Štúdia možností a potenciálu technológie „blockchain“ pri zlepšovaní eGovernment riešení

Verzia 2.3

19. marec 2019

Obsah

1 Základné informácie

1.1 Úvod

Táto štúdia (Štúdia možností a potenciálu technológie „blockchain“ pri zlepšovaní eGovernment riešení) vznikla na základe plnenia Zmluvy o poskytnutí služieb č.155/2018 uzavretej dňa 14. septembra 2018 medzi Úradom podpredsedu vlády SR pre investície a informatizáciu (ďalej aj len „ÚPPVII“) a Ernst & Young, s.r.o. (ďalej aj len „EY“ alebo „my“) a zverejnenej v Centrálnom registri zmlúv dňa 18. septembra 2018 (ďalej aj „Zmluva“).

Táto štúdia je určená zodpovedným pracovníkom ÚPPVII pre doplnenie ich prehľadu o inovatívnych informačných technológiách a podporu ich rozhodovania pri ďalšom smerovaní informatizácie verejnej správy v Slovenskej republike.

Technológia blockchain (ďalej aj „blockchain“) je úžasná technológia a jej nasadenie mimo kryptomien v súkromnom a verejnom sektore je pre jej unikátne vlastnosti veľmi atraktívne. Blockchain dokáže nastoliť dôveru informáciám a procesom v heterogénnom prostredí, kde mnoho dát zapisuje mnoho entít a využíva ho mnoho používateľov. Blockchain dokáže poskytnúť dôveryhodné a auditovateľné záznamy a môže tiež viesť k úsporám, vyššej efektivite a efektívnosti informačných systémov.

Využitie blockchainu mimo kryptomien je stále nová a dynamicky sa vyvíjajúca oblasť. Vývoj treba neustále sledovať a prispôsobovať ďalšiu stratégiu využitia. Ako konštatuje nedávna štúdia EU Blockchain Observatory and Forum[1], „experimentovanie musí pokračovať“. Je potrebné hlbšie preskúmať nielen technologickú uskutočniteľnosť a legislatívny rámec, ale aj ekonomické a sociálne dopady.

[1] Blockchain for Government and Public Services, https://www.eublockchainforum.eu/reports

1.2 Manažérske zhrnutie

Slovenská vláda sa dlhodobo snaží o zlepšovanie služieb občanom a zefektívnenie verejnej správy mnohými prostriedkami, medzi iným aj informatizáciou. Blockchain, pre niektoré svoje unikátne vlastnosti, nemohol uniknúť pozornosti.

Cieľom štúdie je predstaviť túto technológiu, jej hlavné vlastnosti, vysvetliť, kedy môže byť jej použitie vhodné a aké výhody môže priniesť jej nasadenie v štátnej správe, ako aj naznačiť konkrétne projekty, pri ktorých je možné túto technológiu využiť.

Druhá časť tejto štúdie je zameraná na prichádzajúce technológie Fintech. Smernica Európskej únie PSD2 umožňuje vznik nových, revolučných finančných služieb. Cieľom štúdie je tiež načrtnúť možnosti Fintech služieb, prestaviť niektoré konkrétne riešenia realizované v zahraničí, podporné schémy aplikované v zahraničí a možný systém podpory na Slovensku.

Témy adresované touto štúdiou sú usporiadané v tejto základnej štruktúre:

- V kapitole 2 sú najprv formou otázok a odpovedí zodpovedané základné otázky o blockchaine a jeho využití mimo kryptomien. Ďalej nasleduje technický popis a základné stavebné prvky, ktoré sú nevyhnutné pre pochopenie prínosu tejto technológie. Vysvetlené sú algoritmy konsenzu, topológia a štruktúra blockchain siete, porovnanie tradičnej databázy a „záznamníka údajov" (ledger) na báze blockchainu, vzťah ku kryptomenám, smart kontrakty a tzv. „off-chain storage". Tiež je spomenutá história a súčasné využitie, načrtnuté sú možné prevádzkové modely a vzťah s informačnou bezpečnosťou a GDPR. Dôležitou časťou je pojednanie o kritériách vhodnosti nasadenia blockchain pre daný problém a súčasné námietky, výzvy a trendy v tejto oblasti.
- Kapitola 3 sa venuje súvislostiam riadenia informačnej bezpečnosti a technológie blockchain. Okrem analyzovania kontrolných mechanizmov implementovaných v tejto technológii, kapitola ponúka aj opačný pohľad – kedy technológia blockchain môže poslúžiť ako kontrolný mechanizmus v rámci systému riadenia informačnej bezpečnosti. V tejto kapitole sa tiež zaoberáme ďalšími vybranými témami súvisiacimi s informačnou bezpečnosťou ako je GDPR, eID či bezpečnosť v ISVS.
- Kapitola 3 predstavuje blockchain iniciatívy a konkrétne riešenia vo svete, Európskej únii a vznikajúci ekosystém na Slovensku. Európska únia podporuje skúmanie nasadzovania tejto technológie aj cez EU Blockchain Partnership a EU Blockchain Observatory and Forum. Ďalej je predstavených mnoho súčasných projektov využívajúcich blockchain v rôznom štádiu vývoja, od ohláseného zámeru až po funkčné a nasadené riešenia.
- Konkrétne riešenia, potenciálne aplikovateľné pre Slovensko, využívajúce technológiu blockchain sú ponúknuté na zváženie v kapitole 5. Táto kapitola obsahuje všeobecné odporúčania, orientačný časový rámec a postup realizácie, niekoľko jednoduchých „quick-win" projektov a naznačené sú základné definície viacerých ďalších komplexnejších projektov.
- Fintech riešeniam a ich podpore sa venuje kapitola 6. Najprv sú Fintech riešenia predstavené vo všeobecnosti. Kapitola ďalej uvádza konkrétne riešenia vo svete a na Slovensku a takisto sa venuje nástrojom podpory, prehľadu nástrojov, analýze Fintech riešení a odporúčaniam.
- Záver obsahuje zoznam konkrétnych odporúčaní pre nasadzovanie blockchain riešení a podporu Fintech.

Keďže je však problematika blockchain pomerne komplexná téma, na ktorú je možné nazerať z rôznych uhlov pohľadu (blockchain je možné vnímať ako distribuovanú aplikáciu, distribuovanú databázu – register záznamov alebo infraštruktúru či komunikačnú sieť) a ktorá zahŕňa množstvo netriviálnych technických, organizačných a procesných aspektov a má viacero ďalších súvislostí, nie je možné na obmedzenom priestore, ktorý poskytuje táto štúdia jej úplné pokrytie.

O značnej šírke a hĺbke tejto problematiky svedčí aj neustále rastúci počet rôznych, častokrát veľmi rozsiahlych a viac alebo menej odborných publikácií a iných typov materiálov (vhodnou formou s dobrou

vyjadrovacou kvalitou sa javia byť napr. rôzne interaktívne prezentácie, videá, simulátory alebo demonštračné prototypy, dostupné sú však častokrát aj zdrojové kódy rôznych blockchain technológií).

Mnohé takéto materiály sú verejne dostupné a ľahko dohľadateľné a preto čitateľov, v ktorých táto štúdia vzbudí záujem o blockchain a jeho potenciálne využitie aj pri riešení problémov a úloh verejnej správy, povzbudzujeme v pokračovaní získavať ďalšie užitočné informácie.

Na tomto mieste považujeme za potrebné tiež zdôrazniť, že cieľom tejto štúdie nie je definovať plán (alebo podnietiť vytvorenie takéhoto plánu) implementácie ďalších eGovernment projektov „za každú cenu" využívajúcich technológiu blockchain, prípadne „dôrazne odporúčať" takéto konkrétne projekty. Naopak, cieľom štúdie je opakovane zdôrazňovať potrebu dôkladného analyzovania výhod, nevýhod, príležitostí a hrozieb pri využívaní tejto pomerne novej, z mnohých hľadísk veľmi sľubnej technológie pri riešení určitej (z pohľadu „celého vesmíru" však stále veľmi obmedzenej) triedy problémov. Pred rozhodnutím o implementácii konkrétneho „blockchain" projektu, je potrebné takúto analýzu prínosov a nákladov vykonať v kontexte existujúcich „tradičných" riešení alebo riešení z obdobia tzv. „budovania eGovernmentu".

V záujme šírenia povedomia o možnostiach využitia decentralizovaných riešení vo verejnej správe, ako aj plnenia úloh iniciatívy EU Blockchain Partnership, pritom môže byť vhodné analýzu konkrétneho prípadu použitia technológie blockchain doplniť o vytvorenie porovnávacieho funkčného prototypu. Pomocou takéhoto prototypu bude možné zainteresovaným stranám – vrátane verejnosti – demonštrovať výhody technológie blockchain napr. pri zvyšovaní transparentnosti a analyzovateľnosti priebehu procesov alebo konaní verejnej správy ako aj pri zvyšovaní miery uistenia o informačnej bezpečnosti spracúvaných údajov.

1.3 Zameranie a ciele štúdie

Článok Zmluvy	Referencia v Štúdii
Zameranie Štúdie	
3.a) zmapovanie súčasného stavu riešení eGovernmentu (stratégií, plánov, ukončených a prebiehajúcich projektov) a ich obmedzení a nedostatkov, ktoré je potenciálne možné adresovať zavedením „blockchain" technológie	Kapitola 5.1, 5.1.1, 5.3, 5.4
3.b) zmapovanie ďalších požiadaviek a potrieb na dostupnosť, spoľahlivosť a bezpečnosť služieb a údajov poskytovaných občanom verejnou správou, ktoré je potenciálne možné adresovať zavedením „blockchain" technológie,	Kapitola 5.1, 5.1.1, 5.3, 5.4
3.c) identifikovanie rozdielov medzi súčasným a požadovaným stavom (v zmysle dvojice písmen vyššie),	Kapitola 5.1, 5.1.1, 5.3, 5.4
3.d) identifikovanie triedy problémov, ktoré je možné riešiť implementovaním distribuovaných a decentralizovaných technológií, k akým patrí aj blockchain	Kapitola 2.5 a 2.13, stručnejšie v 2.1
3.e) kvalitatívne (a ak je to možné a relevantné aj kvantitatívne) porovnanie jednotlivých distribuovaných a decentralizovaných technológií (s dôrazom na technológiu „blockchain") voči „tradičným" technológiám pri riešení danej triedy problémov	Kapitola 2.5 a 3
3.f) rámcové definovanie potenciálnych projektov (predmet, ciele, harmonogram, zdroje, predpoklady a súvislosti s inými projektami) pre aplikácie („use cases"), v ktorých sa ukáže ako výhodné riešenie technológia blockchain	Kapitola 5.2, 5.3 a 5.4

Článok Zmluvy	Referencia v Štúdii
3.g) návrh mechanizmu podpory spoločností typu a/alebo služieb typu „fintech" (typicky malé a stredné podniky) v SR, aj s využitím financovania z Operačného programu integrovaná infraštruktúra, prioritná os 8	Kapitola 6
Ciele Štúdie	
4.a) poskytnutie prehľadu o základných princípoch a prvkoch „blockchain" technológie a jej uplatnení v rámci e-Government aplikácií a služieb občanom	Kapitola 2 a 3
4.b) prehľad výhod a nedostatkov aplikácie „blockchain" technológie v prostredí e-Governmentu	Kapitola 2.13, 3 a 5
4.c) definícia tém, otázok a výziev v skúmanej oblasti pre najbližšie obdobia (infraštruktúra a architektúra súčasného e-Governmentu v SR, „blockchain modely", legislatívny rámec, centralizovaný model vs. decentralizovaný model, bezpečnosť, finančná udržateľnosť, rezistencia voči zmenám, pripravenosť verejnosti a pod.),	Kapitola 2, 3, 4, 5 a 7
4.d) prehľad potenciálnych kľúčových úloh a rolí štátu pri adopcii „blockchain" technológie	Kapitola 4.5
4.e) poskytnutie prehľadu o súčasných významných iniciatívach vedúcich k zavádzaniu „blockchain" technológie na úrovni EÚ a v prostrediach verejnej správy členských štátov EÚ,	Kapitola 4.1, 4.2, 4.3, 4.4
4.f) poskytnutie detailného prehľadu o najvýznamnejších aplikáciách („use cases") zavedenia „blockchain" technológie v prostredí eGovernmentu v podmienkach SR a ostatných členských krajín EÚ	Kapitola 4.4 a 4.6
4.g) rámcový prehľad potenciálnych dopadov aplikácie „blockchain" technológie na efektivitu a účinnosť aktivít a služieb poskytovaných štátom	Kapitola 2.13, **Error! Reference source not found.** a 3, konkrétnejšie v popisoch projektov v kapitole 5.2, 5.3 a 5.4
4.h) rámcový prehľad potenciálnych dopadov na občanov využívajúcich služby, ktorých fungovanie je založené na aplikácii „blockchain" technológie	Kapitola 2.13, **Error! Reference source not found.** a 3, konkrétnejšie v popisoch projektov v kapitole 5.2, 5.3 a 5.4
4.i) prehľad tzv. „quick wins" pri aplikácii „blockchain" technológie v prostredí e-Governmentu,	Kapitola 5.3
4.j) rozšírenie povedomia o vlastnostiach a možnostiach technológie „blockchain" medzi pracovníkmi zodpovednými za riadenie budovania eGovernment riešení	Kapitola 2, 3, 4 a 5 2, 3, 4 a 5
4.k) podpora malých a stredných podnikov typu „fintech" v oblasti rozvoja ich služieb v SR	Kapitola 6
4.l) vypracovanie odporúčaní na realizáciu aktivít zo strany ÚPPVII, vychádzajúcich z hore uvedených výstupov Štúdie, vrátane indikácie časovej postupnosti týchto aktivít.	Kapitola 7

1.4 Použité skratky a definície pojmov

Termín	Vysvetlenie
AML/CFT	Anti-Money Laundering/Combating the Financing of Terrorism: opatrenia na zabránenie praniu špinavých peňazí a financovanie terorizmu
BFT	Byzantine fault tolerance: odolnosť distribuovaného výpočtového systému voči chybám, komponent sa môže javiť ako funkčný niektorým pozorovateľom a nefunkčný iným
blockchain	Distribuovaná, decentralizovaná databáza uchovávajúca neustále sa rozširujúci počet záznamov, ktoré sú chránené proti neoprávnenému zásahu tak z vonkajšej strany, ako aj zo strany samotných uzlov siete
BTC	Bitcoin: najznámejšia kryptomena
CBDC	Central bank digital currency: virtuálna kryptomena vydávaná centrálou bankou ako digitálna forma klasickej (FIAT) meny
CMDB	Configuration management database: databáza HW a SW, konfigurácii a vzťahov medzi nimi
DLT	Distributed ledger technology: súbor záznamov (databáza) distribuovaný, replikovaný a synchronizovaný na viacerých miestach bez potreby centrálneho administrátora alebo centrálneho dátového skladu
EDPS	European Data Protection Supervisor: Európska rada pre dozor nad ochranou údajov
eID	Elektronická identifikačná karta
eIDAS	Nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES
ERP	Enterprise resource planning
Ethereum	Kryptomena, ktorá má implementované aj smart kontrakty; v súčasnosti druhá najväčšia kryptomena podľa trhovej kapitalizácie a denných obratov
Fintech	Financial technology: je súbor nových technológií a inovácií ktoré súperia s tradičnými metódami poskytovania finančných služieb
fork (v blockchaine)	Dva alebo viac paralelných reťazcov blokov, viac v kapitole "Fork"
FTP	File Transfer Protocol
GDPR	Všeobecné nariadenie o ochrane údajov. Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorého cieľom je výrazné zvýšenie ochrany osobných údajov občanov. Na Slovensku je zavedené zákonom č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov z 29. novembra 2017.
hash	Hašovacia funkcia: zo vstupného reťazca ľubovoľnej dĺžky vráti vypočítaný reťazec fixnej dĺžky (viac v príslušnej kapitole)
IB, KM, ISMS	Informačná bezpečnosť; Kontrolný mechanizmus; Systém riadenia informačnej bezpečnosti (Information security management system)
ICO	Initial coin offering: kontroverzný spôsob získavania financovania pre nové projekty formou predaja novej kryptomeny
ISVS	Informačný systém verejnej správy
mining pool	Združenie ťažiarov(minerov): každý ťažiar v rámci blockchainu dostane za úlohu vykonať len časť potrebného výpočtu a získava podiel na odmene podľa dodaného výkonu
minovanie	Z anglického výrazu "mining": ťažba kryptomeny vyžadujúca veľký výpočtový výkon

Termín	Vysvetlenie
off-chain storage	Dátovo objemné súbory sú ukladané mimo blockchainu a do blockchainu sa ukladá len ich hash
Orákulum	Dôveryhodný zdroj externých informácií
PoW	Proof of work: konsenzuálny algoritmus založený na hrubej výpočtovej sile (viac v príslušnej kapitole)
RSA	Rivest–Shamir–Adleman: Systém asymetrickej kryptografie využívajúci verejný a privátny kľúč
smart kontrakt	Protokol alebo software zabezpečujúci, overujúci alebo vynucujúci dohodu alebo realizáciu zmluvy
tokenizácia aktív	Aktíva z reálneho sveta (auto, byt, úložná kapacita atď.) sú reprezentované tokenom vo virtuálnom svete; blockchain eviduje využívanie týchto aktív a zabezpečuje jedinečné pridelenie aktíva
uzol blockchainu	Uzol siete blockchain má kompletnú kópiu blockchainu, zúčastňuje sa na ťažení/validovaní nových blokov
používateľ blockchainu	Môže čítať a zapisovať do blockchainu, ale na rozdiel od uzla nemusí mať celú kópiu blockchainu, nezúčastňuje sa na ťažení/validovaní blokov

1.5 Zoznam obrázkov

1.6 Zoznam tabuliek

2 Blockchain vo všeobecnosti

2.1 Blockchain: základné otázky a odpovede

V tejto kapitole sme sa pokúsili v krátkosti zhrnúť základné otázky a stručné odpovede na tému blockchain. Podrobnejšie vysvetlenie je možné nájsť nižšie v tejto štúdii.

Čo je to blockchain?

Technológia blockchain je infraštruktúra, ktorá umožňuje rôznym distribuovaným softvérovým aplikáciám ukladať, uchovávať a sprístupňovať údaje (ale aj predpisy o spracovaní údajov - tzv. smart kontrakty) spôsobom, ktorý zaručuje vysokú **dostupnosť** a **integritu** týchto údajov (údaje sú autentické, nepopierateľné, nie je možné ich meniť a sú prakticky nezničiteľné), a ak je to žiaduce aj **dôvernosť**. Z praktických dôvodov sa typický jedná o údajové záznamy menšieho rozsahu – do blockchainu sa ukladajú len základné údaje o transakciách, udalostiach alebo správach vznikajúcich v rámci ekosystému vzájomne komunikujúcich účastníkov (strán). Kľúčovou vlastnosťou blockchainu je skutočnosť, že takýto komunikačný systém nemusí organizovať ani naň dohliadať žiadna centrálna autorita – hovoríme, že systém nemá "rozhodcu", ktorého by bolo potrebné rešpektovať a ktorý by si musel túto svoju autoritu prácne budovať a udržiavať. Hovoríme tiež, že technológia blockchain je distribuovaná a decentralizovaná a je schopná spontánne vytvoriť absolútnu dôveru účastníkov v prostredí potenciálnej vzájomnej nedôvery.

Prečo vôbec vznikol?

Technológiu blockchain vyvinul Satoshi Nakamoto v roku 2008 ako verejne prístupnú infraštruktúru poskytujúcu služby pre realizovanie transakcií v alternatívnej kryptomene Bitcoin. Táto prvá blockchain aplikácia bola odpoveďou na všeobecné strácanie dôvery v centrálne finančné inštitúcie, ktorých zlyhanie stálo na začiatku finančnej krízy z roku 2008. Technológia blockchain tak ukázala, ako je možné riešiť tzv. "double spending" problém bez potreby centrálnej autority a vo všeobecnosti naznačila ako môžu moderné technológie nahradiť tradičné (centralizované) zmýšľanie a riešenia.

Ako funguje blockchain?

Blockchain pripomína neustále rastúci záznamník „údajových viet“ (transakcií), pričom sémantiku týchto údajov si určuje konkrétna distribuovaná softvérová aplikácia. Transakcie postupne generované používateľmi takejto aplikácie sú „balíčkované“ do tzv. blokov, pričom každý novovzniknutý blok sa kryptograficky previaže s predchádzajúcim blokom. Toto sa deje prakticky súčasne a synchronizovane vo všetkých "hlavných" uzloch siete blockchain. Táto na prvý pohľad nadbytočná redundancia údajov a úkonov je v skutočnosti veľmi užitočná - okrem vysokej dostupnosti (a praktickej nezničiteľnosti údajov) slúži aj na efektívne detekovanie individuálnych úmyselných alebo náhodných odchýlok od "spoločnej verzie blockchainu" a ich opravu. Pre fungovanie blockchainu je kľúčová kombinácia kryptografických algoritmov a internetových sieťových protokolov (známa už zo sedemdesiatych, resp. deväťdesiatych rokov minulého storočia). Kryptografia (najmä hašovacia funkcia a asymetrické šifrovanie) slúži na už spomínané previazanie blokov, na udržiavanie integrity údajov (t. j. autenticity a nepopierateľnosti záznamu nových a nemennosti uložený údajov), ale tiež na "spravodlivý" (teda náhodný) výber uzla, ktorý bude validovať transakcie a vytvárať nový blok transakcií; sieťové protokoly potom slúžia na rýchlu

synchronizáciu času, údajov a spoločných (konsenzuálnych) rozhodnutí v rámci všetkých uzlov blockchain siete.

Akú rolu vo fungovaní blockchainu zohráva tzv. ťaženie a virtuálne meny?

