a iné.
Na nasledujúcom obrázku si ukážeme ako by prebiehal obchod bez tretej strany.



V prvej časti obrázku vidíme aktuálny priebeh pri v rámci obchodných vzťahov. Ide napríklad o predaj nehnuteľnosti. Na jednej strane je predávajúci, na druhej strane kupujúci a tretiu stranu zastupuje banka, právnici, katastrálny úrad a ďalšie iné potrebné inštitúcie. Obidve strany dôverujú tretím stranám, že obchod prebehne v súlade so zákonom, kupujúci sa stane právoplatným vlastníkom nehnuteľnosti a predávajúci dostane dohodnutú protihodnotu. Vďaka technológii blockchain by mohli byť všetky tretie strany v rámci tejto transakcie odstránené. Všetky detaily ohľadom vlastníctva, prevodu peňažných prostriedkov by boli zachytené a uložené v bloku v rámci štruktúry blockchain-data, ktorej kópiu majú všetci používatelia v sieti. Za týchto podmienok je jednoduché zistiť kto je vlastníkom nehnuteľnosti, či prebehla transakcia v súlade so zákonom aj či bola zrealizovaná úhrada. Dôvera sa presunula z centrálnej entity na všetkých používateľov, ktorí majú k dispozícií jednotný nemenný záznam o danom obchode. Vďaka tejto funkcii technológie blockchain sa eliminoval priestor na podvody a manipuláciu s ukladanými dátami so zámerom nezákonného zvýhodnenia niektorej zo strán.

3.1.4 Eliminácia príležitostí na nezákonné a nemorálne konanie podvody, korupcia, sprenevera majetku, daňové úniky

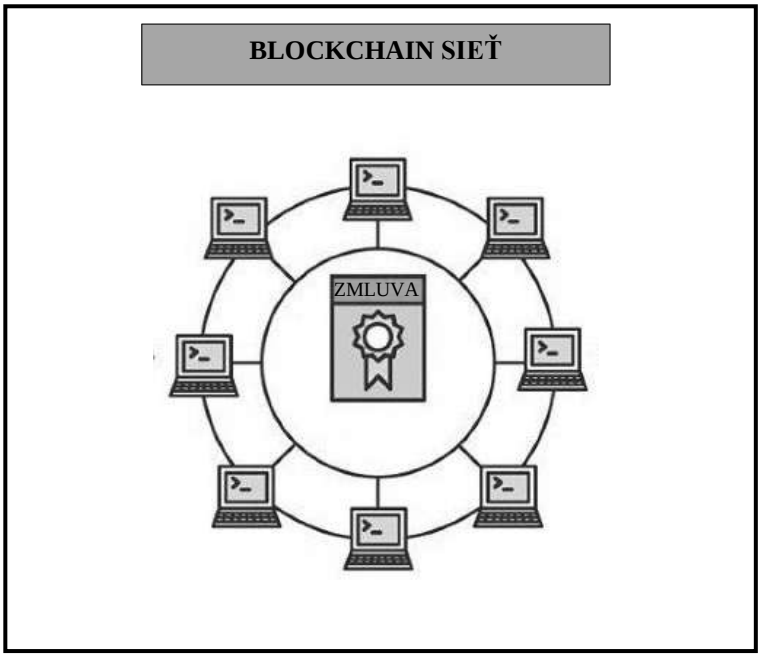
Vieme, že technológia blockchain funguje ako decentralizovaná sieť, v ktorej neexistuje žiadna centrálna nadradená jednotka. Všetci pripojení používatelia sú si rovnocenní a každý má prístup a rovnakú kópiu vkladaných dát do blockchain štruktúry. Blok je označený časovou pečiatkou, zabezpečený hash hodnotou a spojený s predchádzajúcim blokom v reťazci. Blockchain zabezpečuje informácie o pôvode majetku, kto bol jeho vlastníkom a kto je jeho aktuálnym vlastníkom. Predtým, ako je možné do štruktúry blockchain pripojiť blok s transakciou, sa musia účastníci siete konsenzuálne dohodnúť, že transakcia je platná prostredníctvom. Týmto spôsobom je výrazne eliminovaná možnosť pridávať do data štruktúry fiktívne transakcie, prevádzať majetok na podozrivé účty a používateľov. Ak by bola aplikácia blockchain verejná a umožňovala by aj náhľad do siete bez možnosti pridávania transakcií, vytvorilo by to priestor pre uľahčenie a zefektívnenie práce daňových kontrolných inštitúcií. Mali by prístup k transakciám v reálnom čase, čím by bolo znížené riziko manipulácie a úpravy s finančnými záznamami z dôvodu úpravy daňového základu. Ak by všetky transakcie, vrátane štátnych, prebiehali prostredníctvom technológie blockchain znížil by sa priestor na korupciu. Blockchain eliminuje mnohé druhy nezákonného a nemorálneho konania,

