EKONOMICKÁ UNIVERZITA V BRATISLAVE
FAKULTA HOSPODÁRSKEJ INFORMATIKY
Evidenčné číslo: 103004/I/2024/36122163740154372

Metódy využitia technológie blockchain vo verejnom sektore

Diplomová práca

Bratislava 2024 **Bc. Michael Macek**

EKONOMICKÁ UNIVERZITA V BRATISLAVE
FAKULTA HOSPODÁRSKEJ INFORMATIKY
Evidenčné číslo: 103003/I/2024/31622163740154372

Metódy využitia technológie blockchain vo verejnom sektore

Diplomová práca

Študijný program: Informačný manažment

Študijný odbor: ekonómia a manažment

Školiace stredisko: KAI FHI - Katedra aplikovanej informatiky

Vedúci záverečnej práce: RNDr. Eva Rakovská, PhD.

Bratislava 2024 **Bc. Michael Macek**

Ekonomická univerzita v Bratislave
Fakulta hospodárskej informatiky

PRIHLÁŠKA NA ZÁVEREČNÚ PRÁCU

Meno a priezvisko študenta: Bc. Michael Macek
Študijný program: informačný manažment (Jednoodborové štúdium, inžiniersky II. st., denná forma)
Študijný odbor: 8. - ekonómia a manažment
Typ záverečnej práce: Inžinierska záverečná práca
Jazyk záverečnej práce: slovenský
Sekundárny jazyk: anglický

Názov: Možnosti využitia technológie blockchain vo verejnom sektore

Anotácia: Diplomová práca je zameraná na utvorenie komplexného obrazu inovatívnej technológií blockchain. V teoretickej časti je detailne popísaný jej princíp fungovania, možnosti použitia a ich silné a slabé stránky. Praktická časť je venovaná detailnému opisu vybranej sféry použitia technológie blockchain. V praktickej časti detailne vysvetlí a implementuje vybranú oblasť možnosti využitia.

Vedúci: RNDr. Eva Rakovská, PhD.
Katedra: KAI FHI - Katedra aplikovanej informatiky
Vedúci katedry: Ing. Mgr. Peter Schmidt, PhD.

Dátum schválenia: 14.03.2023

podpis študenta

Poďakovanie

Touto cestou chcem vyjadriť úprimnú vďaku vedúcej záverečnej práce, RNDr. Eve Rakovskej, PhD., za jej venovaný čas, cenné usmernenia, odborné rady a neustálu podporu počas celého procesu. Vaše znalosti a skúsenosti boli pre mňa veľkým zdrojom inšpirácie, a vaša trpezlivosť a ochota ma viedli pri písaní tejto záverečnej práce.

Na záver by som rád využil túto príležitosť a poďakoval sa svojmu okoliu, najmä mojim rodičom, za poskytnutú možnosť študovať a za neoceniteľnú pomoc a podporu. Osobitne by som chcel poďakovať môjmu otcovi, ktorého múdrosť a celoživotná podpora ma viedla k odovzdaniu tejto záverečnej práce.

ABSTRAKT

MACEK, Michael: *Možnosti využitia technológie blockchain vo verejnom sektore* – Ekonomická univerzita v Bratislave, Fakulta hospodárskej informatiky; Katedra aplikovanej informatiky – Vedúci záverečnej práce: RNDr. Eva Rakovská, PhD. – Bratislava: FHI EU, 2024, 76s

Hlavným zámerom tejto záverečnej práce bolo ukázať, kde a ako môže technológia blockchain prispieť k efektívnemu fungovaniu verejného sektora. Preto sme sa zamerali na identifikáciu oblastí, kde táto nová technológia ponúka najväčší potenciál a praktické využitie. Naša práca je štruktúrovaná do štyroch kapitol a je doplnená 22 obrázkami a 7 tabuľkami. V úvodnej kapitole sme podrobne charakterizovali technológiu blockchain a jej základné princípy, ako je hašovanie, konsenzus, rôzne typy blockchainov a inteligentné zmluvy. V nasledujúcej kapitole sme stanovili hlavný cieľ a čiastkové ciele našej práce. Tretia kapitola sa zaoberala metodológiou výskumu a použitými metódami, ktoré sme uplatnili pri tvorbe tejto práce. V štvrtej a poslednej časti sme sa venovali konkrétnym príkladom použitia technológie blockchain a zhodnotili sme jej potenciál v rôznych odvetviach, ako sú vládne a finančné služby, zdravotníctvo a doprava.

Kľúčové slová:

blockchain, technológia distribuovaných záznamov, verejný sektor, decentralizácia

ABSTRACT

MACEK, Michael: *The potential applications of blockchain technology in the public sector* – University of Economics in Bratislava, Faculty of Economic Informatics; Department of Applied Informatics – Thesis supervisor: RNDr . Eva Rakovská, PhD. – Bratislava: FHI EU, 2024, 76p

The main aim of this diploma thesis was to demonstrate where and how blockchain technology can contribute to the efficient functioning of the public sector. Therefore, we focused on identifying areas where this new technology offers the greatest potential and practical utility. The thesis is structured into four chapters and contains 22 figures and 7 tables. In the first chapter, we extensively characterized blockchain technology and its fundamental principles, such as hashing, consensus, various types of blockchains, and smart contracts. In the following chapter, we established the main goal and partial objectives of our work. The third chapter is devoted to the research methodology and the methods used while writing this thesis. In the fourth and final part, we characterised specific examples of blockchain technology usage and evaluated its potential in various sectors, such as government, financial services, healthcare, and transportation.

Keywords:

blockchain, distributed ledger technology, public sector, decentralization

OBSAH str.

Zoznam ilustrácií

Zoznam tabuliek

Úvod

Sedemdesiate roky minulého storočia priniesli svetu mnohé inovácie, ale vytvorenie kryptografie s verejným kľúčom je možno jednou z najcennejších, hoci podceňovaných inovácií. Predtým bola kryptografia vo všeobecnosti prevažne doménou vojenských a spravodajských služieb, ktoré zabezpečovali svoju vlastnú komunikáciu. Výskumné aktivity v tejto oblasti boli väčšinou obmedzené na agentúry s 3 písmenami, či už tie, ktoré spadali priamo pod vládny dohľad, ako NSA, alebo súkromné podniky s príslušnými licenciami, ako napríklad IBM. Významným míľnikom bola počiatočná fáza a následná publikácia kryptografie s verejným kľúčom Martinom Hellmanom, Whitfieldom Diffiem a Ralphom Merkleom. [3]

Stuart Haber a W. Scott Stornetta uviedli zabezpečený reťazec blokov (súbor záznamov) v roku 1991. V roku 2008 osoba alebo skupina pod pseudonymom „Satoshi Nakamoto“ konceptualizovala a implementovala technológiu blockchain. Ich návrh zahŕňal použitie hašovania v blockchain systéme na zabezpečenie nezmeniteľnosti a nemožnosti odstránenia záznamov uložených v systéme blockchain. Tento vynález viedol k novému technologickému pokroku, ktorý zmenil mnohé odvetvia a systémy. Schopnosť zabezpečiť dáta prostredníctvom decentralizovaného systému, ktorý je úplne transparentný a overiteľný, zmenila technologický svet a bola kľúčová pre vznik kryptomien. Tento dizajn blockchainu sa stal základnou technológiou nielen pre bitcoin a ďalšie digitálne meny, ale aj pre súkromný a verejný sektor. [15] Práve na verejný sektor je zameraná táto záverečná práca - ako je napríklad tvorba transparentných verejných obstarávaní, vytvorenie bezpečnejšieho volebného systému či možnosti overovania univerzitných diplomov.

Záverečná práca sa zaoberá technológiou blockchain a jej využitím mimo oblasti kryptomien. V prvej kapitole sa zameriavame na teoretické základy, kde vysvetľujeme charakteristiky tejto technológie a princípy, ako je hašovanie, konsenzus, typy blockchainu či inteligentné zmluvy. V druhej a tretej kapitole stanovujeme ciele práce a vysvetľujeme metodiku výskumu, ktorú použijeme na ich dosiahnutie.

V štvrtej časti sa venujeme konkrétnym prípadom použitia a zhodnoteniu potenciálu tejto technológie v rôznych odvetviach, vrátane vládnych a finančných služieb, zdravotníctva či dopravy.

1 Súčasný stav riešenej problematiky doma a v zahraničí

"Technológia blockchain je pre mnohých revolučná, podobne ako nástup internetu" *(Rosic, 2016*).

"Blockchain je nezničiteľná sieť ekonomických transakcií, ktorá v budúcnosti môže slúžiť nielen finančníctvu, ale v podstate všetkému, čo má hodnotu." (*Don & Alex Tapscott, autori knihy Blockchain Revolution 2016*)

Často sa o nej hovorí ako o novom "stroji dôvery", pretože umožňuje ľuďom interakciu a vykonávanie transakcií aj bez predchádzajúceho vzťahu. Hoci o tejto technológii čítame čoraz viac, len málo zdrojov ju vysvetľuje zrozumiteľným spôsobom a ešte menej sa zameriava na jej uplatnenie vo verejnom sektore. Napríklad, v oblasti tvorby transparentných volebných systémov alebo možností v zdravotníctve a školstve [16]

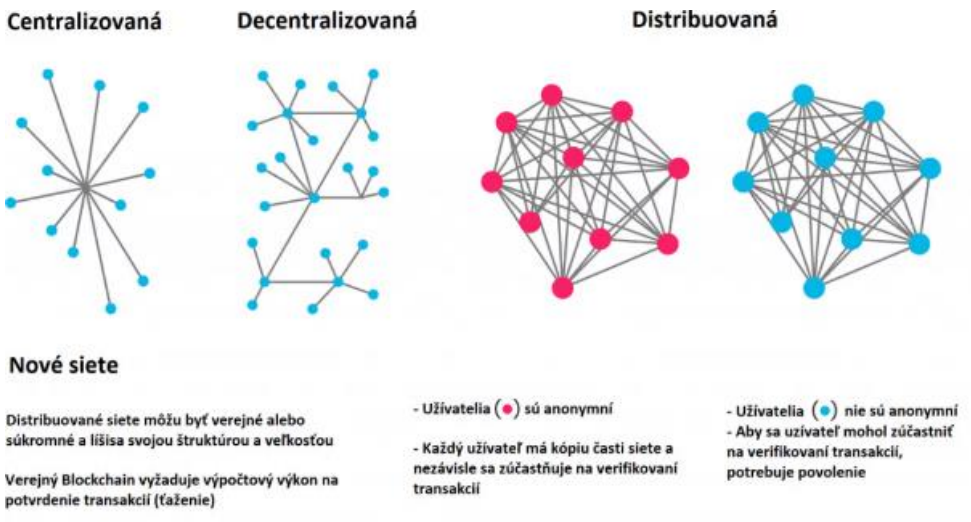
1.1 Blockchain vo všeobecnosti

Technológia blockchain je formou distribuovanej účtovnej knihy (DLT), ktorá funguje ako otvorený a dôveryhodný zoznam transakcií od jednej strany k druhej (alebo viacerým), ktorý nie je uložený centrálne. Namiesto toho je kópia uložená u každého používateľa, ktorý používa softvér blockchain a je pripojený k sieti blockchain - nazývaný tiež uzol. Namiesto toho, aby centrálna autorita udržiavala databázu, všetky uzly majú kópiu knižnice a aktualizácie knižnice technológie blockchain sa šíria cez sieť v priebehu niekoľkých minút alebo sekúnd. V týchto sieťach musí väčšina uzlov prehodnotiť a overiť transakciu, než ju je možné overiť a zapísať. Týmto spôsobom nikto nemôže manipulovať s knižnicou, každý ju môže preskúmať a dôverovať jej. Pre jednotlivé transakcie používa blockchain kryptografiu na zabezpečenie transakcií. [17]

Teda blockchain je decentralizovaný systém s rastúcimi zoznamami záznamov, známymi ako bloky, ktoré sú bezpečne prepojené pomocou kryptografických hašov. Každý blok obsahuje haš predchádzajúceho bloku, časovú pečiatku a údaje o transakciách. Tieto údaje sú často organizované do štruktúry Merkleho stromu (Merkle tree). Pretože každý blok obsahuje informácie o predchádzajúcom bloku, efektívne vytvárajú reťazec, pričom každý ďalší blok odkazuje na predchádzajúci. To znamená, že transakcie v blockchaine sú nezvratné, pretože akonáhle sú zaznamenané, údaje v akomkoľvek bloku nemôžu byť retroaktívne zmenené bez zmeny všetkých nasledujúcich blokov. [18]

Blockchain je obvykle riadený peer-to-peer (P2P) počítačovou sieťou, kde uzly spoločne dodržiavajú protokol algoritmu konsenzu na pridávanie a overovanie nových transakčných blokov. Hoci záznamy v blockchaine nie sú úplne nezmeniteľné kvôli možnosti blockchain rozvetvení (forkov), považujeme sa ich za bezpečné z hľadiska dizajnu a demonštrujú distribuovaný výpočtový systém s vysokou odolnosťou voči chybám typickou pre byzantskú odolnosť. [2]

Ako sme už spomenuli v úvode, blockchain je špecifický typ databázy, ktorý je rozložený a šírený medzi účastníkmi siete. Termín decentralizácia sa často zamieňa s distribúciou. Distribúcia sa týka miesta uloženia dát. V prípade distribuovaných databáz sú dáta uložené na viacerých miestach (počítačových zariadeniach). Decentralizácia sa zasa týka úrovne kontroly a rozhodovania. Verejný blockchain je teda decentralizovaný, kde rozhodovanie a kontrola sú rozložené medzi účastníkov siete. Neexistuje tu žiadna centrálna autorita, ktorá by napríklad rozhodovala o obsahu nového bloku v transakciách na blockchaine. [19]



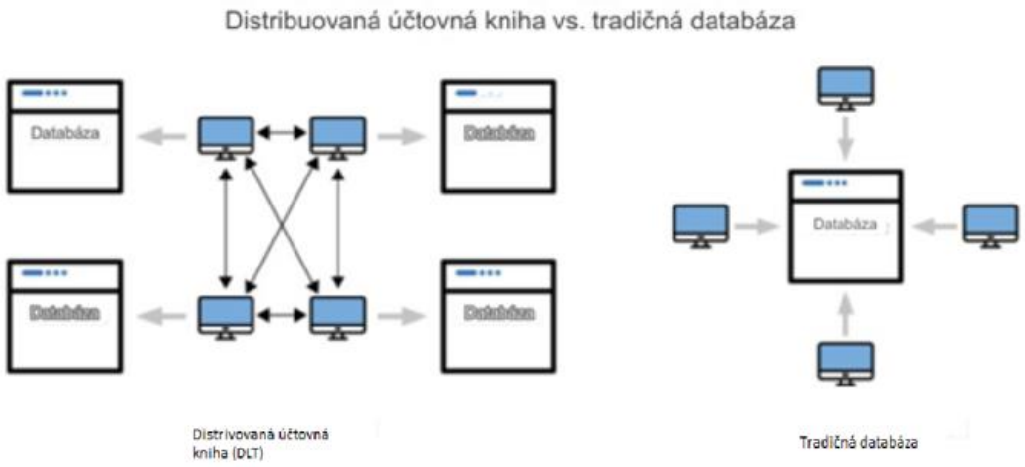
Obrázok 1: Graficky znázornený rozdiel komunikácie uzlov

Zdroj: [20]

1.2 Porovnanie sieti blockchain a tradičnej databázy

V tradičných databázach používaných v priemysle alebo štátnej správe sa zvyčajne využíva technológia klient-server. Používateľ sa pripája na centrálny server, ktorý mu umožňuje pristupovať k dátam v závislosti od udelených oprávnení. Kontrolu nad databázou má administrátor, či už je to konkrétna osoba alebo organizácia so stanovenými rolami a

procesmi. Administrátor má v tomto systéme plnú kontrolu nad databázou a jej obsahom. [21]



Obrázok 2: Porovnanie distribuovanej účtovnej knihy (DLT) a tradičnej databázy

Zdroj: [22]

Problémom môže byť kompromitácia administrátora, čo môže umožniť útočníkovi neoprávnene meniť, mazať alebo zapisovať dáta, ktoré odporujú pravidlám. Skúsenosti ukazujú, že sa nejedná len o teoretickú hrozbu. Blockchain je decentralizovaná databáza bez jedného dedikovaného administrátora. Všetky záznamy sú zdieľané a verifikované v širšej skupine validátorov, a sú nemeniteľné a nezmazateľné. Blockchain je teda vhodný práve tam, kde sú buď vysoké požiadavky na integritu dát, kde je narušená dôveryhodnosť centrálnej autority, resp. jej schopnosť zabrániť neoprávnenému prístupu, alebo by vytvorenie dostatočne dôveryhodnej autority bolo príliš nákladné, čo sumarizuje **tabuľka 1**. [17]

Vlastnosť / Riešenie	Centralizovaný systém	Privátny blockchain	Konzorčný blockchain	Verejný blockchain
Súkromie	vysoké	vysoké	stredné	nízke
Bezpečnosť	nízka	stredná	vysoká	najvyššia
Škálovateľnosť	najvyššia	stredná	stredná	nízka
Sila centrálnej autority	najvyššia	stredná	stredná	žiadna

Tabuľka 1: Porovnanie kľúčových vlastnosti s typom systému

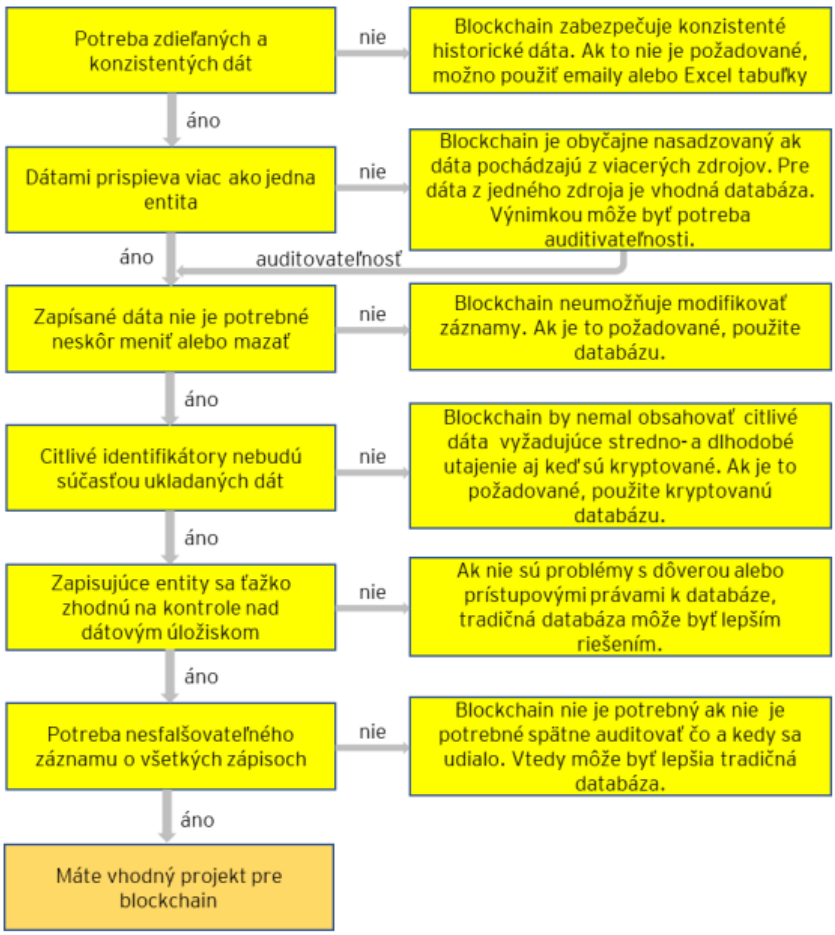
Zdroj: [17]

Technológia blockchain a hlavne jej využitie mimo kryptomien je stále veľmi nová a málo prebádaná oblasť. Spoločnosti a vlády sa snažia o zavádzanie tejto technológie, no jej nasadenie nie je vždy vhodné – oblasti vhodného nasadenia stále nie sú ustálené a vyvíjajú sa. Nižšie sú zosumarizované hlavné znaky, kedy je vhodné využiť blockchain.

Blockchain je vhodné použiť, ak musí riešenie reflektovať: [17] [16]

1. **Mnoho účastníkov**: Keď je potrebné zabezpečiť a spravovať transakcie medzi veľkým počtom účastníkov.
2. **Potreba nastolenia dôvery**: Pri potrebe vytvoriť dôveru medzi účastníkmi, najmä ak neexistuje centrálne autoritatívny zdroj dôvery.
3. **Neexistencia alebo nedôveryhodnosť tretej strany**: V prípade, že neexistuje dôveryhodná tretia strana alebo je ťažké jej dôverovať.
4. **Charakter transakcií**: Pre úlohy, ktoré majú charakter transakcií, ako napríklad finančné transakcie alebo správa digitálnych aktív.
5. **Globálny digitálny identifikátor**: V prípade potreby globálneho digitálneho identifikátora, ktorý je dôveryhodný a nezmeniteľný.
6. **Kryptograficky zabezpečená evidencia vlastníctva**: Pri potrebe zabezpečiť dôveryhodnú evidenciu vlastníctva prostredníctvom kryptografických prostriedkov.
7. **Zjednodušenie riešenia sporov**: Ak je potrebné zjednodušiť riešenie sporov prostredníctvom transparentnosti a nezvratnosti transakcií.
8. **Zdieľanie histórie transakcií**: Pre potrebu zdieľania histórie transakcií a pôvodu digitálnych aktív medzi účastníkmi.
9. **Monitorovanie aktivít v reálnom čase**: Ak je potrebné, aby regulátor mohol monitorovať aktivity regulovaných subjektov v reálnom čase.