Pojem ťaženie (alebo tzv. mining) je vlastný blockchain sieťam využívajúcim tzv. proof-of-work algoritmus pri vytváraní nasledujúceho bloku. Uzly súperia o to, kto prvý nájde blok (vyťaží ho). Spomedzi množstva uzlov (tzv. ťažiarov, hovorovo minerov) sa náhodne vyberie práve jeden uzol a to tak, že všetky ostatné uzly tento výber jednoznačne akceptujú (teda aj v tomto prípade platí, že v blockchaine nepotrebujeme centrálneho rozhodcu). Vybraný uzol je potom zodpovedný za validovanie aktuálnych transakcií a ich uloženie do nasledujúceho bloku. Týmto náhodným výberom sa pritom zabráni prípadnému podvodníkovi naplánovať si útok na konkrétnu množinu novovznikajúcich transakcií. Tento spôsob zabezpečenia konsenzu môže byť energetický náročný a z hľadiska negatívneho dopadu na životné prostredie neakceptovateľný, naviac sa vzhľadom na existenciu iných, rovnaký účel plniacich, konsenzuálnych algoritmov (napr. proof-of-stake) javí byť zbytočný. Virtuálne (krypto) meny môžu plniť v riešeniach využívajúcich technológiu blockchain tri úlohy:

- kryptomena ako odmena pre ťažiara – motivuje vytvárať a prevádzkovať kľúčové uzly pre fungovanie blockchain siete (v tejto súvislosti hovoríme o „palive“ pre blockchain sieť),
- kryptomena ako zhodnotenie investície do projektu financovaného formou crowdfundingu,
- kryptomena ako alternatíva k tradičnej mene pre realizáciu finančných transakcií špecializovanou aplikáciou využívajúcou technológiu blockchain (ako napr. Bitcoin).

Kedy má význam použiť technológiu blockchain?

Dnes máme k dispozícii viaceré odborné zdroje, ktoré poskytujú návod pri rozhodovaní medzi voľbou decentralizovaného riešenia založeného na technológii blockchain a tradičným – centralizovaným riešením. Medzi hlavné znaky indikujúce vhodnosť blockchain riešenia patria tieto:

- intenzívna komunikácia (komplexná matica interakcií) medzi viacerými nezávislými entitami (organizáciami či firmami), ktoré nezdieľajú spoločný centralizovaný informačný systém,
- potreba rozšíriť viditeľnosť (zdieľanie) údajov medzi viac ako dvojicou účastníkov (používateľov),
- zvýšené nároky na informačnú bezpečnosť – dostupnosť, integritu, ale aj dôvernosť údajov, ktoré nie je možné (resp. nebolo by to efektívne) uspokojiť tradičnými, tzv. všeobecnými kontrolnými mechanizmami informačnej bezpečnosti.

Čo je potrebné pre nasadenie aplikácie využívajúcej blockchain?

Ak už existuje blockchain infraštruktúra (napr. sa rozhodneme využiť existujúci verejný blockchain), potom je potrebné: vytvoriť distribuovanú aplikáciu, integrovať ju do zvolenej blockchain infraštruktúry, integrovať ju do existujúceho IT prostredia (napr. ERP alebo produkčného informačného systému organizácie). Používateľov už obyčajne netreba presviedčať o výhodách takéhoto riešenia – blockchain technológia pre nich môže zostať ukrytá (výhody sa časom prejavia v podobe rôznych merateľných ukazovateľov týkajúcich sa kvality a dostupnosti relevantných údajov). Ak blockchain infraštruktúru zatiaľ nemáme, musíme ju zriadiť. Je potrebné zvoliť typ vlastníctva siete, typ konsenzu medzi uzlami siete, topológiu uzlov siete, model motivácie validátorov, technicky zriadiť uzly pre validáciu blokov a logicky ich prepojiť do spoločnej blockchain siete.

V akých konkrétnych oblastiach je možné túto technológiu využiť?

Technológia blockchain sa javí byť užitočná v rôznych situáciách a pri riešení rôznych tried problémov, napr.:

- efektívne riadenie v dodávateľských reťazcoch (či zložitých projektoch - napr. stavebných alebo IT) vďaka rozšírenej "viditeľnosti" údajov kľúčových pre správne rozhodovanie,
- sledovanie originality, dodržiavania postupov ako aj zloženia produktov počas ich celého životného cyklu (napr. pri výrobe, skladovaní a preprave potravín alebo liečiv),
- transparentné zaznamenávanie histórie stavov, úkonov a rozhodnutí v ekosystéme komunikujúcich strán (napr. medzi inštitúciami verejnej správy alebo dodávateľom outsourcovaných služieb a jeho zákazníkmi),
- transparentné a spravodlivé zdieľanie zdrojov medzi skupinami účastníkov predstavujúcich ponuku týchto zdrojov a dopyt po nich.

Rôzne scenáre využitia technológie blockchain je možné hľadať nielen v komerčnom a verejnom sektore ale najmä v prieniku oboch sektorov.

Kde bude blockchain nenahraditeľný?

Univerzálna odpoveď je „nikde". Zrejme všetky aktuálne problémy a úlohy je možné riešiť aj tradičnými metódami. Zdá sa však, že niektoré z nich je predsa len možné riešiť pomocou technológie blockchain „lepšie". Niekedy sa revolúcia, ktorú v 90. rokoch spôsobili podnikové (ERP) informačné systémy vnútri organizácií prirovnáva k revolúcii, ktorú spôsobí blockchain pri riadení celého ekosystému vzájomne obchodné prepojených ale inak formálne nezávislých organizácií. Vlastnosti blockchainu ako autentickosť a nepopierateľnosť údajov ako aj nemožnosť ich zničenia alebo zmeny však naznačujú, že blockchain môže byť obrovským prínosom aj v súvislosti s prípravou tzv. veľkých dát, ktorých kvalita (úplnosť, presnosť a pravosť) je rozhodujúca pre ich správnu interpretáciu a prípadné využitie pri strojovom učení. Blockchain by tiež nám - ľuďom mohol v budúcnosti pomôcť pri zabezpečení záznamov (logov) o činnosti robotov, tak aby v prípade, že sa inteligentné roboty poza náš chrbát navzájom dohodnú na niečom, čo sme od nich neočakávali, aspoň nemohli „pozametať stopy" (ak ich vôbec spravili) nasvedčujúce takémuto konaniu.

2.2 Technický popis

Blockchain, z anglického "block chain" - reťaz blokov, je typ decentralizovanej distribuovanej databázy, v ktorej je zoznam záznamov vedený v na seba nadväzujúcich blokoch. Záznamom je akákoľvek informácia, ktorá sa má v databáze uchovať, napr. záznam o prevode peňažných prostriedkov z účtu platiteľa na účet príjemcu, záznam o vytvorení dokumentu, záznam o prebratí zásielky atď. Nové bloky a záznamy sa do blockchainu iba pridávajú, pričom každý ďalší blok odkazuje na blok predchádzajúci. Tým pádom, zmena jedného bloku by znamenala kaskádovite zmenu všetkých nasledujúcich blokov. To, pri správnej implementácii, robí záznamy prakticky permanentné a nezmeniteľné. Záznamy v rámci bloku sú tiež usporiadané. Na overenie autenticity jednotlivých záznamov a blokov sa používajú kryptografické nástroje, ako hashovacie funkcie, hashové stromy („merkle tree"), digitálne podpisy a pod.

Jednotlivé záznamy sú overované (validované) každým účastníkom siete, aby spĺňali kritéria danej databázy (napríklad overenie, že daný záznam nesie potrebný digitálny podpis). Validačné kritéria sú zdieľané medzi všetkými účastníkmi siete, sú vyhodnotiteľné v konečnom čase a vyhodnocujú sa vždy

rovnako vzhľadom k aktuálnemu stavy databázy, bez ohľadu na akom počítači alebo v akom čase sa spustia, t. j. nezávisia od náhodných alebo externých premenných. Použitie externých premenných, akou je napríklad aktuálna hodnota aktíva na trhoch, vyžaduje, aby tieto premenné boli najskôr do databázy hodnoverne vložené tzv. orákulom. Orákulum je dôveryhodný zdroj externých informácií, ktoré sú zapisované ako samostatné záznamy do blockchainu. Orákulum, ako jediný zdroj informácií, však môže predstavovať slabé miesto bezpečnosti, a preto sa silne odporúča použiť nejakú decentralizovanú, BFT implementáciu (viď nižšie Problém byzantských generálov a tolerancia byzantínskych chýb).

Spôsob vytvárania a výberu nových blokov v rámci decentralizovanej siete sa volá algoritmus konsenzu. Konsenzus je vlastnosť blockchainu, v rámci ktorej každý účastník vidí rovnakú, úplne usporiadanú množinu platných (validných) záznamov a blokov. Algoritmus sa stará o to, aby sa vybrali iba transakcie, ktoré sú v rámci daného usporiadania validné, a tiež zaisťuje, že je veľmi ťažké zmeniť jeden alebo viac minulých blokov a záznamov, čím sa má zabezpečiť nemennosť záznamov. Čím hlbšie v minulosti by sa mala zmena odohrať, tým viac blokov nasledujúcich po zmene by bolo potrebné nahradiť. Algoritmy konsenzu používajú techniky, aby cena tejto náhrady rástla proporcionálne s jej veľkosťou a množstvom účastníkov, až za úroveň praktickej použiteľnosti takéhoto typu útoku. Viac informácií o rôznych algoritmoch konsenzu je uvedených v kapitole 2.6.

Hlavné vlastnosti blockchainu, ktoré ho odlišujú od iných typov databáz, sú teda:

1. Umožňuje pripojiť sa viacerým až mnohým uzlom,
2. Obsahuje implicitnú ochranu pred nesprávnych správaním sa ľubovoľného uzla,
3. Zabezpečuje rovnaký pohľad na množinu transakcií pre všetkých účastníkov siete,
4. Zabezpečuje spätnú nemeniteľnosť zapísaných záznamov kýmkoľvek. Žiaden účastník nemá v tomto smere privilegované postavenie,
5. Všetci účastníci vidia záznamy zapísané v blockchaine ako validné.

Z toho vyplýva, že blockchain rieši problém transparentnosti a dôvery medzi jednotlivými účastníkmi. Na jednej strane zabezpečuje, že čo je raz zapísané je nemenné, overiteľné každým účastníkom, a v prípade opatrenia záznamu digitálnym podpisom autorom autentické a nepopierateľné, na strane druhej algoritmicky overuje validnosť záznamov a bráni vzniku konfliktov.

V širšom zmysle sa za blockchain považujú aj iné typy decentralizovaných databáz (distributed ledgers, DLT), ktoré nemusia používať zoskupovanie záznamov do reťazca blokov, ale zdieľajú s blockchainom kľúčové vlastnosti.

Z hľadiska prístupu môžeme blockchain siete rozdeliť na tieto základné typy:

1. Verejný blockchain – ktokoľvek má možnosť pripojiť sa a zúčastniť sa na vytváraní nových blokov. Každý si môže stiahnuť aktuálnu množinu blokov a záznamov, a stať sa tak overovateľom zapísaných informácií. Prípadný pokus o nekalé chovanie (zmena historického záznamu, pokus zapísať nevalidnú informáciu atď.) je tak verejnosťou rýchlo odhaliteľný.
2. Konzorčný blockchain – iba členovia konzorcia (určení centrálne) sa môžu pripojiť, resp. zúčastniť. Obmedzený počet účastníkov, ktorí sa môžu pripojiť a ich schvaľovanie, obmedzujú použitie tejto databázy ako zdroja dôveryhodných a nemenných informácií. Je potrebné dôslednejšie analyzovať vlastnosti daného algoritmu konsenzu, aby sa zistila nákladnosť rôznych typov útokov a tým ich praktická realizovateľnosť. Variantom je Konzorčný blockchain s verejným prístupom na čítanie,

pri ktorom si konzorcium udržuje právo na vytváranie blokov a prístup na čítanie je otvorený verejnosti.

3. Súkromný blockchain – obmedzený na členov určitej organizácie. To, že jedna organizácia spravuje všetky kópie databázy, ju robí externe nedôveryhodnou.

Je dôležité pripomenúť, že hranica medzi jednotlivými typmi nie je úplne striktná a veľmi závisí aj od spôsobov správy (governance) daného blockchainu. Príkladom môže byť blockchain s verejným prístupom, ktorý je ale od začiatku nastavený tak, že pri vytváraní blokov výrazne zvýhodňuje skupinu účastníkov, napríklad zakladateľov (viď PoS a DPoS systémy, v ktorých si zakladatelia nechali rozhodujúcu časť tokenov).

Zvolený typ prístupu závisí od danej aplikácie a jej konkrétnych potrieb. V prípadoch, keď je verejná kontrola jednou zo zásadných požiadaviek, je verejný blockchain alebo konzorčný blockchain ideálnym riešením. V prípade, že sa zdieľajú informácie neverejného charakteru v úzkej skupine, môže byť vhodné zvoliť súkromný blockchain.

2.3 Hash funkcia

Jedným z kľúčových komponentov technológie blockchain je kryptografická hašovacia funkcia (hash). Hašovacia funkcia má mnohonásobné využitie v oblasti blockchainu. Takáto funkcia vypočíta zo vstupného reťazca prakticky akejkoľvek dĺžky (jeden znak, stovky, tisíce alebo aj miliardy znakov) výstupný reťazec fixnej dĺžky. Kryptografická hašovacia funkcia má tieto vlastnosti:

1. Rýchlosť: hash je možné na dostupných výpočtových systémoch vypočítať rýchlo.
2. Jednosmernosť: inverznú funkciu je extrémne ťažké, ba prakticky nemožné nájsť. Zo znalosti výstupného reťazca nevieme vypočítať vstupný reťazec.
3. Bezkolíznosť: pri moderných silných hašovacích funkciách nevieme v reálnom (predstaviteľnom) čase nájsť dva rôzne vstupy vedúce k rovnakému výstupu; k danému vstupu nevieme nájsť iný vstup produkujúci rovnaký výstup (alebo je to extrémne nepravdepodobné).
4. Lavínovitosť: malá zmena vstupu (napr. jeden bit) spôsobí podstatnú zmenu výstupu (obvykle sa zmení väčšina znakov výstupného reťazca).

Hash sa využíva v rámci technológie blockchain najčastejšie na:

1. Previazanie blokov blockchainu a ich zabezpečenie proti zmene,
2. Pri ukladaní väčších súborov mimo blockchainu (off-chain) – do blockchainu ukladáme ich hash ako elektronický odtlačok,
3. Pri konsenzuálnom algoritme Proof of work je často používanou úlohou nájdenie reťazca, ktorého pridaním získame špecifický hash (napr. pri Bitcoine hľadáme hash začínajúci sa niekoľkými nulami).

Hash funkcií je mnoho, dnes sa v blockchaine najčastejšie využíva funkcia SHA-256. Príklady hash-ov sú uvedené v tabuľke nižšie:

Vstupný reťazec	SHA-256 hash
abc	ba7816bf8f01cfea414140de5dae2223b00361a396177a9cb410ff61f20015ad
abC	0a2432a1e349d8fdb9bfca91bba9e9f2836990fe937193d84deef26c6f3b8f76
ab c	bd1b09f907871923193bb63452854c85de56d36a51cc3137ebb4928a3228bf82

Tabuľka 1: Príklady hašovania (hašovacia funkcia SHA256)

2.4 Autentifikácia a autorizácia na blockchaine

Autentifikácia, resp. autentifikácia identity, je overenie totožnosti používateľa (fyzickej alebo právnickej osoby, prípadne informačného systému). V prípade overovania v informačných technológiách sa najčastejšie používajú metódy podľa toho, čo daná osoba:

- má (napríklad digitálny podpisový kľúč v hardwarovej alebo softwarovej podobe, mobilný telefón, kam sa doručí jednorazový token),
- čo vie (heslo, PIN, ...) alebo
- čím je (biometria).

V prípade vytvárania záznamov do blockchainu bez centrálnej autority sa vývoj zameriava na neinteraktívne spôsoby overovania totožnosti, predovšetkým prostredníctvom digitálnych podpisov („key authentication"). Digitálny podpis vyžaduje, aby overovaná osoba mala v držaní súkromný (ďalej aj „privátny") kľúč, ktorým sa kryptograficky podpíše odoslaná správa. Príslušný verejný kľúč je potom nejakým dôveryhodným spôsobom distribuovaný overovateľom – buď ako tzv. digitálny certifikát vydaný kvalifikovaným poskytovateľom dôveryhodných služieb (kvalifikovaný certifikát) alebo priradením kľúča k danej osobe priamo v blockchaine kvalifikovanou osobou.

S autentifikáciou úzko súvisí aj proveniencia – pôvod vzniku informácie. Podpísaný záznam zároveň nesie nepopierateľnú informáciu o pôvodcovi.

Autorizácia je proces, v rámci ktorého sa danej osobe priradia oprávnenia vykonať nejakú činnosť v informačnom systéme – napríklad či má daná osoba možnosť podať určitý návrh, prečítať daný záznam alebo schváliť použitie prostriedkov. Autorizácia nasleduje obvykle po autentifikácii, keď daný systém už vie, kto k nemu pristupuje, ale musí ešte overiť, či daným spôsobom pristúpiť môže. Výnimkou sú ale schémy, kde autorizácia závisí na držbe, nie na osobe držiteľa („prístup do skladu má každý, kto má kľúč, bez ohľadu na jeho identitu", „prístup k zašifrovanému dokumentu má každý, kto má príslušný dešifrovací kľúč"), alebo autorizácia vyžaduje spoluprácu viacerých osôb („zmluvu musia schváliť aspoň dvaja konatelia").

Autentifikáciu aj autorizáciu v blockchaine overovatelia vykonávajú automaticky, algoritmicky. Z hľadiska použiteľnosti je dôležité, aby dané riešenie poskytovalo autentifikačné a autorizačné schémy, ktoré sú vhodné pre danú aplikáciu.

Prístup závisí od	Počet účastníkov	
	jeden	viacero
Identity	Jednoduchý systém účtov, každému používateľovi prislúcha jeden účet, autentifikácia pomocou súkromného kľúča danej osoby alebo certifikátu, každý účet má priradené právomoci.	Flexibilný systém účtov, kde okrem účtov prislúchajúcich daným osobám môžu existovať skupinové účty s pokročilými pravidlami správy (napr. prístup k firemnému účtu majú buď konateľ, alebo väčšina správnej rady). K prístupu k takýmto účtom je potreba, aby sa zúčastnili potrební účastníci.
Držby	Systém, kde každému zdroju / skupine zdrojov je priradený kľúč, držitelia kľúčov so zdrojmi môžu manipulovať.	Systém, kde každému zdroju / skupine zdrojov je priradený kľúč, držitelia kľúčov so zdrojmi môžu manipulovať. Môže sa vyžadovať viac kľúčov k manipulácii (napr. schémy „dva z troch").

Tabuľka 2: Možné riešenia prístupu k blockchainu

V prípade distribuovanej, plne replikovanej databázy je potrebné dodať, že každý pripojený počítač má túto databázu k dispozícii. Na odopretie prístupu na čítanie k danému obsahu preto treba použiť iné prostriedky, napríklad kryptografiu, kde dané zdroje sú zašifrované a k čítaniu je potrebný dešifrovací kľúč. Ak niekto daný dešifrovací kľúč získa, prístup k danému obsahu sa v budúcnosti nedá odobrať. Toto platí aj pre DLT, ktoré riadia prístup na čítanie – akonáhle je obsah niekomu sprístupnený, nie je možné zaistiť, aby k nemu stratil prístup. Obdobou je možnosť urobiť kópie fyzického spisu – ak je niekomu daný spis do držby, možno predpokladať, že informácie z neho bude mať k dispozícii aj v budúcnosti.

2.5 Porovnanie blockchainu a tradičných databázových technológií

Ak si odmyslíme „malé" databázy, tradičné databázy používané v priemysle alebo štátnej správe vo väčšine prípadov využívajú technológiu klient – server. Klient (používateľ) sa pripája na centrálny uzol – server. Server mu, v závislosti od udelených prístupových práv (autorizácie), umožňuje dáta čítať, vytvárať, meniť a/alebo mazať. Kontrolu nad databázou má vždy dedikovaný administrátor. Pod pojmom administrátor sa v tomto prípade nemyslí nutne jedna fyzická osoba – systémový administrátor, ale organizácia so svojimi rolami a procesmi zodpovedná za stav danej databázy (napríklad Správa katastra, súd vedúci súdne spisy, orgány činné v trestnom konaní vedúce vyšetrovacie spisy, alebo aj IT oddelenie korporácie udržujúce vlastný dátový sklad.

V tomto riešení má administrátor prakticky neobmedzenú kontrolu nad databázou, jej obsahom a pravidlami. Potenciálnym problémom je kompromitácia administrátora, či už v technickej alebo personálnej rovine, ktorá by útočníkovi umožnila obísť dané pravidlá a dáta neoprávnene zmeniť alebo vymazať, alebo zapísať skutočnosti, ktoré odporujú pravidlám. Skúsenosti ukazujú, že sa nejedná iba 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.

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 3: Porovnanie centralizovaného systému a blockchain

2.6 Algoritmus konsenzu

Ako už bolo popísané, blockchain môžeme chápať ako distribuovanú databázu, kde všetci účastníci vidia v rovnakom čase rovnaký obsah. Na dosiahnutie tohto konsenzuálneho stavu sa používajú tzv. algoritmy, resp. protokoly konsenzu.

2.6.1 Problém byzantských generálov a tolerancia byzantínskych chýb

Podobný problém sa v teórii hier objavil už dávnejšie ako „problém byzantských generálov": skupina byzantských generálov, z ktorých každý vedie časť armády, obkľúči mesto. Potrebujú sa dohodnúť, či zaútočiť alebo nie. Pre úspech musia zaútočiť všetci, alebo nikto – ak by zaútočila iba časť armády, riskujú porážku a stratu veľkej časti armády, čo je najhorší možný výsledok. Časť generálov chce zaútočiť, časť nie. Niektorí z generálov tiež môžu spolupracovať s nepriateľom a manipulovať rozhodnutie v neprospech misie. Keďže sa každý generál so svojou armádou nachádza na inom mieste, komunikujú spolu iba pomocou poslov. Poslovia však nie sú spoľahliví – môžu byť zajatí alebo môžu prenášanú správu zameniť.

Tolerancia byzantínskych chýb (BFT z anglického „byzantine fault tolerance") znamená schopnosť systému vysporiadať sa s „byzantínskymi" chybami (časť skupiny sleduje vlastné ciele, komunikácia nemusí byť spoľahlivá a pod.).

Algoritmus konsenzu je BFT spôsob, akým skupina dospeje k rovnakému rozhodnutiu o zaradení, resp. nezaradení transakcie alebo bloku.