pretože všetky transakcie pridávané do štruktúry sú neustále kontrolované a auditované všetkými uzlami v sieti. Tento princíp nedovoľuje konať nezákonne potichu a konať nezákonne pred očami všetkých je našťastie stále pre väčšinu odrádzajúce.

3.1.5 Posilnenie istoty správnosti, jednotnosti a bezpečnosti histórie transakcií

Všetky vkladané transakcie do systému musia byť vždy schválené na základe procesu proof-of-work. Vďaka tomuto mechanizmu konsenzu, na ktorom blockchain funguje sa zvyšuje istota používateľov, že údaje v blockchain data štruktúre sú správne. Na obrázku môžeme vidieť ako systém schválil prostredníctvom konsenzu, že zmluva je legitímna. Existuje iba jedna jediná schválená verzia zmluvy, ktorá je rozposlaná každému používateľovi. Každý používateľ má istotu, že existuje jediná jednotná verzia zmluvy. Systém vždy vytvára jednu jedinú štruktúru blockchain-data, ktorá chronologicky uchováva vďaka hash hodnotám celú históriu transakcií. Tá je automaticky aktualizovaná u všetkých uzlov v sieti. Je nemožné, aby mal jeden uzol inú štruktúru blockchain-data ako iný uzol, tým pádom systém poskytuje používateľom istotu, že dáta sú jednotné a neexistuje žiadna iná verzia dát.

Obrázok 8 Mechanizmus konsenzu zabezpečujúci správnosť údajov



3.1.6 Eliminácia potreby fyzickej papierovej formy uchovávania dát a zníženie nákladov a úspora času

Pri použití blockchain aplikácií sú všetky údaje, dokumenty a transakcie vedené v digitálnej forme. Vďaka možnosti každého používateľa vlastniť kópiu vkladaných dát nie je potrebné, aby sa evidovali zmluvy, potvrdenia, listy vlastníctva jednoducho dokumenty vo fyzickej papierovej forme. Všetky dáta sú vždy dostupné a dostupnosť dát nie je ohrozená ani dočasným výpadkom siete, nakoľko existuje v sieti xy kópií. Rovnako vďaka tomu neexistuje hrozba znehodnotenia či zmiznutia dát, pokiaľ nedôjde k ukončeniu peer-to-peer siete.

Všetky spomínané výhody zavedenia metódy blockchain do praxe v oblasti účtovníctva a audítorstva v konečnom dôsledku prispievajú k časových a nákladovým úsporám. Spoločnosti by mali možnosť znížiť potrebu manuálneho zásahu pri zhromažďovaní, zmene a zdieľaní údajov. Dokumenty z účtovníctva potrebné na audit by boli ľahšie dostupné. V dôsledku toho by sa zamestnanci mohli zamerať výlučne na činnosti s pridanou hodnotou a potrebou ľudského faktora. Zosúlaďovanie dát v požadovaných intervaloch sú jasnými príkladmi časovo náročných a drahých procesov, ktoré by mohli zjednodušiť od základov činnosti finančných inštitúcií prijatím technológie blockchain. Finančné spoločnosti by boli schopné zdieľať digitálne výkazy všetkých zaznamenávaných dát napríklad vlastníctva aktív, sledovať vykonávanie, zúčtovanie a vyrovnanie transakcií s cennými papiermi mimo svojich pôvodných vlastníckych databáz bez toho, aby bolo potrebné zapojenie centrálneho systému správy databáz. Nahradením tretích strán aplikáciami blockchain by sa odstránili poplatky za správu, výdaj a overovanie dokumentov správcovským centrálnym entitám. Podľa štúdie Santander FinTech (2019) by technológia blockchain mohla do roku 2022 znížiť náklady na infraštruktúru finančných služieb okolo 15 miliardami USD až 20 miliárd dolárov ročne, čím by sa poskytla možnosť vyradiť z prevádzky staršie systémy a infraštruktúru a výrazne znížiť náklady na informačné technológie.