Nasledujúci vývojový diagram slúži na posúdenie vhodnosti využitia technológie blockchain. [17]



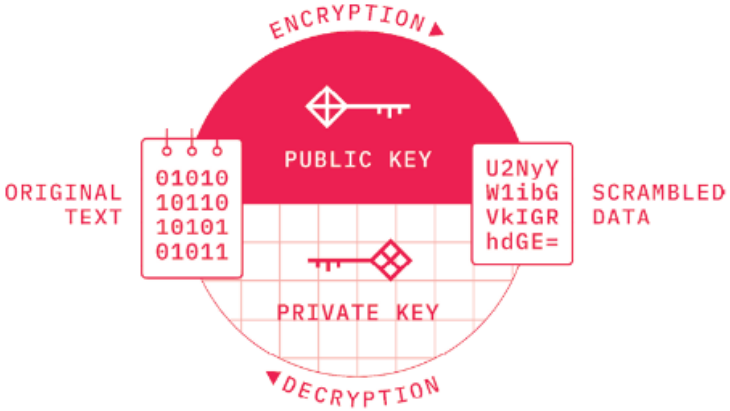
Tabuľka 2:Vývojový diagram vhodnosti použitia blockchainu

Zdroj: [17]

1.3 Kryptografia verejným kľúčom (PKI)

Kryptografia verejným kľúčom je založená na asymetrickom šifrovaní, a teda používa dva kľúče - privátny a verejný. Verejný kľúč slúži na šifrovanie, a ako vyplýva z názvu, môže byť zdieľaný verejne, zatiaľ čo privátny kľúč slúži na dešifrovanie a nemal by byť zdieľaný so žiadnou treťou stranou okrem prijímateľa správy. [23]

Pri blockchaine sa tento princíp nevyužíva na šifrovanie, ale na generovanie digitálnych podpisov a na vytvorenie párového kľúča. Verejný kľúč, odvodený z privátneho kľúča, určuje adresu prijímateľa transakcie. Verejný kľúč slúži na prijímanie transakcií, zatiaľ čo privátny kľúč umožňuje autorizáciu odchádzajúcich transakcií digitálnym podpisom. Tento podpis môžu overiť všetci účastníci siete, pričom nie je potrebné zverejniť privátny kľúč odosielateľa. Tento princíp vysvetľujú **obrázok 3** a **obrázok 4**.



Obrázok 3: Ukážka kryptografie verejným kľúčom

Zdroj: [3]

Obrázok 4: Ukážka kryptografie verejným kľúčom pri dvoch uzloch

Zdroj: [24]

1.4 Peer-to-peer sieť (P2P)

Sieť peer-to-peer (P2P) je decentralizovaná a distribuovaná, čo znamená, že uzly nie sú pripojené k centrálnej autorite alebo serveru. V P2P sieti sú všetky uzly nezávislé a priamo prepojené, aby mohli vykonávať transakcie alebo výmenu informácií. Vo verejnom blockchaine nie je potrebné dôverovať každému uzlu osobne. Sieť a bezpečnosť sú navrhnuté tak, aby umožnili autentické a legitímne transakcie, aj keď identita odosielateľa a príjemcu zostane anonymná. P2P je bezpečná sieť s priamym kontaktom medzi dvoma

uzlami. Účastnícky uzol takejto siete nemá geografické obmedzenia a môže byť súčasťou siete odkiaľkoľvek na svete. [3] [4]

Blockchain funguje ako distribuovaná účtovná kniha, kde dátový záznam nie je udržiavaný centrálnou autoritou, ale je dostupný na každom uzle P2P siete. Každý účastnícky uzol uchováva aktualizované kópie dátového záznamu alebo účtovnej knihy v systéme blockchain. Napríklad, vo verejnej bitcoin sieti majú všetky uzly rovnakú kópiu záznamu o všetkých bitcoinových transakciách. Týmto spôsobom je celá sieť odolná voči podvodom, pretože každý má legitímnu kópiu záznamov a nemôže sa falšovať žiadna transakcia. [18]

Celú históriu bitcoin transakcií je možné si podrobne overiť napríklad na [25].

1.5 Hašovanie

Hašovanie je kryptografický proces, ktorý používame na zabezpečenie údajov v blockchain sieti. Bežne sa používajú rôzne typy hašovacích funkcií, ako napríklad MD5, SHA1 alebo SHA256. V blockchain sieti sa často využíva SHA-256 (Secure Hash Algorithm) na hašovanie transakcií. [5] [26]

Šifra SHA-256 je navrhnutá tak, aby bola odolná voči hrubému prehľadávaniu, čo znamená, že je takmer nemožné nájsť dve rôzne vstupy, ktoré by vytvorili rovnaký haš. Táto vlastnosť robí SHA-256 veľmi dôležitou pre rôzne aplikácie kryptografie, vrátane kryptomeny Bitcoin. [27]

Vstupná hodnota môže obsahovať ľubovoľný prvok, ako je text, čísla, mediálne súbory atď. akejkoľvek dĺžky. Výstup hašovania však bude mať vždy rovnakú dĺžku. Tento výstup variabilného vstupu s pevnou dĺžkou je známy ako hodnota haš.

Hašovanie je kľúčovým prvkom bezpečnosti blockchainu. Umožňuje zabezpečiť údaje o transakciách tak, že sú chránené pred neoprávneným prístupom a zmenou. Údaje, keď sú zahašované a uložené v blockchaine, sú takmer nezraniteľné voči krádeži alebo zneužitiu. Ak niekto skúsi zmeniť haš bloku alebo transakcie, vyžaduje to obrovskú časovú a výpočtovú náročnosť. Dokonca aj malá zmena v údajoch v bloku spôsobí zmenu hašu, čo narúša celý reťazec. Týmto spôsobom blockchain odhalí akékoľvek pokusy o zmenu údajov. SHA-256, používaný v blockchainoch, je považovaný za jednu z najbezpečnejších hašovacích funkcií a zatiaľ nebol narušený. [17] [18] [23]

Kryptografická hašovacia funkcia má tieto kľúčové vlastnosti:

1. Je jednosmerná: Znamená to, že z výstupu je takmer matematicky a výpočtovo
2. nemožné získať vstup. Počítanie výstupu by malo byť naopak rýchle.
3. Haš musí byť náhodný: Bezpečné hašovacie funkcie by mali produkovať výrazne
4. odlišné výstupy. Aj keby sa vstup líšil iba o jeden bit, tak výstup musí byť odlišný.
5. Je odolná voči kolíziám: To je prípad, keď hašovacia funkcia vytvorí dva rovnaké výstupy pre viac vstupov. Táto situácia by sa nemala stávať.
6. Adresy v blockchaine sú odvodené od procesu hašovania verejných kľúčov. Je veľmi dôležité, aby tu nedochádzalo ku kolíziám, napríklad generovaním rovnakého hašu pre rozdielne adresy.
7. Bloky v sieti blockchain sú na seba viazané hašom. [23]

Vstup:	Výstup: haš pomocou hašovacieho algoritmu: SHA-256
Michael Macek	699869d70756468d7f8ba28bfc0ed7f6ac3900b844d39c6cf7ceed404e0988b1
záverečná práca	6232925e42db78f97b35c411c0bc2b7df85ca9ee460feb961575945ba0c14d87
Michael Macek záverečná práca	9093226bfb6134d99a3df32665c16788ec78066f53913b108dadccabad0b00c1

Obrázok 5: Ukážka hašovania pomocou SHA-256

Zdroj: Vlastné spracovanie

1.6 Bloky a ich štruktúra v blockchaine

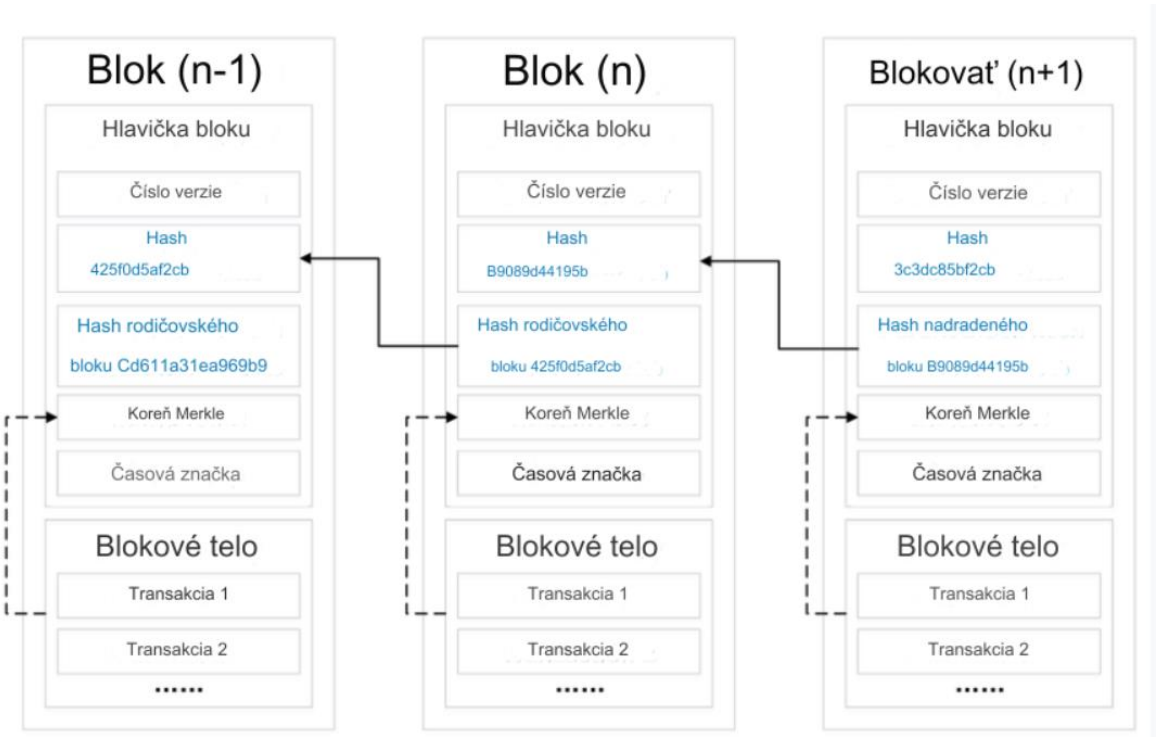
Jeden blok v blockchaine má hlavičku bloku, počítadlo transakcií, veľkosť bloku a údaje o transakcii. Jediný blok v blockchaine teda obsahuje informácie o dátach a iných aspektoch bloku. [24]

Tabuľka 3 a **obrázok 6** popisujú najpoužívanejšiu štruktúru bloku.

Pole	Veľkosť poľa	Význam
Hlavička bloku	80 bajtov	Obsahuje haš, haš predchádzajúceho bloku, časovú pečiatku, nonce ...
Veľkosť bloku	4 bajty	Zobrazuje veľkosť celého bloku.
Počítadlo transakcií	1-9 bajtov	Zobrazuje celkový počet transakcií obsiahnutých v bloku.
Transakcie	najmenej 400 bajtov	Obsahuje všetky transakcie v bloku.

Tabuľka 3: Popis štruktúry blokov v blockchaine

Zdroj: spracované podľa [4]



Obrázok 6: Tradičné reťazenie blokov a s ich komponentami

Zdroj: [28]

1.6.1 *Hlavička bloku*

Hlavička bloku je kľúčovou súčasťou, pretože obsahuje všetky dôležité informácie o bloku a transakciách. Obsahuje tiež unikátny haš predchádzajúceho bloku, čo pomáha udržiavať integritu v sieti blockchain. Nižšie v tabuľke nájdete šesť hlavných komponentov hlavičky bloku.

Pole	Veľkosť poľa	Význam
Verzia bloku	4 bajty	Číslo verzie bloku na sledovanie aktualizácií softvéru alebo protokolu.
Haš predchádzajúceho bloku.	32 bajtov	Haš predchádzajúceho bloku.
Koreň Merkle (Merkle root)	32 bajtov	Hodnota haš koreňa Merkle tree (Hašovacieho stromu) transakcií aktuálneho bloku. Tento haš koreňa je známy ako Merkle root.
Časová pečiatka (Time stamp)	4 bajty	Čas vytvorenia bloku.
Nonce	4 bajty	Číslo potrebné pre proces konsenzu Proof of Work (PoW).
Cieľ obťažnosti	4 bajty	Cieľová obťažnosť nastavená pre algoritmus Proof-of-Work. (V prípade ak blockchain funguje na báze PoW).

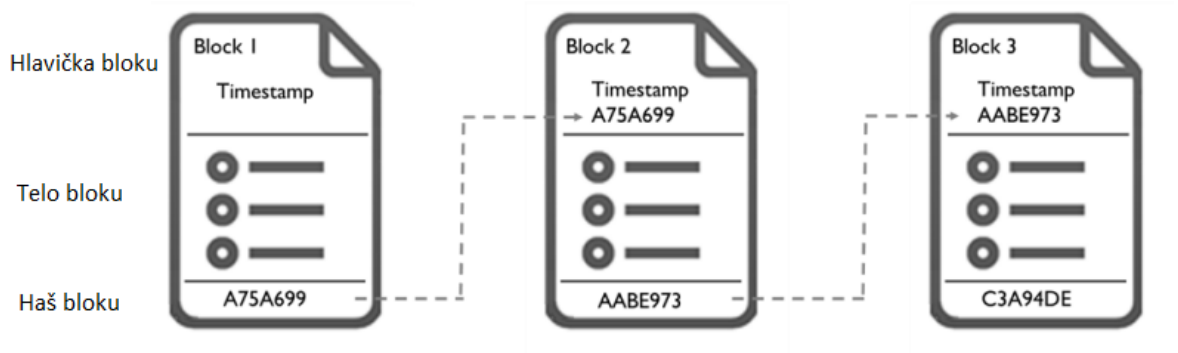
Tabuľka 4: Popis štruktúry hlavičky bloku v blockchaine

Zdroj: spracované podľa [4]

Blockchain uzly používajú blokový haš jedného bloku (predchádzajúceho) na jeho prepojenie s nasledujúcim blokom. Systém vytvára blokový haš pomocou kryptografických metód algoritmu SHA256, čo zabezpečuje bezpečnosť každého bloku podobne ako digitálny odtlačok prsta alebo podpis. [3]

1.6.2 *Zoskupenie blokov v reťazci*

Blok sa skladá z dvoch častí: tela, ktoré obsahuje zaznamenané transakcie, a hlavičky, ktorá obsahuje dôležité údaje ako verziu, haš predchádzajúceho bloku, merkle root, časovú pečiatku, nonce a cieľovú obtiažnosť. Bloky sú spojené do reťazca pomocou hašov predchádzajúcich blokov, čím vytvárajú "blockchain“ [23]



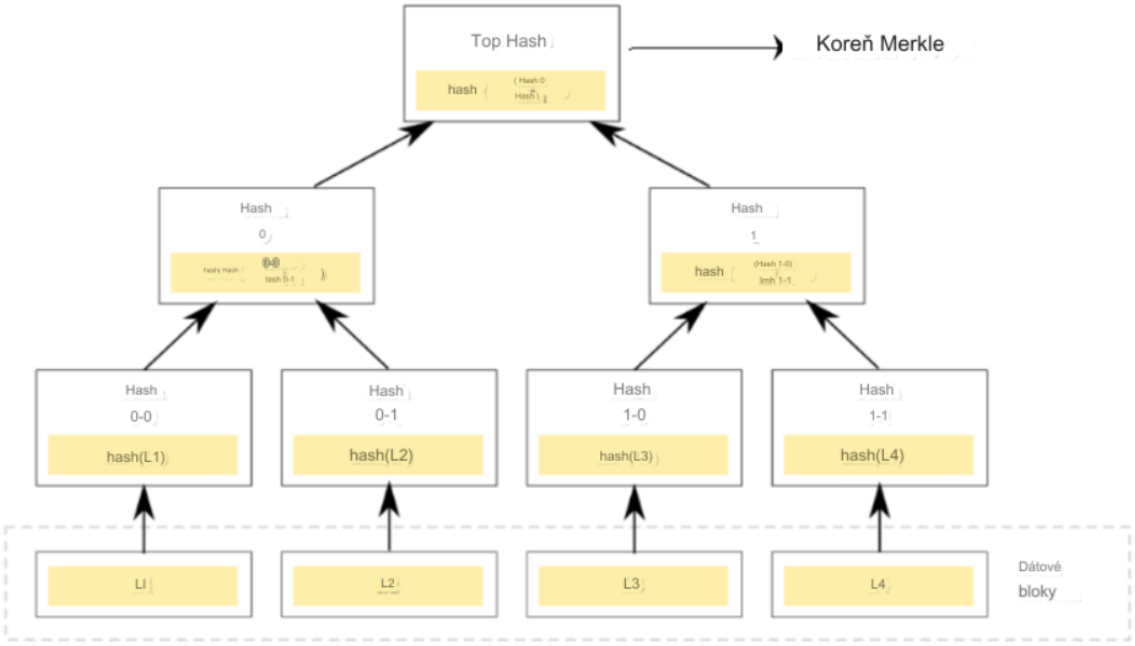
Obrázok 7: Jednoduché znázornenie blockchainu obsahujúci tri základné bloky

Zdroj: spracované podľa [6])

Prvý blok, známy aj ako blok Genesis, je očíslovaný číslom 0, ďalší blok 1 a tak ďalej. Pri pridávaní nového bloku systém vytvorí preň jedinečnú hodnotu hašu. Ďalší blok potom využije túto hodnotu hašu ako „haš predchádzajúceho bloku“, čím vytvorí bezpečné spojenie v reťazci blokov. Táto štruktúra blockchainu je odolná voči falšovaniu, pretože akákoľvek zmena v transakčných údajoch v jednom bloku zmení hodnotu haš, čo naruší integritu celej reťazca. Aby niekto urobil zmenu v údajoch blockchainu, potrebuje obrovský výpočtový výkon na prepočítanie hašu celej siete blockchain. [3] [6]

1.6.3 *Hašovacie stromy*

Pomocou hašovacích stromov (Merkleho stromov / Merkleho koreňa) môže byť v jednom riadku zobrazený obrovský zoznam transakcií alebo iných informácií. Ak zmeníme jeden symbol v zozname, zmení sa aj strom a konečný haš. To znamená, že sa zmení aj vrchol stromu. Preto nemôžete jednoducho nahradiť transakciu v bloku alebo zmeniť existujúce údaje. Hašovací strom je efektívny spôsob zaznamenávania transakcií v blockchaine. Existuje aj Merkle Proof, ktorý overuje platnosť informácií pomocou hašov. Namiesto preverovania celého dátového poľa stačí skontrolovať jednotlivé haše v strome, čo šetrí výpočtový výkon. [29]



Obrázok 8: Ukážka vetvenia hašovacieho stromu

Zdroj: [30]

1.7 Inteligentná zmluva (smart contract)

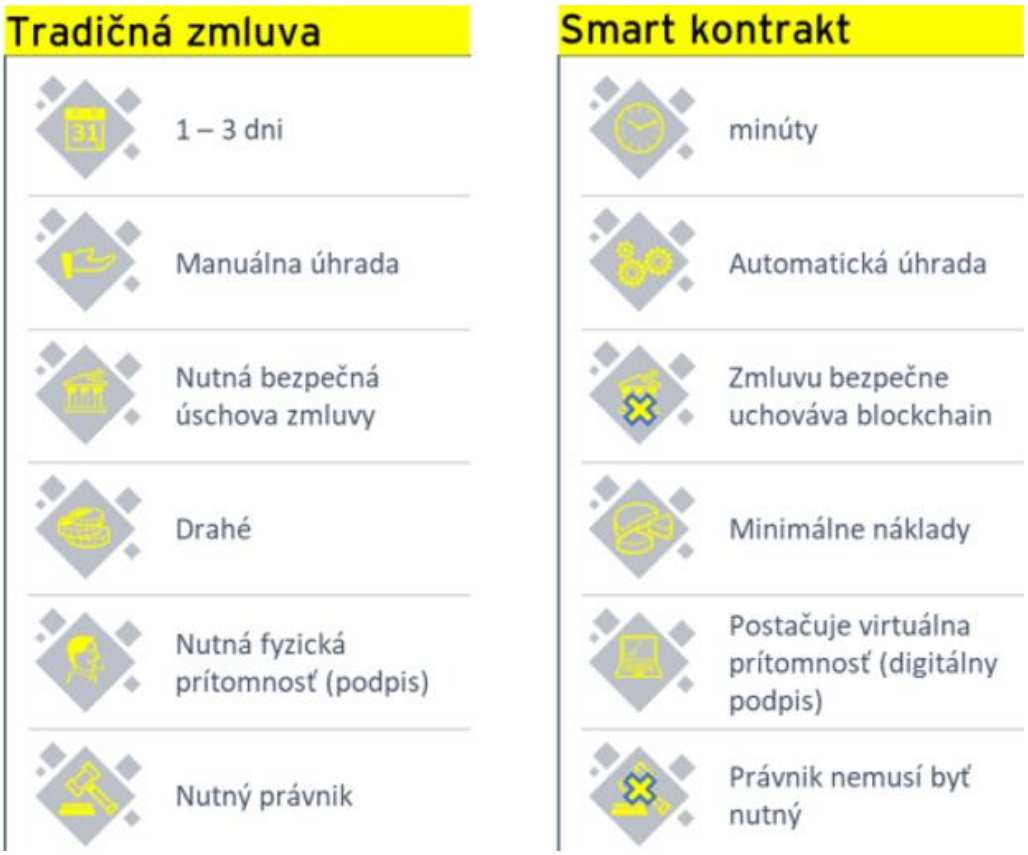
„Smart kontrakty majú za cieľ poskytnúť digitálny pracovný postup, pri ktorom musí byť splnená séria nevyhnutných a záväzných krokov, kým sa nedosiahne výsledok alebo zmluva sa ukončí. Sú „vykonávané presne podľa programu bez akéhokoľvek možného výpadku, cenzúry, podvodu alebo zasahovania tretích strán“ (Marchionni, 2018).