2.6.2 Proof of Work

PoW – dôkaz prácou – je najstarším algoritmom konsenzu používaným v blockchaine. Spočíva v tom, že v rámci každého kola je vybraný jeden uzol, ktorý vygeneruje ďalší blok. Vybraný je ten uzol, ktorý dokáže najrýchlejšie vypočítať zložitý matematický problém (vynaloží potrebné množstvo práce), a podá o tom dôkaz. Spoľahlivosť tohto algoritmu závisí od celkovej výpočtovej sily siete – čím je sila vyššia, tým je sieť menej náchylná na manipuláciu. Na druhej strane, vyššia výpočtová sila znamená aj vyššiu energetickú náročnosť.

2.6.3 Proof of Stake

PoS – dôkaz vkladom – je ďalším algoritmom používaným v blockchainových sieťach. Potenciálni lídri musia vložiť vklad v podobe kryptomeny a proporcionálne k vkladu majú šancu vygenerovať blok. Tento algoritmus závisí od kryptomeny prepojenej s daným blockchainom.

2.6.4 Practical Byzantine Fault Tolerance

PBFT algoritmus je – 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 verejné blockchainy.

2.6.5 Proof of Elapsed Time

PoET algoritmus predpokladá náhodné zvolenie lídra, ktorý v danom kole generuje blok. Aby bol výber skutočne náhodný, je potrebné splniť dve podmienky: náhodný parameter, určujúci ďalšieho lídra, nie je ovplyvniteľný žiadnym účastníkom a množina účastníkov (validátorov) musí zostať uzavretá. Prvá podmienka sa v prípade PoET algoritmu realizuje pomocou špeciálneho hardwaru (pozri Intel Software Guard Extension). Uzavretá skupina validátorov a potreba špeciálneho hardware predpokladá použitie v privátnych a konzorčných blockchainových sieťach.

2.6.6 Delegated Proof of Stake

Delegated Proof of Stake – delegovaný PoS je tiež založený na výbere lídra. Skupina potenciálnych lídrov danej veľkosti je vybraná hlasovaním účastníkov. Títo sa potom v pseudonáhodnom poradí stávajú lídrami pre dané kolo a vytvárajú bloky. DPoS je veľmi efektívny algoritmus, ktorý dokáže rýchlo dosiahnuť konsenzus. Podobne ako PoS je ale typicky závislý na kryptomene zviazanej s daným blockchainom.

2.6.7 Ďalšie algoritmy

Variantom DPoS a PoET je algoritmus „Proof of Authority". Zo skupiny dopredu vybraných validátorov - potenciálnych lídrov – je pseudonáhodne vybraný líder pre ďalšie kolo, ktorý vytvorí nový blok. Skupina validátorov je vybraná a udržiavaná konzorciom.

Federated Byzantine Agreement – federatívna byzantínska dohoda je typ protokolu, v ktorom každý účastník dôveruje iba určitej skupine iných účastníkov. V rámci týchto jednotlivých skupín dochádza potom k rýchlemu vytvoreniu konsenzu, a nakoľko sa skupiny prelínajú, celá sieť postupne iteruje k rovnakému stavu. Nevýhodou je práve požiadavka na prelínanie sa skupín, ktoré je nevyhnutnou podmienkou na dosiahnutie celosieťového konsenzu. Bez splnenia tejto podmienky môžu vzniknúť navzájom disjunktné „ostrovy dôvery" s rôznym stavom.

Zhrnutie a rámcové porovnanie konsenzuálnych algoritmov popísaných v predchádzajúcich častiach je uvedené v nasledujúcej tabuľke:

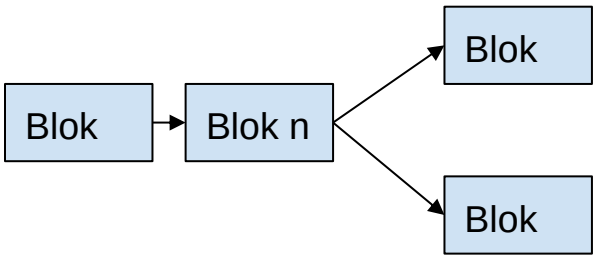
Názov **Vybrané dodatočné verejne dostupné informácie**	**Typické použitie**	**Výhody/nevýhody**
Proof of Work https://en.wikipedia.org/wiki/Proof-of-work_system	Verejný blockchain	(+) Bezpečnosť v anonymnom prostredí (-) Energetická náročnosť
Proof of Stake https://en.wikipedia.org/wiki/Proof-of-stake	Verejný blockchain s vlastnou kryptomenou	(+) Bezpečnosť v anonymnom prostredí (-) Naviazanosť na kryptomenu
Practical Byzantine Fault Tolerance https://en.wikipedia.org/wiki/Byzantine_fault_tolerance	Privátny a konzorčný blockchain	(+) Efektívny algoritmus (krátka latencia, vysoká priepustnosť) v malej skupine validátorov
Proof of Elapsed Time	Privátny a konzorčný blockchain	(+) Efektívny algoritmus (krátka latencia, vysoká priepustnosť) (-) Závislosť na špecializovanom HW
DPoS	Verejný blockchain s vlastnou kryptomenou	(+) Efektívny algoritmus (krátka latencia, vysoká priepustnosť) (-) Naviazanosť na kryptomenu
FBA	Verejný a konzorčný blockchain	(+) Vysoko decentralizované riešenie (+) Vyššia priepustnosť (-) Môže byť náročnejšie na nastavenie
Proof of Authority https://en.wikipedia.org/wiki/Proof-of-	Privátny a konzorčný	(+) Efektívny algoritmus (krátka latencia, vysoká priepustnosť)

Názov Vybrané dodatočné verejne dostupné informácie	Typické použitie	Výhody/nevýhody
authority	blockchain	(-) Vysoká miera centralizácie

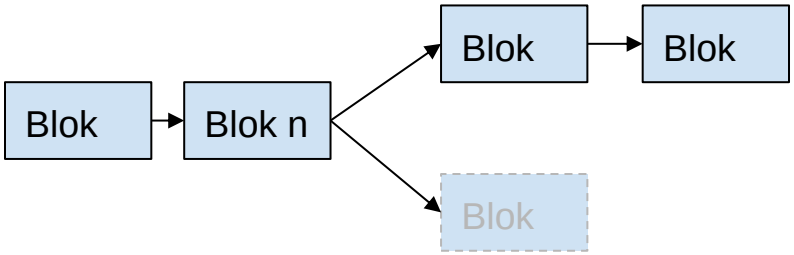
Tabuľka 4: Porovnanie konsenzuálnych mechanizmov

2.7 Fork

V určitých prípadoch môže prísť k prípadu, že validátori vytvoria jeden alebo viac navzájom si konkurujúcich reťazcov blokov. Dôvodom môžu byť problémy s prepojením jednotlivých častí siete brániace distribúcii nového bloku naprieč sieťou, softwarová chyba, úmysel atď. Podobnej situácii sa vraví „fork" a jednotlivé algoritmy konsenzu sa s podobnou situáciou vedia vyrovnať. Vyberie sa „hlavný reťazec" (obvykle ten najdlhší známy reťazec blokov) a ostatné, ktorým sa vraví „osirené" (z angl. výrazu „orphaned"), sa zahodia.



Obrázok 1: Fork – dva paralelné bloky



Obrázok 2: Fork – jeden z paralelných blokov bol vybraný ako pokračovateľ

2.8 Topológia blockchainovej siete

Ako už bolo naznačené v predchádzajúcich častiach, na technológiu blockchain je možné nazerať z rôznych uhlov pohľadu – blockchain ako distribuovaná aplikácia, databáza, infraštruktúra alebo komunikačná sieť. Práve pri poslednom pohľade na blockchain uvažujeme aj o jeho „implementácii v priestore".

Historicky bol blockchain navrhnutý ako peer-to-peer sieť rovnocenných uzlov, prevádzkovaných na rovnakej softwarovej báze, z ktorých každý sa mohol, po splnení podmienok, stať validátorom. Ak autor vytvoril nový záznam, ten mohol byť poslaný na ktorýkoľvek uzol v sieti. Ten urobil prvotnú validáciu, a cez príslušný protokol ho poslal svojim peerom – partnerským uzlom ďalej. Tie ho, po overení, poslali zase ďalej. Jednotlivé uzly držali zoznam tzv. nepotvrdených transakcií. Validátor (konsenzuálne zvolený) v danom kole z tohto zoznamu vybral podmnožinu navzájom nekonfliktných transakcií, ktoré

zaradil do novovytvoreného bloku, ktorý sa zase, cez peer-to-peer sieť šíril do ostatných uzlov. Tie si ho potom zaradia do zoznamu známych blokov. Každý z týchto uzlov teda drží úplný blockchain, t. j. zreťazený zoznam blokov. V momente, keď autor záznamu obdržal blok so svojím záznamom, vedel, že tento bol úspešne zaradený. V závislosti od algoritmu konsenzu môže byť pre zvýšenie pravdepodobnosti, že nedôjde k forku a osireniu príslušného bloku, potrebné čakať na potvrdenie ďalšími blokmi.

Dnes sú topológie blockchainov oveľa flexibilnejšie, okrem spomínaných uzlov sa môžu objavovať tzv. ľahký klient, ktorý, na rozdiel od vyššie spomínaného "plného uzlu", nedrží v pamäti celý stav blockchainu, ale iba určitú malú časť. Tiež sa objavujú rôzne cloudové aplikácie, ktoré poskytujú používateľsky priateľskejšie prostredie k nejakej blockchainovej službe.

Aktívna práca s blockchainom, používajúcim podpisy asymetrickej kryptografie, predpokladá, že používateľ má k dispozícii príslušné súkromné kľúče na nejakom vhodnom úložisku. Tým môže byť pevný disk na jeho počítači, USB kľúč, cloudové úložisko, špeciálne hardwarové zariadenie, na ktorom je uložený súkromný kľúč, ale napríklad aj papier s vytlačeným súkromným kľúčom. Týmto úložiskám sa zvykne hovoriť „peňaženka" (z anglického výrazu „wallet"), nakoľko v počiatkoch úložiská slúžili najmä na prístup k mene bitcoin.

2.9 Smart kontrakty

Ako inteligentný (smart) kontrakt je označovaný protokol, ktorý zaisťuje automatickú realizáciu zmlúv a dohôd.

V širšom zmysle sa za inteligentný kontrakt považuje akýkoľvek software, bežiaci autonómne bez kontroly používateľa, resp. používateľov alebo akejkoľvek tretej strany, spracovávajúci dodané vstupy na výstupy. Príkladom môže byť presmerovanie 10 % z príjmov, ktoré prídu zamestnancovi na účet, automaticky na sporiaci účet, pravidelná platba nájomného po dobu trvania nájmu, vedenie zálohy do doby, kým nenastanú podmienky na jej uvoľnenie alebo vyhodnotenie podmienok na získanie podpory. Vstupom je typicky nová používateľská transakcia, ktorá spustí program smart kontraktu. Ten spočíta a vráti výstup, a prípadne uloží zmenený stav.

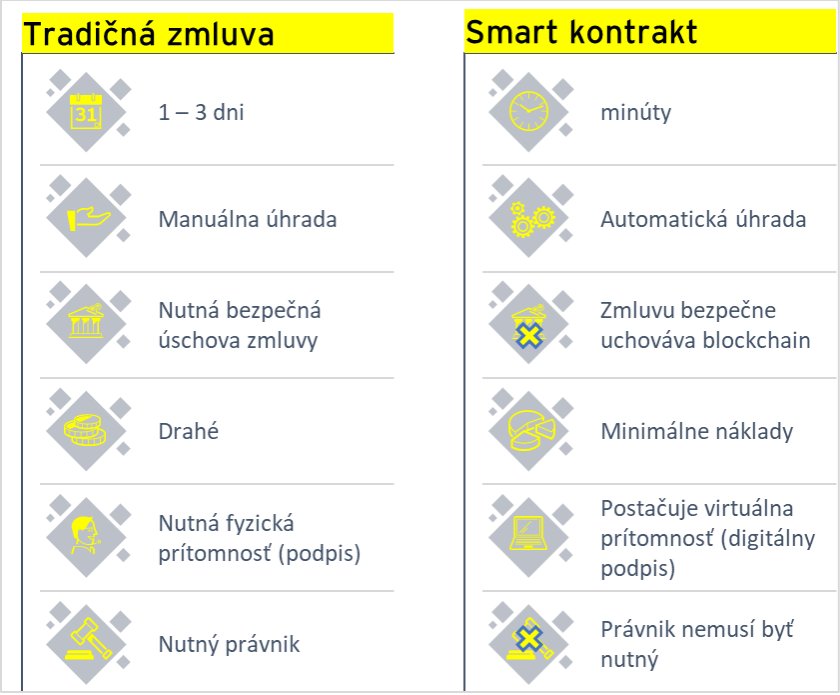
Distribuovaná blockchainová sieť predstavuje vhodné prostredie na beh inteligentných kontraktov. Používatelia si môžu nahrať svoj software ako špeciálny záznam do blockchainu. Každý počítač, kde daný blockchain beží potom vie tento software spustiť. Každý nový záznam v blockchainovej databáze môže byť vstupom pre tento inteligentný kontrakt. Ak nový záznam spustí program smart kontraktu, program vykoná potrebný výpočet, vráti výstup a podľa potreby uloží zmenený stav. Toto sa deje deterministicky, vždy s rovnakým výsledkom na ktoromkoľvek počítači, kde blockchain beží.

Používateľské inteligentné kontrakty nahraté do blockchainu sú viditeľné pre každého, ako akýkoľvek iný záznam, vrátane všetkých potenciálnych chýb a bezpečnostných slabín. Táto transparentnosť a možnosť identifikovať „odlišný" výsledok výpočtu (spôsobený či už neúmyselnou vadou alebo zámernou kompromitáciou konkrétneho výpočtového uzla), predstavuje z hľadiska riadenia informačnej bezpečnosti (najmä rizika neautorizovaného spustenia alebo zmeny funkcionality aplikačného kódu) obrovskú výhodu.

Zároveň si je však potrebné uvedomovať aj zvýšené riziko súvisiace s nasadením (v tomto prípade na mnohé výpočtové uzly) nesprávneho kódu inteligentného kontraktu (nedostatočne otestovaného alebo zámerne „poškodeného") a to najmä v prípadoch, kedy decentralizované spúšťanie takýchto

kontraktov (bez možnosti centralizovaného/manuálneho zásahu a opravy výsledku), môže mať ťažko napraviteľné dôsledky (napríklad vyplatenie finančných a iných prostriedkov, automatické priznanie práv a pod.).

Je tiež dôležité zmieniť, že zatiaľ neexistuje štandard pre tvorbu inteligentných kontraktov. Ich implementácia je závislá od zvoleného riešenia, použitého programovacieho jazyka, cez spôsob práce s dlhodobými dátami až po rôzne limitácie platformy, na ktorej bežia.



Obrázok 3: Porovnanie tradičnej zmluvy a smart kontraktu

2.10 Off-chain storage

Vzhľadom k tomu, že všetky záznamy blockchainu sú udržiavané na mnohých uzloch, nie je veľmi žiadúce ukladať do nich veľké objemy dát. V prípadoch, keď treba zabezpečiť permanentné, nemenné poskytnutie veľkých súborov dát, môžu sa tieto uložiť na nejaké cloudové úložisko. Do blockchainu sa potom iba zapíše záznam, aké súbory, kedy a kde boli uložené, vrátane hashu týchto súborov. Tak si prípadný overovateľ v budúcnosti môže overiť, že dáta sú pôvodné a neboli zmenené, resp. dá sa ukázať, že dané dáta zodpovedajú dátam opísaným v blockchaine.

Úložisko pre dáta samotné môže byť napríklad webová stránka organizácie, cloudové úložisko, privátny FTP server alebo decentralizované úložisko na protokole typu torrent (v tom prípade by sa ako odkaz na miesto uloženia súboru použil tzv. magnet link) alebo IPFS.

2.11 Štandardizácia a interoperabilita

Blockchain je relatívne mladá technológia. Jednotlivé implementácie vo väčšej alebo menšej miere využívajú štandardizované produkty a riešenia (napr. v oblasti kryptografie), rôzne blockchainové riešenia, aplikácie alebo inteligentné kontrakty samotné však zatiaľ štandardizované nie sú. Rôzne implementácie prinášajú vlastné riešenia, ako aj vlastné limitácie.

To sa ale v dohľadnej dobe môže zmeniť. International Telecommunication Union (ITU), špecializovaná agentúra OSN, kladúca si za cieľ okrem iného vytvárať technické štandardy, ako aj International Organization for Standardization (ISO), vytvorili pracovné skupiny pre oblasť blockchain-u a DLT, ktoré už na príslušných štandardoch pracujú.

Interoperabilita blockchainu s externými aplikáciami a/alebo inými blockchainami závisí od konkrétnej implementácie, ale všeobecne je na vysokej úrovni. Mnohé projekty ponúkajú rozsiahle API a SDK pre integráciu externých aplikácií na programátorskej úrovni, a viaceré sú, alebo sa dajú bez väčšej námahy prepojiť s najpoužívanejšími ERP systémami.

2.12 História blockchainu a súčasné využitie

Prvé úvahy o možnostiach dosiahnutia konsenzu v počítačových sieťach, kde samotné počítače alebo sieť sú nespoľahlivé, sa objavili už pred rokom 2000[2]. Ako rok vzniku možno považovať rok 2008, kedy Satoshi Nakamoto navrhol a popísal fungovanie siete Bitcoin[3]. Následne v januári roku 2009 zverejnil zdrojový kód a spustil sieť Bitcoin. Bitcoin sa stal prvou modernou kryptomenou, ktorú nasledovalo mnoho ďalších kryptomien (až po súčasných približne 1600 – 2000). Pokusy o zavedenie kryptomien existovali už skôr (ecash alebo NetCash), avšak nikdy nedosiahli väčšiu popularitu. Bitcoin a ostatné kryptomeny sa tešia veľkej popularite približne od roku 2013. V súčasnosti je celková trhová kapitalizácia verejne obchodovaných kryptomien asi 211 miliárd USD a denný obrat asi 13 miliárd USD. V roku 2013 bola navrhnutá a v roku 2015 spustená sieť Ethereum, podporujúca smart kontrakty.

Približne od roku 2014 sa objavujú úvahy o využití blockchainu na iné účely ako kryptomeny a sú oznámené prvé projekty využívajúce blockchain ako distribuovanú databázu pre využitie v podnikovej sfére, štátnej správe, prípadne inde. Vznikajú tiež blockchain siete určené špeciálne pre rôzne obchodné aplikácie, nie pre kryptomeny. V rokoch 2016-2018 sú ohlásené stovky projektov vyžívajúcich blockchain vo všetkých sférach života. Najzaujímavejšie z nich sú popísané nižšie v tejto štúdii.

2.13 Kedy použiť blockchain, výhody a nevýhody

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 vhodné vždy – 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:

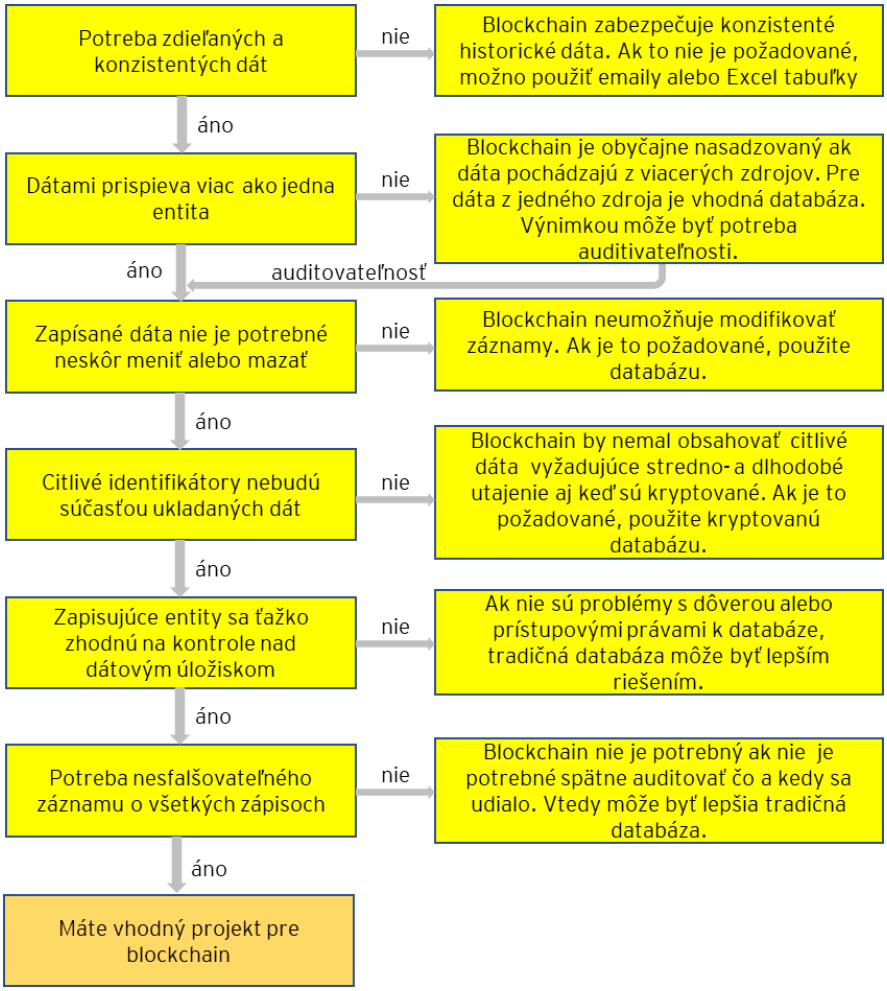
- Mnoho účastníkov,
- Potrebu nastolenia dôvery,
- Neexistenciu tretej strany alebo tretia strana je málo dôveryhodná,
- Úlohy, ktoré majú charakter transakcií,
- Potrebu globálneho (medzinárodného, celosvetového) digitálneho identifikátora,

[2] Lamport, Leslie. "The Part-Time Parliament." ACM Transactions on Computer; Systems, vol. 16, no. 2, Jan. 1998, pp. 133–169

[3] Nakamoto, S., "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008

- Potrebu kryptograficky zabezpečeného systému evidencie vlastníctva,
- Potrebu zjednodušenia riešenia sporov,
- Potrebu zdieľania histórie transakcií a pôvodu digitálnych aktív,
- Potrebu regulátora monitorovať aktivity regulovaných v reálnom čase.