3.2 Perspektívy auditu z pohľadu využitia technológie blockchain

Vieme, že audit sa venuje overovaniu správnosti finančných výkazov, vecnej a formálnej správnosti účtovných dokladov. Preto môžeme konštatovať, že všetky výhody rozobrané v predchádzajúcej častiach budú schopné meniť povahu súčasných postupov auditu. Nasledujúcej tabuľke si zosumarizujeme tradičné metódy auditu a následne ich porovnáme s procesmi, ktoré by sa využívali po zavedení technológie blockchain.

Tabuľka 1 Porovnanie auditu teraz a po zavedení technológie blockchain

ÚKON	TRADIČNÁ METÓDA	AUDIT FORMOU BLOCKCHAIN
Pozorovanie a zisťovanie	písomné alebo ústne interview s pracovníkmi	overenie pracovných postupov blockchain data štruktúry, monitorovanie procesov a kontrolného systému, identifikácia narušovateľov procesov
Konfirmácie	kontrola zostatkov účtov prostredníctvom banky	prepojenie dátových tokov pomocou aplikácií blockchain, zúčastňovanie sa na reťazci a poskytovanie konsenzu
Overovanie záznamov, dokumentov a hmotného majetku	vytiahnutie vzorky a jej overovanie a porovnávanie, fyzická inventúra	overovanie presnosti a správnosti prvotných vstupov do blockchain data štruktúry
Prepočty a porovnania	vyňatie a prepočítavanie čísel na ich overenie, testovanie postupov na ich overenie	automatické monitorovanie a prepočítavanie. blockchain dát v požadovaných intervaloch, automatické sledovanie všetkých transakcií a identifikácia nesúladov
Analytické postupy	prezeranie, rozklad a štatistiky	filtrovanie blockchain dát v reálnom čase pomocou rovníc kontinuity a ďalších štatistík

V tabuľke 1 môžeme vidieť porovnanie, že aplikácia na princípe technológie blockchain dokáže nahradiť tradičné postupy pri audite. Priniesla by so sebou automatizovanú kontrolu dát, dokázala by vďaka hash hodnotám jednoducho identifikovať narušiteľov procesov a preveriť fungovanie kontrolného systému. Konfirmácie zo strany bánk by neboli viac potrebné, pretože by bola presunutá ich zodpovednosť za správnosť zostatkov účtov na blockchainovú sieť, kde je správnosť zabezpečovaná prostredníctvom konsenzuálnych dohôd. Overovanie vzorky vykazovaných údajov by bolo nahradené overovaním vstupných údajov, nakoľko chybovosť v rámci štruktúry blockchain-data môže byť vďaka vlastnostiam blockchainu spôsobená výlučne chybovosťou vstupných údajov, nie zlyhaním funkcionality blockchain siete. Rovnako by už nebolo potrebné vyťahovanie vzorky a prepočítavanie, pretože by to nahradili automatické procesy kontroly nesúladov a overovania. Na základe tejto komparácie môžeme konštatovať, že zavedením blockchainu do oblasti audítorstva by sa výrazne zjednodušil a zrýchlil proces auditu.

Záver

V našej práci sme pozornosť upriamili na analýzu funkcií a vlastností technológie blockchain s cieľom zistiť, či je schopná konkurovať súčasne používaným metódam v oblasti účtovníctva a audítorstva. V prvej časti sme sa venovali tomu, akú podporu pri zvádzaní technológie do praxe poskytuje súčasná národná a nadnárodná legislatíva. Následne sme si v jednotlivých podkapitolách rozobrali hlavné funkcie a vlastnosti blockchainu a zhrnuli kľúčové oblasti fungovania, ktoré sú potrebné na porozumenie toho, ako by mohla technológia blockchain ponúknuť náhradu za tradičné aktuálne používané metódy. Na základe získaných teoretických poznatkov sme dospeli k súhrnu významných všeobecných výhod, ktoré blockchain poskytuje. Nakoľko oblasť účtovníctva a audítorstva pracuje s dátami, ktoré hodnotí, uchováva a interpretuje, blockchain poskytuje veľký priestor na jeho implementáciu. Analýze toho, akým spôsobom a čo by prinieslo jeho využívanie v tejto sfére sme sa venovali v podkapitole 1.3, ktorá potvrdila, že všeobecné výhody sú uplatniteľné v rôznych oblastiach. Výsledky našej analýzy uvádzame v tretej kapitole, ktorá na praktických príkladoch ilustruje jednotlivé výhody vyplývajúce z využívania technológie blockchain. Jej implementácia do praxe poskytuje okrem zjednodušenia a zefektívnenia pracovných postupov aj riešenia niektorých nedostatkov problémov v mnohých odvetviach. Vďaka decentralizácií systému, mechanizmu konsenzov a zabezpečenia integrity prostredníctvom hash hodnôt výrazne eliminuje priestor pre nedôveru, sklony ku korupcii, nezákonnému konaniu a netransparetnosti.