Inteligentná zmluva (Smart contract) môže byť definovaná ako počítačový protokol, ktorý je určený na vykonávanie, overovanie či vynucovanie kontraktu v digitálnom decentralizovanom prostredí. Tento koncept bol predstavený v roku 1994 americkým počítačovým expertom a odborníkom na kryptografii Nickom Szabo, ale svoje reálne využitie našiel až s príchodom technológie blockchain. [3] [31]

Smart kontrakty získali nedávno pozornosť, najmä v kontexte technológie blockchain. Smart kontrakt je zmluva, ktorá môže overiť svoju správnosť a presadiť preddefinované pravidlá, a preto sú smart kontrakty samovýkonávacie a samoregulačné. Avšak smart kontrakt bez vhodnej infraštruktúry vôbec nie je "chytrý", pretože potrebuje takúto infraštruktúru na beh, vykonávanie a overovanie týchto kontraktov. Blockchain je vhodná infraštruktúra pre smart kontrakty, ktorá môže fungovať v plne autonómnom a

decentralizovanom spôsobe. Smart kontrakty môžu byť použité pre finančné služby (napríklad Bitcoin) alebo pre všeobecné služby (napríklad Ethereum). Blockchain vykonáva, overuje a zbiera a ukladá smart kontrakty do blokov. Každý blok má odkaz na aspoň jeden predchodcu, odtiaľ pochádza termín blockchain. [21] [32]

V kontexte verejného sektora si vieme predstaviť, že smart kontrakty poskytnú možnosť zabezpečenia istoty a transparentnosti v transakčných procesoch. Príkladom jednoduchého procesu môžu byť náhrady za pracovné cesty zamestnancov. Potenciálnym príkladom zložitejšieho procesu môže byť určenie a riadenie časov, kedy by sa poskytovala sociálna pomoc, a podmienok, za ktorých by sa mala pokračovať alebo zastaviť. [16]



Obrázok 9: Porovnanie tradičnej zmluvy a inteligentnej zmluvy

Zdroj: [17]

1.8 Topológia siete

Sieť blockchain je možné chápať z rôznych hľadísk - ako distribuovanú aplikáciu, databázu, infraštruktúru alebo komunikačnú sieť. Keď hovoríme o blockchaine ako komunikačnej sieti, zvažujeme aj jeho "implementáciu v priestore". [4]

Pôvodne bol blockchain navrhnutý ako peer-to-peer sieť rovnocenných uzlov, kde každý mohol byť validátorom po splnení určitých podmienok. Nový záznam mohol byť poslaný na ktorýkoľvek uzol v sieti, ktorý ho validoval a poslal ďalej svojim peerom. Jednotlivé uzly držali zoznam nepotvrdených transakcií, a konsenzuálne zvolený validátor vybral podmnožinu nekonfliktných transakcií, ktoré zaradil do nového bloku. Každý uzol drží úplný blockchain, teda zreťazený zoznam blokov. [17]

Dnes sú topológie blockchainov oveľa flexibilnejšie, a okrem plných uzlov sa môžu objavovať aj ľahkí klienti, ktoré uchovávajú len časť stavu blockchainu. Existujú aj rôzne cloudové aplikácie, ktoré poskytujú používateľsky prívetivejšie prostredie k blockchainovým službám. [17]

Aktívna práca s blockchainom vyžaduje použitie asymetrickej kryptografie a prístup k súkromným kľúčom. Tieto kľúče môžu byť uložené na rôznych miestach, ako sú pevný disk počítača, USB kľúč, cloudové úložisko, špeciálne hardwarové zariadenie alebo dokonca papier s vytlačeným kľúčom. [3]

1.9 Ukladanie veľkých dát

S ohľadom na distribuované udržiavanie všetkých záznamov v sieti blockchain, nie je vhodné ukladať doň veľké objemy dát. V prípade, že je potrebné zabezpečiť trvalé a nezmeniteľné poskytnutie väčších súborov dát, je možné tieto uložiť do cloudového úložiska. Do blockchainu sa následne zapíše záznam o tom, ktoré súbory boli kedy a kde uložené, spolu s hašom týchto súborov. Týmto spôsobom si overovateľ v budúcnosti môže overiť autenticitu dát a overiť, že nebol žiadny zásah do ich obsahu. Možnosti úložiska samotných dát môžu zahŕňať webové stránky organizácie, cloudové úložisko, privátny FTP server alebo decentralizované úložisko v rámci protokolu typu torrent alebo IPFS. [17]

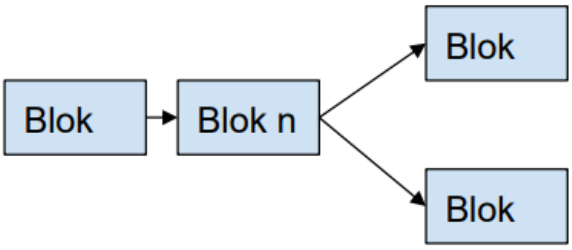
1.10 Rozvetvenie blockchainu

Rozvetvenie v blockchaine sa odkazuje na zmenu protokolu siete, ktorá vedie k vytvoreniu dvoch samostatných verzií histórie blockchainu. Predstavuje odchýlku v blockchaine, kde sa jediný reťazec rozvetví na dva alebo viac reťazcov, ktoré bežia paralelne. Rozvetvenia nastávajú vtedy, keď uzly nedosiahnu zhodu o platnom blockchaine. V dôsledku toho sa blockchain rozvetví do dvoch alebo viacerých potenciálnych ďalších ciest, pričom rôzne skupiny uzlov prijímajú rôzne verzie blockchainu. [18] [23]

Význam Rozvetvenia Blockchainu: Rozvetvenia zohrávajú dôležitú úlohu v evolúcii blockchainových sietí z niekoľkých dôvodov:

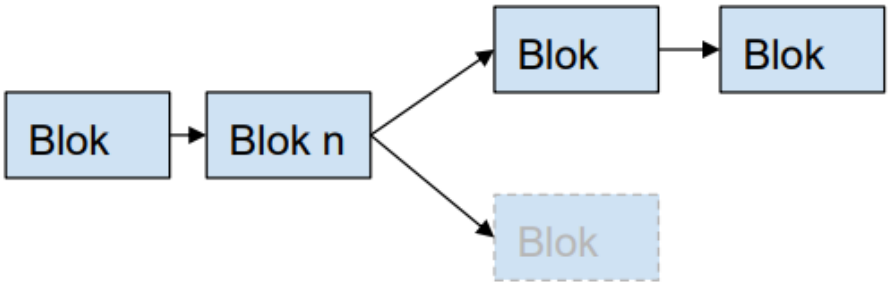
1. **Možnosť pridávania nových funkcií**: Rozvetvenia umožňujú blockchainom pridávať nové funkcie a funkcionalitu prostredníctvom aktualizácií protokolu. Napríklad, SegWit bol aktivovaný na Bitcoine prostredníctvom softvérového rozvetvenia.
2. **Riešenie chýb:** Rozvetvenia môžu pomôcť v návrate transakcií a opravách chýb v prípade zneužitia, ako sa stalo pri preplnení Bitcoinu v roku 2010.
3. **Rozdelenie komunity**: Keď v komunitách existujú nesúlady ohľadom budúceho smerovania blockchainu, rozvetvenia poskytujú spôsob, ako oba tábory presadzujú vlastnú víziu.
4. **Experimentovanie**: Nové blockchain siete sa môžu odvetviť z existujúcich, aby experimentovali s novými konceptmi, ako sú alternatívne modely konsenzu.

Celkovo rozvetvenie predstavuje decentralizovanú a otvorenú povahu verejných blockchainov tým, že poskytuje mechanizmus pre zmenu a evolúciu. [1]



Obrázok 10: Existencia dvoch paralelných blockchainov

Zdroj: [17]



Obrázok 11: Fork - výber pokračovateľa

Zdroj: [17]

Typy Rozvetvení v blockchain sieti: Existujú dva hlavné typy rozvetvení, ktoré môžu nastať v blockchaine:

1. **Tvrdé Rozvetvenie (Hard Fork)**: Tvrdé rozvetvenie sa odkazuje na trvalé rozvetvenie blockchainu, pri ktorom uzly používajúce starý softvér už nebudú akceptovať novú verziu. To vedie k vytvoreniu dvoch samostatných blockchainov so spoločnou históriou až po miesto rozvetvenia. Všetky uzly musia upgradovať na novú verziu protokolu, aby mohli pokračovať v overovaní transakcií na novom rozvetvenom blockchaine. Tvrdé rozvetvenia nie sú spätne kompatibilné.
2. **Mäkké Rozvetvenie (Soft Fork)**: Mäkké rozvetvenie je zmena protokolu, ktorá je stále spätne kompatibilná s predchádzajúcou verziou blockchainu. To znamená, že uzly, ktoré sa neaktualizujú, stále môžu overovať transakcie na novom reťazci. Mäkké rozvetvenia vyžadujú len väčšinu uzlov, aby sa upgradovali na uplatnenie nových pravidiel. Neaktualizované uzly na starom softvéri stále môžu vykonávať transakcie na blockchaine, ale nemusia mať prístup k novým funkciám. [4] [23]

1.11 Algoritmy konsenzu

Ako sme už predtým diskutovali, dôležitým aspektom technológie blockchain je, že väčšina uzlov musí preskúmať a schváliť transakcie v bloku predtým, než môže byť blok overený a zaznamenaný. Týmto spôsobom nikto nemôže falšovať účtovnú knihu, každý ju môže skontrolovať a je jej možné dôverovať. Ako dôjsť k dohode (konsenzu) medzi nedôveryhodnými uzlami v sieti blockchain je transformácia problému byzantských generálov. [16] [21]

Spoľahlivý počítačový systém musí byť schopný vyrovnať sa so zlyhaním jedného alebo viacerých svojich komponentov. Zlyhaný komponent môže prejaviť typ správania, ktorý je často prehliadaný, a to posielanie protirečivých informácií rôznym častiam systému. Problém zvládania tohto typu zlyhania je abstraktne vyjadrený ako problém byzantských generálov“ [33]

Konsenzus medzi nedôveryhodnými uzlami v sieti blockchain sa dá porovnať s problémom byzantských generálov. Skupina generálov, ktorí viedli byzantské vojsko, mali rozdielne názory na útok na mesto. Niektorí chceli útočiť, iní nie. Rozdelenie by však viedlo k neúspechu útoku. Preto museli generáli dosiahnuť dohodu, či útočiť alebo nie. Dosiahnutie konsenzu v blockchainovej sieti je podobne náročné, pretože chýba centrálna autorita na zabezpečenie dohody medzi uzlami. [3] [5]

V blockchaine sa dohodou ako takou myslí hlavne dohodu o tom, kto zverejní ďalší blok s validnými transakciami a dohodu o aktuálnom stave decentralizovanej distribuovanej databázy v sieti účastníkov. Musí tu teda existovať mechanizmus, ktorý bude zaisťovať tieto procesy a správny chod systému. Preto sú v blockchaine zabudované rôzne druhy konsenzuálnych algoritmov pre rôzne typy blockchainu, ktoré zaisťujú dosiahnutie konsenzu medzi uzlami v sieti. [34]

Na dosiahnutie tohto konsenzuálneho stavu sa používajú tzv. algoritmy, resp. protokoly konsenzu ako napríklad: Proof of Work, Proof of Stake, Practical Byzantine Fault Tolerance, Proof of Elapsed Time, Delegated Proof of Stake, Proof of Authority a ďalšie.

1.11.1 *Proof of work (PoW)*

PoW model — najčastejší konsenzuálny model používaný vrátane platformy Bitcoin, vyžaduje aby ťažobný uzol na zverejnenie bloku do blockchainu vynaložil spracovávacie zdroje na riešenie ťažkej hádanky. Ich presné riešenie hádanky slúži ako dôkaz, že vykonali potrebnú prácu na zverejnenie bloku. Proces riešenia hádanky zámerne stojí peniaze v podobe spracovávaného času a elektriny, ale proces potvrdenia správnosti riešenia je zámerne veľmi jednoduchý. [35] [38]

Keď používateľ dokončí prácu, pošle svoj blok na ostatné uzly v sieti. Ostatné uzly potom overia, či práca bola dokončená a či je blok a jeho obsah transakcií platný. Ak áno, uzly pridajú blok do svojej kópie účtovnej knihy a rozdelia blok po celej sieti.

PoW model je vhodný pre verejný blockchain, ktorý umožňuje každému prispievať dáta do účtovnej knihy a pre každého držiteľa účtovnej knihy mať identické kópie. Keďže každý môže prispieť, medzi používateľmi existuje vzájomná nedôvera. PoW model pomáha zabezpečiť, že každý používateľ má približne rovnakú šancu na to, aby mohol riešiť hádanku, čím sa zabráni určitým používateľom kontrolovať, ktoré bloky sa pridajú do reťazca. [16]

1.11.2 *Proof of stake (PoS)*

PoS systém sa podobá PoW, ale s významným rozdielom - váha uzlov nie je určená ich výpočtovou silou, ale množstvom mincí, ktoré držia. Ak uzol vlastní 10 % mincí v obehu danej kryptomeny, to sa rovná zhruba získaniu každého desiateho bloku. Trend popularizácie PoS je evidentný, ako dokazuje napríklad Ethereum, druhá najväčšia kryptomenová sieť. [1]

V rámci PoS systémov existuje veľké množstvo variácií a nastavení, ktoré môžu ovplyvniť zabezpečenie siete. Jednou z častých kritík PoS systémov je ich menšia bezpečnostná záruka, pretože vytvorenie blokov je bez nákladov, a tým pádom validátor blokov môže teoreticky vytvoriť viac verzií blockchainu, čo predstavuje potenciálny vektor útoku. Existuje niekoľko možných riešení na zmiernenie tohto rizika, pričom jedným z najpopulárnejších je penalizácia validátorov, ktorí porušujú protokol. [2]

1.11.3 *Proof of Authority (PoA)*

Dôkaz autority (PoA) poskytuje schopnosť overovať a publikovať nové bloky do blockchainu pre autorizovaných používateľov, nazývaných validátormi. Na rozdiel od konsenzuálnych modelov ako je Dôkaz práce (PoW) a Dôkaz podielu (PoS) musí byť identita používateľa známa a overená. Toto je kritické, pretože identita je jediným overením autority používateľa na pridávanie nových blokov do reťazca. V porovnaní s PoW je PoA oveľa rýchlejším modelom spracovania nových blokov, pretože nie je potrebné dlhé a náročné spracovanie počítača. Dôkaz autority môže byť použitý v oboch typoch blockchainu (privátnom aj verejnom). Logika tohto modelu je: „Osoby, ktorých identita (a reputácia ako vedľajší produkt) je ohrozená zabezpečením siete, sú motivované chrániť sieť. [37]

Tento konsenzuálny model sa môže zdať najznámejší pre používateľov, ktorí majú skúsenosti s prácou s databázami, v ktorých môžu editovať alebo pridávať dáta iba špecifikovaní autorizovaní používatelia. Preto môže byť najvhodnejší pre mnohé aplikácie technológie blockchain vo verejnom sektore, pretože sa môže prispôsobiť reprezentácii zložitosti procesov hodnotenia a rozhodovania vlády. [16]

1.11.4 *Practical Byzantine Fault Tolerance (PBFT)*

PBFT (vo voľnom preklade Praktická byzantská odolnosť voči chybám) je algoritmus zjednodušene založený na hlasovaní validátorov o stave transakcie. Z toho dôvodu musí byť množina účastníkov (validátorov) uzavretá. Pre malú skupinu validátorov je to veľmi

efektívny algoritmus, ktorý dokáže rýchlo dosiahnuť konsenzus. Jeho zložitosť ale s počtom validátorov rýchlo rastie. Vzhľadom k uzavretej skupine validátorov nie je preto príliš vhodný pre verejný blockchain, naopak je častokrát vhodným algoritmom pre menší privátny blockchain. [17]

1.12 Typy blockchainov

Primárne existujú dva typy blockchainu: **Súkromný** a **verejný** blockchain. Existuje však aj niekoľko variácií, napríklad **konzorcium** a **hybridný** blockchain.

Verejné a súkromné blockchainy sú dve hlavné kategórie. Verejné blockchainy, často spojené s kryptomenami, umožňujú účasť komukoľvek a majú decentralizovanú povahu. Naopak, súkromné blockchainy, bežnejšie v korporátnom prostredí, majú obmedzený prístup a sú rýchlejšie, ale centralizovanejšie. [21]

1.12.1 *Verejný blockchain*

Verejný blockchain je decentralizovaný účtovný systém, označovaný tiež ako „permissionless ledger“, ku ktorému sa môže prihlásiť každý s prístupom na internet a stať sa autorizovaným uzlom. Uzol alebo používateľ môže pristupovať k záznamom, overovať transakcie a vykonávať dôkazy o práci pre nové bloky, vrátane ťažby. Hlavnými účelmi verejných blockchainov sú ťažba a výmena kryptomien. Bitcoin a litecoin sú najznámejšími príkladmi verejných blockchainov. [24] [39]

Výhody používania verejného blockchainu:

1. **Dôveryhodnosť**: Užívatelia nemusia dôverovať osobne ostatným uzlom, pretože proces overovania zabezpečuje, že nedochádza k podvodom.
2. **Bezpečnosť**: S väčšou sieťou je ťažšie hacknúť záznamy, pretože každý uzol vykonáva overovanie transakcií a dôkaz o práci (PoW).
3. **Otvorenosť a transparentnosť**: Údaje sú transparentné a k dispozícii na každom uzle, čo zabezpečuje, že systém je úplne otvorený a transparentný.

Nevýhody používania verejného blockchainu:

1. **Nízke TPS**: Verejné blockchainy majú obmedzenú rýchlosť spracovania transakcií kvôli časovo náročnému overovaniu každého uzla. Napríklad, Bitcoin zvláda len 7 transakcií za sekundu a Ethereum 15, zatiaľ čo súkromné siete ako Visa dosahujú 24 000 TPS.

2. **Problémy so škálovateľnosťou**: Pomalá rýchlosť a spracovanie transakcií sťažujú škálovateľnosť verejných blockchainov, čo sa zhoršuje so zväčšovaním siete. Avšak riešenia ako bitcoin Lightning Network pomáhajú tento problém riešiť.
3. **Vysoká spotreba energie**: Proces overovania práce vyžaduje špeciálny hardvér a spotrebúva veľa energie, čo je environmentálny a ekonomický problém.

1.12.2 *Privátny blockchain*

Súkromný blockchain je obmedzený na uzavretú sieť, typicky používaný v organizáciách alebo firmách, kde len vybraní členovia majú prístup. Riadenie zabezpečenia a oprávnení je v rukách riadiacej organizácie. Súkromné blockchainy sa využívajú napríklad na hlasovanie, riadenie dodávateľského reťazca, digitálnu identitu a iné účely. Príklady súkromných blockchainov zahŕňajú projekty ako Multichain, Hyperledger (Fabric, Sawtooth), Corda, a ďalšie. [24] [40]

Výhody používania privátneho blockchainu:

Rýchlejšie transakcie: Menší počet uzlov v privátnom blockchaine umožňuje efektívnejšie dosiahnutie konsenzu a tým aj rýchlejší pohyb transakcií. Keďže je tu určitá miera dôvery medzi uzlami, tak tento typ blockchainu môže využívať odlišné konsenzuálne algoritmy (napríklad spomenutý Practical Byzantine Fault Tolerance) medzi uzlami a rýchlejšie dosiahnuť konsenzus. Tieto faktory zaisťujú rýchlejší pohyb transakcií v sieti. Privátny blockchain môže zvládnuť až tisíce transakcií za sekundu, čo v porovnaní so 7 transakciami predstavuje zásadný rýchlostný rozdiel.

Škálovateľnosť: Vzhľadom k centrálnej kontrole veľkosti siete je privátny blockchain lepšie škálovateľný ako verejný blockchain.

Nevýhody používania privátneho blockchainu:

Centralizácia: Privátny blockchain používa centrálny systém na správu identít a pridávanie uzlov do siete. To odchýlilo blockchain od pôvodnej myšlienky decentralizácie a transparentnosti, ale môže byť výhodné pre niektoré prípady a odvetvia, kde nie je vhodná úplná transparentnosť a decentralizácia.

Nižšia bezpečnosť: S menším počtom uzlov v sieti môže byť pre útočníka jednoduchšie prevziať kontrolu nad sieťou, čo znižuje jej bezpečnosť. [1] [40]

1.12.3 *Blockchain konzorcia*

Blockchain konzorcium je typ blockchainu, kde viac ako jedna organizácia riadi sieť. Proces konsenzu je riadený vybranou skupinou uzlov. Napríklad, môže existovať 15 finančných inštitúcií, pričom každá prevádzkuje uzol, a aby bol blok platný, musí byť podpísaných aspoň 10 z týchto inštitúcií. Právo čítať blockchain môže byť verejné alebo obmedzené na účastníkov, ale existujú aj hybridné prístupy, ako sú koreňové haš bloky s verejnými API, ktoré umožňujú verejnosti získať obmedzené informácie o stave blockchainu. Takýto blockchain sa označuje ako "čiastočne decentralizovaný". Banky, vládne organizácie a podobné subjekty zvyčajne využívajú blockchain konzorcium. Príklady sú Energy Web Foundation a R3. [36] [40]

1.12.4 *Hybridný blockchain*

Hybridný blockchain kombinuje prvky súkromného a verejného blockchainu., využíva výhody oboch prístupov, čo umožňuje vytvoriť systém, ktorý poskytuje kontrolu nad prístupom k údajom uloženým v blockchaine. [18]

V hybridnej sieti môžu používatelia riadiť, kto má prístup k akým údajom. Časť údajov alebo záznamov môže byť zverejnená na verejnom blockchaine, zatiaľ čo zvyšok zostane súkromný v súkromnej sieti. Flexibilita hybridného blockchainu umožňuje jednoduché pripojenie k súkromnému blockchainu s viacerými verejnými blockchainmi. [36]

Transakcie v súkromnej sieti hybridného blockchainu sa obvykle overujú v rámci tejto siete, ale používatelia ich môžu aj overiť vo verejnom blockchaine. Verejný blockchain zvyšuje bezpečnosť prostredníctvom väčšieho množstva uzlov na overenie. [24] [36]

Príkladom hybridného blockchainu je Dragonchain.