Nasledujúci vývojový diagram slúži na rýchle úvodné posúdenie vhodnosti využiť blockchain pre zamýšľaný projekt:[4]



Obrázok 4: Kedy použiť blockchain

V kapitole 2.2 je vysvetlené fungovanie technológie blockchain a v kapitole 3 vzťah a dôsledky pre informačnú bezpečnosť. Z toho vyplývajú špecifické vlastnosti tejto technológie a tiež obvyklé hlavné prínosy využitia:

- Transparentnosť a sledovateľnosť: tým, že všetci užívatelia zdieľajú tie isté dáta namiesto individuálnych kópií, celý súbor transakcií je transparentnejší. Konsenzuálny mechanizmus zabezpečí zhodu všetkých užívateľov na jednej verzii záznamov, viac v kapitole 2.6. Vysoká miera

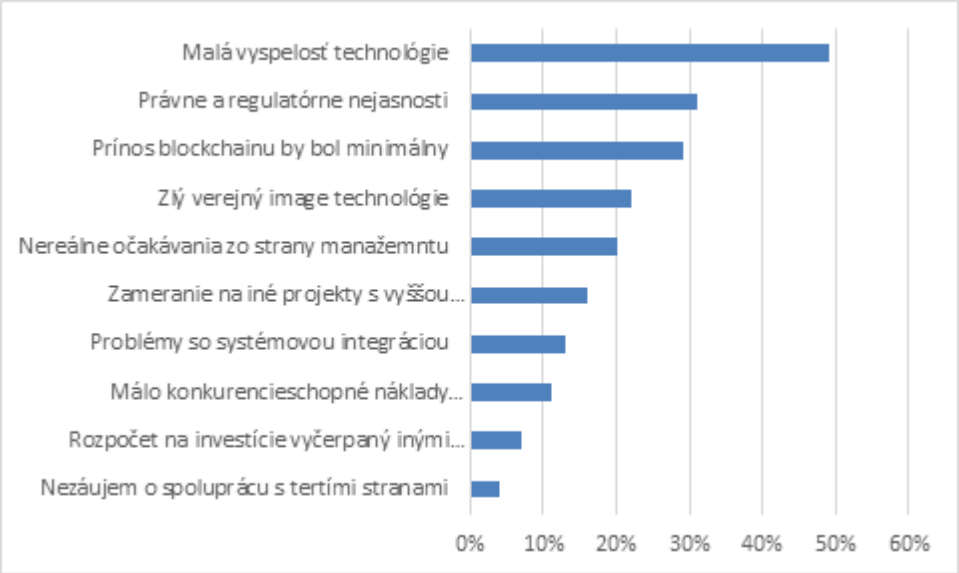
[4] NISTIR 8202 Blockchain Technology Overview, October 2018

transparentnosti, auditovateľnosti a analyzovateľnosti údajov môže byť použitá na udržiavanie konzistencie údajov (na aplikačnej úrovni potom aj súladu s relevantnými predpismi a normami),

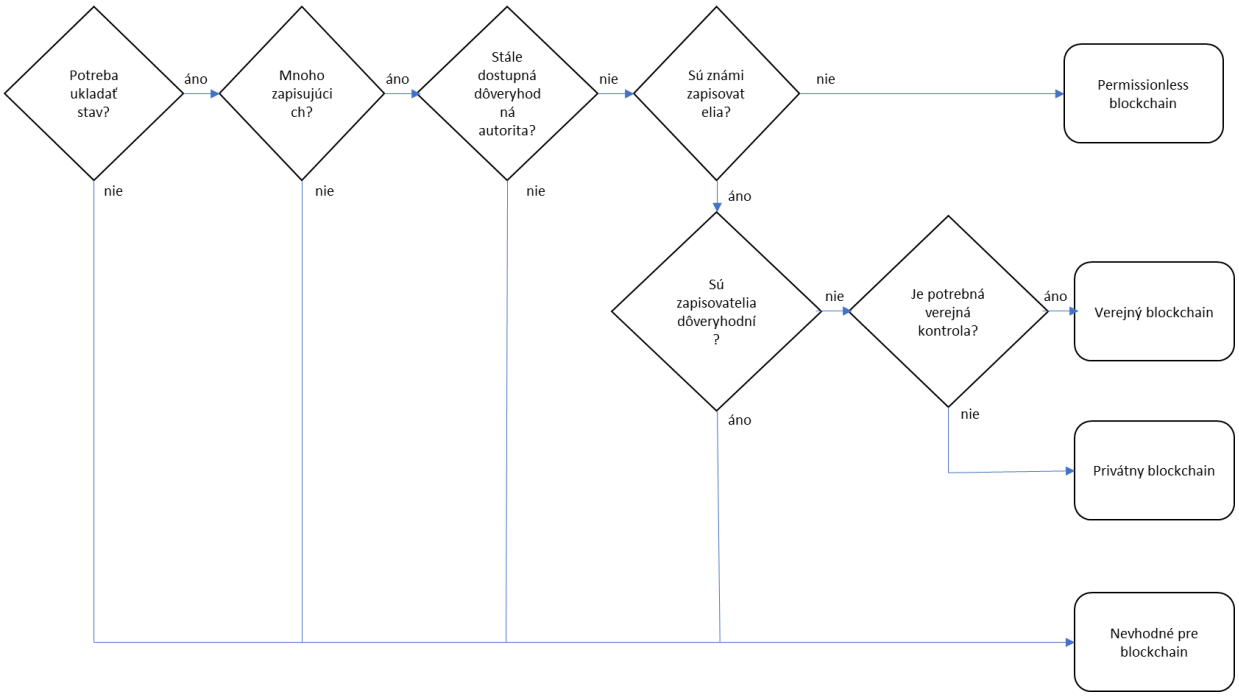
- Možnosť verejnej kontroly: viditeľnosť transakcií všetkým užívateľom umožňuje kedykoľvek verejnú kontrolu transakcií, každý používateľ si môže samostatne overiť (uistiť sa) správnosť spracovania všetkých údajov v blockchain, t. j. či nastali podmienky na spracovanie a transformáciu vstupných údajov na výstupné; v prípade uloženia predpisu transformácie – smart kontraktu vidí aj samotný algoritmus spracovania; (napr. každý používateľ môže vidieť anonymizované výsledky hlasovania a môže si spočítať výsledok volieb a overiť korektnosť ich priebehu),
- Integrita dát: údaje nemôžu byť modifikované ani vymazané neautorizovaným alebo náhodným spôsobom, autor údajov nemôže žiadnemu inému uzlu poprieť svoje autorstvo. Z princípov fungovania technológie blockchain uvedených v kapitole 2 vyplýva nemennosť konsenzom overených uložených údajov čo vedie k dôveryhodnosti uložených záznamov,
- Zníženie nákladov a komplexnosti: zavedenie jediného zdroja dôveryhodných dát bez potreby tretích strán môže viesť zvýšenej efektívnosti, efektivite a tiež k zníženým celkovým nákladom spracovania a uchovávania,
- Trvalé a nemeniteľné digitálne zaznamenávanie: z princípu fungovania technológie blockchain vyplýva, že údaje nemôžu byť modifikované ani vymazané neautorizovaným alebo náhodným spôsobom a takúto zmenu alebo zneplatnenie pôvodných údajov je možné vykonať len vložením nového opravného záznamu logicky previazaného s pôvodným,
- Preukázateľné a overené transakcie: potreba všeobecnej zhody uzlov siete umožňuje prevenciu pred vložením nesprávnych údajov (napr. neúplných, neexistujúcich, nepresných účtovných dokladov; nesprávnych, neúplných, neaktuálnych osobných údajov a pod.). Spravodlivý (náhodný) výber uzla zodpovedného za vytvorenie nového bloku záznamov a nutnosť konsenzu ostatných uzlov pri zápise nového bloku významne eliminuje možnosť podvodného konania uzlov zodpovedných za vytváranie nových blokov,
- Redundancia uložených dát: dáta sú automaticky replikované na mnohých miestach (uzloch) takže v prípade poruchy alebo straty dát na jednom, prípadne viacerých uzloch, ostáva stále mnoho kópií na ostatných uzloch, čím je zabezpečená mnohonásobná redundancia uložených dát, viac v úvode kapitoly 2.2 a 2.8,
- Nastolenie dôvery: tým, že všetci užívatelia majú prístup k celej histórii transakcií, zhodnú sa na nej a nie je ju možné spätne meniť, zvyšuje sa, prípadne sa až nastoľuje dôvera v tieto dáta,
- Možnosť efektívneho zavedenia smart kontraktov – podrobnejšie vysvetlené v kapitole 2.9

Námietky, riziká, hrozby a nevýhody technológie blockchain sú silno závislé ma konkrétnej implementácii technológie a preto sú vyžadujú podrobné vysvetlené uvedené v kapitole 2.15, 3.2.1 a 3.3.2.

Nasledujúci graf ukazuje hlavné bariéry zavádzania technológie blockchain podľa nedávnej štúdie EY:



Obrázok 5: Hlavné bariéry zavádzania technológie blockchain



Obrázok 6: Aký blockchain je vhodný?[5]

2.14 Blockchain a kryptomeny

Kryptomena je digitálne aktívum, zabezpečené pomocou silnej asymetrickej kryptografie. Historicky, prvé implementácie blockchainu sa zameriavali práve na vytvorenie a správu kryptomien. Použitie transparentnej peer-to-peer technológie s automatickou validáciou záznamov o prevodoch, akou je

[5] Do you need a Blockchain? K. Wüst, A. Gervais, Department of Computer Science, ETH Zurich, Switzerland

blockchain, na vedenie účtovnej knihy kryptomeny je prirodzené, a dodnes väčšina verejných blockchainov používa nejakú formu kryptomeny. Tou sa realizuje napr. platba za použitie a je nejakým spôsobom zviazaná s algoritmom konsenzu. Treba ale dodať, že napriek tomu, že je to pretrvávajúca prax, spojenie blockchainu a kryptomeny nie je povinné, a v mnohých aplikáciách ani žiadúce. Blockchain je v médiách a očiach verejnosti spájaný hlavne s kryptomenami. Kryptomeny a blockchain však môžu fungovať jedno bez druhého, avšak ich spojenie v istých prípadoch je obojstranne výhodné. Kryptomeny a blockchain majú štyri hlavné prieniky, spoločné oblasti nasadenia:

- Kryptomena ako náhrada FIAT meny pri platobnom styku a investovaní,
- Kryptomena ako odmena prevádzkovateľa siete (uzla),
- Kryptomena ako poplatok za použitie siete (obvykle len za zápis),
- Kryptomena ako reprezentácia objektov, práv atď. z reálneho sveta vo forme tokenov (Tokenizácia asetov).

Kryptomena ako náhrada FIAT meny pri platobnom styku a investovaní

Toto využitie je asi najznámejšie, mnoho ľudí a spoločností investovalo do kryptomien za účelom zisku, prípadne diverzifikácie investičného portfólia. Využitie pri platobnom styku, ktoré malo byť lacnejšie, rýchlejšie a anonymné, zatiaľ úplne nenaplnilo očakávania: poplatky sú niekedy vyššie ako pri klasickom platobnom styku, rýchlosť (napr. u Bitcoinu) je podstatne nižšia ako pri autorizácii platby kartou a anonymita je tiež diskutabilná. Problémom je tiež obyčajne veľmi vysoká volatilita.

Kryptomena ako odmena prevádzkovateľa siete (uzla)

Prevádzkovateľ uzla musel investovať do vybudovania uzla a hradiť náklady spojené s jeho prevádzkou. Vo verejných blockchainoch je za toto odmeňovaný kryptomenou na základe svojej úspešnosti ťaženia/validovania blokov podľa konsenzuálneho algoritmu použitého v danej sieti. Výškou odmeny môžeme riadiť rozvoj siete, motivovať príchod nových prevádzkovateľov uzlov alebo naopak znížiť poplatky pri dostatočnom množstve uzlov. V privátnych alebo konzorčných blockchainoch takáto odmena nemusí existovať, prevádzkovatelia môžu mať inú motiváciu budovať a prevádzkovať uzly siete (dohoda, nariadenia, povinnosť, iné výhody).

Kryptomena ako poplatok za použitie siete (obvykle len za zápis)

Užívatelia blockchain siete môžu platiť za každé použitie siete a z týchto poplatkov môže byť financovaná prevádzka a rozvoj siete. Poplatok je vyberaný obvykle len za zápis, čítanie je zdarma. Poplatok obvykle závisí od dĺžky transakcie v bajtoch, za dlhšiu, ktorá viac zaťaží sieť, sa platí viac. Tento model je obvyklý vo verejných blockchainoch a zabraňuje nadužívaniu alebo zneužívaniu siete. Poplatok nemusí byť fixný – jeho premenlivou výškou možno reagovať na náhle zmeny zaťaženia siete, avšak v takomto prípade nie je možné predpovedať výšku poplatku v danom čase a výška poplatku môže byť vyššia.

Kryptomena ako reprezentácia objektov, práv atď. z reálneho sveta vo forme tokenov (Tokenizácia asetov)

Tokenizácia asetov je jedným z hlavných možných využití blockchainu mimo kryptomien. Využíva sa pri nej unikátna vlastnosť blockchainu spoľahlivo riadiť, evidovať a zabraňovať zneužitiu (viacnásobnému

použitiu) kryptomien-tokenov. Namiesto termínu kryptomena je vhodnejšie použitie termínu token. Objekty zo skutočného sveta v tomto prípade reprezentujeme vo virtuálnom svete tokenom a jeho používanie riadime a sledujeme pomocou blockchainu. Môže ísť napríklad o zdieľané vlastníctvo dopravných prostriedkov (napr. auto, jachta, bicykel), nehnuteľností (napr. apartmán, kancelárske priestory) alebo aj výpočtový výkon či úložnú kapacitu v dátovom centre. Token potom reprezentuje právo k dopravnému prostriedku alebo apartmánu v danom čase alebo úložnú kapacitu v dátovom centre. Blockchain slúži na nakladanie s týmito tokenmi medzi viacerými používateľmi, zabraňuje viacnásobnému použitiu (napr. apartmán alebo jachta v jednom čase) a eviduje ich využitie používateľmi.

Blockchain však môže existovať aj bez kryptomien, prípadne kryptomeny-tokeny môžu byť použité len na dva, jeden alebo žiaden z účelov uvedených vyššie. Kryptomeny-tokeny daného blockchainu tiež nemusia byť verejne obchodovateľné s pohyblivým kurzom. Napríklad pri platbe občana za služby štátu (zápis do registra X, žiadosť o povolenie Y) môže byť vytvorená kryptomena-token (kolok), ktorú dostane občan zdarma v istom množstve a ďalšie si môže dokúpiť za poplatok.

2.15 Námietky proti blockchainu a vysvetlenia

Všeobecné povedomie o blockchaine je stále nízke. Väčšina ľudí už niečo počula o kryptomenách, ale celkové vedomosti o blockchaine sú obmedzené. Informácie v médiách sú často negatívne a zavádzajúce. Z toho vyplýva istá averzia k technológii blockchain. Nižšie sme zozbierali najčastejšie zaznievajúce námietky/tvrdenia a pokúsili sa o vysvetlenie skutočného stavu, prípadne naznačenie možných riešení.

Ťažba kryptomien je neefektívna, neekologická, energeticky náročná a nezmyselná

Táto námietka platí hlavne pre blockchain siete založené na konsenzuálnom algoritme PoW. Napríklad ťažba Bitcoinu spotrebováva asi 73 TWh energie ročne, čo je asi 0,33 % svetovej spotreby energie a tiež približne spotreba Rakúska[6]. Novšie blockchain siete však využívajú modernejšie konsenzuálne algoritmy, ako napr. PoS (Proof of Stake), ktoré sú mnohonásobne nižšie energeticky náročné. Pre rozsiahlejšie nasadenie v prostredí e-Governmentu odporúčame vyhnúť sa PoW blockchainom.

Blockchain vždy postupne smeruje k centralizácii a tým stráca zmysel

Hlavne u blockchainov využívajúcich PoW sledujeme združovanie do tzv. mining pools. Napríklad najväčšie ťažobné združenie v sieti Bitcoin dosahuje až 30 % úspešnosť. U modernejších blockchainov využívajúcich iné konsenzuálne algoritmy (napríklad PoS) je toto riziko nižšie a nižšia je aj motivácia k združovaniu sa v ťažobných združeniach. Vo všeobecnosti sa treba snažiť o čo najväčšiu diverzitu uzlov, rôzne platformy, operačné systémy, geografické polohy, vlastníctvo a pod.

Blockchain sa využíva na pranie špinavých peňazí a platby v šedej či čiernej ekonomike, aj väčšina ICO sú podvody.

Anonymita platieb v kryptomenách a nedostatok regulácie skutočne môže viesť k využívaniu platieb v šedej a čiernej ekonomike. Navrhované projekty sa však vyhýbajú kryptomenám ako platidlu a využívajú blockchain ako databázu, prípadne ho využívajú v zmysle tokenizácie aktív. Blockchain v navrhovaných projektoch naopak prináša dôveru a väčšiu transparentnosť.

[6] https://digiconomist.net/bitcoin-energy-consumption

Blockchain je disruptívna technológia, ktorá spôsobí stratu pracovných miest, krach firiem, zatvorenie úradov

Blockchain je revolučná technológia a má tendenciu narúšať existujúce podnikateľské modely a zefektívňovať procesy. Dôsledkom môže byť lokálna strata pracovných miest, avšak blockchain prináša aj mnoho nových príležitostí a nové podnikateľské modely.

Blockchain je pomalý (Bitcoin)

Blockchain Bitcoinu je oveľa pomalší a má menšiu časovú kapacitu (maximálny počet transakcií za minútu) ako súčasné, modernejšie blockchainy. Bitcoin vytvára nový blok približne každých 10 minút, moderné blockchainy vytvárajú nové bloky rádovo v sekundách. Kapacita Bitcoinu je len do 7 transakcií za sekundu (podľa obsahu), Ethereum do 15 tx/sec, niektoré modernejšie dosahujú až viac ako 1,000 transakcií za sekundu.

Blockchain je v rozpore s GDPR

Táto problematika je vysvetlená nižšie v bode 3.4.1.

2.16 Súčasné výzvy a trendy

Odklon od PoW smerom k iným algoritmom

Vzhľadom na vysokú a stále sa zvyšujúcu energetickú náročnosť konsenzuálnych algoritmov založených na výpočtovom výkone (PoW), badať u nových blockchain projektov odklon od PoW smerom k energeticky efektívnejším algoritmom ako sú PoS, DPoS a pod. Prehľad porovnanie rôznych konsenzuálnych algoritmov je uvedený vyššie v tejto kapitole.

Snaha o redukciu objemu dát ukladaných do blockchainu a ukladanie väčších dát off-chain

Vzhľadom na požiadavku rýchlej odozvy, menších nárokov na prenosové kapacity siete či menších nárokov na úložný priestor uzlov blockchainu vidíme snahu minimalizovať objem dát ukladaných do blockchainu a presun objemnejších dát off-chain, t. j. na iné úložiská mimo blockchainu. Do blockchainu sa potom ukladajú len ich hashe, aby bolo možné overiť pravosť dokumentu. Príklady off-chain storage sú napr. IPFS (InterPlanetary File system), StorJ a pod.

Tokenizácia aktív

Silným trendom vo využívaní blockchainu je tokenizácia aktív. Aktíva zo skutočného sveta sa reprezentujú vo virtuálnom svete v forme tokenov. Token je niečo ako kryptomena, len s tým rozdielom, že reprezentuje aktívum (alebo jeho časť) z reálneho sveta. Môže ísť o dopravný prostriedok (napr. auto, bicykel, jachtu), nehnuteľnosť (napr. chata, dovolenkový apartmán), výpočtový výkon, kapacitu v cloudovom úložisku, emisné povolenky a mnohé ďalšie. Tokeny je potom možné s využitím blockchainu ľahko prevádzať, obchodovať s nimi, sledovať ich využitie a hlavne zabezpečiť proti zneužitiu viacnásobným použitím (napr. že aktívum auto bude v jednom čase pridelené len jednému používateľovi).

Smart kontrakty

Jedným z často uvádzaných trendov je aj využívanie smart kontraktov v blockchaine. Lákavé sú nízke náklady, bezpečnosť, jednoznačnosť, nepotrebnosť tretej strany a vykonateľnosť zmluvy. Blockchain podporujúci smart kontrakty je však zložitejší a potenciálne drahší, prípadne pomalší. Po incidente s DAO v roku 2016 pri ktorom bolo ukradnutých 50 mil. USD (neskôr však vrátených), sú relevantné aj otázky ohľadom bezpečnosti smart kontraktov. Vzhľadom k chýbajúcej regulácii môže byť otázna právna záväznosť takejto zmluvy alebo problematické riešenie súdnych sporov.

Nasledujúca tabuľka sumarizuje niektoré výzvy a rizika technológie blockchain:[7]

Oblasť	**Výzvy a riziká**
Výzvy adopcie novej technológie	Užívateľská skúsenosť (user experience)
	Použiteľnosť technológie
	Rýchlosť systému
	Všeobecná verejná dôvera
	Nedostatok povedomia o technológii
Technologické bariéry	Nízka transakčná kapacita
	Škálovateľnosť
Bezpečnostné riziká	Riziká kybernetickej bezpečnosti
	Úniky dát
	Limitovaná ochrana kryptografických kľúčov
Právne a regulatórne výzvy	Nejasná jurisdikcia
	Identifikácia zodpovedných
	Legislatívny rámec kontraktov
	Regulácia ohľadom ochrany osobných údajov
Riziká spojené s interoperabilitou	Nedostatok blockchain štandardov
	Vývoj vhodných dátových modelov
	Vhodné protokoly pre autentifikáciu a komunikáciu
Energetická náročnosť	Proof-of-work konsenzuálny algoritmus
	Škálovateľnosť proof-of-stake a proof-of-authority
	Zníženie energetickej náročnosti

Tabuľka 5: Blockchain výzvy a riziká

[7] Building Block(chain)s for a Better Planet, WORLD ECONOMIC FORUM

3 Blockchain a informačná bezpečnosť

Prakticky každý pokus definovať alebo popísať technológiu blockchain – jej vlastnosti a spôsob fungovania sa nezaobíde bez použitia pojmov (napr. autentickosť, auditovateľnosť, nemennosť, nezničiteľnosť, nepopierateľnosť), ktoré sa používajú aj pri popise problematiky riadenia informačnej bezpečnosti. Už toto konštatovanie naznačuje, že blockchain má s informačnou bezpečnosťou (ďalej aj „IB“) viacero styčných bodov.