Blockchain je zatiaľ budúcnosť. Inovácie v oblasti blockchain aplikácií naprieč rôznymi odvetviami však stále napredujú. Podniky v súčasnosti prehodnocujú svoje obchodné modely a posudzujú potrebu zavedenia riešení blockchain. Pri implementácií je dôležité mať na pamäti, že technológia blockchain by mala súčasné procesy zjednodušiť a zefektívniť. V rámci účtovníctva a audítorstva by blockchain zmenil tradičný systém práce. Pracovné postupy by sa zjednodušili a zefektívnili, čo poskytuje priestor presunu ľudského faktoru do oblastí, ktoré vyžadujú odbornosť a samostatné posúdenie. Rovnaký dopad by mal aj na audítorstvo. Tak ako počítače a internet zmenili a zefektívnili pracovné postupy vo všetkých odvetviach, technológia blockchain má potenciál pretvárať povahu fungovania dnešného finančného sektora. Poskytuje spôsob na rozsiahlu automatizáciu a digitalizáciu nielen účtovných procesov v súlade s regulačnými požiadavkami.

Veríme, že naše spracovanie témy poslúži čitateľom a študentom ako dobrý základ, pre pochopenie technológie blockchain a následne ponúkne priestor pre ďalšie možnosti jej využitia.

Použitá literatúra

Knižné publikácie

1. BERG, CH. – DAVIDSON, S. – POTTS, J. (2019). *Understanding the Blockchain economy: an introduction to institutional cryptoecnomics.* Cheltenham: Edward Elgar. 217 p. ISBN: 1788974999.
2. DRESCHER, D. (2017). *Blockchain basics: A non-technical introduction in 25 steps.* Germany: Apress, 259 p. ISBN-13 (pbk): 978-1-4842-2603-2.
3. HACIOGLU, U. (2019). *Blockchain economics and financial market innovation. Switzerland: Springer*, 568 p. ISBN 978-3-030-25275-5.
4. HOLBROOK, J. (2020) *Architecting enterprise blockchain solutions.* Canada: Wiley, 2020. 400 p. ISBN: 1119557690.
5. HABER, S. – STORNETTA S.W. (1991). (Online) *How toTime-Stamp a Digital Document. Journal of Cryptology*. Vol. 3, No. 2, s. 99 – 111,. ISSN 1432-1378.
6. HOSP, J. (2019). *Blockchain 2.0 simply explained: Far more than just Bitcoin. 1st edition.* Hong Kong: I-Unlimited, 299 p. ISBN: 1798916983.
7. MAILUND, T. (2019). *The joys of hashing: hash table programming with C. Denmark: Apress, 378 p. ISBN-13: 978-1484240656.*
8. ORAM, A. (2001).*Peer-to-peer: Harnessing the power of disruptive technologies* by. Sebastopol: O Reilly and Associates. 432 p. ISBN 13: 9780596001100.
9. PARISI, A. (2019) *Securing blockchain networks like Ethereum and hyperledger fabric,* Birmingham:Packt, 246 s. ISBN: 9781838646486
10. SCOTT, J.(2020). *Machine learning and blockchain: The power of convergence.* Hempton: Independently published, 52 p. ISBN-13: 978-1708224028.
11. STEIN SMITH, S.(2020). *Blockchain, artificial intelligence and financial services.* Switzerland: Springer, 263 p. ISBN: 3030297608.
12. TAPSCOTT, D. – TAPSCOTT, A.(2018) *Blockchain revolution, New York:Penguin,* 352 p. ISBN: 9781101980149.
13. UPADHYAY, N.(2019). *Transforming social media business models through Blockchain.* India: Emerald Publishing, 104 p. ISBN: 1838673024.
14. WELFARE, A. (2019). *Commercializing blockchain: Strategic applications in the real world, 1st Edition.* United Kingdom: Wiley, 352 p. ISBN: 978-1119578017.