2 Cieľ práce

Hlavným cieľom záverečnej práce je poskytnúť komplexný prehľad o inovatívnej technológií blockchain. V teoretickej časti práce sa zameriame na detailné popísanie princípov fungovania týchto technológií, ich potenciálne možnosti použitia a ich výhody a nevýhody. V praktickej časti sa budeme venovať SWOT analýze, podrobnému opisu vybranej oblasti aplikácie technológie blockchain a jej implementácii. Cieľom je poskytnúť ucelený pohľad na technológiu blockchain a jej praktické využitie v konkrétnej oblasti.

Následne aby sme tento cieľ splnili je potrebné venovať sa čiastkovým cieľom , ktoré nám slúžili ako oporné body, tieto čiastkové ciele sú:

1. Porozumieť rozdielu medzi tradičným databázovým prístupom a prístupom založeným na technológii blockchain.
2. Definovať základné komponenty blockchainu a pochopiť ich funkciu.
3. Vysvetliť najpoužívanejšie algoritmy konsenzu v rámci blockchainových sietí.
4. Charakterizovať rôzne typy sietí blockchain.
5. Opísať silné, slabé stránky, príležitosti a hrozby blockchainu vo verejnom sketore.
6. Identifikovať vhodné odvetvia pre technológiu blockchain a popísať ich potenciálne prínosy.

3 Metodika práce a metódy skúmania

V procese prípravy záverečnej práce sme realizovali literárny výskum, ktorý zahrňoval systematickú štúdiu literatúry. Tento postup štúdia a rešerše bol zameraný na dôkladné preskúmanie, analýzu a selekciu existujúcich zdrojov súvisiacich s preskúmavanou problematikou. Okrem knižných publikácií sme sa pozreli aj odborné vedecké články a relevantné online zdroje. Následne sme získané informácie detailne analyzovali a syntetizovali v súlade so zadaním práce - *Možností využitia technológie blockchain vo verejnej sfére*.

Spomedzi teoretických metód skúmania sme pracovali so skupinou všeobecných metód ako analýza, syntéza, indukcia či dedukcia ako aj špeciálnych – komparatívnych metód.

Analýze sme podrobili viaceré teoretické východiská autorov zaoberajúcich sa problematikou technológie blockchain. Rovnako sme siahli po poznatkoch z oblasti technológie v zameraní na konsenzuálne algoritmy či topológie sieti. Inšpirovali sme sa autormi ako Antonopoulos (2014), Buterin (2015), Bashir (2018), Zheng (2017) či Stancel (2022). Na základe dôkladnej analýzy sme vybrali najpodstatnejšie informácie a fakty z množstva odborných poznatkov a publikácií, v ktorých sme hľadali súvislosti medzi nimi.

Tento proces získavania informácii nám umožnil prehľad o skúmanom probléme a o súčasnom stave. Pomocou použitia syntézy a substitučnej metódy sme z nadobudnutých informácií koncipovali túto záverečnú prácu. Pomocou komparatívnych metód sme porovnávali typy sietí blockchain v rôznych ohľadoch. Z toho sme napokon pomocou dedukcie a doplnenia informácií z rôznych zdrojov nadobudli nové informácie a poznatky.

Pre dosiahnutie hlavného cieľa sme v praktickej časti metódou syntézy združili poznatky a informácie z teoretickej časti, ktoré sme využili na utvorenie jednotlivých návrhov implementácie technológie blockchain vo vybraných odvetviach verejnej sféry a ich konkrétnych prípadoch použitia. Pomocou komparatívnej analýzy sme následne porovnali a podrobne popísali podstatu daného riešenia, výhody, nevýhody, ale aj potenciálne limitácie. V tejto časti sme pre jednoduchšie pochopenie a zobrazenie návrhov použili aj rôzne grafické metódy, napríklad diagramy.

V závere záverečnej práce sme použili metódu indukcie, pri ktorej sme získané údaje a poznatky zosumarizovali do konzistentného záveru.

4 Výsledky práce a diskusia

Dnešný verejný sektor kladie stále väčší dôraz na využitie informačných technológií s cieľom znižovať náklady a zefektívňovať komunikáciu. Blockchain, ktorý bol pôvodne známy ako základná technológia za digitálnou menou Bitcoin, teraz nájde svoje uplatnenie aj vo verejnej sfére. Jeho decentralizovaná povaha a schopnosť poskytovať dôveru a transparentnosť v dátach otvára cestu k mnohým inovatívnym využitiam a príležitostiam v rôznych oblastiach verejných služieb služieb ako napríklad. [21]

1. **Transparentná a bezpečná správa údajov**: Blockchain poskytuje dôveru v dátové transakcie a záznamy, čo umožňuje verejným inštitúciám zabezpečiť transparentnosť a integritu údajov v oblastiach ako správa záznamov o volebných úkonoch, verejných obstarávaniach, alebo sledovateľnosti verejných finančných prostriedkov.
2. **Zjednodušený proces identifikácie a autentifikácie**: Blockchain umožňuje vytvorenie digitálnych identít, ktoré sú odolné voči falšovaniu a zaručujú dôveru v autentifikáciu používateľov. To má obrovský potenciál v oblasti riadenia a správy digitálnych identít, zabezpečení prístupu k zdrojom verejných služieb a boja proti krádežiam identity.
3. **Optimalizácia procesov a eliminácia byrokracie**: Implementácia blockchainu môže zefektívniť procesy v mnohých verejných sektoroch, ako napríklad evidencia majetku, správa príspevkov a dotácií, alebo riadenie dodávok v rámci verejných zdravotníckych služieb.
4. **Zvyšovanie transparentnosti a zodpovednosti**: Blockchain umožňuje verejným inštitúciám zvýšiť transparentnosť a zodpovednosť voči občanom. Verejné financie, zmluvy a rozhodnutia môžu byť zaznamenané do blockchainu, čo umožňuje občanom sledovať a overiť tieto procesy.
5. **Inovácie v oblasti digitálneho hlasovania**: Blockchain poskytuje bezpečné a spoľahlivé riešenia pre digitálne hlasovanie, čím sa môže zvýšiť účasť občanov a zjednodušiť proces voľby. [17] [21]

4.1 SWOT analýza

SWOT analýza je nástroj, ktorý umožňuje systematicky posúdiť silné stránky, slabé stránky, príležitosti a hrozby súvisiace s implementáciou pre naše potreby blockchainu vo

verejnej sfére, poskytuje hlavné usmernenia pre strategické plánovanie a riadenie rizík, čo je nevyhnutné pre úspešné zavádzanie nových technológií.

Využíva kombináciu interných a externých faktorov na identifikáciu silných a slabých stránok, príležitostí a hrozieb, ktoré vyplývajú z vonkajšieho prostredia. [48]

	Systémové prostredie	*Externé prostredie*	
Želané	**Silné stránky:**	**Silné stránky:**	*Existujúci faktor*
	Decentralizovaná štruktúra	Automatizácia	
	Efektívne zdieľanie informácií	Podpora vlády	
	Dôveryhodnosť	Medzinárodné normy a spolupráce	
	Robustné riadenie rizík	Financovanie výskumu a vývoja	
	Integrita medzi procesmi		
	Vysoké bezpečnostné opatrenia		
	Systematická správa údajov		
	Kontrolovateľnosť		
	Silný vzťah medzi zainteresovanými		
	stranami		
	Menej pirátstva, falšovania		
	Nižšie náklady		
	Nemennosť údajov		
Neželané	**Slabé stánky:**	**Slabé stánky:**	*Existujúci faktor*
	Vysoká spotreba el. energie	Správanie používateľov	
	Veľkosť ukladaných dát	Zväčša vyššie počiatočné náklady	
	Problém s rozdelením (fork) kap. 1.10	Integrácia s existujúcimi systémami	
	Nízka škálovateľnosť		
	Nízka prispôsobiteľnosť		
	Nízka transakčná rýchlosť		
Želané	**Príležitosti:**	**Príležitosti:**	*Potencionálny faktor*
	Podpora vzniku nových modelov	Automatizácia vládnych nariadení	
	Zlepšenie efektivity procesov vo verejnom sektore (napr. volebného systému)	Zmeny v globálnych menových systémoch	
	Technologická vyspelosť používateľov	Používateľská skúsenosť (UX)	
Neželané	**Hrozby:**	**Hrozby:**	*Potencionálny faktor*
	Potencionálna nízka bezpečnosť (kvantové počítače)	Regulačné a právne riziká	
	Hrozby spôsobené zvýšenou transparentnoťou	Akceptácia a dôvera verejnosti	
		Nejasnosť budúceho výskumu	

Tabuľka 5: SWOT analýza verejného blockchainu

Zdroj: spracované podľa [48] [49] [50] [51]

Na základe predchádzajúcej tabuľky môžeme konštatovať, že technológiu blockchain je vhodné implementovať pre potreby verejnej sféry ak potrebujeme:

1. **Zabezpečenie transparentnosti:** Blockchain môže byť užitočný pri zabezpečení transparentnosti verejných procesov a transakcií. Verejné inštitúcie môžu využiť blockchain na vytvorenie verejných záznamov, ktoré sú transparentné, nezmeniteľné a prístupné všetkým (ako napríklad volebný systém založený na sieti blockchain).
2. **Zlepšenie bezpečnosti údajov:** Vo verejnej sfére je bezpečnosť údajov kľúčovou prioritou. Blockchain poskytuje vysokú úroveň bezpečnosti údajov prostredníctvom decentralizovaného a nezmeniteľného záznamu transakcií.
3. **Automatizácia procesov:** Implementácia smart kontraktov v blockchaine môže pomôcť automatizovať procesy vo verejnej správe, čím sa znižuje byrokracia a zvyšuje efektívnosť.
4. **Zlepšenie riadenia identít:** Blockchain môže byť použitý na efektívne riadenie a overovanie identít občanov, čo môže prispieť k zvýšeniu bezpečnosti a efektivity verejných služieb.
5. **Zvýšenie decentralizácie a odolnosti:** Vytvorenie decentralizovaných systémov prostredníctvom sieti blockchain môže eliminovať centrálne orgány a znížiť riziko jedného bodu zlyhania.
6. **Znižovanie korupcie:** Transparentnosť a nezmeniteľnosť blockchainu môžu pomôcť znižovať korupciu a zlepšovať správu verejných prostriedkov.
7. **Zlepšenie služieb pre občanov:** Implementácia blockchainu môže viesť k lepším a efektívnejším službám pre občanov, či už ide o zlepšenie procesov spravovania úradov, zjednodušenie platobných systémov alebo zabezpečenie transparentného volebného systému.
8. **Podpora inovácií a hospodárskeho rozvoja:** Podpora a investície do blockchainových projektov môžu posilniť inovácie vo verejnej sfére a prispieť k hospodárskemu rozvoju krajiny. [17] [48] [49]

Existuje však niekoľko situácií, kedy nie je vhodné využiť blockchain vo verejnej sfére, najmä v prípade:

1. **Nízkej potreby decentralizácie:** Ak neexistuje potreba alebo prínos z decentralizácie procesov alebo údajov, použitie blockchainu môže byť nadbytočné a neefektívne.
2. **Vysokých nákladov na implementáciu:** Implementácia blockchainu môže byť nákladná, a ak neexistujú dostatočné zdroje na financovanie projektu, môže to byť nevhodné pre verejnú sféru, kde sú rozpočtové obmedzenia dôležité.

3. **Technologickým obmedzeniam:** Ak je blockchain technologicky príliš zložitý alebo nezrelý na účinné použitie vo verejných službách, môže to viesť k problémom s implementáciou a prevádzkou.
4. **Nedostatočnej podpore zainteresovaných strán**: Ak neexistuje dostatočná podpora alebo konsenzus medzi zainteresovanými stranami, vrátane verejných inštitúcií, občianskej spoločnosti a súkromného sektora, môže byť ťažké dosiahnuť úspešné nasadenie blockchainu.
5. **Regulačných a právnych prekážok**: Existujú prípady, keď právne prostredie nie je pripravené na použitie blockchainu alebo sú potrebné značné zmeny v právnych predpisoch, aby sa umožnilo jeho implementáciu. To môže spomaliť alebo znemožniť jeho použitie vo verejnej sfére.
6. **Nedostatočného prípadu použitia:** Ak neexistuje jasný prípad použitia alebo výhody pre použitie blockchainu vo verejnej sfére, môže byť lepšie hľadať iné technologické riešenia, ktoré lepšie zodpovedajú potrebám a požiadavkám. [17] [51]

Nakoľko sa jedná stále o pomerne novú technológiu, treba zvážiť aj riziká (kombináciu hrozieb, zraniteľností a dopadu na informačné aktívum) ako napríklad:

1. **Riziká a mnohé praktické komplikácie:** Riziká a mnohé praktické komplikácie spojené s riadením životného cyklu samotnej technológie blockchain a aplikácií využívajúcich blockchain a ich integrácie do okolitého IT prostredia (analýza, návrh, vývoj, testovanie, nasadenie, riadenie zmien, riadenie prevádzky).
2. **Riziká spojené s riadením asymetrických šifrovacích kľúčov:** najmä s bezpečným uchovávaním privátneho kľúča
3. **Zmeny v právnych predpisoch:** Regulácia okolo blockchainu je stále v pohybe a môže sa líšiť medzi jednotlivými krajinami a regiónmi. Nekonzistentné alebo nejasné právne predpisy môžu spôsobiť právnu neistotu a komplikovať použitie blockchainu vo verejnej sfére.
4. **Zodpovednosť a transparentnosť:** Zodpovednosť za chyby alebo zlyhania v blockchainových systémoch môže byť nejasná, čo môže viesť k nedostatočnej transparentnosti a zodpovednosti.
5. **Správa identít:** Zabezpečenie správy identít na blockchaine môže byť výzvou. Riziká týkajúce sa ochrany súkromia a bezpečnosti údajov môžu vznikať v súvislosti s uchovávaním citlivých informácií na verejnej blockchainovej sieti.

6. **Energetická náročnosť:** Niektoré blockchainové siete, najmä tie, ktoré používajú metódu PoW, môžu byť veľmi energeticky náročné. To môže mať negatívny dopad na životné prostredie a môže byť neefektívne vo verejnej sfére, kde sú potrebné udržateľné a ekologické technológie. [17] [48] [49] [50]

Blockchain je nová a relatívne komplexná technológia, a preto existuje riziko technických chýb, bezpečnostných zraniteľností a nedostatkov v implementácii, ktoré by mohli mať vážne následky na bezpečnosť a integritu údajov. Ďalším významným rizikom je možnosť vyzradenia všetkých údajov uložených v blockchain v zašifrovanej podobe v prípade prelomenia použitej šifry, typicky pomocou tzv. kvantového počítača. V takomto prípade by bolo extrémne zložité prešifrovať tieto pôvodné a kompromitované údaje, vzhľadom na nemennosť a distribuovanosť údajov v sieti blockchain, pomocou dodatočne zmodernizovaných šifrovacích algoritmov alebo komplexnejších kľúčov. Pri používaní blockchainu vo verejnej sfére je teda nevyhnutné zvážiť tieto technologické riziká a prijať opatrenia na ich minimalizovanie a riadenie. [17]

Nasledujúce kapitoly sú venované vhodným príkladom využitia technológie blockchain vo verejnom sektore.

4.2 OECD a e-Government

Blockchain štúdia organizácie OECD Organizácia pre hospodársku spoluprácu a rozvoj (OECD) vydala dokument Blockchains Unchained: „Blockchain Technology and its Use in the Public Sector“. Ktorá má za cieľ informovať vedúcich predstaviteľov, zamestnancov verejnej správy ako aj odborníkov o blockchain technológií, jej možných dopadoch, výzvach a príležitostiach v rámci poskytovania verejných služieb, ktorým môžu vlády čeliť. Z príručky a prípadových štúdií vyplýva, že vo verejnom sektore má technológia blockchain potenciál zlepšiť efektívnosť, znížiť byrokratické bariéry a potenciálne nezhody medzi inštitúciami, zlepšiť zdieľanie vedomostí a podporiť automatizáciu prostredníctvom smart kontraktov. Z iniciatív uvedených v **tabuľke 6** možno vidieť trendy, v akých typoch projektov a priemyselných odvetviach sa začína používať blockchain technológia vo verejnom sektore. [17]

Obrázok 12: Prehľad krajín využívajúcich technológiu blockchain

Zdroj: [17]

Poradie	Typy projektov (počet)	Odvetvie (počet)
1	Stratégia / Výskum (42)	Vládne služby (173)
2	Identita (poverenia / licencie / osvedčenia) (25)	Finančné služby (73)
3	Osobné záznamy (zdravotné, finančné, atď.) (25)	Technológia a Internet of Things (26)
4	Hospodársky rozvoj (24)	Zdravotníctvo (23)
5	Finančné služby / Trhová infraštruktúra (20)	Nehnuteľnosti (22)
6	Katastre nehnuteľností (19)	Dodávateľský reťazec (19)
7	Digitálna mena (vydaná centrálnou bankou) (18)	Energetika (13)
8	Výhody / Požiadavky (13)	Doprava (13)
9	Súlad / Podávanie správ (12)	Vzdelávanie (8)
10	Výskum / Štandardy (12)	Telekomunikácie (4)

Tabuľka 6: Top 10 typov projektov

Zdroj: [17]

eGovernment, skratka pre elektronickú vládu, je použitie informačných a komunikačných technológií (ICT) na poskytovanie verejných služieb a riadenie vládnych operácií. Zahrňuje elektronické interakcie medzi občanmi a vládnymi inštitúciami, ako aj medzi rôznymi úrovňami verejnej správy. Cieľom eGovernmentu je zlepšiť efektivitu, transparentnosť, prístupnosť a kvalitu verejných služieb. To zahŕňa poskytovanie online služieb, elektronické podávanie žiadostí a formulárov, elektronickú identifikáciu a autentifikáciu, otvorené dáta a mnoho ďalších aspektov digitalizácie verejnej správy.

Nasledujúci obrázok sumarizuje zavedenie technológie blockchain naprieč rôznymi požiadavkami: vysoký potenciál znamená, že blockchain vie túto požiadavku zabezpečiť lepšie ako iné technológie, stredný že môže pomôcť porovnateľne ako iné technológie, nízky že blockchain má minimálny prínos. [17]

Požiadavka	Popis	Potenciál prínosu blockchain
Bezpečnosť	schopnosť zaistiť dôvernosť, integritu a dostupnosť procesov a ich údajov	vysoký
Auditovateľnosť	schopnosť dodatočne zrekonštruovať priebeh procesu (kto, čo, kedy)	vysoký
Transparentnosť	schopnosť dodatočne preukázať, že proces bol vykonaný v súlade s pravidlami a požiadavkami	vysoký
Integrácia	elektronické prepojenie systémov na okolitý eGovernment ako aj interne medzi systémami rezortu	vysoký
Analyzovatelnosť	dostupnosť relevantných údajov a ich spracovanie pre umožnenie informovaného rozhodovania	stredný
Modernizácia	zoštíhlenie, resp. iný typ vylepšenia existujúceho dizajnu procesov - vynechanie, nahradenie, zlúčenie procesov, aktivít, aktérov a pod.	stredný
Zfunkčnenie	umožnenie vykonať určitú povinnosť (odstránenie nevykonateľnosti)	stredný
Centralizácia	zníženie nákladov zavedením spoločnej prevádzky, podpory, metodiky a tiež predpoklad na elimináciu princípu miestnej príslušnosti (súvisí tiež so zjednotením, transparentnosťou a bezpečnosťou)	stredný
Elektronizácia	náhrada „papierových" údajov (verejné listiny, žiadosti, rozhodnutia a pod.) elektronickými	stredný
Automatizácia	zrýchlenie, zvýšenie spoľahlivosti a kvality (chybovosti) procesov odstránením manuálnych krokov (spracovanie, rozhodovanie)	stredný
Zjednotenie	zaistenie konsolidácie postupov vykonávaných rôznymi inštanciami rovnakého typu aktéra	nízky
Proaktivita	automatické preventívne iniciovanie komunikácie medzi procesom a aktérom - človekom (napr. rôzne notifikácie)	nízky

Tabuľka 7: Porovnanie požiadaviek eGovernmentu s prístupom blockchain

Zdroj: [17]

Pri výbere a nasadení nového systému tvoria náklady nezanedbateľný faktor, náklady môžeme rozdeliť do viacerých aspektov, blockchainové riešenie dôkladne opisuje **obrázok 13 .**

1. **Infraštruktúra a prevádzka:** Implementácia blockchainu si vyžaduje vytvorenie a udržiavanie infraštruktúry, vrátane počítačových serverov, dátových centier a sieťových pripojení. Prevádzka takéhoto systému vyžaduje nielen finančné prostriedky na nákup a údržbu hardvéru, ale aj na energiu a personál na jeho správu. [41]
2. **Bezpečnosť a ochrana údajov:** Blockchain musí byť riadne zabezpečený, aby sa zabránilo zneužitiu, krádeži alebo úniku dát. Implementácia štandardov

bezpečnosti a ochrany údajov vyžaduje čas, zdroje a finančné investície, aby sa zabezpečila integrita a dôvernosť dát uložených v blockchaine. [16] [41]

3. **Školenie a vzdelávanie:** Pre úspešné nasadenie a využívanie blockchainu je nevyhnutné, aby pracovníci vo verejnom sektore získali potrebné znalosti a zručnosti. To môže zahŕňať školenia a vzdelávacie programy pre zamestnancov, aby sa naučili pracovať s touto novou technológiou a porozumeli jej princípom a výhodám. [41]
4. **Legislatívne a regulačné požiadavky:** Implementácia blockchainu môže byť ovplyvnená rôznymi legislatívnymi a regulačnými požiadavkami, ktoré môžu zvyšovať náklady a administratívnu záťaž. Súčasná legislatíva týkajúca sa ochrany údajov a digitálnej identity môže vyžadovať dodatočné opatrenia na zabezpečenie súladu. [42]
5. **Aktualizácie a údržba:** Blockchain musí byť pravidelne aktualizovaný a udržiavaný, aby sa zabezpečila jeho spoľahlivosť a bezpečnosť. Tento proces môže byť náročný na čas a finančné zdroje, najmä ak sa vyžadujú zmeny v protokoloch alebo softvéru blockchainu. [41]