V tejto podkapitole sme sa zamerali na analyzovanie týchto súvislostí, výhod a nevýhod blockchainu z hľadiska riadenia informačnej bezpečnosti a naznačenia prípadov použitia, v ktorých môže blockchain prispieť k zvýšeniu bezpečnosti predmetných informačných aktív.

3.1 Ciele a postupy riadenia informačnej bezpečnosti

Na úvod ponúkame stručné pripomenutie základných pojmov a konceptov informačnej bezpečnosti.

Informačnú bezpečnosť je možné definovať ako stav, kedy sú vo vzťahu k chráneným informačným aktívam na požadovanej úrovni naplnené ciele informačnej bezpečnosti. K cieľom IB (zvyknú sa označovať aj ako CIA) pritom patrí zabezpečiť dostatočnú:

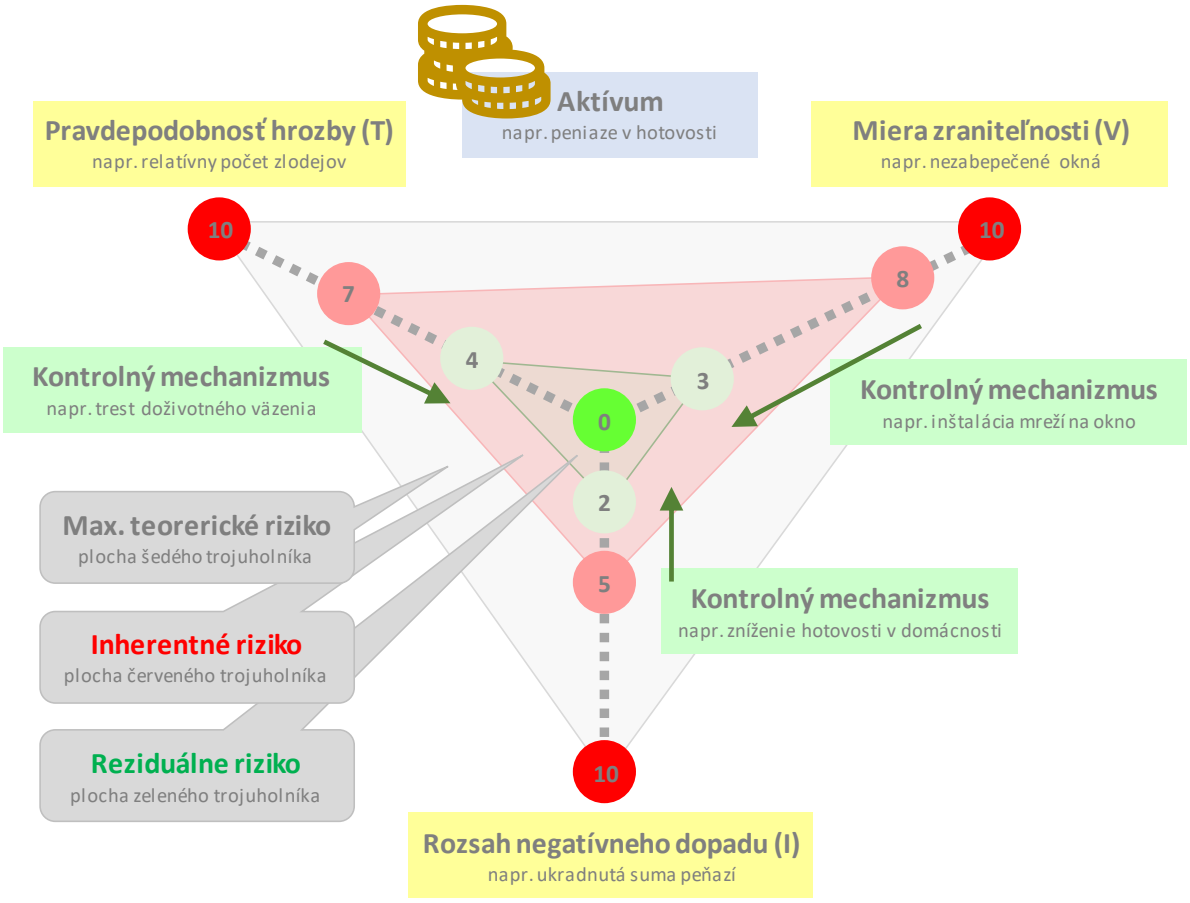
- dôvernosť (confidentiality),
- integritu (integrity) a
- dostupnosť (availability) týchto informačných aktív.

Poznámka: Pod pojmom integrita budeme pre účely tohto dokumentu chápať aj tzv. nepopierateľnosť (non-repudiation) pôvodu – odoslania údajov aj nepopierateľnosť ich prijatia ale tiež autentickosť údajov – schopnosť overiť kto je autor údajov, kedy boli vytvorené a že neboli pozmenené.

Pod riadením informačnej bezpečnosti potom chápeme vykonávanie aktivít, ktoré smerujú k dosiahnutiu spomínaných cieľov IB. Tieto aktivity spočívajú v periodickom vykonávaní nasledujúcich krokov:

- identifikovanie a modelovanie informačných aktív a ich súvislostí,
- analyzovanie rizík, t.j. identifikovanie a kvantifikovanie hrozieb (threats), zraniteľností (vulnerabilities) a potenciálnych (negatívnych) dopadov (impacts) pôsobiacich na tieto aktíva a výpočet tzv. inherentných rizík,
- výber a implementácia vhodných („dostatočne silných“) kontrolných mechanizmov (ďalej aj „KM“) na zmiernenie inherentných rizík na akceptovateľnú mieru (podľa zvolenej stratégie akceptácie rizík) a výpočet tzv. reziduálnych rizík,
- testovanie (návrhu a účinnosti) implementovaných kontrolných mechanizmov informačnej bezpečnosti (t.j. potvrdzovanie, že KM plnia svoju úlohu a naozaj znižujú riziká na akceptovateľnú úroveň), resp. náprava – zdokonaľovanie KM,
- monitorovanie, identifikovanie a riešenie incidentov informačnej bezpečnosti (t.j. situácií kedy mohlo napriek implementovaným KM dôjsť k negatívnemu dopadu na určité informačné aktívum, ktorý spôsobila určitá hrozba a s využitím určitej zraniteľnosti tohto aktíva).

Na nasledujúcom obrázku je zjednodušene schematicky znázornená časť riadenia informačnej bezpečnosti týkajúca sa analýzy rizík.



Obrázok 7: Príklad výpočtu rizika pre informačné aktívum

3.1.1 Riadenie informačnej bezpečnosti vo verejnej správe

Základným všeobecne uznávaným návodom pre riadenie informačnej bezpečnosti je skupina štandardov ISO 27000, ktorá nadväzuje na pôvodnú sériu britských štandardov BS 7799 (toto platí minimálne pre európsky priestor a napr. USA sa riadi štandardami vydanými inštitúciou NIST).

Prakticky všetky európske a národné stratégie a legislatívne úpravy týkajúce sa informačnej (a kybernetickej) bezpečnosti vychádzajú z tejto skupiny štandardov.

Požiadavky na informačnú bezpečnosť pre ISVS sú zdokumentované vo Výnose MF SR o štandardoch pre informačné systémy verejnej správy[8] - Bezpečnostné štandardy, ktoré pokrývajú tieto oblasti:

- Štandardy pre architektúru riadenia (§ 29 – § 32),
- Štandardy minimálneho technického zabezpečenia (§ 33 - § 44).

Je zrejmé, že bezpečnosť údajov a funkcionality systémov je veľmi dôležitým predpokladom úspešnej transformácie z „papierovej" do digitálnej verejnej správy. V súčasnosti v spoločnosti rezonuje najmä potreba chrániť osobné údaje (nariadenie GDPR – viď. aj časť 3.4.1) a tiež hrozby tzv. kybernetickej

[8] http://www.informatizacia.sk/ext_dok-vynos_2014-55_standardy_isvs_s_prilohami/17060c

bezpečnosti (čo je podmnožina širšieho pojmu informačnej bezpečnosti), na ktoré reaguje zákon č. 69/2018 Z.z. o kybernetickej bezpečnosti[9] a týka sa ich aj zákon 45/2011 Z.z. o kritickej infraštruktúre[10].

3.2 Informačná bezpečnosť v blockchain

Táto časť poskytuje pohľad na rolu technológie blockchain pri riadení informačnej bezpečnosti – jej výhody a nevýhody voči tradičným (centralizovaným) riešeniam ale aj jej zraniteľnosti, ktoré typicky nie sú vlastné centralizovaným riešeniam a v prípade novovznikajúcich distribuovaných aplikácií na báze blockchain ich bude potrebné podrobne ďalej skúmať, testovať a sledovať ako sa budú vyvíjať metódy ich zneužívania.

Poznámky:

- Pre účely analýzy potenciálu kontrolných mechanizmov IB implementovaných v technológii blockchain budeme pod informačnými aktívami chápať najmä informačné aktíva typu údaje (dáta – reprezentujúce hodnoty veličín modelovanej reality) ale aj údaje reprezentujúce zdrojové kódy programov (smart kontraktov) spracúvajúcich tieto údaje.
- Pojem údaje pritom môže zahŕňať aj metaúdaje o iných typoch informačných aktív (napr. o informačných službách, hardvéri, softvéri, sieťových prvkoch, priestoroch obsahujúcich IKT a pod.).

3.2.1 Kontrolné mechanizmy technológie Blockchain

Ako už bolo spomenuté v úvodnom odstavci podkapitoly 3 pri diskusiách o technológii blockchain sa častokrát skloňujú pojmy zo slovníka informačnej bezpečnosti. Je to spôsobené tým, že táto technológia implicitne obsahuje viaceré moderné a veľmi účinné kontrolné mechanizmy IB, ktoré sú nevyhnutné na to aby blockchain mohol splniť základnú úlohu, pre ktorú bol vyvinutý – vytvorenie spoľahlivého a dôveryhodného (distribuovaného a decentralizovaného) komunikačného prostredia medzi rôznymi „typmi“ účastníkov (účastníkov z rôznych subjektov, ktorí si vzájomne potenciálne nedôverujú) a to bez toho, aby takýto komunikačný systém musela organizovať, riadiť a dohladovať za týmto účelom určená centrálna autorita.

V súvislosti s „trojuholníkom“ výpočtu informačného rizika (Obrázok 7) platí, že kontrolné mechanizmy blockchainu sa zameriavajú na redukovanie inherentného rizika pomocou znižovania zraniteľnosti informačných aktív typu „údaje“ (viď. poznámky v úvodnom odstavci tejto podkapitoly). Tieto implicitné KM blockchainu nemajú ambíciu znižovať pravdepodobnosť hrozby ani negatívny dopad na informačné aktíva – toto sú z hľadiska technológie blockchain externé, neovplyvniteľné faktory.

KM blockchainu pritom chránia údaje „len“ voči niektorým typom hrozieb, zato však zraniteľnosť údajov dokážu znížiť zásadným spôsobom. Jedná sa najmä o zraniteľnosti voči hrozbám, ktorých dopad spočíva v nesplnení základných cieľov IB, t.j. v:

- nedostupnosti údajov,
- strate alebo zničení údajov,
- zámernom alebo náhodnom modifikovaní údajov,

[9] https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/69/
[10] https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2011/45/20190101

- popretí odoslania alebo prijatia údajov,
- nedoručení, opakovaní (duplikovaniu), rozsynchronizovaní správ alebo transakcií a čiastočne aj
- vkladaní falošných údajov a neautorizovanom prístupe k citlivým údajom.

Kontrolné mechanizmy, ktoré poskytuje technológia blockchain „svojim" distribuovaným aplikáciám majú vo všeobecnosti iný charakter ako využívajú bežné (tradičné) aplikácie a informačné systémy. Základné porovnanie KM je uvedené v nasledujúcej tabuľke.

Poznámky:

- Použitá klasifikácia KM má zdôrazniť rozdiely medzi blockchainom a tradičnými riešeniami, nie je pritom úplná z hľadiska teórie informačnej bezpečnosti.
- Keďže technológia blockchain slúži na zaznamenávanie len pomerne jednoduchých údajových viet (transakcií, správ, udalostí alebo predpisov na ich spracovanie), nemusí jej porovnanie (v oblasti riadenia IB) s tradičnými informačnými systémami, ktoré využívajú častokrát veľmi rozsiahle a komplikované databázy vyznieť spravodlivo. Preto je potrebné vhodne „nakalibrovať" očakávania a tradičné riešenie si radšej predstaviť ako pomerne jednoduchú centralizovanú aplikáciu s jednoduchou databázou, avšak umožňujúcu vzdialený prístup mnohým používateľom vo viacerých roliach.

Klasifikácia KM IB:		**Riešenie využívajúce:**	
Kľúč	**Alternatíva**	**Technológiu blockchain**	**Tradičnú technológiu**
Podľa momentu identifikovania incidentu vo vzťahu k realizácii negatívneho dopadu	Preventívne	Kľúčové pre zabezpečovanie cieľov IB na úrovni infraštruktúry blockchain.	Snaha uprednostňovať preventívne KM. Avšak častokrát pre nižšiu účinnosť sú kompenzované súvisiacimi detektívnymi KM. Typicky má na výslednej množine implementovaných KM významný podiel skupina detektívnych KM (čo vytvára značný priestor, ale predstavuje aj významné náklady, pre prácu interného alebo externého auditu a rôznych analytických a forenzných tímov).
	Detektívne	Implementované najmä na aplikačnej úrovni (distribuovaných aplikáciách, ktoré využívajú blockchain) za účelom podpory biznis procesov, ktoré vyžadujú transparentnosť, auditovateľnosť, analyzovateľnosť histórie vykonaných úkonov, transakcií alebo správ. Opierajú sa pritom o preventívne KM implementované v technológii blockchain.	
Podľa úrovne implementácie v systéme riadenia IB, resp. podľa toho či môžu vytvárať len „nutnú" (všeobecné) alebo aj „postačujúcu" (aplikačné) podmienku splnenia cieľov IB	Všeobecné	Všeobecné KM (IT general controls) sú pre blockchain dôležité pre zaistenie IB pri vývoji, riadení zmien a nasadzovaní samotnej blockchain infraštruktúry ale aj jednotlivých distribuovaných aplikácií do prevádzkového prostredia. ITGC hrajú tiež kľúčovú úlohu pri zabezpečení bodov, v ktorých dochádza k prenosu údajov zo zdrojových systémov (napr. ERP systému alebo senzorov IoT) do blockchainu (t.j. pri prevencii pred vložením nesprávnych údajov „navždy" do blockchainu).	ITGC sú veľmi dôležitou súčasťou ochrany informačných aktív. Uistenie sa o vhodnom návrhu a prevádzkovej účinnosti jednotlivých všeobecných KM je nutnou podmienkou pre spoliehanie sa na konkrétne aplikačné KM (napr. bez správneho riadenia zmien a logických prístupov nie je možné robiť závery ohľadom nastavenia a fungovania kontrolných mechanizmov schvaľovania workflow kroku na základe „kontroly štyroch očí").
	Aplikačné	Implementované v distribuovaných aplikáciách využívajúcich blockchain – viď. poznámky k detektívnym KM.	Používajú sa najmä pre implementáciu biznis kontrolných mechanizmov pri

Klasifikácia KM IB:		Riešenie využívajúce:	
Kľúč	**Alternatíva**	**Technológiu blockchain**	**Tradičnú technológiu**
			elektronizácii biznis procesov. Ich sila typicky závisí od príslušných ITGC.
Podľa spôsobu implementácie	Technické	Technológia blockchain ponúka „svojim" distribuovaným aplikáciám veľmi silné KM tvorené unikátnou kombináciou kryptografických algoritmov a decentralizovaných komunikačných protokolov a stratégií.	Patria sem všetky aplikačné KM a časť ITGC (napr. systém logovania, systém autorizovania fyzických a logických prístupov, systém zálohovania a pod.). Typicky je nutné ochranu pomocou technických KM doplniť aj organizačnými a procesnými KM.
	Organizačné a procesné	Tieto kontrolné mechanizmy sú vďaka KM z iných kategórií a decentralizácií distribuovanej aplikácie využívajúcej blockchain počas jej prevádzky prakticky nepotrebné. Organizačné a procesné KM sú však dôležité v iných fázach životného cyklu technológie blockchain alebo distribuovanej aplikácie – viď. popis k všeobecným kontrolným mechanizmom IB.	Prekrývajú sa s kategóriou všeobecných KM. Od ich návrhu a účinnosti závisí spoľahlivosť technických a aplikačných KM.

Tabuľka 6: Klasifikácia KM a porovnanie blockchain vs. tradičné riešenia

Ako vyplýva z tejto tabuľky (Tabuľka 6) silnou stránkou technológie blockchain v oblasti riadenia informačnej bezpečnosti je súbor implicitne zabudovaných kontrolných mechanizmov klasifikovaných ako [preventívne, aplikačné, technické]. Takto „namiešané" kontrolné mechanizmy majú dobrý potenciál odolávať hrozbám, za ktorých pôvodom stojí či už náhodné alebo úmyselné konanie človeka. Hrozby tohto pôvodu pritom predstavujú rozhodujúcu skupinu hrozieb s typicky najvyšším potenciálom negatívnych dopadov.

Informačná ochrana tradičných riešení má tiež tendenciu opierať sa najmä o preventívne, aplikačné a technické kontrolné mechanizmy, avšak výber a kombinácia týchto KM častokrát neprináša synergický efekt ako je tomu pri technológii blockchain. Napr.:

- použitie elektronického podpisu pre zaistenie autenticity a integrity správ nie je dostatočne pevne zviazané s kontrolnými mechanizmami zaisťujúcimi nezmazateľnosť (resp. nezničiteľnosť) týchto správ alebo s KM brániacimi antedatovaniu (ak nie je použitá kvalifikovaná časová pečiatka, čo je pomerne pokročilý KM, v súčasnosti nie typicky používaný v tradičných riešeniach) a teda aj „dodatočnému vymieňaniu" takýchto správ po vzájomnej dohode medzi odosielateľom a prijímateľom,
- prípadne nie je možné zabrániť uloženiu správ, s ktorými síce súhlasí ich odosielateľ a prijímateľ ale porušujú sémantické pravidlá dohodnuté v rámci širšej skupiny zainteresovaných používateľov a tým porušujú celkovú integritu a konzistenciu databázy (obchádzajú tzv. konsenzus, ktorý využívajú blockchainové riešenia).

Táto nedostatočná synergia najúčinnejších KM (preventívnych, aplikačných, technických) vedie k potrebe ďalej zvyšovať informačnú bezpečnosť pomocou implementácie dodatočných a kompenzačných KM z triedy všeobecných KM (ITGC), detektívnych a organizačno-procesných kontrolných mechanizmov.

Výsledkom tejto taktiky je „cibuľovité" nabaľovanie kontrolných mechanizmov, ktoré sa navzájom podmieňujú, prekrývajú a dopĺňajú. Výsledná úroveň informačnej bezpečnosti sa takýmto spôsobom síce zvyšuje, avšak častokrát je náročné priradiť pridanú hodnotu bezpečnosti konkrétnym KM (a teda uistiť sa o hospodárnosti rozhodnutí ohľadom ich implementácie). S týmto prístupom je tiež spojená vyššia cena implementácie a najmä udržateľnosti takéhoto systému kontrolných mechanizmov (viď. aj Obrázok 8).

Ďalej sa budeme venovať vzťahu medzi všeobecnými vlastnosťami technológie blockchain a cieľmi informačnej bezpečnosti. Pre tento účel budeme na blockchain pozerať ako na systém:

- distribuovaný (D - distributed),
- otvorený (O – open),
- konsenzuálny (C - consensual) a
- zaisťujúci nemennosť údajov (I - immutable).

Argumenty pre a proti dosahovaniu jednotlivých cieľov informačnej bezpečnosti prostredníctvom týchto vlastností blockchain sú uvedené v nasledujúcej tabuľke. Ciele informačnej bezpečnosti označujeme ako:

- C – confidentiality (dôvernosť),
- I – integrity (integrita, vrátane nepopierateľnosti pôvodu a prijatia),
- A – availabilty (dostupnosť).