Internetové zdroje

1. ANTONIOU, A. et. al. *Blockchain and the GDPR*, [dátum prístupu 14.3.2020] Dostupné na: https://www.standict.eu/sites/default/files/report_digital_assets_v1.0.pdf
2. BOUCHER, F. *How blockchain technology could change our lives*. [dátum prístupu 15.3. 2020] Dostupné na: www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA(2017)581948_EN
3. DAISYME, P. (2019) *Establishing blockchain policy* [dátum prístupu 18.4. 2020], Dostupné na: https://www.pwc.com/m1/en/publications/documents/establishing-blockchain-policy-pwc.pdf
4. ERNST & YOUNG, (2018). *Štúdia možností a potenciálu technológie „blockchain" pri zlepšovaní eGovernment riešení.* [dátum prístupu 20.3.2020] Dostupné na:https://www.vicepremier.gov.sk/wp content/uploads/2019/06/UPPVII-blockchain-studia-v2_3-20190318.pdf
5. HOUBEN, R. – SNYERS, A. (2018) *Cryptocurrencies and blockchain* [dátum prístupu 22.4.2020] Dostupné na: https://www.europarl.europa.eu/cmsdata/15071/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf
6. KONST, S. (2000) *Kryptograficky zabezpečené reťazce* [dátum prístupu 22.4 2020] Dostupné na http://www.konst.de/stefan/seclog.pdf
7. MURREN, J. – YOUNG, A. – VERHULST S. (2018) *Case study Adressing transaction cost through blockchain* [dátum prístupu 27.4.2020] Dostupné na: https://blockchan.ge/blockchange-land-registry.pdf
8. PECK, E. M. (2012) *How Bitcoin brought privacy to electronic transactions* [dátum prístupu 19.3.2020]Dostupné na: https://spectrum.ieee.org/computing/software/bitcoin-the-cryptoanarchists-answer-to-cash
9. SANTANDER FINTECH. (2019) *Rebooting financial services* [dátum prístupu 27.3.2020]Dostupné na: https://www.finextra.com/finextra downloads/newsdocs/the%20fintech%202%200%20paper.pdf
10. SEDLIAKOVA, K,(2018) *Inovácie a zmeny v platobných službách podľa PSD2*, [dátum prístupu 18.4. 2020] Dostupné na: http://www.nbs.sk/_img/Documents/_PUBLIK_NBS_FSR/Biatec/Rok2018/01-2018/Biatec_18_1_01.
11. The Institute of Chartered Accountants in England and Wales (2018) *History of blockchain* [dátum prístupu 12.3.2020] Dostupné na: https://www.icae

w.com/technical/technology/blockchain/blockchain- articles/what is blockchain/history

12. The Institute of Chartered Accountants in England and Wales, (2020) [dátum prístupu 12.3.2020] Dostupné na: https://www.icaew.com//media/corporate/files/technical/information-technology/thought-leadership/blockchain-and-the-future-of-accountancy.ashx

Právna úprava

1. Smernica Európskeho parlamentu a Rady (EÚ) č. 2015/2366 z 25. novembra 2015 o platobných službách na vnútornom trhu, ktorou sa menia smernice 2002/65/ES, 2009/110/ES a 2013/36/EÚ a nariadenie (EÚ) č. 1093/2010 a ktorou sa zrušuje smernica 2007/64/ES
2. Smernica Európskeho parlamentu a Rady (EÚ) 2018/843 z 30. mája 2018, ktorou sa mení smernica (EÚ) 2015/849 o predchádzaní využívaniu finančného systému na účely prania špinavých peňazí alebo financovania terorizmu a smernice 2009/138/ES a 2013/36/EÚ
3. Zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov vychádzajúci z Nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679,
4. Zákon č. 431/2002 Z. z. o účtovníctve,
5. Zákon č. 492/2009 Z. z. o platobných službách a o zmene a doplnení niektorých zákonov v znení neskorších predpisov