Obrázok 13: Prehlaď nákladov v spojení s rôznymi blockchainovými riešeniami

Zdroj: [17]

4.3 Využitie blockchainu v zdravotníctve

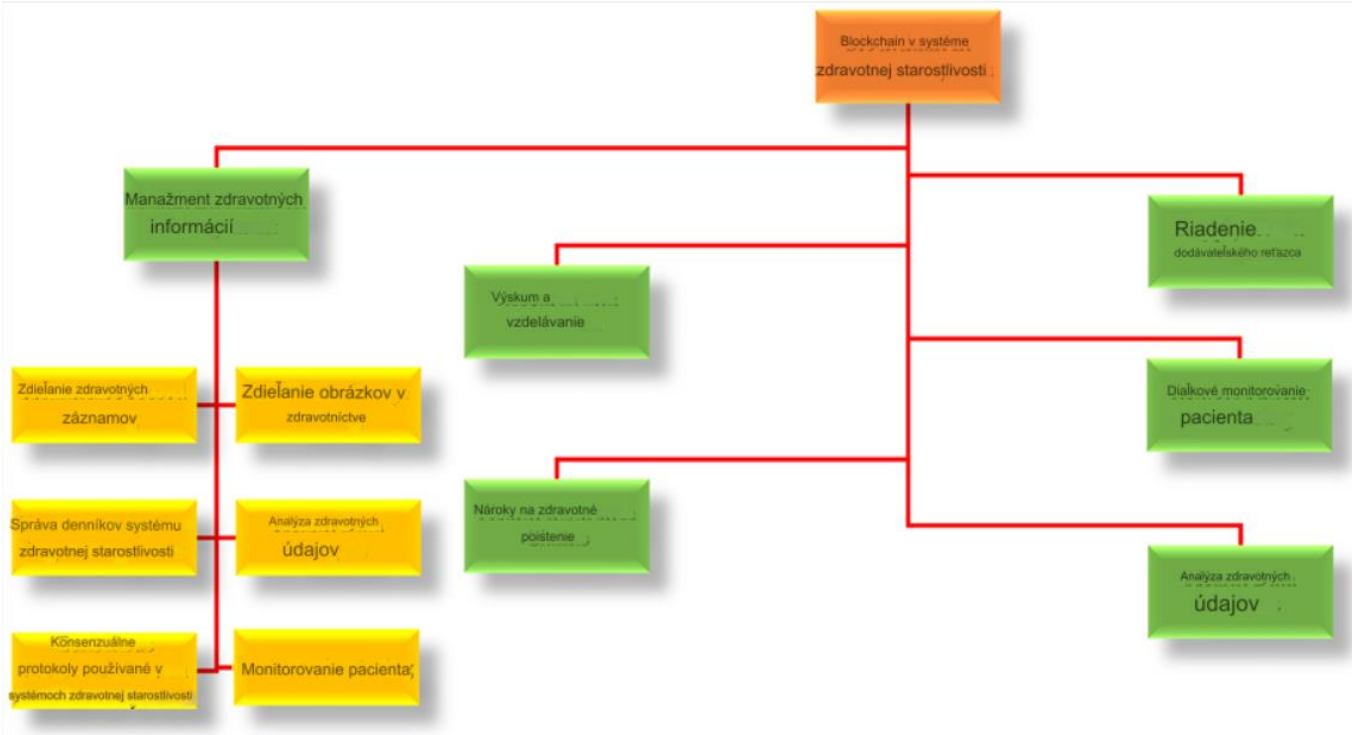
Technológia blockchain má potenciál zlepšiť zdravotnícky sektor tým, že dáva prioritu pacientovi v rámci systému a zvyšuje ochranu, bezpečnosť a bezproblémovú výmenu zdravotných informácií. V podstate by mohlo dôjsť k výraznej transformácii zdravotníckeho priemyslu prostredníctvom širokej implementácie blockchainu, môže vykonávať celý rad úloh, vrátane kontroly epidémií a bezpečného šifrovania údajov pacientov. Nakoniec, umožňovaním bezpečného zdieľania údajov medzi viacerými zdravotníckymi systémami s autorizáciou pacienta môže blockchain zlepšiť digitálnu zdravotnú starostlivosť. [21]

Aplikácie blockchainu dokážu presne identifikovať závažné a dokonca nebezpečné chyby v lekárskej oblasti. Môže tak zlepšiť výkon, bezpečnosť a transparentnosť zdieľania

lekárskych údajov v systéme zdravotnej starostlivosti. Táto technológia pomáha zdravotníckym zariadeniam získať prehľad a vylepšiť analýzu lekárskych záznamov. [43]

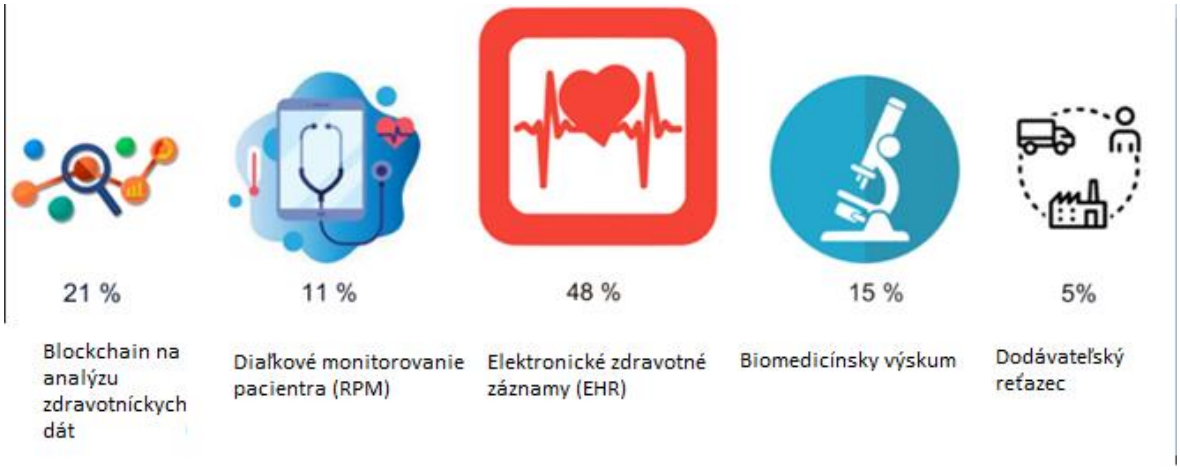
Obrázok 14 odráža rôznorodosť funkcií a kľúčových mechanizmov filozofie blockchainu v mnohých oblastiach zdravotníctva a súvisiacich podoblastí. Ochrana údajov v zdravotníctve, rôzne správy o genómoch, elektronické správy o údajoch, lekárske záznamy, interoperabilita, digitalizované sledovanie a výskyt problémov sú len niektoré z technicky odvodzovaných a pôsobivých funkcií používaných na vývoj a praktizovanie technológie blockchain. Úplne digitalizované aspekty technológie blockchain a jej použitie v aplikáciách súvisiacich s zdravotníctvom sú významné dôvody na jej prijatie. [44]

V nasledujúcich troch podkapitolách sa zameriame na možnosti konkrétnych aplikácií.



Obrázok 14: Blockchain a zdravotný systém

Zdroj: [44]



Zdroj: [44]

Obrázok 15: Súčasný podiel využitia blockchainu v zdravotníctve

4.3.1 *Správa elektronických zdravotných záznamov*

Digitalizácia zdravotných informácií/záznamov priniesla do verejného zdravotníctva významnú zmenu, ale bola kritizovaná pre svoju komplexnosť z dôvodu centralizácie. Technológia blockchain môže vytvoriť bezpečný a flexibilný ekosystém pre výmenu elektronických zdravotných záznamov (EHR), môže zmeniť spôsob, akým sa vymieňajú a ukladajú elektronické zdravotné záznamy pacientov (EHR). Táto technológia umožňuje vytvorenie systému EHR, ktorý je bezpečnejší, transparentnejší a prepojený, čo umožňuje jednoduchý prístup k zdravotným informáciám. [14]

Proces môže byť zhrnutý do štyroch krokov:

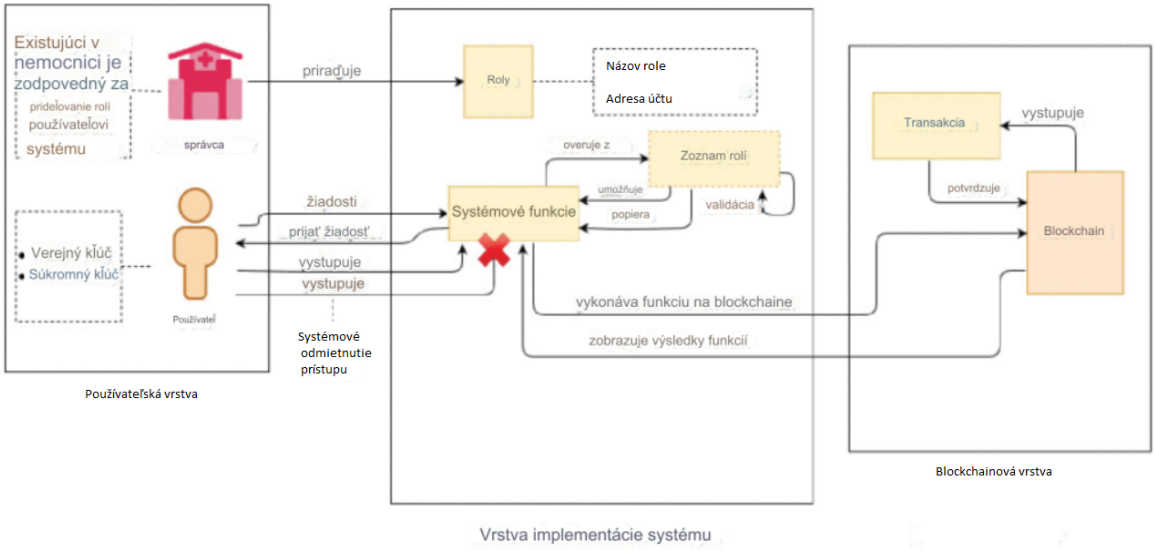
1. Lekár vyšetrí pacienta a zaznamená jeho údaje v informačnom systéme. Tieto údaje sa následne odosielajú na blockchain, kde sa vytvorí transakcia.
2. Každá transakcia je overená a získava jedinečný verejný kľúč, ktorý sa uloží na blockchain.
3. Lekári a zdravotnícke organizácie môžu s použitím súkromného/ dešifrovacieho kľúča vytvoriť dotaz na zašifrované údaje pacienta.
4. Pacienti môžu lekárovi alebo zdravotníckej inštitúcii poskytnúť súkromný kľúč na dešifrovanie údajov. Informácie sú však stále zašifrované pre tých, ktorí nemajú prístupový kľúč. [14]

Pre tento prípad využitia sa javí vhodné využiť hybridný alebo konzorčný blockchain, využívajúci konsenzuálny algoritmus PoW (hoci z dlhodobého hľadiska pribúdajúceho počtu pacientov sa s ním spájajú problémy ako neefektívne využívanie

zdrojov, stále poskytuje robustnú ochranu citlivých údajov) alebo PoA (citlivejší voči neoprávnenej manipulácií s údajmi), pričom uzlami by mohli byť nemocnice, lekárne a iní certifikovaní používatelia.

V súčasnosti existuje niekoľko spoločností zaznamenávajúcich EHR pomocou blockchainu, napríklad: MedRec je decentralizovaný systém na správu lekárskych záznamov, ktorý poskytuje pacientom spoľahlivý záznam ich lekárskej histórie. Tento systém umožňuje jednoduché zdieľanie údajov medzi rôznymi lekárskymi subjektmi s dôrazom na dôvernosť a transparentnosť. Využitím technológie blockchain je zabezpečený transparentný a spätne dohľadateľný záznam všetkých lekárskych interakcií. [44]

Komplexnejší príklad riadenia EHR prostredníctvom blockchainu popisuje **obrázok 16**, viac informácií dostupných na [53]



Obrázok 16: Príklad komplexného EHR založeného na troch vrstvách

Zdroj: [53]

4.3.2 *Odhaľovanie podvodov*

Použitie blockchainu v elektronických záznamoch o pacientoch (EHR) má za cieľ riešiť problémy spojené so súkromím a bezpečnosťou údajov. Informácie o pacientoch budú dôverne spracované pomocou blockchainu a klinické údaje budú bezpečne a efektívne zdieľané. Okrem toho môže pomocou blockchainu byť poskytovaný aj monitoring pacientov

na diaľku s dôrazom na ochranu dát. Poisťovne sa uchyľujú k použitiu blockchainovej technológie na monitorovanie falošných poistných nárokov pacientov. [13] [41]

Zdravotnícke organizácie a verejné inštitúcie majú vážne obavy z podvodov v oblasti zdravotného poistenia, ktoré spôsobujú veľké finančné straty pre poisťovne. Niektoré formy podvodov ohrozujú aj samotné zdravie pacientov, pretože procesy manuálneho spracovania požiadaviek na poistenie často zlyhávajú pri zabezpečení súhlasu všetkých zapojených strán. [13]

V tejto súvislosti sa technológia blockchain, decentralizovaný systém peer-to-peer, javí ako riešenie prostredníctvom bezpečnej, transparentnej a nezmeniteľnej validácie lekárskych nárokov, na druhú stranu oproti tradičnému databázovému spracovaniu si vyžaduje väčšiu kooperáciu zainteresovaných strán (vlády, regulátorov, poisťovní, zdravotných zariadení a pacientov), vyžaduje vyššie počiatočné náklady a v priebehu životného cyklu môže nastať problém s nízkou škálovateľnosťou (čo môže obmedziť rýchlosť/ efektivitu odhalenia zdravotných podvodov).

4.3.3 *Vývoj a správa liečiv*

Farmaceutický výskum a vývoj tvoria zložitú cestu, ktorá zahrňuje objavovanie liekov, ich vývoj a schválenie v rámci farmaceutického dodávateľského reťazca. Avšak problém falšovania liekov vzniká vtedy, keď výrobcovia a regulačné agentúry majú nedostatočnú kontrolu alebo používajú zastaralé informácie. [41]

Pri zvážení potenciálu technológie blockchain vo farmaceutickom odvetví sa otvárajú nové možnosti. Tento systém ponúka spoľahlivý spôsob sledovania farmaceutických produktov od výroby až po ich distribúciu pacientom. Integrovanie blockchainu do farmaceutického dodávateľského reťazca môže zlepšiť transparentnosť a bezpečnosť výrobkov, čím sa minimalizuje riziko falšovania a nízkej kvality liekov. [13] [44]

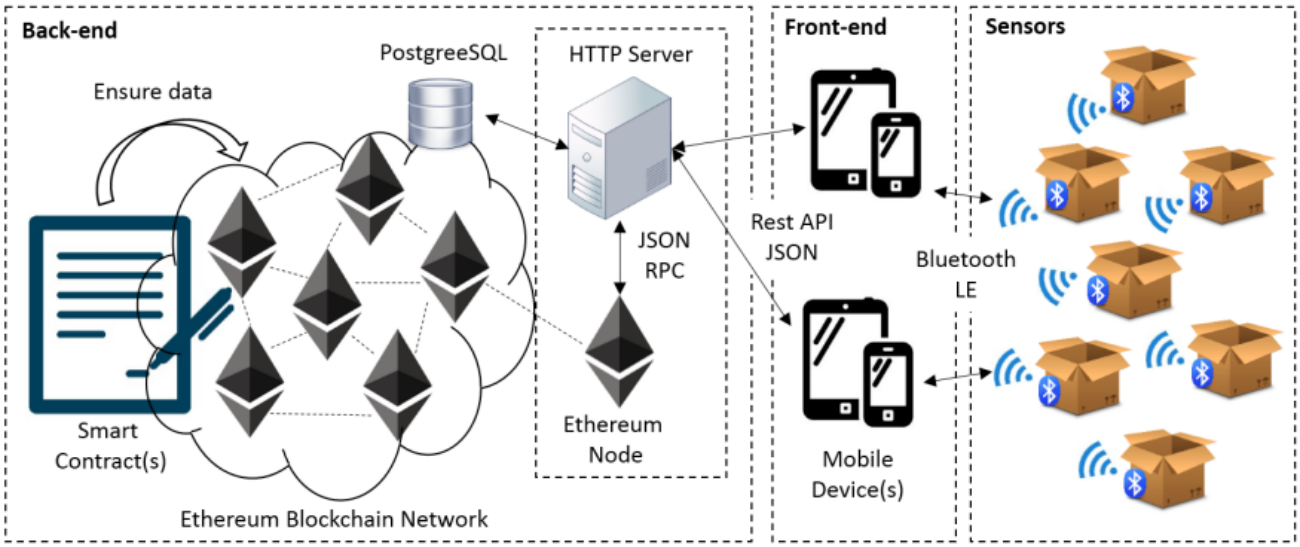
Odhaduje sa, že 10%–30% liekov v nedostatočne rozvinutých krajinách sú falošné. Účinky, ktoré spôsobujú falšované farmaceutika, nie sú len odlišné od tých tradičných; majú tiež osobitné dôsledky na ľudské zdravie. Podľa Svetovej zdravotníckej organizácie je približne 30% liekov uvádzaných na trh v Afrike, Ázii a Latinskej Amerike, žiaľ, falošných. Tieto lieky prechádzajú cez zložitejší, rozptýlený dodávateľský reťazec, čo komplikuje

odhaľovanie falšovaných produktov a poskytuje príležitosti pre falošné farmaceutika, aby sa dostali do skutočného dodávateľského reťazca. [13]

Hoci prúdenie falošných liekov do legálneho reťazca predstavuje hrozbu pre verejné zdravie, technológia blockchain ponúka nádej na zmiernenie týchto rizík. Ako sa tento trend bude rozvíjať, bude zrejmé, že aplikácie blockchainu môžu mať ešte širší dosah a poskytnúť nové riešenia pre globálny trh s liečivami. Aj keď sme len na začiatku porozumenia jej potenciálu, je jasné, že môže mať obrovský vplyv na celé odvetvie. S postupným rozširovaním sa ukáže, ako môže táto technológia transformovať celý dodávateľský reťazec liekov. [32]

Regulácia EÚ ohľadom distribúcie liekov "Good Distribution Practice of medicinal products for human use, (GDP 2013/C 343/01) je účinná od 1. januára 2016. Je povinnosťou nahlásiť akékoľvek odchýlky, ako napríklad teplotu prepravovaných liečiv, distribútorovi a príjemcovi postihnutých liekov, ako aj monitorovať teplotu každého balíka počas celého času. To núti farmaceutické spoločnosti objednávať špeciálne služby od logistických spoločností, ktoré často nie sú nevyhnutné, keďže teplotné kategórie napríklad od 15◦ - 25◦ C sa často dodržiavajú na jar alebo na jeseň, technológia blockchain poskytuje decentralizované a dôveryhodné riešenie , v rámci ktorého sa dáta o liekoch počas logistického procesu môžu ukladať a pristupovať k nim obe strany, ktoré sú zabezpečené prostredníctvom inteligentnej zmluvy (smart kontraktu). [32]

Spoločnosť Modum.io AG monitoruje všetky potrebné údaje počas prepravy liekov prostredníctvom kombinácie senzorov IoT (Internet vecí) s technológiou blockchain Architektúra je štruktúrovaná do back-endu, front-endu a senzorových zariadení IoT, ako je znázornené na **obrázku 17**. [32]



Obrázok 17: Architektúra monitorovania teploty liekov (Modum.io)

Zdroj: [32]

Architektúra je zložená z nasledujúcich stručne popísaných komponentov:

1. **Ethereum blockchain sieť:** slúži na overenie teplotných údajov registrovaných vo front-ende. Smart kontrakty bežia v virtuálnom stroji, nazývanom Ethereum Virtual Machine (EVM), čo umožňuje overenie údajov pomocou smart kontraktov.
2. **Smart kontrakt:** je vydávaný pre každú novú zásielku a zodpovedá za zabezpečenie dodržiavania teplotných a časových údajov počas prepravy, ktoré sú s zásielkou spojené.
3. **Databáza:** relačná databáza používaná na uchovávanie surových teplotných údajov a prihlasovacích údajov používateľov.
4. **Server:** zabezpečuje komunikáciu medzi blockchainovou sieťou a používateľmi front-endu, vytvára a modifikuje smart kontrakty, ako aj ukladá údaje v databáze.
5. **Mobilné zariadenia:** zariadenia používané koncovými používateľmi na registráciu nových zásielok a sledovanie/posielanie záznamov teplotných údajov na Server.
6. **Senzory:** termálne citlivé zariadenia kompatibilné s technológiou Bluetooth nastavené na odosielanie údajov v pevnom intervale dotazovania na mobilné zariadenie. [32]

V back-ende je dodržiavanie teplotných požiadaviek zabezpečené pomocou smart kontraktov napísaných v jazyku Solidity, vysokoúrovňového jazyka určeného na kompiláciu kódu pre EVM. Pre každú novú zásielku alebo skupinu liekov obsahujúcich špecifické

teplotné požiadavky je konfigurovaný a nasadený smart kontrakt na strane servera, aby sa zabezpečili požiadavky na dodržiavanie GDP. Preto sa mapovanie zásielky na jej príslušný smart kontrakt alebo adresa kontraktu vykonáva pomocou relačnej databázy s veľmi nízkou dodatočnou zložitosťou alebo nákladmi. Server v modum.io AG hostuje uzol Ethereum, ktorý sa účastní v sieti Ethereum a môže sledovať zmeny na svojich smart kontraktoch, vytvárať nové smart kontrakty alebo volať funkcie smart kontraktu. Uzol Ethereum komunikuje s HTTP (Hypertext Transfer Protocol) serverom cez JSON (JavaScript Object Notation). Údaje, ktoré sú citlivé alebo príliš veľké (obmedzenú z dôvodu bezpečnosti , škálovateľnosti a rýchlosti) na to, aby sa ukladali do blockchainu, sa ukladajú do databázy PostgreSQL. Sem patria aj surové teplotné údaje, pretože sú príliš veľké na to, aby sa ukladali do smart kontraktu. Smart kontrakt overuje rozsah teploty a ukladá výsledok overenia do smart kontraktu spolu s URL adresou, ktorá ukazuje na surové teplotné údaje a ich haš. [32]

Vo front-ende komunikujú klientské aplikácie Android so serverom pomocou API (rozhranie pre programovanie aplikácií) s použitím JSON na kódovanie a dekódovanie požiadaviek/odpovedí. Pomocou mobilného telefónu môžu používatelia registrovať nové zásielky vrátane regulačných údajov v rámci systému a pre každú zásielku sa vytvorí smart kontrakt. API by malo tiež umožniť príjemcovi zásielky nahrať teplotné merania zaznamenané senzorom na server. Odosielateľ aj príjemca by mali byť informovaní o výsledku kontraktu a mali by mať prístup k teplotným meraniam, najlepšie prostredníctvom grafickej vizualizácie. [32]

4.4 Využitie blockchainu v školstve

Integrácia technológie blockchain do vzdelávacieho systému má veľký potenciál zlepšiť efektívnosť, bezpečnosť a dôveryhodnosť vzdelávacieho procesu. Vytvorením bezpečných a transparentných platforiem na sledovanie a overovanie akademických úspechov študentov môže technológia blockchain pomôcť vytvoriť prístupnejší a dôveryhodnejší vzdelávací systém, uľahčujúci študentom prezentáciu ich zručností a znalostí potenciálnym zamestnávateľom. [11] [16]

Nedávne štúdie a prieskumy však naznačujú, že prijatie technológie blockchain vo vzdelávaní je stále v počiatočných fázach, očakáva sa však, že v nasledujúcich rokoch bude rýchlo rás.