Cieľ IB / Vlastnosť blockchain	**D**istributed	**O**pen	**C**onsensual	**I**mmutable
Confidentiality	(-) citlivé údaje sa nachádzajú na všetkých uzloch; tieto uzly môžu byť pre vlastníka údajov neznáme (nemusí vedieť kde všade sa fyzicky nachádzajú alebo budú nachádzať) (+) zabezpečí spoľahlivé distribuovanie verejných asymetrických kľúčov, pomocou ktorých je možné citlivý obsah zašifrovať (priamo alebo prostredníctvom symetrického kľúča, ktorý je šifrovaný týmto verejným kľúčom) tak, aby bol viditeľný len pre daného(ých) adresáta(ov)	(-) citlivé údaje sú viditeľné (+) citlivé údaje je možné šifrovať – viď. komentár v [C, D] (+) citlivé údaje je možné uložiť „off-chain“	(+) potreba všeobecnej zhody uzlov siete môže slúžiť ako prevencia pred vložením nesprávnych citlivých údajov (napr. nesprávnych, neúplných, neaktuálnych osobných údajov); pozn.: viac sa však dotýka cieľov zaistenia integrity	(-) potenciálny konflikt s požiadavkou GDPR o práve na likvidáciu osobných údajov (-) zašifrované citlivé údaje zostávajú v blockchaine „navždy“, v prípade prelomenia použitej šifry, môže dôjsť k ich prezradeniu (následná modernizácia šifrovacích algoritmov „nezachráni“ pôvodné záznamy) (+) nemôže dôjsť k zmene platných verejných asymetrických kľúčov, ktoré môžu byť použité na ochranu citlivých údajov
Integrity	(+) každý uzol má prístup k verejnému kľúču každého používateľa a vie overiť autenticitu každého údajového záznamu (+) autor údajov nemôže žiadnemu inému uzlu poprieť svoje autorstvo (nepopierateľnosť pôvodu) (+) v kontexte predošlého bodu je pomerne jednoduché implementovať KM, ktorý zabezpečí nepopierateľnosť prijatia správy adresátom(mi) (t.j. adresát najskôr podpíše doručenku a až potom získa obsah	(+) vysoká miera transparentnosti, auditovateľnosti a analyzovateľnosti údajov môže byť použitá na udržiavanie konzistencie údajov (na aplikačnej úrovni potom aj súladu s relevantnými predpismi a normami) (+) každý používateľ si môže samostatne overiť (uistiť sa) správnosť spracovania všetkých údajov v blockchain, t.j. či nastali podmienky na spracovanie a transformáciu vstupných údajov na výstupné; v prípade uloženia predpisu transformácie –	(+) potreba všeobecnej zhody uzlov siete sa využíva ako prevencia pred vložením nesprávnych údajov (napr. neúplných, neexistujúcich, nepresných účtovných dokladov; nesprávnych, neúplných, neaktuálnych osobných údajov a pod.) (+) spravodlivý (náhodný) výber uzla zodpovedného za vytvorenie nového bloku záznamov a nutnosť konsenzu ostatných uzlov pri zápise nového bloku (ak má blok „prežiť“ musí sa jednať o rozhodnutie štatistickej	(+) údaje nemôžu byť modifikované ani vymazané neautorizovaným alebo náhodným spôsobom (-) údaje nemôžu byť modifikované ani vymazané ani autorizovaným spôsobom (+) zmenu alebo zneplatnenie pôvodných údajov je možné vykonať vložením nového opravného záznamu logicky previazaného s pôvodným (+) nemôže dôjsť k zmene platných verejných asymetrických

Cieľ IB / Vlastnosť blockchain	**D**istributed	**O**pen	**C**onsensual	**I**mmutable
	správy)	smart kontraktu vidí aj samotný algoritmus spracovania; (napr. každý používateľ môže vidieť anonymizované výsledky hlasovania a môže si spočítať výsledok volieb a overiť korektnosť ich priebehu) (+) každý používateľ vidí verejný kľúč každého iného používateľa a môže s ním bezpečne komunikovať (pre overenie autentickosti verejného kľúča ani nepotrebuje jeho certifikát – viď. príslušný komentár v [I, I]) (+) vedomie, že všetci „ma vidia" odrádza potenciálnych podvodníkov – viď. aj príslušný komentár v [I, I]	väčšiny) významne eliminuje možnosť podvodného konania uzlov zodpovedných za vytváranie nových blokov (podľa princípu: všetci férovo konajúci sa ľahko zhodnú na tom čo je pravda podľa daných pravidiel ale podvodníci sa na jednej spoločnej verzii podvodu zhodnú oveľa ťažšie)	kľúčov, ktoré sa používajú aj pre zaistenie autenticity údajov (+) verejné asymetrické kľúče nie je potrebné podpisovať certifikačnou autoritou pre zaistenie ich autenticity (-) bod vyššie kladie zvýšené nároky na registračnú autoritu, ktorá musí zabezpečiť spoľahlivé previazanie identity používateľa s jeho verejným kľúčom pri jeho vkladaní do blockchainu (+) vedomie, že nie je možné dodatočne „upratovať stopy" významným spôsobom odrádza potenciálnych podvodníkov (príprava podvodu vopred by musela byť dokonalá, čo typicky nie je možné)
Availability	(+) extrémna redundancia údajov (každý uzol môže obsahovať celý blockchain záznamník) prakticky dokonale zaistí dostupnosť údajov v prípade zničenia alebo dočasného výpadku aj podstatnej časti siete (-) rýchlosť šírenia údajov (skorá dostupnosť novo vytvorených údajov) nemusí byť dostatočná kvôli veľkému počtu uzlov, s ktorými je potrebné údaje synchronizovať	(+) otvorenosť – viditeľnosť všetkých údajov všetkými účastníkmi je tiež prejavom zvýšenej dostupnosti údajov	(-) rýchlosť šírenia údajov (skorá dostupnosť novo vytvorených údajov) nemusí byť dostatočná kvôli dobe trvania získania konsenzu uzlov (+) pri moderných konsenzuálnych algoritmoch (napr. DPoS) je možné dosiahnuť vysoké rýchlosti šírenia údajov (generovanie nového bloku rádovo v jednotkách sekúnd; rádovo tisíce transakcií za sekundu)	(+) nemožnosť zmeny pôvodných údajov je za predpokladu, že bola zachovaná ich integrita pred vložením do blockchainu postačujúcou podmienkou pre zaistenie dostupnosti konzistentných, úplných, presných a existujúcich (nevymyslených) údajov

Tabuľka 7: Vlastnosti blockchain vs ciele informačnej bezpečnosti

3.2.2 Hrozby a zraniteľnosti technológie Blockchain

Samozrejme aj samotná technológia blockchain a ju využívajúce distribuované aplikácie sú informačnými aktívami, s ktorými sú spojené určité hrozby a zraniteľnosti. Do rozhodovania o využití technológie blockchain pri riešení konkrétneho problému alebo uprednostnením či ponechaním tradičného riešenia je potrebné zahrnúť aj výsledky analýzy informačných rizík spojených s použitím jedného aj druhého typu riešenia.

Poznámka: Pojem riziko budeme ďalej používať, v zmysle už uvedenej definície, ako výslednú kombináciu pojmov hrozba, zraniteľnosť a dopad na informačné aktívum.

V predchádzajúcich častiach už boli spomenuté rôzne riziká blockchain riešení ako:

- Riziká spojené s riadením asymetrických šifrovacích kľúčov, najmä s bezpečným uchovávaním privátneho kľúča (čo je však problematika dôležitá aj mimo diskusie o blockchaine).
- 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).
- Riziká spojené so spoliehaním sa na správne fungovanie konsenzuálnych algoritmov, riadením smart kontraktov a iných „novodobých" prvkov technológie blockchain (ktoré na rozdiel napr. od použitých kryptografických algoritmov alebo sieťových protokolov neprešli takým vývojom a neboli podrobené „testovaním v praxi" v takom rozsahu) – je preukázaná správnosť týchto algoritmov a mechanizmov matematickými dôkazmi? Alebo sú aspoň dostatočne otestované všetky aspekty týchto algoritmov a mechanizmov?

  Poznámka: V súčasnosti je teoreticky spracovaných mnoho typov problémov a útokov v závislosti na konkrétnej implementácii technológie blockchain. Napr. pri použití PoS (proof of stake) konsenzuálneho algoritmu je možné zaoberať sa témami[11]: Nothing at stake problem, Initial Distribution Problem, Long Range Attack, Bribe Attack, Coin Age Accumulation Attack, Precomputing Attack a pod.
- Riziko vyzradenia všetkých údajov uložených v blockchain v zašifrovanej podobe (s cieľom chrániť ich dôvernosť) v prípade prelomenia použitej šifry (typicky použitím hrubej výpočtovej sily pomocou tzv. kvantového počítača). V takomto prípade bude extrémne zložité (vzhľadom na nemennosť a distribuovanosť údajov v blockchain) „prešifrovať" tieto pôvodné a kompromitované údaje pomocou dodatočne zmodernizovaných šifrovacích algoritmov, resp. komplexnejších kľúčov.

  Poznámka: Zároveň chápeme, že toto riziko je spojené najmä s používaním asymetrickej kryptografie RSA a pravdepodobnosť prelomenia šifry je pri použití kryptografie založenej na eliptických krivkách (ktorá je typicky používaná v moderných blockchain riešeniach namiesto RSA kryptografie) podstatne nižšia až zanedbateľná.
- Riziká súvisiace s vložením nesprávnych alebo neautorizovaných údajov do blockchain, ktoré v ňom zostanú „naveky" (toto je možné riešiť vhodným komunikačným protokolom, ktorý napr. následne do blockchainu zaradí opravný alebo storno záznam a logicky ho prepojiť s pôvodným chybným záznamom). Obdobne je potrebné riadiť riziká spojené s kvalitou údajov a ich ďalším spracovaním a interpretáciou pri ich výstupe z blockchainu, t.j. od momentu, kedy blockchain prestáva zabezpečovať ich nemennosť.

  Poznámka: Niekedy sa v súvislosti s blockchainom nesprávne konštatuje, že „blockchain je zárukou pravdy". V skutočnosti však blockchain nie je ani len „zárukou správnosti", je však „zárukou nemennosti" (čo je samé o sebe veľmi užitočná vlastnosť). O tom či je v blockchaine uložený údaj „pravdivý" alebo „správny" rozhoduje zdroj tohto údaju (človek alebo integrovaný informačný systém) – jeho sémantika, validačné pravidlá a iné kontrolné mechanizmy.

K týmto rizikám je potrebné pridať aj ďalšie dnes diskutované riziká ako napr.:

- Strata decentralizácie uzlov blockchain siete pri získaní kontroly nad viac ako 50% uzlami tejto siete (tzv. 51% útok, napr. z perspektívy prípravy tohto dokumentu nedávno zdokumentovaný incident[12]).

  Poznámka: Takýto útok je v skutočnosti permanentným stavom v blockchain riešeniach označovaných ako privátne. Javí sa, že experimentovanie s takýmito „nie poctivými" blockchain riešeniami bude

[11] Proof of Stake versus Proof of Work, White Paper, BitFury Group, 2015

[12] https://www.theverge.com/2019/1/9/18174407/ethereum-classic-hack-51-percent-attack-double-spend-crypto

v najbližšej dobe prevládať a to až pokým si táto inovatívna technológia nezíska dostatočnú dôveru a nebude schopná zodpovedať na všetky relevantné pochybnosti a nebude pripravená reagovať na relevantné riziká. Uvedené môže čiastočne platiť aj pre tzv. konzorčné blockchainy a to v prípade ak majú členovia konzorcia (inak typicky právne samostatné entity alebo na prvý pohľad nezávislí používatelia) nejakého spoločného „majiteľa" (viď. napr. prípad použitia blockchainu v časti 5.4.2 Rozšírenie viditeľnosti v dodávateľských reťazcov).

- Riziká postupnej degradácie systému a straty schopnosti poskytovať distribuovaným aplikáciám dostatočné výkonové a prevádzkové parametre, napr. pri nekontrolovanom pribúdaní uzlov siete alebo vkladaní smart kontraktov (zložité, príp. bez ukončovacích podmienok, často a na mnohých uzloch spúšťané a pod.).
- Riziká súvisiace s chýbajúcimi reguláciami a štandardami pre oblasť decentralizovaných riešení (ak je vôbec snaha o reguláciu a štandardizáciu v prostredí z princípu vylučujúcom autority vôbec zmysluplná a možná).
- Riziká spojené s nejasným rozdelením právomocí a povinností súvisiacich so strategickým (governance) a projektovým riadením a riadením prevádzky, vrátane dostatočného motivovania prevádzkovateľov uzlov (kľúčová časť blockchain infraštruktúry), aby ku generovaniu nových údajových blokov pristupovali zodpovedne.

  Poznámka: Javí sa, že jedna z najsilnejších vlastností blockchain, ktorou je decentralizácia a vylúčenie centrálnych autorít môže byť zároveň jeho významnou slabou stránkou. Kto sa podujme byť sponzorom a kto riešiteľom projektu a aká bude ich motivácia na implementáciu distribuovaného a decentralizovaného riešenia slúžiaceho rovnocenne viacerým nezávislým entitám, keď ich roly typicky skončia v momente uvedenia riešenia do prevádzky?

Vzhľadom na to, že vývoj a prevádzkovanie blockchainových a iných decentralizovaných riešení je pomerne mladým odvetvím v rámci softvérového inžinierstva (nehovoriac o tom, že aj samotné SW inžinierstvo je relatívne mladým odborom napr. v porovnaní so stavebníctvom), je potrebné pamätať na to, že o niektorých relevantných rizikách dnes ešte ani nevieme a o niektorých len tušíme, zatiaľ však ešte nemáme prakticky overené, aký priebeh a dopady môžu mať incidenty s nimi spojené, resp. ako je potrebné na ne reagovať a či je to vôbec možné.

Podrobnejšia analýza rizík technológie blockchain nie je predmetom tohto dokumentu. Vzhľadom na veľmi rôznorodé možnosti implementácie technológie blockchain (použité kryptografické algoritmy, zvolený spôsob dosiahnutia konsenzu v sieti, rozsah a typy služieb poskytované na aplikačnej úrovni, pravidlá a topológia siete a pod.), ani nie je možné takúto analýzu zovšeobecňovať. Analýzu rizík je potrebné spracovať pre konkrétnu implementáciu technológie blockchain a potom pre konkrétnu distribuovanú aplikáciu a jej integráciu na okolité IT prostredie (napr. pôvodný podnikový systém, resp. informačný systém verejnej správy).

3.2.3 Závery z hodnotenia IB poskytovanej technológiou blockchain

Aplikácie využívajúce pre ukladanie a prípadne aj spracovanie svojich údajov blockchain majú štandardne k dispozícii sadu veľmi účinných kontrolných mechanizmov informačnej bezpečnosti, ktoré im poskytuje táto technológia veľmi spoľahlivým a konzistentným spôsobom.

Ako sme už uviedli vyššie blockchain si dokáže poradiť s mnohými incidentmi informačnej bezpečnosti spôsobenými zlyhaním technických prostriedkov (individuálne poruchy alebo výpadky hardvéru v jednotlivým uzloch siete alebo zdržania či chyby pri prenose údajov medzi uzlami a pod.). Naviac blockchain vie odolávať alebo významne prispieť k odhaľovaniu mnohých typov úmyselných útokov na informačnú bezpečnosť, ale aj náhodných chýb, nepresností, vynechaní alebo omeškaní spôsobených

autorizovanými používateľmi informačných systémov.

Z vyhodnotenia spôsobov implementovania a kombinovania rôznych typov kontrolných mechanizmov informačnej bezpečnosti a porovnania medzi tradičným riešením a riešením využívajúcim technológiu blockchain vyplýva tento, podľa nášho názoru kľúčový, záver vyznievajúci v prospech technológie blockchain:

- zatiaľ čo kontrolné mechanizmy typicky implementované v tradičných riešeniach dokážu poskytnúť primeranú úroveň uistenia, že ciele informačnej bezpečnosti týkajúce sa informačných aktív typu údaje môžu byť splnené, tak
- technológia blockchain, prostredníctvom jedinečnej kombinácie implicitne zabudovaných kontrolných mechanizmov dáva oveľa silnejší prísľub splnenia týchto cieľov, a to najmä prísľub zachovania integrity a dostupnosti údajov – údaje uložené v blockchaine sú s takmer určitosťou dostupné, autentické a nepopierateľné a od momentu ich vloženia do blockchainu nedošlo k ich modifikovaniu alebo vymazaniu.

Netreba pritom podľahnúť prílišnému optimizmu a uvedomovať si informačné riziká technológie blockchain, ktorým sme sa venovali v predošlej časti. Pri zavádzaní inovatívnych (až disruptívnych - prelomových) technológií k akým patrí aj blockchain, ktoré majú veľký potenciál ovplyvniť a zmeniť mnohé aspekty nášho fungovania a podnikania, je potrebná špeciálna obozretnosť vo vzťahu k informačnej bezpečnosti. Je potrebné si uvedomiť, že početnosť a typy útokov na tieto technológie budú pribúdať minimálne takou rýchlosťou ako budú pribúdať riešenia využívajúce tieto technológie.

Blockchain má tiež veľký potenciál stať sa nástrojom prevencie rôznych typov podvodov uskutočňovaných v podnikových procesoch alebo procesoch verejnej správy. Vychádzame z predpokladu, že podvodníci často postupujú tak, že podvod, dopredu pripravia len čiastočne a neskôr sa spoliehajú na dodatočné upravovanie a mazanie elektronických stôp (keď si myslia, že majú takú možnosť). Keďže blockchain úpravu a mazanie údajov vylučuje, úspešne vykonaný podvod by musel byť vopred dokonale pripravený, čo by vyžadovalo podstatne vyššie náklady, čas a zrejme aj skúsenosti. Naviac by takýto podvodník prežil ďalšie obdobia neistoty, či predsa len niekedy v budúcnosti niekto náhodne alebo systematicky nevypátra nejakú medzeru v jeho starostlivo pripravenom postupe.

Tieto „nástrahy" blockchainu budú mať zrejme značný odrádzajúci účinok pre podvodné konanie rôzneho druhu. Paradoxne môžu tiež vyvolať odpor voči zavádzaniu tejto prelomovej technológie do niektorých procesov alebo odvetví – najmä tam, kde je drobné, z pohľadu používateľa neškodné, „prispôsobovanie si" niektorých údajov (napr. časových) alebo procesných úkonov (napr. dobrovoľné zdieľanie používateľských účtov kvôli zastupiteľnosti alebo iné obchádzanie formálnych pravidiel, ktoré za istých okolností môžu viesť k znefunkčneniu alebo zablokovaniu procesov) je bežnou súčasťou práce. Zdá sa, že aj otvorenosti a transparentnosti bude potrebné stanoviť určité limity – viď. tiež riziko potenciálneho rozporu s požiadavkami GDPR, ktoré sa samozrejme netýka len blockchainu ale vo všeobecnosti aktuálnej problematiky spracovania „veľkých dát".

Čo sa týka ekonomiky, t.j. nákladov na kontrolné mechanizmy informačnej bezpečnosti a prínosov zo zníženia negatívnych dopadov incidentov informačnej bezpečnosti, porovnanie medzi tradičným a blockchain riešením poskytuje diagram nižšie (Obrázok 8).

Poznámka: Priebeh funkcií nevychádza zo skutočných meraní. Reprezentujú len známe hypotetické

modely štandardných priebehov funkcií nákladov na informačnú bezpečnosť[13]. Účelom diagramu je graficky demonštrovať názor autora tohto dokumentu získaný na základe vykonaných kvalitatívnych analýz.

Samozrejme kľúčovým kritériom pri rozhodovaní pomocou akej stratégie (a technológie) a akými kontrolnými mechanizmami budú informačné riziká redukované na akceptovateľnú mieru (tak aby boli dostatočne splnené ciele informačnej bezpečnosti), je minimalizácia nákladov na implementáciu KM plus nákladov z negatívnych dopadov incidentov, ktoré sú prejavom reziduálnych rizík.

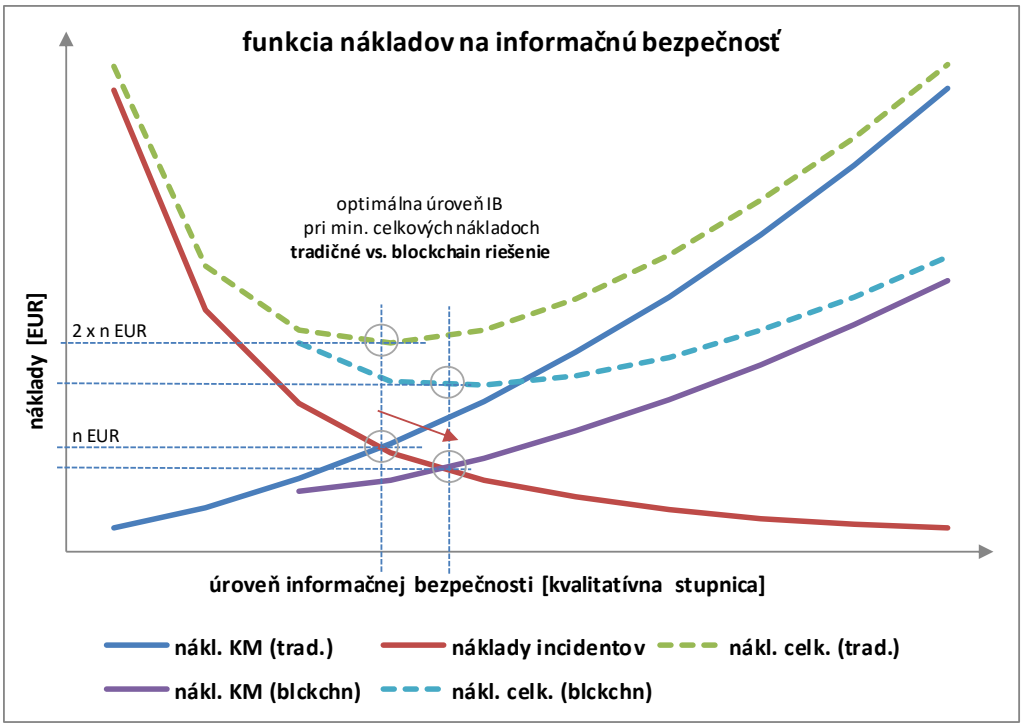
Pre diagram (Obrázok 8) platia tieto konštatovania a predpoklady:

- červená čiara: funkcia nákladov na dopady v závislosti na úrovni (výške) informačnej bezpečnosti je spoločná pre tradičné aj blockchain riešenie,
- modrá čiara: funkcia nákladov na KM v závislosti na úrovni informačnej bezpečnosti v tradičnom riešení (absolútnu bezpečnosť nie je možné dosiahnuť => pri červenej čiare blížiacej sa k nule rastie do nekonečna),
- fialová čiara: funkcia nákladov na KM v závislosti na úrovni informačnej bezpečnosti v blockchain riešení (absolútnu bezpečnosť nie je možné dosiahnuť => pri červenej čiare blížiacej sa k nule rastie do nekonečna avšak nie tak strmo ako modrá čiara), pričom:
  - počiatočné náklady na blockchain riešenie, ktoré už implicitne obsahuje účinné KM sú vyššie ale zároveň zaručujú „od začiatku“ vyššiu mieru bezpečnosti => začína „neskôr“ a „vyššie“ ako modrá čiara,
  - dodatočné zvýšenie informačnej bezpečnosti buď nie je potrebné alebo spočíva len v jednoduchších opatreniach, t.j. nie je také drahé => nerastie tak rýchlo ako modrá čiara,
- zelená prerušovaná čiara: výsledný priebeh nákladov na informačnú bezpečnosť pri použití tradičného riešenia, t.j. súčet červenej a modrej čiary,
- tyrkysová prerušovaná čiara: výsledný priebeh nákladov na informačnú bezpečnosť pri použití blockchain riešenia, t.j. súčet červenej a fialovej čiary.

Diagram znázorňuje, že minimálne náklady na informačnú bezpečnosť sa v oboch prípadoch dosahujú v priesečníku funkcie nákladov na dopady a funkcie nákladov na KM (vďaka spomínanému štandardnému priebehu funkcií nákladov na IB). Zároveň pri použití blockchain riešenia pozorujeme posun priesečníka týchto funkcií smerom vpravo a nadol (červená šípka). To znamená, že riešenie blockchain umožňuje dosiahnuť vyššiu úroveň informačnej bezpečnosti pri nižších nákladoch na kontrolné mechanizmy informačnej bezpečnosti.