Jedným z možných použití technológie blockchain je, že môže slúžiť ako decentralizované trvalé nemenné úložisko rôznych druhov informácií. Vytváranie a vydávanie rôznych digitálnych certifikátov je s blockchainom relatívne jednoduché. Napríklad sa vytvorí digitálny súbor PDF, ktorý obsahuje informácie, ako sú meno študenta, titul, rok ukončenia štúdia, názov univerzity, dátum vydania atď. Následne sa digitálny súbor podpisuje pomocou súkromného kľúča, ku ktorému má prístup iba vydávajúca inštitúcia. Podpis sa pripojí k samotnému certifikátu. Ďalej sa vytvorí haš dokumentu pomocou algoritmu SHA-256, ktorý sa dá použiť na overenie, či nikto neporušil obsah digitálneho súboru. Nakoniec sa súkromný kľúč znova použije na vytvorenie záznamu v blockchaine, čo znamená, že v tomto prípade certifikát sa vydáva študentovi v daný deň. To umožňuje overiť, komu bol certifikát vydaný a kým bol vydaný. Zároveň je možné overiť aj obsah samotného certifikátu - všetko iba prostredníctvom napríklad bitcoinového blockchainu a nie je potrebné sa obracať na vydávajúcu inštitúciu. [16] [21]

Univerzita v Nikózii sa stala prvou univerzitou na svete, ktorá vydávala akademické osvedčenia, ktorých pravosť sa dá overiť prostredníctvom bitcoinového blockchainu. Tieto certifikáty sa vydávajú od roku 2015 študentom, ktorí úspešne ukončili alebo sa zúčastnili na DFIN-511 (Úvod do digitálnych mien), čo je prvý univerzitný kurz ponúkaný na tému kryptomeny. Od roku 2017 začala UNIC vydávať všetky univerzitné diplomy na bitcoinovom blockchaine pomocou vlastnej technológie, ktorá sa vyvinula ako open-source. [11]

Obrázok 18 ukazuje príklad výstupu diplomu emitovaného v bitcoinovom blockchaine.

Obrázok 18: Ukážka diplomu uloženého na bitcoinvom blockchaine

Zdroj: Vlastné spracovanie

Univerzita v Nikózii (UNIC) má takmer desaťročnú históriu ako vedúca univerzita v oblasti kryptomien a blockchainu, keď v roku 2014 spustila prvý študijný program zameraný na kryptomeny na svete. IFF, dôležitý inštitút UNIC, hrá kľúčovú úlohu pri rozšírení cieľov UNIC, vzdeláva viac ako 145 000 študentov cez rôzne kurzy v oblasti blockchainu, kryptomien, metaverzu a využitia blockchainu v verejnej sfére.

Spoločne UNIC a IFF smerujú inovácie, pôsobia ako akademický lídri pre Observatórium a Fórum pre blockchain EÚ (iniciatíva Európskej komisie na zrýchlenie rozvoja blockchainu v rámci EÚ) a boli vybrané aj na členstvo v Technologickom poradnom výbore Európskej centrálnej banky (ECB). [16]

Na svete však existuje viac univerzít, ktoré používajú blockchain v rôznych aspektoch svojich vzdelávacích systémov. Tu je niekoľko príkladov univerzít, ktoré ju implementovali vo svojom vzdelávaní:

1. **Massachusetts Institute of Technology (MIT):** MIT bol na čele využívania blockchainu vo vzdelávaní a už v roku 2015 spustil vlastný systém digitálnych certifikátov založený na sieti blockchain. Tento systém umožňuje študentom získavať bezpečné a overiteľné digitálne certifikáty za svoje kurzy a úspechy.

2. **Stanfordská univerzita:** Stanfordská univerzita skúma použitie technológie blockchain vo vzdelávaní vrátane jej použitia na správu digitálnej identity, bezpečné zdieľanie údajov a bezpečnú správu certifikátov.
3. **University College London (UCL):** UCL implementovala blockchainovú platformu pre bezpečné a transparentné riadenie údajov, ktorá sa používa na ukladanie a správu študentských záznamov, výskumných údajov a iných citlivých informácií.
4. **University of Melbourne:** University of Melbourne v Austrálii skúma použitie technológie blockchain vo vzdelávaní, vrátane jej použitia na bezpečné zdieľanie údajov, bezpečnú správu certifikátov, a správa digitálnej identity [11] [12]

Dokonca Khaled Mili sa venuje vytvoreniu systému BlockDipls založeného na technológií blockchain, ktorá má za cieľ znížiť falšovanie záverečných prác, fungujúcu na Ethereum sieti. Viac informácií na [54].

Práve implementáciu technológie blockchain do školstva považujem za vhodnú, najmä pre overenie univerzitných diplomov, kde by táto technológia mohla mať významný vplyv, treba však zvážiť všetky jej stánky ako:

Silné stránky spojené so zabezpečením a šifrovaním údajov (čo zvyšuje bezpečnosť údajov študentov a akademických výsledkov), verejným prístupom (čo umožňuje jednoduché overenie pravosti diplomov a zabraňuje falšovaniu diplomov a certifikátov) či minimalizovaní falšovania(pre nezmeniteľnosť a transparentnosť blockchainu čím znižuje riziko falšovania diplomov a certifikátov).

Slabé stránky spojené s technologickými prekážkami (nutnými technickými znalosťami a investíciami do infraštruktúry), potrebou štandardizácie či ochranou osobných údajov (nakoľko zdieľanie akademických diplomov a nemennosť dát vzbudzuje obavu o ochrane osobných údajov študentov).

Príležitosti spojené s verejným financovaním (rozvoj blockchainu v školstve môže byť podporovaný verejnými financiami a grantmi, ktoré môžu podporiť výskum a implementáciu), či zvýšením dôveryhodnosti (škôl a iných inštitúcií súvisiacich s akademickými výsledkami študentov).

Hrozby vyplývajúce so zvýšenej transparentnosti (v súvislosti s ochranou osobných údajov), kybernetickými rizikami (útokom hrubou silou, manipuláciou s údajmi pred vložením) či regulačnými obmedzeniami. [48] [51][55]

V rámci školstva by blockchain mohol fungovať na verejnej alebo súkromnej blockchain sieti. Verejná sieť by umožňovala transparentný a otvorený prístup k záznamom, čo by zvyšovalo dôveru v overovanie akademických údajov. Naopak, súkromná sieť by umožňovala väčšiu kontrolu a prispôsobenie sa špecifickým potrebám vzdelávacieho prostredia. Pri využití verejnej sa môžeme inšpirovať UNIC, ktorá využíva bitcoin blockchain (najmä pre robustný PoW). Prípadne Ethereum ktoré je známe svojou schopnosťou vykonávať inteligentné zmluvy a poskytnutím dostatočnej úrovni bezpečnosti a dôvery.

Využívané by mohli byť tri druhy uzlov:

1. **Uzly vzdelávacích inštitúcií:** Tieto uzly by zahŕňali univerzity, stredné školy a ďalšie vzdelávacie organizácie. Boli by zodpovedné za pridávanie nových záznamov o diplomoch a certifikátoch do blockchainu.
2. **Uzly školských administratívnych orgánov:** Tieto uzly by zahŕňali orgány, ktoré sú zodpovedné za správu a dohľad nad vzdelávacími inštitúciami (napr. MŠVVaM). Ich úlohou by bolo monitorovať integritu a spoľahlivosť záznamov v blockchaine a zabezpečiť dodržiavanie pravidiel a predpisov v školstve.
3. **Archivačné uzly:** Tieto uzly by slúžili ako archívne úložisko pre dlhodobé uchovávanie dôležitých akademických záznamov. Ich úlohou by bolo zabezpečiť, aby historické údaje v blockchaine zostali dostupné a nezmenené aj v budúcnosti.

Fungovanie by mohlo prebiehať nasledovne:

1. **Vydanie diplomu**: Po úspešnom absolvovaní štúdia by univerzita vytvorila digitálny záznam o udelení diplomu, ktorý by sa uložil do blockchainu spolu s unikátnym identifikátorom.
2. **Overenie diplomu:** Osoba alebo organizácia, ktorá chce overiť platnosť diplomu, by skenovaním QR kódu alebo zadávaním identifikátora získala prístup k verejnému blockchainu a mohla by overiť, či je diplom platný a autentický.

3. **Aktualizácia údajov:** Ak by došlo k zmene statusu diplomu (napríklad odvolanie alebo aktualizácia informácií), nové údaje by sa zaznamenali do blockchainu a predchádzajúce záznamy by zostali nezmenené. [11] [56] [57]

4.5 Volebný systém založený na technológií blockchain

Hlasovanie je kľúčovým prvkom demokracie, avšak napriek zavedeným bezpečnostným opatreniam nie je imúnne voči podvodom. Moderné volebné systémy sú často pomalé a výsledky nie sú vždy overiteľné. E-volebné systémy založené na blockchaine ponúkajú riešenie mnohých týchto problémov a zabezpečujú výhody ako: [8] [37]

1. predchádzanie podvodom, zníženie ľudskej účasti,
2. zrýchlenie spracovania výsledkov,
3. zníženie počtu znehodnotených hlasovacích lístkov vylepšením prezentácie a automatickou validáciou hlasovacích lístkov,
4. zníženie nákladov v dôsledku klesajúcich prevádzkových nákladov na voľby,
5. zvýšenie zapojenia do demokratického procesu vďaka ľahšej dostupnosti (vzdialené hlasovanie), potenciál pre väčšiu priamu demokraciu.

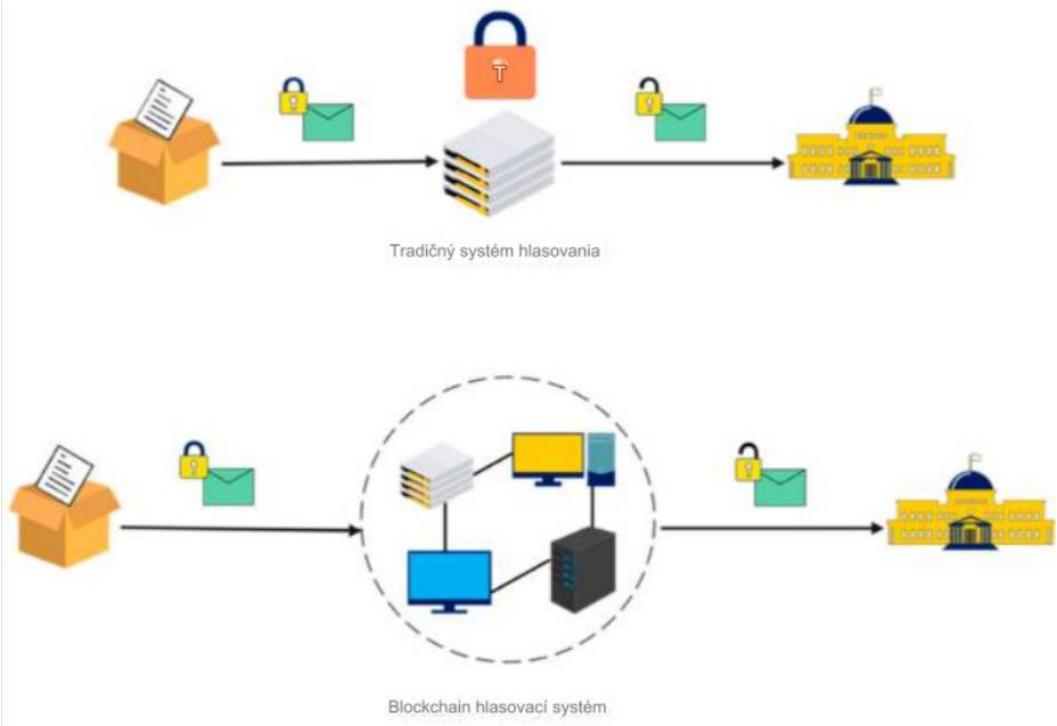
V súčasnosti existuje množstvo volebných systémov, ako napríklad Voatz, Polyas a Luxoft, ktoré sa zakladajú na rôznych spôsoboch overovania totožnosti voličov, ako je biometria, rodné číslo alebo rozpoznávanie tváre. Tieto systémy využívajú rôzne typy blockchainov, vrátane Bitcoinu, Ethereumu a Hyperledger Fabric. A využívajú rôzne volebné modely: niektoré umožňujú voličovi zmeniť svoj hlas, iné nie, niektoré dokonca umožňujú odoslať prázdny hlas. [9]

Avšak, hoci tieto hlasovacie systémy sú dostupné, majú problémy so škálovateľnosťou. Sú vhodné pre použitie v menších rozsahoch, ale nie sú dostatočne efektívne na vyriešenie potrieb volebného procesu na vnútroštátnej úrovni najmä pre ich náročnejšiu škálovateľnosť, kde sa zaoberáme s miliónmi transakcií. [8] [9]

V prípade použitia Ethereum siete je očakávaný čas vytvorenia nového bloku medzi 10 a 19 sekundami. Pre inteligentné zmluvy je čas potrebný na potvrdenie transakcie približne 38 sekúnd (v závislosti od ceny "gasu" (prioritizácie) stanovenej pre transakciu. [52]

Na **obrázku 19** je zrejmý hlavný rozdiel medzi tradičnými a blockchainovými volebnými systémami. Zatiaľ čo v tradičných systémoch existuje centrálna autorita, ktorá

riadi celý proces, v blockchainových systémoch nie je žiadna centrálna autorita a údaje sú distribuované v rôznych uzloch. To zabezpečuje integritu hlasov a ich efektívnu kontrolu. [9]



Obrázok 19: Grafické znázornenie architektúry hlasovacích systémov

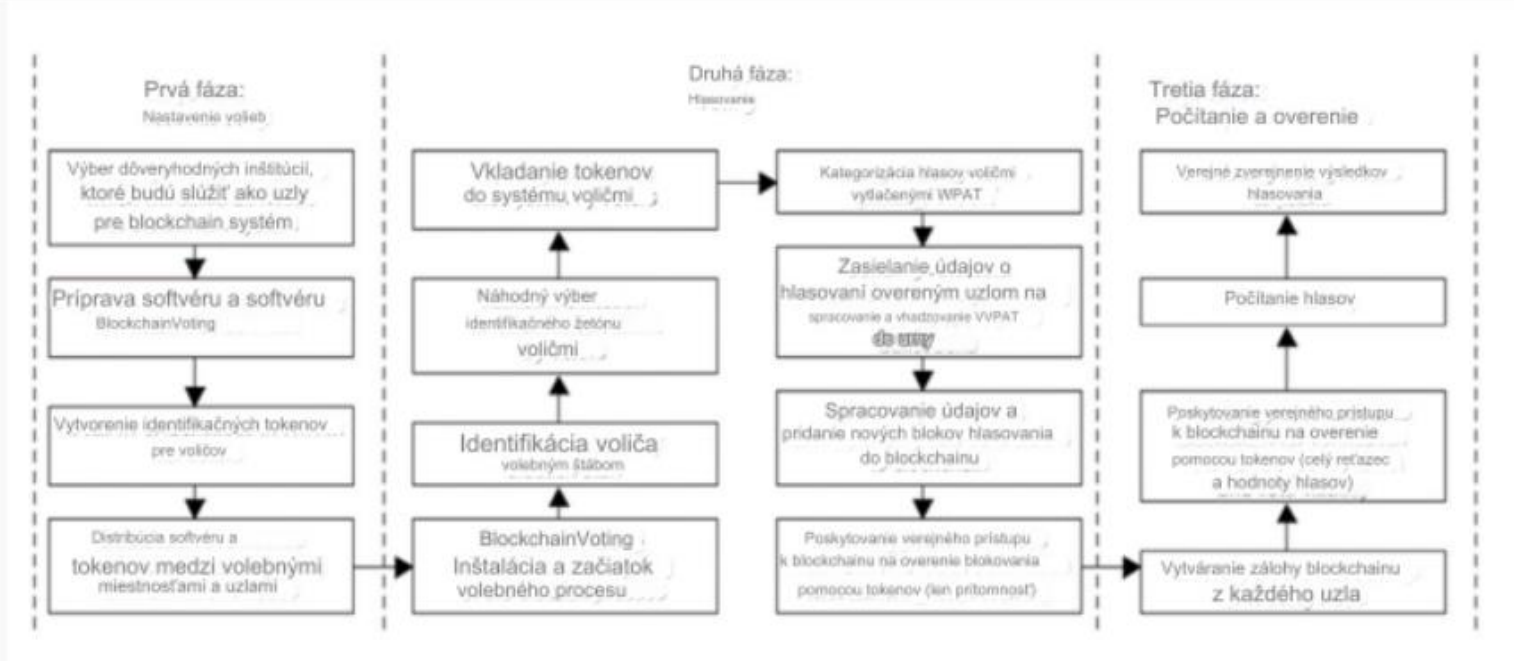
Zdroj: [9]

Pawlak a spol., (2018), navrhli systém, ktorý využíva inteligentné a multi-agentové koncepcie pre Auditovateľný systém hlasovania na blockchaine (ABVS), ktorý zlúči elektronické hlasovanie s technológiou blockchain do jednej aplikácie bez supervízie na internetové hlasovanie, ktorá je overená od začiatku do konca. Navrhovaný systém sa skladá z troch fáz: [37]

1. fáza inicializácie,
2. fáza hlasovania,
3. fáza počítania a overovania.