Poznámka: Aj v tomto prípade je potrebné zdôrazniť, že pod tradičným riešením máme na mysli riešenie zredukované rozsahom a obsahom na úroveň typickej distribuovanej aplikácie využívajúcej technológiu blockchain (viď. príslušná poznámka v časti 3.2.1 Kontrolné mechanizmy technológie Blockchain).

[13] napr. podľa: Computers & Security: Introducing cybernomics - A unifying economic framework for measuring cyber risk, 2017



Obrázok 8: Funkcia nákladov na informačnú bezpečnosť (tradičné vs. blockchain riešenie)

3.3 Blockchain ako kontrolný mechanizmus

Pre lepšie pokrytie problematiky „Informačná bezpečnosť v blockchain" je vhodné pozrieť sa na technológiu blockchain nielen ako na technológiu, ktorá obsahuje a používa kontrolné mechanizmy informačnej bezpečnosti, ale zároveň aj ako na nástroj, pomocou ktorého je možné vytvárať ďalšie – zložené a veľmi účinné kontrolné mechanizmy IB.

V zmysle klasifikácie kontrolných mechanizmov uvedenej v časti 3.2.1 Kontrolné mechanizmy technológie Blockchain sa bude typicky jednať o kontrolné mechanizmy z kategórie [preventívne, ale aj detektívne, všeobecné, technické].

Zoznam aplikácií (prípadne nápadov), ktoré môžu mať povahu kontrolných mechanizmov využívajúcich technológiu blockchain pre zlepšenie svojich možností chrániť iné informačné aktíva, môže byť veľmi rozsiahly. Preto nižšie uvedený zoznam je potrebné chápať ako základný zdroj inšpirácie pre ďalšie analyzovanie potenciálu technológie blockchain v oblasti implementácie kontrolných mechanizmov informačnej bezpečnosti.

Poznámka: Ďalšie prípady použitia technológie blockchain sú rozpracované v podkapitolách 5.3 a 5.3.3.

3.3.1 Log udalostí

Spoľahlivé úložisko (ďalej aj „log") udalostí z rôznych navzájom súvisiacich zdrojov predstavuje kľúčový detektívny nástroj systému riadenia informačnej bezpečnosti (ISMS), pomocou ktorého sa vykonáva monitorovanie, vyhodnocovanie a eskalovanie incidentov z oblasti prevádzky informačných a komunikačných technológií (ďalej aj „IKT") a systémov (najmä súlad s príslušnými SLA dohodami), správanie interných a externých používateľov IKT (najmä súlad s politikou informačnej bezpečnosti), ale

tiež vykonávanie podnikových procesov alebo procesov verejnej správy (súlad s príslušnými pravidlami, procedúrami a legislatívnymi požiadavkami).

Okrem toho, že spoľahlivý log udalostí musí obsahovať všetky relevantné údaje, ktoré musia byť úplné, presné a existujúce (t.j. nie vymyslené), musí takýto log byť stály – nemenný (nemal by pritom existovať „oficiálny" dôvod na takúto zmenu – čo sa raz stalo je fakt, ktorý má zostať zapísaný). Na takúto úlohu sa veľmi dobre hodí zápis údajov o udalostiach do blockchainu.

Implementácia logu udalostí využívajúca blockchain môže mať takéto vlastnosti:

- do blockchain sa zapisujú len základné atribúty: kedy, kto, čo, komu, kde, prečo, v akej hodnote a pod.
- jednotlivé udalosti nemusia byť v blockchain vzájomne logicky previazané, analýza súvislostí a interpretácia zistení sa vykoná na aplikačnej úrovni (dôležitú rolu pritom zohrá spoľahlivá časová značka na udalosti),
- ďalšie prípadné údaje (prílohy) sa ukladajú do úložiska mimo blockchain (off–chain), do blockchain sa uloží hash tejto prílohy, ktorý ju spoľahlivo „zviaže" s ostatnými údajmi o zaznamenanej udalosti,
- kontrolné mechanizmy blockchainu zabezpečujú:
  - autenticitu a nepopierateľnosť pôvodu (každá udalosť vložená do blockchainu je podpísaná privátnym kľúčom „autora" a každý „čitateľ" logu sa o autenticite a integrite udalosti môže presvedčiť – má k dispozícii v blockchaine uložený verejný kľúč autora),
  - spoľahlivosť časovej značky – okrem času, ktorý udalosti pripisuje jej autor (typicky zdrojový systém), je záznam opatrený aj časom, kedy nastala jeho validácia (pridáva nezávislý – „náhodne" vybraný validátor, svedok, resp. ťažiar),
  - už spomínanú nemennosť (záznamy nie je možné modifikovať ani zmazať) a tiež vysokú dostupnosť (neprerušovaný prístupu k údajom a ich nezničiteľnosť).

Poznámka: Tento prípad použitia technológie blockchain môže byť analogicky aplikovaný aj pre spoľahlivé zaznamenávanie iných typov udalostí (vo všeobecnosti akýchkoľvek). V prípade verejnej správy – napr. udalostí týkajúcich sa spracovania agend na určitom úseku správy a to zvlášť v prípadoch, kedy sa príslušné procesy týkajú viacerých (až mnohých) entít – inštitúcií verejnej správy, ale aj občanov a podnikateľov, napr.:

- udalosti na úseku zbraní a streliva, ktoré generujú entity ako: MV SR, riaditeľstvá PZ SR, výrobcovia zbraní, predajcovia zbraní, prevádzkovatelia strelníc, držitelia zbrojných preukazov, osoby posudzujúce spôsobilosť a bezúhonnosť držiteľov ZP a ďalší) alebo
- udalosti súvisiace so stavebným a územným konaním, ktoré generujú entity ako: občania, podnikatelia MDV SR, stavebné úrady a množstvo ďalších zainteresovaných strán, ktoré sa ku konaniam vyjadrujú

3.3.2 Správa informačných aktív a konfigurácií

Zodpovedná správa informačných aktív a konfigurácií je základným predpokladom úspešného fungovania modernej servisne orientovanej IT organizácie, či už poskytuje IT služby interným alebo externým zákazníkom. Pre efektívne poskytovanie IT služieb v zmysle dohodnutých výkonových a bezpečnostných úrovní (podľa SLA – Service level agreement), je potrebné pracovať s aktuálnymi a spoľahlivými informáciami o stave a vzájomných súvislostiach medzi položkami informačných aktív (služba, hardvér, sw server, sw aplikácia, sw licencia, operačný systém, logický uzol, komponent technickej infraštruktúry, ale napríklad aj priestor obsahujúci IKT).

Keďže stavy a vzťahy medzi jednotlivými informačnými aktívami sú veľmi dynamické a je dôležité

spoľahlivo poznať kto (resp. čo) a prečo spôsobilo konkrétnu zmenu a tiež mať istotu, že medzi dvoma zdôvodnenými zmenami stavu nenastali žiadne iné zmeny ako aj mať možnosť spätne dohľadať aký celkový stav platil v danom časovom reze – aj v tomto prípade sa môže osvedčiť riešenie využívajúce technológiu blockchain.

Poznámky:

- Od Logu udalostí sa tento prípad použitia odlišuje aj tým, že jednotlivé záznamy uložené v blockchain budú vzájomne logicky previazané (modelovanie relácií medzi informačnými aktívami, resp. väzieb medzi záznamom udalosti, ktorá zmenu spôsobila a jej dôsledkami).
- Riešenia pre správu informačných aktív a konfigurácií sa tiež označujú ako konfiguračné databázy (resp. CMDB – Configuration management database podľa metodického rámca ITIL).
- Tieto riešenia slúžia okrem spomínanej podpory poskytovania IT služieb aj pre ďalšie procesy IT organizácie, napr.: riadenie zmien, riadenie incidentov a problémov, riadenie softvérových licencií, výpočet analýzy informačných rizík a pod.
- Tento prípad použitia technológie blockchain môže byť analogicky aplikovaný aj pre správu majetku alebo správy iných logických či fyzických vzájomne interagujúcich objektov.

3.3.3 Riadenie identít a prístupov

Obdobné požiadavky a potreby ako má správa informačných aktív a konfigurácií (časť 3.3.2) platia aj pre riadenie používateľských identít a fyzických a logických prístupov k informačným aktívam.

V skutočnosti môže byť správa identít a prístupov súčasťou rozšírenej konfiguračnej databázy informačných aktív (používatelia a prístupové roly do informačných systémov ako samostatný typ informačných aktív), z ktorej vybrané údaje môžu byť spravované v blockchaine.

Poznámky:

- Nemáme pritom na mysli, že údaje v blockchaine budú používané autorizačným mechanizmom konkrétneho informačného systému pre riadenie prístupov k jeho informačným zdrojom v reálnom čase (i keď ani takého implementácie nemusia byť nereálne).
- Relácie medzi informačným aktívom typu používateľ a inými informačnými aktívami môžu byť typu: je zaradený do (roly), vlastní, prevádzkuje, administruje, používa (napr. ak používa tak v akom režime prístupu: číta, zapisuje, vymazáva, spúšťa) a pod.

Skúmaniu v oblasti využitia technológie blockchain v rôznych riešeniach pre riadenie identít a prístupov s cieľom zdokonaliť poskytovanie elektronických verejných aj komerčných služieb venujú v súčasnosti mnoho energie:

- komerčné firmy (napr. globálna iniciatíva ID2020[14] alebo napr. aj spoločnosť EY[15, 16]), ale aj

[14] https://id2020.org/digital-identity-1/

[15] https://www.ey.com/en_gl/digital/how-blockchain-can-help-create-better-public-services

[16] https://www.ey.com/en_gl/health/how-blockchain-technology-can-change-the-care-continuum

- medzinárodné inštitúcie – napr. iniciatívy OECD[17] (pozri tiež časť 4.3 Blockchain štúdia) alebo iniciatívy EÚ[18] (pozri tiež časť 4.1 EU Blockchain Observatory and Forum a 4.2 EU blockchain Partnership).

Pozornosť sa pritom upriamuje aj na aspekty súvisiace s relevantnými reguláciami ako sú KYC (Know your customer), AML (Anti-money laundering) a GDRP (General data protection regulation, v súvislosti s riadením prístupov viď. aj časť 3.4.1 Ochrana osobných údajov (nariadenie GDPR)).

Veľmi zaujímavou myšlienkou sa v súvislosti s riadením elektronických identít javí byť potenciál technológie blockchain výrazne zjednodušiť procesy PKI „odľahčením" súčasnej komplikovanej a kľúčovej úlohy certifikačných autorít (koncept rozpracovaný viacerými autormi [napr. 19], vrátane autorov tohto dokumentu). Základom tejto myšlienky je úvaha, že verejný kľúč používateľa vložený do spoľahlivého blockchainu pod dohľadom zodpovednej registračnej autority (RA), už nemusí byť podpisovaný privátnym kľúčom certifikačnej autority (CA). Autenticitu a integritu tohto verejného kľúča je možné overiť napr. volaním príslušného smart kontraktu tohto blockchainu.

Poznámka: Pozri tiež tabuľku (Tabuľka 7) v časti 3.2.1 Kontrolné mechanizmy technológie Blockchain a časť 3.4.3 eID a eIDAS.

3.3.4 Komunikačný middleware

Slabou stránkou digitalizácie vo všeobecnosti a špeciálne informatizácie verejnej správy sa javí byť integrácia informačných systémov. Už implementácia interfejsu medzi dvoma systémami prevádzkovanými jedným vlastníkom býva často problematická, nehovoriac o prepájaní množstva informačných systémov, ktoré sú vlastnené a prevádzkované rôznymi – samostatnými entitami (čo je aj prípad IISVS – integrovaného informačného systému verejnej správy).

Dôvernosť, integrita a dostupnosť údajov prenášaných medzi informačnými systémami sú pritom problémy, ktorými sa zaoberá informačná bezpečnosť.

Podľa pôvodnej Národnej koncepcie informatizácie verejnej správy SR (NKIVS) z roku 2008 má byť integrácia jednotlivých informačných systémov verejnej správy (ISVS) zabezpečovaná vzájomnými volaniami tzv. služieb eGovernmentu jednak medzi koncovými používateľmi – typicky občan a podnikateľ (koncové eGov služby) ale tiež medzi ISVS navzájom (podporné eGov služby). Okrem špecifických – agendových ISVS sa majú tejto komunikácie zúčastňovať aj tzv. základné komponenty IISVS (Obrázok 9), vrátane modul G2G výmeny dokumentov.

Túto pôvodnú myšlienku sa však doposiaľ podarilo naplniť len čiastočne (napr. pomocou postupne budovaného systému Centrálnej správy referenčných údajov – CSRÚ). Zo základných komponentov IISVS fungujú len niektoré a poskytujú zatiaľ menší rozsah služieb ako bolo pôvodne plánované. Väčším problémom však je agendové ISVS z rôznych rezortov, ktoré sa podieľajú na riešení spoločnej životnej situácie občana alebo podnikateľa nie sú zintegrované (zorchestrované) tak ako sa pôvodne plánovalo (t.j. servisne orientovaným spôsobom) ale prevažne núdzovo – samostatným 1:1 interfejsom.

Takéto heterogénne a nekonzistentné riešenie IISVS je veľmi nevýhodné z mnohých dôvodov vrátane nemožnosti komplexne monitorovať a vyhodnocovať dianie v celom eGovernmente „z jedného miesta"

[17] https://oecd-opsi.org/wp-content/uploads/2018/06/Blockchains-Unchained-Guide.pdf

[18] https://www.eublockchainforum.eu/sites/default/files/reports/workshop_3_report_-_government_services2fdigital_id.pdf

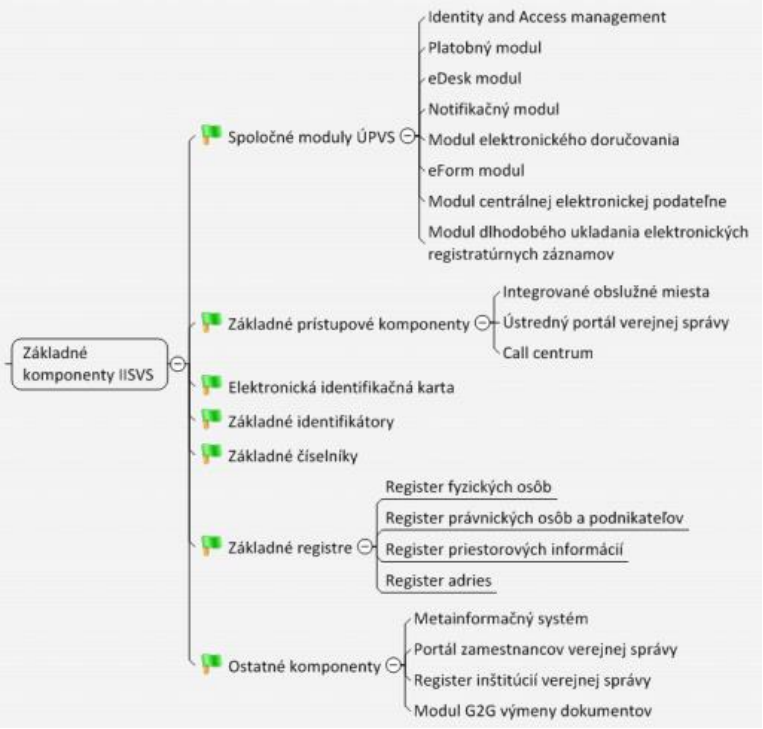
[19] https://www.linkedin.com/pulse/eidas-blockchain-simplifies-pki-robert-bielecki

(či už zo strany osoby zodpovednej za riadenie národnej informatizácie, ale aj informačnej a kybernetickej bezpečnosti, alebo zo strany verejnosti).

Samotná technológia blockchain tento problém nevyrieši avšak môže byť významným prínosom k jeho riešeniu. Po zaregistrovaní sa do spoločného middleware, ktorý využíva technológiu blockchain si môžu jednotlivé ISVS „zrazu" posielať medzi sebou správy veľmi bezpečným spôsobom – viď. argumentáciu v predchádzajúcich častiach tejto kapitoly o autenticite a nepopierateľnosti pôvodu správy, jednoznačnosti adresovania správy (môže byť 1:1 ale aj 1:n) a nepopierateľnosti jej prijatia, nemožnosti zmeniť, vymazať alebo zničiť správu, ochrane dôverného obsahu a tiež možnosti nespochybniteľne pripojiť digitálne odtlačky akýchkoľvek príloh správy.

Záznam v blockchaine typu správa medzi ISVS potom môže byť nositeľom požiadavky na volanie služby z iného ISVS alebo odpoveďou na takúto požiadavku – výstupom z volania služby.

Poznámka: Komunikovanie prostredníctvom blockchainu pritom nemusí byť len výsadou ISVS, takéto bezpečné komunikačné médium môžu využívať aj priamo úradníci inštitúcií verejnej správy (IVS) pri vzájomnej komunikácií alebo komunikácií s občanmi a podnikateľmi a naopak.



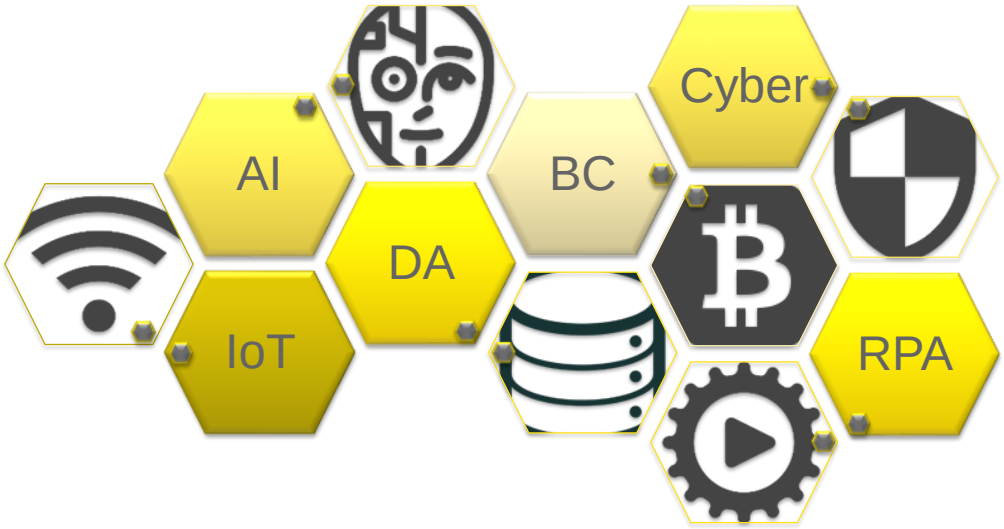
Obrázok 9: Základné komponenty IISVS podľa NKIVS z 2008

3.3.5 Blockchain a iné inovatívne technológie

V súčasnosti sa na technológiu blockchain pozeráme skôr ako na nástroj, ktorý zrejme má potenciál zlepšiť niektoré súčasné riešenia, avšak nie je nevyhnutný. T.j. všetko vieme dostatočne dobre vyriešiť aj bez blockchainu, tak ako sme zvyknutí pomocou tradičných riešení spoliehajúcich sa na centrálne autority. Veríme, že pohľad na blockchain sa bude postupne upravovať a význam tejto technológie bude rásť a to aj v súvislosti s rastom významu iných tzv. inovatívnych technológií a ich vzájomnej prepojenosti (pozri tiež časť 12 a otázku „Kde bude blockchain nenahraditeľný?").

V EY máme na mysli, okrem BC (Blockchain) najmä technológie znázornené na nasledujúcom obrázku (Obrázok 10). Stručný popis súvislosti blockchainu s ostatnými inovatívnymi technológiami, z pohľadu informačnej bezpečnosti, je naznačený v tomto zozname:

- IoT (Internet of things): Blockchain ako spoľahlivé a bezpečné úložisko údajov produkovaných senzormi IoT,
- DA (Data analytics) a AI (Artificial intelligence): Blockchain ako zdroj spoľahlivých (čiastočne zvalidovaných pri zapisovaní do blokov) a nemenných údajov (napr. od IoT) pre ďalšie spracovanie, interpretáciu a využitie pri strojovom učení,
- Cyber (Cyber security): Blockchain ako kontrolný mechanizmus informačnej bezpečnosti (hlavná téma tejto časti štúdie),
- RPA (Robotic process automation) a AI: Blockchain napr. ako spoľahlivý log úkonov (inteligentných) robotov pre overovanie súladu ich konania s predpísanými pravidlami.



Obrázok 10: Vybrané inovatívne – prelomové technológie

3.4 Poznámky k ďalším vybraným témam IB

V tejto časti sa ďalej zameriavame na aspekty technológie blockchain súvisiace s riadením informačnej bezpečnosti v kontexte ďalších tém, ktoré sú relevantné pre informatizáciu verejnej správy a jej zosúladenie s príslušnými národnými a európskymi nariadeniami a pravidlami. Zoznam analyzovaných tém nie je úplný a je potrebné ho chápať ako príspevok do ďalšej diskusie.

3.4.1 Ochrana osobných údajov (nariadenie GDPR)

Nariadenie GDPR (General Data Protection Regulation) bolo schválené Európskou úniou v roku 2016 a vošlo do platnosti v roku 2018 s cieľom chrániť osobné údaje obyvateľov. Možný nesúlad technológie blockchain a GDPR je častou námietkou. EU Blockchain Observatory and Forum vydalo v októbri 2018 report „Blockchain and the GDPR“, v ktorom sú vysvetlené úskalia súladu s GDPR a načrtnuté možné

riešenia[20].

Hlavné práva podľa GDPR:

- Právo na opravu nesprávnych údajov,
- Právo na vymazanie (niekedy označované ako „právo byť zabudnutý“),
- Právo na prístup: subjekt má právo zistiť aké informácie sú o ňom ukladané,
- Práva spojené s automatizovaným spracovaním.

Táto správa vysvetľuje, že dodržiavanie GDPR sa netýka technológie ako takej, ale ako sa technológia používa. Rovnako ako neexistuje žiadny GDPR kompatibilný Internet, nehovoríme o kompatibilite blockchainu a GDPR, ale len o prípadoch a aplikáciách kompatibilných s GDPR. Implementácia je samozrejme jednoduchšia u privátnych ako u verejných blockchainov. Hlavné oblasti potenciálneho rozporu sú tieto:

- Identifikácia a povinnosti spracovateľov dát,
- Anonymizácia osobných údajov,
- Výkon niektorých práv subjektov (napríklad ide o právo na vymazanie údajov, čo je v blockchaine vo všeobecnosti problém; diskusie o tom, čo možno považovať za vymazanie stále prebiehajú).