Výhoda agentovo založeného riešenia ABVS elektronického volebného systému spočíva v maximalizácii bezpečnosti hlasovania. V hlasovacej fáze operujú dva typy agentov (hlasovací agent a autorizačno-konfiguračný agent), vďaka čomu je aplikácia vo volebných miestnostiach redukovaná na sprostredkovateľa medzi agentmi a voličom, ktorý bude riadiť všetky úlohy súvisiace so spracovaním a prenosom hlasov. Agenti by boli taktiež emitovaní

uzlami, ktoré nie je možné zmeniť, a bolo by ľahké zistiť akékoľvek pokusy o hackovanie systému. Navrhovaný systém je možné vidieť na **obrázku 20**. [37]



Obrázok 20: ABVS systém hlasovania

Zdroj: [37]

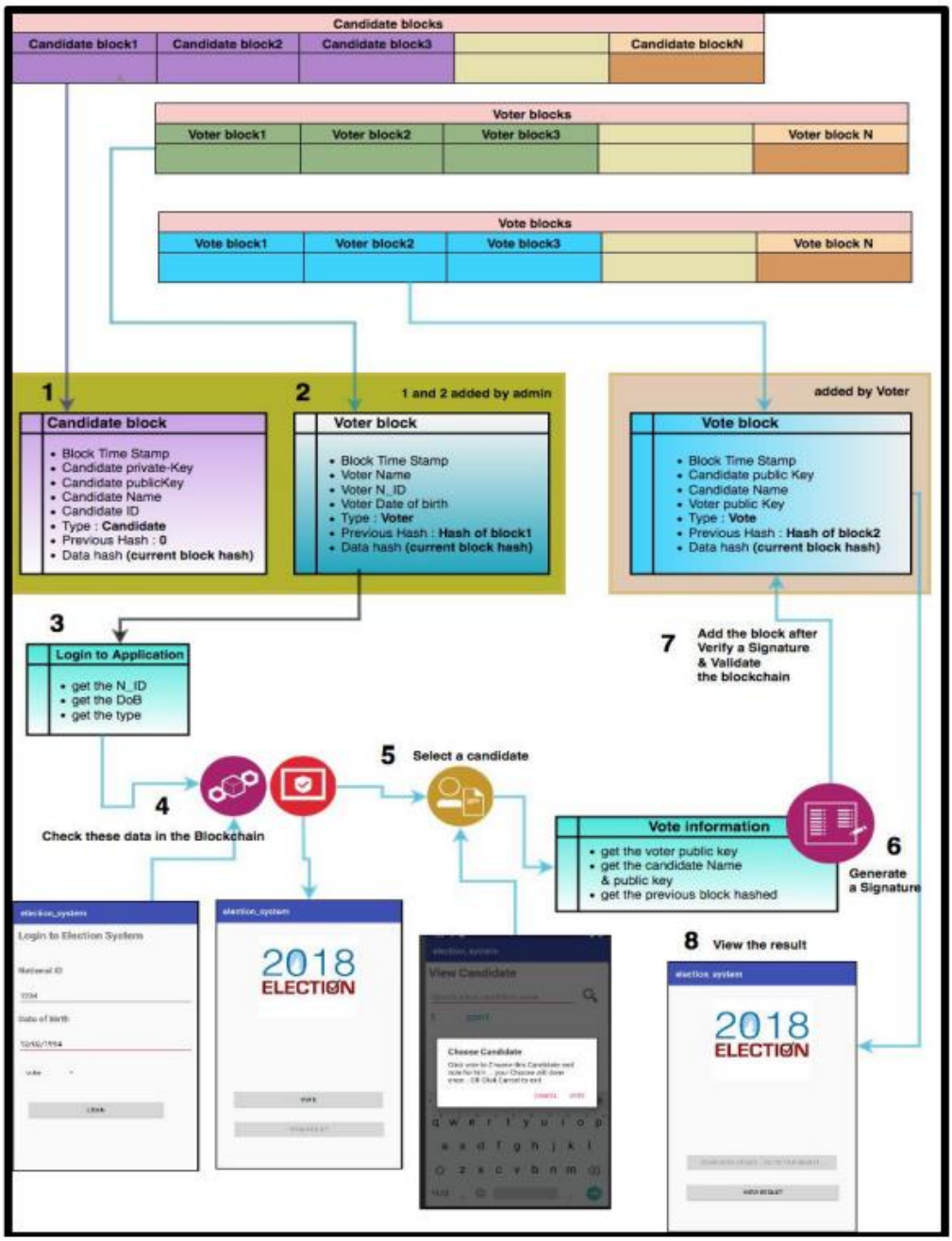
Noor Mohammedali a Ali Al-Sherbaz (2019) navrhli systém, ktorý využíva technológiu blockchain na ukladanie hlasov ako transakcií. Každá transakcia obsahuje haš celého hlasu vo forme Merkleho stromu, časovú pečiatku hlasovania, výber hlasu, jedinečné ID na overenie identity používateľa a jednorazové heslo na autentifikáciu. [10]

Dáta o výbere hlasu majú dĺžku 4 bajty s jedným bitom, ktorý označuje výber kandidátov. Merkleho koreň je uložený v bloku, ktorý je podobný bloku používanému v bitcoine. Použitie štruktúry Merkleho stromu vedie k významným úsporám miesta a umožňuje efektívne získavanie hlasov. Pre hlasovanie a zobrazenie výsledkov sa využíva webové rozhranie. [10]

Pred samotným hlasovaním sú zobrazené detaily kandidátov, ktoré sa získavajú prostredníctvom funkcie registrácie kandidátov. Okrem toho je k dispozícii informačný panel kandidáta, ktorý poskytuje informácie o demografii voličov pre prijaté hlasy a zobrazuje živé štatistiky z volieb. Každý volič je overený pomocou jedinečného ID čísla, čo eliminuje potrebu registrácie pred hlasovaním. Autentifikácia je zabezpečená jednorazovým

heslom zaslaným na mobilné číslo voliča. Preto existujú dva pohľady pre voliča: overenie a získanie detailov pred odoslaním hlasu a následné zobrazenie výsledkov, vrátane živých štatistík z volieb. [10] [37]

Po prijatí hlasu sa jeho riadenie preberá ťažiacimi uzlami v blockchaine, pričom webový rámec odosiela požiadavky na bránový uzol, ktorý slúži ako prístupový bod k blockchainu. Skript s názvom "Read Blockchain" je používaný webovým serverom na monitorovanie blockchainovej siete a aktualizáciu SQL servera v webovom rámci, aby sa zmeny v blockchaine odzrkadlili vo výsledkoch, ktoré sú zobrazené všetkým používateľom. Viac informácií dostupných na [10].



Obrázok 21: Mohammedali a Sherbaz návrh hlasovacieho systému

Zdroj: [10]

4.6 Využitie blockchainu v doprave

Kryptotechnológie vďaka transparentnosti a nemennej histórii zápisov na blockchaine môžu nájsť uplatnenie aj v oblasti rôznych registrov, ktoré v rámci verejnej správy fungujú centralizovane. Takýto register by mohol by zavedený napríklad v oblasti predaja jazdených áut. Takzvané „stáčanie“ kilometrov stále predstavuje obrovský problém (dopad v krajinách EÚ sa odhaduje na 5,6 až 9,6 mld. EUR ročne). [21]

Blockchain by mohol priniesť vyššiu transparentnosť a všeobecnú dôveru k záznamom o „meraniach“ stavu km, ktoré pomôžu prípadné stáčanie odhaliť. [7]

Výrobcovia áut sa snažia vymyslieť bezpečné spôsoby uchovávania kilometrov vozidiel v ich palubných počítačoch, no vždy existuje riziko, že tieto mechanizmy bude možné obísť. Hlavným problémom je, že ak sa informácie ukladajú a čítajú priamo v palubnom počítači, môžu byť ľahko kompromitované. Preto sú kilometre často upravované. Využitím technológie blockchain mimo vozidla by sa manipulácia s kilometrami stala oveľa ťažšou. Táto technológia poskytuje ochranu proti akémukoľvek zásahom do informácií. [21]

V dnešnej dobe, kedy sme všetci online, môže byť výhodou, že sa kilometre pravidelne ukladajú do decentralizovanej databázy. Záznamy o kilometroch sa môžu vykonávať pomocou čipov nainštalovaných vo vozidlách, čo umožní ich prenos do decentralizovanej databázy. Takto je možné jednoducho overiť informácie o kilometroch vozidla.[7] [21] [46]

Niektoré vlády alebo kupujúci požadujú technické riešenia na zastavenie manipulácie s kilometrami od autoservisov, predajcov alebo poskytovateľov služieb.

Odometer/ počítadlo stavu prejdených kilometov založený na technológii blockchain by umožnil zaznamenávať kilometre všetkých vozidiel na svete a zároveň dodržiavať právne predpisy a chrániť sa pred manipuláciou. Vozidlá by týždenne ukladali údaje do blockchainovej databázy, čo by prinieslo väčšiu ochranu pred manipuláciou. [21] [45]

Obrázok 22 popisuje uloženie stavu prejdených kilometrov do siete blockchain pomocou OBD2 pripojenia k vozidlu.

Obrázok 22: Návrh overovania kilometrov uložených v sieti blockchain

Zdroj: [45]

Vzhľadom na rozsah záverečnej práce uvádzam v skratke ďalšie možnosti aplikácie blockchainu v sektore dopravy, kde v súčasnosti napreduje Austrália – návrhy sú podrobnejšie rozpísané v [7] [46].

1. **Integrované platobné systémy**: Využitie blockchainu na vytvorenie bezpečných a transparentných platobných systémov pre rôzne formy dopravy, ako sú verejná doprava, nájomné služby automobilov, jazda na žiadanie (ridesharing) a mýto.
2. **Delenie údajov o doprave**: Blockchain by mohol umožniť bezpečné a dôveryhodné zdieľanie údajov o doprave medzi rôznymi subjektmi, ako sú vládne agentúry, dopravné spoločnosti a občianske iniciatívy. To by mohlo viesť k lepšiemu porozumeniu dopravnej situácie a efektívnejšiemu plánovaniu dopravy.
3. **Identifikácia vozidiel a vodičov**: Využitie blockchainu na správu identifikácie vozidiel a vodičov by mohlo pomôcť zlepšiť bezpečnosť cestnej premávky a zamedziť podvodom spojeným s falšovaním dokumentov alebo identít.
4. **Smart kontrakty pre reguláciu**: Použitie inteligentných zmlúv na automatizáciu a transparentnosť procesov regulácie v oblasti dopravy. Mohli by byť využité na sledovanie dodržiavania predpisov a povinností, ako sú kontrolné a bezpečnostné audity vozidiel a dopravných spoločností.

5. **Dopravná logistika**: Blockchain môže byť využitý na sledovanie a optimalizáciu dopravných trás, správu zásobovania a skladovanie údajov o zásielkach. To by mohlo prispieť k efektívnejšiemu pohybu tovaru a znižovaniu časových a finančných nákladov.

Integrácia blockchainu do Land Transport by mohla pomôcť modernizovať a zefektívniť dopravné systémy v Austrálii, čo by mohlo viesť k lepšej bezpečnosti, efektívnosti a udržateľnosti. Avšak, pri implementácii by bolo dôležité zvážiť otázky týkajúce sa súkromia, bezpečnosti a interoperability blockchainu s existujúcimi systémami. [7] [46]

4.7 Blockchain a verejné obstarávanie

Verejné obstarávanie je jednou z oblastí, kde môže byť využitie kryptotechnológií, vrátane blockchainu, prospešné. Verejné obstarávanie zahŕňa rôzne práce, služby a tovary, je často kritizované pre svoju možnú korupciu a nedostatok transparentnosti Použitím inteligentných zmlúv môžu byť verejné obstarávania transparentnejšie, zautomatizované a rovnako samo-vynútiteľné. [21]

Prostredníctvom blockchainu by mohol mať každý občan v krajine prístup k údajom, teda kto vyhral tender, či splnil jeho podmienky, prípadne aká bola jeho ponuka. Zároveň môže ostať identita zatajená a pomocou šifrovania a blockchainu môžu jednotlivé strany vo verejnom obstarávaní identitu potvrdiť, teda potvrdiť prepojenie medzi identitou virtuálnou a reálnou. Pomocou inteligentných zmlúv by sa pri verejnom obstarávaní mohli selektovať ponuky na základe zadaných vstupov. To znamená podmienok, ktoré by mala ponuka spĺňať. [21]

Napríklad nákladovosť, počet potrebných ľudí, strojov a podobne. Záleží na obstarávanom predmete. Zároveň môže byť neskôr použitá iná inteligentná zmluva, ktorá by uvoľnila prostriedky len na základe zrealizovania určitej fázy zákazky. [21]

Napríklad pri diaľniciach postavenie mosta, či asfaltovanie cesty. Ak by práca nebola dokončená podľa stanovených podmienok v inteligentnej zmluve, finančné prostriedky by sa neuvoľnili. [21]

Kanadská vláda pracuje na skúšobnom procese využitia technológie blockchain na zvýšenie transparentnosti grantov v oblasti výskumu. Národná rada pre výskum (NRC) využíva Catena Blockchain Suite, kanadský produkt postavený na blockchainovej platforme Ethereum, na zverejňovanie informácií o Programe pomoci pre priemyselný výskum (NRC

IRAP) a jeho financovaní v reálnom čase. Každá zmena v grantoch, ktorú urobí NRC, sa automaticky zaznamená v blockchainovej sieti Ethereum. Tieto zmeny sa tiež prejavia v online databázach, ktoré sú verejnosti prístupné, a informácie je možné filtrovať podľa rôznych kritérií, ako je finančná hodnota, dátum, prijímateľ a región. Tento systém by mal zvýšiť transparentnosť poskytovaných grantov a umožniť obyvateľom sledovať, kam smerujú finančné prostriedky. [17] [21]

UN World Food Programme (WFP): WFP spustilo pilotný projekt v roku 2017, ktorý využíva blockchain na zabezpečenie transparentnosti a sledovateľnosti potravinových dodávok v núdzových situáciách. [53]

Za najväčší prínos považujem: transparentnosť, dôveryhodnosť a možnosť zníženia prostredníkov, čo vedie k zníženiu korupcie automatizácií schvaľovacích procesov.

Treba si však uvedomiť, že technológia blockchain je stále pomerne nová, z čoho môžu vyplývať mnohé riziká ako napríklad: bezpečnostné obavy (51% útok), prelomenie hašu a PKI (najmä s možným nástupom kvantových počítačov), regulačné a právne prekážky (napr. GDPR).

4.8 Blockchain a transparentná platba poplatkov

Tým, že blockchain presne zaznamenáva transakcie platieb a obsahuje ich celú históriu, tak sa prakticky hodí na každú oblasť, kde sa posielajú platby a je potrebné zachovať transparentnosť platieb. A to preto, že najmä vo verejnom sektore, či už na úrovni štátneho rozpočtu, alebo krajov, miest a obcí, sa evidujú rôzne poplatky a dane od fyzických a právnických osôb. Pomocou blockchainu by mohli byť platby vykonávané instantne a automatizovane. Zároveň by sa zachovala transparentnosť a prehľadnosť histórie platieb a presne by sa vedelo, ktorá fyzická či právnická osoba uhradila aký poplatok alebo daň. Na strane druhej túto oblasť riešia aj klasické databázy, avšak neposkytujú až takú vysokú mieru dôveryhodnosti. [21]

Systémy založené na blockchaine získali významnú pozornosť pre ich potenciál zvýšiť transparentnosť, znižovať úniky daní a zjednodušiť daňové procesy. Integrovanie technológie blockchain do daňových politík môže priniesť viacero výhod, ako napríklad:

1. **Transparentnosť a Nezmeniteľnosť:** Schopnosť blockchainu zlepšiť transparentnosť, znížiť úniky daní a automatizovať daňové procesy prináša

významné výhody. Blockchain môže riešiť tieto výzvy poskytnutím auditovateľného a nezmeniteľného záznamu transakcií, čím zvyšuje daňovú transparentnosť.

2. **Vylepšená sledovateľnosť daní:** Integrácia technológie blockchain do daňových politík môže adresovať výzvy súvisiace so sledovaním a zdanením online podnikov. Táto integrácia môže modernizovať daňovú administratívu, zvýšiť výber príjmov a podporiť zodpovednosť digitálnej ekonomiky.
3. **Inteligentné zmluvy:** Inteligentné zmluvy (smart kontrakty), ktoré umožňujú čiastočné alebo úplné samo-vykonateľné doložky zmlúv, môžu automatizovať daňové výpočty a platby, čím znižujú administratívne náklady.
4. **Zníženie administratívneho zaťaženia pri spracovaní daní:** Automatizované daňové výpočty a platby prostredníctvom smart kontraktov zjednodušujú procesy výberu daní, čím znižujú administratívne úsilie.
5. **Reportovanie v reálnom čase:** Schopnosť blockchainu poskytovať informácie o transakciách a príjmoch v reálnom čase znižuje časové oneskorenie pri reportovaní daní.
6. **Daňovanie cezhraničných transakcií:** Blockchain môže zjednodušiť výpočty cezhraničných daní a konverziu mien, zabezpečujúc presné a konzistentné zdanenie naprieč rôznymi jurisdikciami. [47]

Na druhú stranu existujú obmedzenia ako:

1. **Regulácia:** V niektorých jurisdikciách môžu byť platobné operácie na blockchaine podrobené prísnym regulačným požiadavkám, čo môže viesť k právnym problémom a komplikáciám.
2. **Nestabilita cien:** V prípade využitia platby kryptomenou (nie tzv. „stablecoinom“ ako napr. Tether), ktoré sú často používané na blockchainových sieťach, môže byť platba veľmi nestála a podliehať výrazným fluktuáciám, čo môže viesť k riziku straty hodnoty.
3. **Nízka škálovateľnosť:** Niektoré blockchainové siete môžu mať obmedzenú kapacitu spracovania transakcií, čo môže spôsobiť oneskorenie pri spracovaní platobných operácií v prípade veľkého objemu transakcií. [47]

Overovanie digitálnej identity: Blockchain môže poskytnúť bezpečný a decentralizovaný spôsob overovania digitálnych identít online podnikov, čím sa znižuje riziko podvodov.

Príkladom inovatívneho využitia blockchainu v verejnej správe je mesto Rotterdam v Holandsku, kde sa turistické dane vyberajú prostredníctvom inteligentných zmlúv. Týmto spôsobom sa zamestnanci mesta zbavujú niektorých povinností a činností súvisiacich s turistickými daňami. Vo Švajčiarsku, v oblasti Chiasso v kantóne Ticino, obyvatelia už od roku 2018 môžu platiť dane a poplatky v Bitcoinoch. [21]

V snahe modernizovať verejné služby a zefektívniť daňové procesy bolo Estónsko priekopníkom v prijímaní blockchainu do svojej elektronickej správy, vrátane daňových procesov. Podobne aj austrálsky daňový úrad skúmal možnosti využitia blockchainu na zefektívnenie vykazovania daní a dodržiavania predpisov. [16] [21]

Aj keď v USA ešte nebol celoštátny záväzok k implementácii blockchainu do daňových systémov, niektoré štáty, ako Ohio, už experimentujú s prijímaním daňových platieb v kryptomene, čo naznačuje ochotu skúmať možnosti blockchainu v oblasti daní. V Spojených arabských emirátoch, najmä v Dubaji, sa od roku 2016 intenzívne skúma využitie blockchainu vo verejných službách, vrátane zdaňovania, s cieľom posilniť transparentnosť a efektivitu správy. [21]

V rozvíjajúcich sa a menej regulačných ekonomikách, ako je Ghana, má blockchain potenciál nahradiť nefunkčné, slabé a neefektívne inštitúcie a procesy. Jeho aplikácie môžu zahŕňať prevody finančných prostriedkov, vyrovnanie obchodov, hlasovanie a mnoho ďalších oblastí. [47]

4.9 Blockchain ako digitálny notár

Jedným z možných spôsobov využitia blockchainu je digitálne označovanie alebo značkovanie údajov. Ide v podstate o digitálnu notársku službu, ktorá sa však oproti tradičnej notárskej službe zaobíde bez nedôveryhodnej tretej strany. Blockchain totiž poskytuje všetky charakteristiky dôveryhodnej tretej strany, čo umožňuje bezpečné online transakcie. Je to decentralizovaná a distribuovaná sieť, v ktorej sú zapísané transakcie nezvratne. Čo umožňuje účastníkom lacnejšie overiť a auditovať transakcie. [21]

Označenie súboru na blockchaine dokáže preukázať, že dokument existoval v určitom okamihu. Ak užívateľ podpísal dokument pred označkovaním, môže tvrdiť, že dokument bol v jeho držbe v čase označenia. Ďalšou výhodou je, že užívateľ môže dokázať pôvod, dátum, autentickosť a integritu súborov bez toho, aby zdieľal ich obsah. [21]

Napríklad hudobník A môže vytvoriť novú skladbu a uložiť ju do počítača. Po uložení skladby aplikácia automaticky vytvorí digitálne podpísané časové označenie na bitcoinovom blockchaine. Jeho známy, hudobník B, ho neskôr navštívi a po vypočutí jeho skladby sa ju rozhodne ukradnúť. O pár dní neskôr vydá tú istú pieseň, len pod iným názvom. V prípade, že hudobník A správne podpísal a označil skladbu, tak vlastní silný argument voči hudobníkovi B, a teda, že mu ukradol jeho autorské dielo. Časovú pečiatku v blockchaine je možné použiť na akýkoľvek súbor, a to napr. „holý“ text TXT, PDF, Microsoft Word (DOC, DOCX), obrázky (TIFF, JPEG atď.), tabuľky (XLS, XLSX), kresby (CAD) s akýmkoľvek obsahom. [21]

Pečiatkovanie je úplne decentralizované, čo znamená, že nie je potrebná tretia strana ani centralizovaná internetová služba, aby užívateľ mohol v budúcnosti dokázať autenticitu dokumentu. Užívateľ môže preukázať pečiatku dokumentu odkazom na odtlačok dokumentu (haš) na verejne dostupnom blockchaine. [17] [21]

Na trhu existuje niekoľko projektov, platforiem a nástrojov, ktoré umožňujú využitie blockchainových technológií na služby časových pečiatok. Notárske činnosti zvyčajne vykonáva štát, ale v dnešnej dobe sa kryptotechnológie stávajú alternatívnym spôsobom vykonávania niektorých procesov, ako je prevod majetku alebo vlastníctva. Tieto technológie umožňujú vytvorenie transparentných a nezvratných záznamov, na ktorých môžu byť následne postavené automatizované procesy, ako napríklad pri prevode majetku alebo platení. [21]

OriginStamp je jednou z takýchto služieb, ktorá využíva blockchain na ukladanie časových pečiatok, zaručujúcich nezvratnosť a ochranu pred neoprávneným zásahom do obsahu. Táto služba, spustená v roku 2014, poskytuje možnosť hašovať súbory, e-maily alebo text a ukladať ich vytvorené haše do blockchainu, čím umožňuje overenie ich autenticity. V súdnych sporoch môžu digitálne dôkazy, ako časové pečiatky vytvorené pomocou technológie blockchain, slúžiť ako overiteľné dôkazy o vytvorení dokumentu. Tieto dôkazy sú uznávané v rôznych jurisdikciách, čo prispieva k ich právnej dôveryhodnosti. Cieľom platformy OriginStamp je poskytnúť lacnejšie a bezpečnejšie riešenie než tradičné notárske služby a umožniť overenie už podpísaných súborov, aby sa zabránilo možným konfliktom o vlastníctvo alebo autenticitu dokumentov. [21]

4.10 Ďalšie možnosti využitia technologie blockchain vo verejnej sfére

Využitie technológie blockchain má množstvo potenciálnych využití vo verejnej sfére ako napríklad aj v oblasti poľnohospodárskych dotácií, evidencie pasov, stavebného konania, živnostenského a obchodného registra, ako aj registrov udelených súhlasov podľa GDPR a očkovacích preukazov prináša potenciál zvýšenia transparentnosti, dôveryhodnosti a efektivity verejných procesov. Tieto projekty by mohli byť kandidátmi na medzinárodnú spoluprácu.

1. **Poľnohospodárske dotácie evidované cez blockchain:** V tejto oblasti je cítiť silná verejná požiadavka na vyššiu transparentnosť, dôveryhodnosť a zabránenie podvodom. Pozemky/pôda by mohla byť tokenizovaná podľa druhu pre zabránenie viacnásobného poberania a podvodom pri dotáciách na iný druh pozemku. Register užívateľov pôdy by mohol byť realizovaný cez blockchain.
2. **Pasy uložené v blockchaine:** Databáza vydaných, zrušených a stratených pasov by mohla byť ukladaná do blockchainu. Takáto databáza by mohla byť celoeurópska a tento projekt by mohol by byť kandidátom na cezhraničnú spoluprácu v rámci European blockchain partnership.
3. **Stavebné konanie v blockchaine:** Metaúdaje o jednotlivých úkonoch stavebného konania ako sú: žiadosti, vyjadrenia, súhlasi a rozhodnutia, by mohli byť ukladané do blockchainu. V tomto prípade sa použitie technológie blockchain javí byť mimoriadne vhodné – procesov stavebného konania sa zúčastňuje mnoho inštitúcií a častokrát je s nimi spojená nedôvera, podozrenia na podvody, zdĺhavé konanie a minimálna elektronizácia. Existuje silný verejný záujem o sprehľadnenie, zefektívnenie a zrýchlenie tohto procesu. Tento projekt je veľmi komplexný, obsahuje mnoho účastníkov, proces je komplikovaný a preto mu musí predchádzať dôsledná príprava, plánovanie, štúdia uskutočniteľnosti atď. Možno však začať s jednoduchším pilotným projektom s obmedzenou funkcionalitou, prípadne testovať prevádzku v menšej obci.
4. **Živnostenský a obchodný register:** Živnostenský a obchodný register by mohol byť v blockchaine. Okrem evidentných všeobecných výhod by bolo možné cez tokenizáciu aktív prevádzať obchodné podiely vo firmách a sledovať históriu týchto prevodov.
5. **Register udelených súhlasov podľa GDPR:** Do blockchainu by sa mohli zapisovať udelené súhlasy so spracovaním osobných údajov a tiež odňatie

súhlasu alebo žiadosť o vymazanie. Týmto by sa tiež zjednodušilo preukazovanie udelenia súhlasu v prípade sporov.

6. **Medzinárodný očkovací preukaz :** Záznamy o očkovaní uložené v blockchaine. Pri vstupe do krajiny by povinné očkovanie mohlo byť preukazované záznamom v blockchaine. Tento projekt vyžaduje medzinárodnú spoluprácu a mohol by byť kandidátom na cezhraničnú spoluprácu v rámci European blockchain partnership. [16] [17]

5 Záver

Blockchain, ktorý stojí za vznikom všetkých virtuálnych mien, je mnohými nadšencami propagovaný ako najsľubnejšia technológia súčasnej doby. Ako sme si v tejto práci vysvetlili, zaručuje maximálnu možnú dôveru pri overovaní vlastníctva akéhokoľvek digitálneho aktíva bez potreby akejkoľvek centrálnej autority. Tým, a ďalšími svojimi pozitívnymi vlastnosťami ponúka prostredie nielen pre virtuálne meny, ale aj mnohé ďalšie oblasti a prípady použitia.

Hlavným cieľom záverečnej práce bolo navrhnúť a zhodnotiť, v ktorých odvetviach našej spoločnosti má novodobá technológia blockchain najväčší potenciál a praktické využitie. Aby sme tento cieľ splnili, bolo potrebné najskôr pochopiť, čo blockchain vlastne je, aké jednotlivé typy existujú, aké sú ich výhody a nevýhody, aká je jeho architektúra a ako vlastne funguje. Spomenutým témam sme sa venovali v prvej, teoretickej časti tejto práce. Až po objasnení a porozumení všetkých teoretických pojmov sme mohli prejsť na výber najvhodnejších oblastí pre konkrétne návrhy implementácie tejto technológie.

Pre navrhované využitie technológie blockchain sme sa rozhodli sústrediť na verejný sektor, kde sme sa venovali možnostiam využitia v zdravotníctve - ako napríklad správe elektronických zdravotných záznamov, školstve - uverejňovaniu univerzitných diplomov prostredníctvom platformy blockchain, transparentnému volebnému systému či transparentnej platbe poplatkov. Pri všetkých prípadoch vidíme najväčšiu výhodu najmä v odstránení centrálnej autority a rôznych sprostredkovateľov, čo s určitosťou vedie k zníženiu nákladov zúčastnených subjektov.

Pri návrhu sme vysvetlili a graficky znázornili, ako by blockchain svojimi hlavnými výhodami, teda decentralizáciou, absenciou sprostredkovateľa, dôveryhodnosťou a nemennosťou dát prispel k zlepšeniu verejného sektora.

Hoci technológia blockchain vykazuje významný potenciál vo všetkých preskúmaných oblastiach, je nevyhnutné zohľadniť aj jej obmedzenia. Okrem problémov so škálovateľnosťou a vysokou spotrebou energie existuje aj skeptický postoj vlády, nevhodné právne podmienky a nedostatočná technologická gramotnosť obyvateľstva. V súčasnom období digitálnej transformácie priemyselného prostredia a ekonomiky je kľúčové prekonať

tieto nedostatky, zvýšiť povedomie ľudí o technológii blockchain a umožniť jej širšie a aktívnejšie využitie.

Minulý rok sme oslávili pätnáste výročie od verejného uvedenia konceptu technológie blockchain v dokumente od Satoshiho Nakamota. Počas uplynulého obdobia blockchain výrazne získal na popularite a používaní, prilákal veľké investície a predstavil nové produkty a služby - od počítačov a softvéru na ťažbu po poradenské spoločnosti. Napriek tomu je 15 rokov krátkym obdobím pre technologickú zmenu. Podobne ako prvý funkčný prototyp internetu, ktorý sa objavil v 60. rokoch, trvalo desaťročia, kým sa technológia dostala na úroveň, kde bola inovácia World Wide Web v 90. rokoch. Aj napriek rýchlemu tempu technologického pokroku sa technológia blockchainu nachádza vo veľmi raných fázach vývoja. Preto je dôležité pozerať sa dopredu o desaťročie a zohľadniť stále existujúce kľúčové neistoty týkajúce sa budúcnosti technológie blockchainu.

Integrácia blockchainu do verejných sektorov prináša výzvy. Aj keď má technológia potenciál zmeniť dodávku a riadenie verejných služieb, stále prebieha diskusia o jej vývoji v týchto oblastiach. Pre dosiahnutie spoľahlivosti, autoritatívnosti a dlhodobého zachovania je nevyhnutné stanoviť normy, nasadiť robustné manažérske systémy a zabezpečiť primeranú bezpečnosť pre služby a platformy založené na blockchainu.

Zoznam použitej literatúry

[1] ZHENG, Zibin, Shaoan XIE, Hongning DAI, Xiangping CHEN a Huaimin WANG. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In: 2017 IEEE International Congress on Big Data (BigData Congress) [online]. [cit. 2022-05-19]. ISBN 978-1-5386-1996-4.

[2] Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). Bitcoin a technológie kryptomien: komplexné úvody. Princeton, New Jersey: Princeton University Press. ISBN 978-0-691-17169.

[3] Stancel, D. (2022). Coinstory: the evolution of bitcoin & cryptocurrencies. Ilustroval MARTINEZZZ. [Galanta]: [IS-Justice Servis]. ISBN 9788097421908.

[4] ANTONOPOULOS A. 2017 : Mastering Bitcoin: Programming the Open Blockchain, 2nd edition, Sebastopol: O'Reilly Media ISBN: 978-1491954386.

[5] BASHIR, I. (2018). Mastering Blockchain: Distributed ledger technology, decentralization, and smart contracts explained, 2nd Edition. ISBN 978-1788839044.

[6] ARVIND, Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder, "Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction", (2016) Princeton University Press, Princeton. ISBN 978-0691171692.

[7] National Transport Commission (2016) „Land Transport Regulation 2040: Technology, trends and other factors of change", ISBN 978-0-9946335-0-7.

[8] Hajian Berenjestanaki, M.; Barzegar, H.R.; El Ioini, N.; Pahl, C. Blockchain-Based E-Voting Systems: A Technology Review. Electronics 2024, 13, 17 [online] [cit. 10.02.2024]. Dostupné na https://doi.org/10.3390/electronics13010017.

[9] Jafar, Uzma et al. "Blockchain for Electronic Voting System-Review and Open Research Challenges." Sensors (Basel, Switzerland) vol. 21,17 5874. 31 Aug. 2021 [online] [cit. 15.03.2024]. Dostupné na : https://doi.org/10.3390/s21175874.

[10] Noor Mohammedali and Ali Al-Sherbaz 2019 Election system based on Blockchain technology Int. J. of Computer Science & Information Technology (IJCSIT) 11, No 5 pp 13-31. [online] [cit. 20.03.2024]. Dostupné na https://aircconline.com/ijcsit/V11N5/11519ijcsit02.pdf.

[11] Castro, R.Q., & Au-Yong-Oliveira, M. (2021). Blockchain and university diplomas. European Journal of Investigation in Health, Psychology and Education, [online] [cit. 27.02.2024]. Dostupné na https://doi.org/10.3390/ejihpe11010013 .

[12] Koshiry, A. E., Eliwa, E. H. I., El-Hafeez, T. A., & Shams, M. Y. (2023). Unlocking the power of blockchain in education: An overview of innovations and outcomes. Blockchain. Research and Applications, 4(4), 100165 [online] [cit. 15.04.2024]. Dostupné na https://doi.org/10.1016/j.bcra.2023.100165.

[13] Haleem, A., Javaid, M., Singh, R. P., Suman, R., & Rab, S. (2021). Blockchain technology applications in healthcare: An overview. International Journal of Intelligent Networks, [online] [cit. 05.02.2024]. Dostupné na https://doi.org/10.1016/j.ijin.2021.09.005.

[14] Lemieux, V. L. (2016). Trusting records: is Blockchain technology the answer? Records Management Journal, 26(2), 110–139. [online] [cit. 20.03.2024]. Dostupné na https://doi.org/10.1108/rmj-12-2015-0042.

[15] Understanding Public vs. Private Blockchain - SelfKey. Self-Sovereign Identity for more Freedom and Privacy - SelfKey [online]. Copyright © 2017 [cit. 27.06.2023]. Dostupné z: https://selfkey.org/understanding-public-vs-private-blockchain/.

[16] OECD (2022). The OECD Handbook on Blockchain and Cryptocurrency Policy. [online] [cit. 20.03.2024] Dostupné z: https://www.oecd-ilibrary.org/docserver/3c32c429-en.pdf?expires=1712773672&id=id&accname=guest&checksum=6BCFF213A5F74BAC91250B7C704654BC.

[17] Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky. (2019). UPPVII blockchain štúdia. dostupné z https://mirri.gov.sk/wp-content/uploads/2019/06/UPPVII-blockchain-studia-v2_3-20190318.pdf.

[18] CAICT (China Academy of Information and Communications Technology). (2019). Blockchain white paper: Current status, challenges, and future directions. [online] [cit. 12.03.2024] Dostupné z: http://www.caict.ac.cn/english/yjcg/bps/201901/P020190131402018699770.pdfPO.

[19] NITZSCH, Julia. What's the difference between Decentralized and Distributed? [online]. [cit. 08.06.2023]. Dostupné z: https://medium.com/nakamo-to/whats-the-difference-between-decentralized-and-distributed-1b8de5e7f5a4.

[20] Co je Blockchain a jak funguje - KRYPTOMAGAZIN.cz. Bitcoin, Blockchain, zpravodajský portál o kryptoměnách [online]. Copyright © kryptomagazin.cz [cit. 25.11.2023]. Dostupné z: https://kryptomagazin.cz/co-je-blockchain/.

[21] Implementačná agentúra MPSVR SR [online]. Prínos blockchainu / krypto-technológií pre podnikateľský a verejný sektor. Copyright © [cit. 20.03.2024]. Dostupné z: https://www.ia.gov.sk/data/files/np_PKSD/Analyzy/RUZ/RUZ_AV_Kryptotechnologie_prinos_final.pdf.

[22] Edrees, Zahir. (2020). An Overview of Blockchain Technology in Government Sectors: Use Cases, Benefits and Challenges. [online] [cit. 10.01.2024]. Dostupné z: https://www.researchgate.net/publication/340647969_An_Overview_of_Blockchain_Technology_in_Government_Sectors_Use_Cases_Benefits_and_Challenges.

[23] Yaga, D., Mell, P., Roby, N. a Scarfone, K. (2018). Prehľad technológie blockchain. NIST medzirezortná/vnútorná správa (NISTIR), Národný inštitút pre štandardy a technológie, Gaithersburg, MD, [online] [cit. 22.03.2024]. https://doi.org/10.6028/NIST.IR.8202.

[24] DATAFLAIR TEAM. Understanding the basics of blockchain – Nourish the roots of technology [online]. 2019 [cit.29.05.2023]. Dostupné z: https://data-flair.training/blogs/basics-of-blockchain-technology/.

[25] https://www.blockchain.com/explorer?view=btc.

[26] NOHE, Patrick. Re-Hashed: The Difference Between SHA-1, SHA-2 and SHA-256 Hash Algorithms. [online]. [cit. 21.05.2023]. Dostupné z: https://www.thesslstore.com/blog/difference-sha-1-sha-2-sha-256-hash-algorithms/.

[27] Gilbert, H., Handschuh, H. (2004). Security Analysis of SHA-256 and Sisters. In: Matsui, M., Zuccherato, R.J. (eds) Selected Areas in Cryptography. SAC 2003. Lecture Notes in Computer Science, vol 3006. Springer, Berlin, Heidelberg. [online] [cit. 20.04.2024] Dostupné z: https://doi.org/10.1007/978-3-540-24654-1_13.

[28] Chen, R., Wu, X., & Liu, X. (2023). RSETP: A Reliable Security Education and Training Platform Based on the Alliance Blockchain. Electronics, 12, 1427 [online] [cit. 10.2.2024] dostupné z https://doi.org/10.3390/electronics12061427.

[29] Merkle Tree Explained by Changelly. Exchange Crypto online — Cryptocurrency Exchange platform [online]. Copyright © Changelly 2015 [cit. 28.06.2022]. Dostupné z: https://changelly.com/blog/merkle-tree-explain/.

[30] Montes, J., Ramírez Alba, C. E., Gutierrez, M., & Larios-Rosillo, V. (2019). Smart Contracts for supply chain applicable to Smart Cities daily operations. In 2019 International Smart Cities Conference (ISC) (pp. 565-570) [online] [cit. 19.11.2023]. Dostupné z https://doi.org/10.1109/ISC246665.2019.9071650.

[31] ROSIC, Ameer. Smart Contracts: The Blockchain Technology That Will Replace Lawyers. [online]. [cit. 11.05.2023]. Dostupné z https://blockgeeks.com/guides/smart-contracts/.

[32] T. Bocek, B. B. Rodrigues, T. Strasser, & B. Stiller. (2017). Blockchains everywhere - a use-case of blockchains in the pharma supply-chain. In 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM) (pp. 772-777). Lisbon, Portugal. [online] [cit. 12.03.2023]. Dostupné z: https://doi.org/10.23919/INM.2017.7987376.

[33] Lamport, L., Shostak, R., & Pease, M. (1982). The Byzantine generals problem. ACM Transactions on Programming Languages and Systems (TOPLAS), 4(3), 382–401 [online] [cit. 15.01.2024]. Dostupné z https://doi.org/10.1145/3335772.3335936.

[34] Moorkattil, Xavier. "Blockchain White Paper" (2022) [online] [cit. 29.10.2023]. Dostupné na https://ssrn.com/abstract=4176506 .

[35] Proof of Work (PoW) Definition. Investopedia: Sharper insight, better investing. [online] [cit. 12.01.2023]. Dostupné z: https://www.investopedia.com/terms/p/proof-work.asp.

[36] Bacon, Jean and Michels, Johan David and Millard, Christopher and Singh, Jatinder, Blockchain Demystified Queen Mary School of Law Legal Studies Research Paper [online] [cit.13.07.2022] Dostupné z https://ssrn.com/abstract=3091218.

[37] Sahib, R. H., & Al-Shamery, E. S. (2021). A review on distributed blockchain technology for e-voting systems. Journal of Physics. Conference Series, 1804(1), 012050 [online] [cit. 15.03.2024]. Dostupné z https://doi.org/10.1088/1742-6596/1804/1/012050.

[38] Mohammedali, N. A., & Al-Sherbaz, A. (2019). Election system based on blockchain technology. International Journal of Computer Science and Information [online] [cit. 20.03.2024]. Dostupné z https://doi.org/10.5121/ijcsit.2019.11502.

[39] Understanding Public vs. Private Blockchain - SelfKey. Self-Sovereign Identity for more Freedom and Privacy - SelfKey [online]. Copyright © 2017 [cit. 27.06.2022]. Dostupné z: https://selfkey.org/understanding-public-vs-private-blockchain/

[40] BUTERIN, V. 2015. On Public and Private Blockchains | Ethereum Foundation Blog. Home | Ethereum Foundation Blog [online]. [cit. 24.11.2023]. Dostupné z: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/

[41] D. Cagigas, J. Clifton, D. Diaz-Fuentes and M. Fernández-Gutiérrez, "Blockchain for Public Services: A Systematic Literature Review," in IEEE, 2021, [online] [cit. 24.11.2023]. Dostupné z https://ieeexplore.ieee.org/document/9326290 .

[42] Elli Androulaki, et al., Evaluating User Privacy in Bitcoin, FIN. CRYPTOGRAPHY & DATA SECURITY (2013) [online] [cit. 24.2.2024]. Dostupné na http://eprint.iacr.org/2012/596.pdf.

[43] Edrees, Zahir. (2020). An Overview of Blockchain Technology in Government Sectors Use Cases, Benefits and Challenges. [online] [cit. 20.04.2024] Dostupné na https://www.researchgate.net/publication/340647969_An_Overview_of_Blockchain_Technology_in_Government_Sectors_Use_Cases_Benefits_and_Challenges.

[44] Singh Y, Jabbar MA, Kumar Shandilya S, Vovk O and Hnatiuk Y (2023) Exploring applications of blockchain in healthcare: road map and future directions. Front. Public Health [online] [cit. 28.01.2024]. Dostupné na https://www.frontiersin.org/journals/public-health/articles/10.3389/fpubh.2023.1229386/full.

[45] Y Wu, J M Bauer, “E-government in China: deployment and driving forces of provincial government portals,” Chinese Journal of Communication, vol.3, pp.290-31, March 2010 [online] [cit. 07.12.2023]. Dostupné na https://www.slideshare.net/irjetjournal/irjetoverview-of-blockchain-technology-in-governmentpublic-sectors.

[46] Bratanova, A., Devaraj, D., Horton, J., & Dawson, D. (2019). Blockchain 2030: A look at the future of blockchain in Australia. ResearchGate. [online] [cit. 17.02.2024]. Dostupné na https://doi.org/10.13140/RG.2.2.22133.42720.

[47] Anomah, S., Ayeboafo, B., Aduamoah, M., & Agyabeng, O. (2024). Blockchain Technology integration in tax Policy: Navigating challenges and unlocking opportunities for improving the taxation of Ghana's digital economy. Scientific African, 24, e02210 [online] [cit. 10.04.2024]. Dostupné na https://doi.org/10.1016/j.sciaf.2024.e02210.

[48] Niranjanamurthy M, Analysis of Blockchain technology: pros, cons and SWOT. (n.d.). [online] [cit. 02.05.2024]. Dostupné na ResearchGate. https://www.researchgate.net/publication/323865742_Analysis_of_Blockchain_technology_pros_cons_and_SWOT.

[49] Firsova, N., Abrhám, J. (2021). Economic perspectives of the Blockchain technology: Application of a SWOT analysis. Terra Economicus 19(1): 78–90. [online] [cit. 02.05.2024]. Dostupné na ResearchGate. https://www.researchgate.net/publication/350908192_Economic_perspectives_of_the_Blockchain_technology_Application_of_a_SWOT_analysis.

[50] Yontar E, Challenges, Threats and Advantages of using blockchain technology in the framework of sustainability of the logistics sector. (n.d.) [online] [cit. 03.05.2024]. Dostupné na: ResearchGate. https://www.researchgate.net/publication/363102003_Challenges_Threats_and_Advantages_of_Using_Blockchain_Technology_in_the_Framework_of_Sustainability_of_the_Logistics_Sector.

[51] Nwagwu, U. (2020). A SWOT analysis on the use of blockchain in supply chains [online] [cit. 01.05.2024]. Dostupné na: https://www.researchgate.net/publication/363265211_A_SWOT_ANALYSIS_ON_THE_USE_OF_BLOCKCHAIN_IN_SUPPLY_CHAINS.

[52] A. Shahnaz, U. Qamar and A. Khalid, "Using Blockchain for Electronic Health Records,"(2019) [online] [cit. 02.05.2024]. Dostupné na https://ieeexplore.ieee.org/abstract/document/8863359.

[53] UN World Food Programme: Toward Zero Hunger with Analytics [online] [cit. 03.05.2024]. Dostupné na.https://www.researchgate.net/publication/358322460_UN_World_Food_Programme_Toward_Zero_Hunger_with_Analytics.

[54] A. Mili, Blockchain-Enabled Diploma Traceability and Fraud Detection: The BlockDIPLS Framework. [online] [cit. 02.05.2024]. Dostupné na. https://www.researchgate.net/publication/380011265_Blockchain-Enabled_Diploma_Traceability_and_Fraud_Detection_The_BlockDipls_Framework.

[55] DIRK A. ZETZSCHE, ROSS P. BUCKLEY AND DOUGLAS W. ARNER , The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain Cloudflare. ResearchGate [online] [cit. 15.08.2023]. Dostupné na: The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain (researchgate.net).

[56] Chiș, D., & Caramihai, M. (2023). Blockchain in Higher Education: A Secure Traceability Architecture for Degree Verification. [online] [cit. 03.05.2024]. Dostupné na: https://www.intechopen.com/chapters/1145787.

[57] Caramihai M, Severin I. A. (2023). Blockchain-Based Solution for Diploma Management in Universities. Sustainability. [online] [cit. 19.04.2024] Dostupné na: https://www.mdpi.com/2071-1050/15/20/15169.