Tieto otázky zatiaľ neboli definitívne rozhodnuté orgánmi na ochranu osobných údajov, Európskou radou na ochranu údajov (EDPS) a ani súdom. Hlavné odporúčania vyššie uvedeného reportu sú:

- Najprv sa zamerať na celkový obraz: aká je pridaná hodnota, ako sú dáta využívané a či je ich nutné ukladať do blockchainu,
- Vyhýbať sa ukladaniu osobných údajov do blockchainu. Snažiť sa o „zahmlievanie“, kryptovanie a agregovanie s cieľom anonymizácie dát,
- Ukladať osobné údaje off-chain alebo využiť privátny blockchain. Dobre zvážiť problematiku osobných údajov pri prepájaní privátnych a verejných blockchainov,
- Neprestávať inovovať a byť maximálne transparentný k používateľom.

3.4.2 Ochrana údajov na účtovných dokladoch

Súčasťou digitalizácie ekonomiky je aj riešenie na prvý pohľad veľmi jednoduchých úloh ako je digitalizácia a podľa možnosti aj úplné vylúčenie papierových faktúr, resp. vo všeobecnosti účtovných dokladov. Táto snaha zaznamenáva v posledných rokoch rastúci trend a to tiež v súvislosti s nástupom tzv. shared service centier (SSC), ktoré denne spracujú kvantum účtovných dokladov. Možnosť skonvertovať papierovú faktúru do elektronickej podoby hneď na začiatku jej životného cyklu a vyhnúť sa ďalej paralelnej úschove papierového „originálu“ prináša obrovské finančné úspory.

Požiadavky na kvalitu a bezpečnosť elektronicky spracúvaných a uchovávaných faktúr stanovuje Zákon č. 222/2004 Z. z. o dani z pridanej hodnoty[21], ktorý v paragrafe 71 konštatuje aj:

[20] https://www.eublockchainforum.eu/reports

[21] https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2004/222/20190101

- elektronickou faktúrou je faktúra, ktorá obsahuje údaje podľa § 74 a je vydaná a prijatá v akomkoľvek elektronickom formáte; elektronickú faktúru možno vydať len so súhlasom príjemcu tovaru alebo služby,
- vierohodnosťou pôvodu faktúry sa rozumie potvrdenie totožnosti dodávateľa tovaru alebo služby alebo osoby, ktorá v mene dodávateľa vyhotovila faktúru,
- neporušenosťou obsahu faktúry sa rozumie zachovanie obsahu faktúry,
- elektronickou výmenou údajov sa rozumie prenos údajov elektronickou formou z počítača do počítača s využitím schválenej normy štruktúry odkazu elektronickej výmeny.
- Zdaniteľná osoba je povinná zabezpečiť vierohodnosť pôvodu, neporušenosť obsahu a čitateľnosť faktúry od jej vydania do konca obdobia na uchovávanie faktúry. Ako spôsob zabezpečenia vierohodnosti pôvodu, neporušenosti obsahu a čitateľnosti faktúry možno použiť:
  - kontrolné mechanizmy podnikových procesov, ktoré spoľahlivo zabezpečia priraditeľnosť faktúry k dokumentom súvisiacim s dodaním tovaru alebo služby,
  - zaručený elektronický podpis podľa osobitného predpisu29) alebo zákona platného v inom členskom štáte upravujúceho použitie zaručeného elektronického podpisu,
  - elektronickú výmenu údajov, ak zmluva týkajúca sa tejto výmeny ustanoví použitie postupov zabezpečujúcich vierohodnosť pôvodu a neporušenosť obsahu údajov,
  - iný spôsob zabezpečujúci vierohodnosť pôvodu a neporušenosť obsahu faktúry.

Poznámka: Ďalšie podrobnosti je možné nájsť aj v nariadení EÚ 2010/45 „The Invoicing directive" a jeho „Explaratory notes"[22].

Kľúčové sú teda požiadavky z § 71 bod (3) na zabezpečenie:

- vierohodnosti pôvodu,
- neporušenosti obsahu,
- čitateľnosti a dostupnosti faktúry počas obdobia stanoveného týmto zákonom.

V zmysle už uvedeného (viď. najmä časť 3.2.1) na tomto mieste už len konštatujeme, že presne takúto ochranu údajov poskytuje technológia blockchain. Na rozdiel od tradičných spôsobov znižovania rizík informačnej bezpečnosti – t.j. najmä vrstvením všeobecných a aplikačných kontrolných mechanizmov, sa v tomto prípade tiež javí byť riešenie informačnej bezpečnosti opierajúce sa implicitné kontrolné mechanizmy blockchainu nielen účinnejšie (takmer 100% istota – viď. závery v časti 3.2.3) ale aj lacnejšie.

Podobnú úlohu, akú má daňová kontrola pri preverovaní splnenia požiadaviek na elektronicky spracúvané a uchovávané faktúry, má aj audítor finančných výkazov vo vzťahu ku všetkým účtovným dokladom. Okrem samozrejmej požiadavky na dostupnosť (vrátane čitateľnosti) týchto dokladov overuje audítor najmä (trojicu CEA):

- úplnosť (completeness),
- existenciu (existence, t.j. že údaje na dokladoch sú pravé a nie vymyslené) a ich
- presnosť (accuracy).

22 https://ec.europa.eu/taxation_customs/sites/taxation/files/resources/documents/taxation/vat/traders/invoicing_rules/explanatory_notes_en.pdf

Táto trojica predpokladov, ktoré sú predmetom auditu, spadá pod pojem integrita (v informačnej bezpečnosti). Integrita údajov môže byť veľmi úspešne zabezpečená technológiou blockchain a tak spôsobiť doslova revolúciu v prístupe k výkonu auditu.

Poznámka: Závery tejto časti o využiteľnosti technológie blockchain pri zaistení informačnej bezpečnosti údajov o účtovných dokladoch a o potenciálnej zásadnej zmene – zjednodušení prístupu k auditu takto uložených údajov, sú platné nielen pre komerčnú ale aj verejnú správu.

3.4.3 eID a eIDAS

Slovenská republika zaviedla technológiu občianskych preukazov / elektronických dokladov o pobyte s čipom na platforme Infineon Technologies SLE78CFX3000P / Atos CardOS 5.0 (ďalej zjednodušene iba eID). Tieto eID sa používajú na uloženie a prácu s privátnym kľúčom prislúchajúcim ku kvalifikovaným certifikátom, využívajúcim technológiu RSA s dĺžkou kľúča 3072 bitov. Následne eID s platným certifikátom umožňuje vytvárať elektronické podpisy a prístup k štátnym elektronickým službám.

Nevýhodou technológie RSA je predovšetkým dĺžka elektronického podpisu, ktorá je rovná dĺžke kľúča, t.j. V tomto prípade 384 bytov (znakov). Preto väčšina blockchainových implementácií používa novšiu technológiu elektronických podpisov ECC/ECDSA (elliptic curve cryptography - kryptografia na eliptických krivkách; elliptic curve digital signature algorithm - algoritmus elektronických podpisov na eliptických krivkách), väčšinou na krivke SECP256K1 s dĺžkou kľúča 256 bitov, generujúcu podpisy o dĺžke 65 znakov. 256 bitové ECC kľúče sú, z hľadiska bezpečnosti, považované za ekvivalentné 3072 bitovým RSA kľúčom. V prípade blockchain-u, ktorý uchováva podpis každého záznamu, takmer šesťnásobný rozdiel v dĺžke môže predstavovať významnú kapacitnú úsporu.

Z vyššie uvedeného pre použitie eID s blockchainom vyplývajú dve možnosti:

- Blockchain bude implementovať technológiu podpisov RSA3072, alebo
- Použiť ECC certifikáty v eID. Podrobnosti implementácie, napríklad použitá eliptická krivka, vyžadujú ďalšiu diskusiu s dodávateľom technológie.

Blockchain môže predstavovať vhodnú platformu pre distribúciu a správu kvalifikovaných certifikátov - databázu, udržujúcu zoznam platných a zrušených certifikátov, naviac umožňujúcu automaticky validovať nové transakcie voči týmto zoznamom. Problematické však je zverejňovanie úplných certifikátov, resp. osobných údajov uvedených v certifikáte (v kvalifikovaných certifikátoch vydávaných na Slovensku sa uvádza napr. aj rodné číslo), priamo na blockchaine.

Je potrebné taktiež spomenúť požiadavku vykonávacieho rozhodnutia komisie (EÚ) 2015/1506, ktorým sa ustanovujú špecifikácie týkajúce sa formátov zdokonalených elektronických podpisov a zdokonalených elektronických pečatí, ktoré môžu subjekty verejného sektora uznávať. Bežná implementácia podpísanej blockchainovej transakcie implementuje vlastný proprietárny formát, ktorý nie je v zozname referenčných formátov.

Pre použitie na národnej úrovni, za predpokladu zosúladenia legislatívy so zvolenou implementáciou, sa dá podpis na transakcii považovať za zdokonalený elektronický podpis. Technicky vzaté, použitý formát, v ktorom je podpis uložený, v princípe na bezpečnosti nepridáva. Podľa použitej aplikácie však môže byť nutné buď zosúladiť implementáciu blockchainu tak, aby formát transakcie bol jedným z formátov XAdES alebo CAdES, alebo vytvoriť vhodné konverzné nástroje pre import a/alebo export.

Poznámka: Pozri aj časť 3.3.3 Riadenie identít a prístupov a koncept zjednodušenia procesov PKI „odľahčením“ role CA.

4 Blockchain vo svete, v EÚ a na Slovensku

4.1 EU Blockchain Observatory and Forum

Európa viditeľne stavia na svojej ambícii stať sa svetovým lídrom v blockchaine. V súlade s touto víziou Európska komisia dňa 1. februára 2018 založila Európske observatórium a fórum pre blockchain (EU Blockchain Observatory and Forum)[23], ktorého hlavnou úlohou je:

- zmapovať existujúce iniciatívy v Európe aj mimo nej,
- monitorovať vývoj, analyzovať trendy a riešiť vznikajúce problémy,
- stať sa vedomostným centrom blockchain,
- podporovať európske subjekty a posilniť európsku angažovanosť so zúčastnenými stranami,
- predstavovať hlavný komunikačný kanál pre Európu, stanoviť víziu a ambície na medzinárodnej scéne,
- byť hybnou silou spoločných krokov smerujúcich k realizácií konkrétnych projektov európskeho záujmu.

V súvislosti s identifikáciou a výskumom existujúcich blockchain iniciatív v celej EÚ aj mimo nej, Európske observatórium a fórum pre blockchain zriadilo dve pracovné skupiny:

- Pracovná skupina pre politiku blockchain a rámcové podmienky (The Blockchain Policy and Framework Conditions Working Group) – zaoberá sa otázkami technológií naprieč odvetviami s cieľom definovať politické, právne a regulačné podmienky potrebné na podporu regulačnej a právnej predvídateľnosti potrebnej na rozsiahlejšie zavedenie blockchain technológie.
- Pracovná skupina pre prípadové štúdie a prechodné scenáre (The Use Cases and Transition Scenarios Working Group) – zameriava sa na najperspektívnejšie prípady použitia blockchain s dôrazom na aplikovanie vo verejnom sektore, ako sú služby v oblasti identifikácie, zdravotnej starostlivosti, energetických a environmentálnych hlásení a služby poskytované verejnými inštitúciami.

Každá pracovná skupina pozostáva z 30 členov, ktorí boli vybraní na základe účasti vo výzve z 15. marca 2018. Zoznam členov pozostáva z vedúcich predstaviteľov z rôznych oblastí a reprezentuje 28 štátov.

4.2 EU blockchain Partnership

Dňa 10. apríla 2018 21 členských štátov a Nórsko podpísalo dohodu, na základe ktorej vytvorili Európske partnerstvo pre blockchain (EU blockchain Partnership) a deklarovali spoluprácu pri zriadení Európskej infraštruktúry blockchainových služieb (European Blockchain Services Infrastructure), ktorá bude podporovať poskytovanie cezhraničných digitálnych verejných služieb, s najvyššími štandardmi v oblasti bezpečnosti a ochrany súkromia. Následne sa k partnerstvu pridalo ďalších päť členských štátov.

S cieľom utvrdiť postavenie Európy ako svetového lídra v oblasti vývoja a implementácie blockchain technológií, Európske partnerstvo pre blockchain má byť prostriedkom spolupráce medzi členskými štátmi pri výmene skúseností a odborných znalostí v technickej a regulačnej oblasti. Partnerstvo sa má taktiež podieľať na príprave a spustení celoeurópskych blockchain aplikácií naprieč jednotným digitálnym

[23] https://www.eublockchainforum.eu/

trhom, z ktorých by profitoval súkromný aj verejný sektor. Partnerstvo má prispieť k vytvoreniu priaznivého prostredia v súlade s právnymi predpismi EÚ a s jasnými modelmi riadenia, ktoré pomôžu službám využívajúcim blockchain prekvitať v celej Európe.

- zakladajúci členovia:

Belgicko	Luxembursko
Bulharsko	Malta
Česká republika	Holandsko
Rakúsko	Nórsko
Estónsko	Poľsko
Fínsko	Portugalsko
Francúzsko	Slovensko
Nemecko	Slovinsko
Írsko	Španielsko
Litva	Švédsko
Lotyšsko	Veľká Británia

- členovia, ktorý sa pridali neskôr:

Cyprus	Taliansko
Dánsko	Rumunsko
Grécko	

- členovia EÚ, ktorý sa k partnerstvu nepridali:

Chorvátsko	Maďarsko

Obrázok 11: Prehľad členov Európskeho partnerstva pre blockchain

4.3 Blockchain štúdia OECD

Organizácia pre hospodársku spoluprácu a rozvoj (OECD) vydala dokument Blockchains Unchained: Blockchain Technology and its Use in the Public Sector[24]. Táto príručka 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. Taktiež pojednáva o oblastiach, kde nie je vhodné blockchain technológiu použiť. V rámci série príloh príručka poskytuje prípadové štúdie, ako aj informácie o špecifických technických aspektoch technológie blockchain. Zatiaľ čo technológia blockchain sa používa najmä vo finančnom sektore (hlavne pri peňažných transakciách), príručka poukazuje hlavne na možnosti využitia aj v iných oblastiach nepeňažného charakteru ako je digitálna identifikácia, vlastníctvo pôdy (katastre), riadenie dodávateľského reťazca a dokonca aj hlasovanie (voľby). 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 na Obrázku 11 možno vidieť trendy, v akých

[24] https://www.oecd-ilibrary.org/docserver/3c32c429-en.pdf?expires=1542286010&id=id&accname=guest&checksum=8010483B01C804FAA819A1FC9B49DD83

typoch projektov a priemyselných odvetviach sa začína používať blockchain technológia vo verejnom sektore (Tabuľka č. 8). Tieto iniciatívy predstavujú praktické aplikácie technológie blockchain, ako aj spoločenstvá z praxe, platformy na zdieľanie nápadov a partnerstvá s cieľom preskúmať a implementovať Blockchain projekty.[25]

Obrázok 12: Prehľad využitia blockchain technológie vo verejnom sektore

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 8: Najrozšírenejšie typy blockchain projektov a ich využitie v odvetviach

Pozn.: Jednotlivé projekty môžu byť zaradené vo viacerých typoch projektov.

[25] https://www.oecd-ilibrary.org/docserver/3c32c429-en.pdf?expires=1542286010&id=id&accname=guest&checksum=8010483B01C804FAA819A1FC9B49DD83

4.4 Projekty využívajúce blockchain v EÚ a vo svete

Zameranie: e-Health / Krajina: Estónsko

Popis: V Estónsku sú vlastníkmi zdravotných údajov samotní pacienti. Od roku 2008 nemocnice sprístupnili zdravotné údaje online. V súčasnosti je viac ako 95 % údajov vytvorených nemocnicami a lekármi digitalizovaných a technológia blockchain sa používa na zabezpečenie integrity uložených elektronických lekárskych záznamov, ako aj protokolov prístupu do systému. Riešenia elektronického zdravotníctva umožňujú Estónsku ponúknuť efektívnejšie preventívne opatrenia, zvyšovať povedomie pacientov a tiež ušetriť miliardy EUR. Každý pacient v Estónsku, ktorý navštívil lekára, má vlastný online záznam o zdravotnom stave v e-Health, ktorý obsahuje poznámky, výsledky testov, digitálne lekárske predpisy, záznamy z RTG vyšetrení a pod. Zároveň pacient má prístup do systému, v rámci ktorého môže sledovať údaje o svojom zdravotnom stave. Vďaka e-Healthu môžu lekári pristupovať k elektronickým záznamom pacienta bez ohľadu na to, kde sa nachádzajú. Vzhľadom ku komplexným údajom, ktoré e-Health poskytuje, majú lekári viac informácií, na základe ktorých môžu robiť lepšie rozhodnutia o diagnóze a liečbe pacienta. Pacienti majú prístup k svojim vlastným záznamom, záznamom ich maloletých detí, ako aj k záznamom ľudí, ktorí im povolili prístup. Prihlásením sa do portálu e-Patient elektronickým dokladom totožnosti si pacient môže prezrieť návštevy u lekára, aktuálne predpisy a skontrolovať, ktorí lekári majú prístup k jeho súborom a prezerali si jeho záznamy.[26]

Podľa štatútu zdravotného IS je zriaďovateľom estónskeho národného zdravotného IS Ministerstvo sociálnych vecí a autorizovaným prevádzkovateľom estónska nadácia eHealth. Zdravotný IS je databáza, ktorá je súčasťou štátneho informačného systému.[27]

Zameranie: e-Obchodný register / Krajina: Estónsko

Popis: e-Obchodný register je jedným z prvých služieb Estónskeho centra registrov a informačných systémov, ktorý bol základom pre vytvorenie portálu pre registráciu spoločností a vizualizovaného obchodného registra. e-Obchodný register je služba založená na databáze oddelení registrov okresných súdov a zobrazovaní údajov všetkých právnických osôb registrovaných v Estónsku v reálnom čase. Záujemca si môže prezerať údaje po prihlásení sa prostredníctvom elektronického dokladu totožnosti. e-Obchodný register umožňuje prezeranie všeobecných údajov o spoločnosti a daňových nedoplatkov, vyhľadávanie podľa mena, kódu v obchodnom registri, sídla, oblasti činností a pod., prezeranie výročných správ, stanov, osobných a obchodných záväzkov, monitorovanie spracovania údajov a zaznamenávanie zmien spoločností v reálnom čase, overenie obchodných a podnikateľských zákazov prislúchajúcich k jednotlivým osobám, vizualizovanie vzťahov medzi rôznymi spoločnosťami a osobami, súčasné a bývalé vzťahy medzi spoločnosťami. Technológia blockchain pomáha zistiť, kedy došlo k zmene informácií o spoločnosti v e-Obchodnom registri a prečo.[28]

Zameranie: e-Kataster nehnuteľností / Krajina: Estónsko

Popis: e-Kataster nehnuteľností je pohodlná a dostupná služba, ktorá umožňuje rýchle a jednoduché overenie všeobecných údajov, veľkosti, vlastníkov, obmedzení a zaťažení nehnuteľností hypotékami

[26] https://e-estonia.com/solutions/healthcare/e-health-record/
[27] https://guardtime.com/technology
[28] https://e-estonia.com/solutions/business-and-finance/e-business-register/

a pod. Využívanie služby je podmienené overením pomocou elektronického dokladu totožnosti alebo prostredníctvom online bankovníctva. Ak záujemca potrebuje údaje o nehnuteľnostiach iba zriedkavo, je možné údaje z katastra čerpať bez uzavretia zmluvy s e-Katastrom nehnuteľností. V prípade potreby prijímania alebo overovania veľkého množstva údajov, je možné sa zaregistrovať ako zákazník e-Katastra nehnuteľností. Zmluvnými zákazníkmi e-Katastra nehnuteľností sú spoločnosti a agentúry, ktoré denne potrebujú väčšie množstvo spoľahlivých údajov o nehnuteľnostiach. Všetky údaje vydané e-Katastrom nehnuteľností sú použiteľné na právne účely. Technológia blockchain pomáha zistiť, kto, kedy a ako zmenil údaje o nehnuteľnostiach v e-Katastri nehnuteľností.[29]

Zameranie: e-Court / Krajina: Estónsko

Popis: V roku 2006 bol spustený Informačný systém súdnictva (KIS), ktorý ponúka jeden informačný systém pre všetky typy prípadov: Estónske súdy prvého a druhého stupňa a Najvyšší súd. KIS umožňuje registráciu súdnych prípadov, vypočutí, rozsudkov, automatické prideľovanie prípadov sudcom, vytvorenie predvolania, uverejnenie rozsudkov na oficiálnych stránkach a zber metaúdajov. Najnovšia generácia KIS obsahuje nové identifikátory založené na potrebách súdov, napríklad typy prípadov, kategórie prípadov a podkategórie. Druhá generácie KIS predstavuje pre sudcov cenný nástroj, keďže umožňuje vyhľadávanie založené aj na frázach konania, vydávanie upomienok a monitorovanie dĺžky času stráveného v každej fáze procesu. Technológia blockchain pomáha zistiť, kto, kedy a ako zmenil údaje o nehnuteľnostiach v Informačnom systéme súdnictva.[30]

Zameranie: i-Voting / Krajina: Estónsko

Popis: i-Hlasovanie je jedinečné riešenie, ktoré jednoducho a pohodlne pomáha zapojiť občanov do procesu riadenia štátu. V roku 2005 sa Estónsko stalo prvou krajinou na svete, ktorá prostredníctvom i-hlasovania realizovala celoštátne voľby a v roku 2007 prvou krajinou, ktorá i-hlasovanie využila v parlamentných voľbách. Internetové hlasovanie alebo i-hlasovanie je nástroj, ktorý umožňuje voličom hlasovať z ktoréhokoľvek počítača pripojeného k internetu kdekoľvek na svete. V porovnaní s ostatnými elektronickými hlasovacími systémami, ktoré sú založené na nákladných a problematických mechanizmoch používaných v iných krajinách, je estónske riešenie jednoduché, elegantné a bezpečné. Volič sa počas určeného obdobia pred hlasovaním prihlási do systému pomocou elektronického dokladu totožnosti alebo mobilného dokladu totožnosti a odovzdá hlasovacie lístky. Identita voliča sa odstráni predtým, ako sa hlasovací lístok dostane k Národnej volebnej komisii pre počítanie, čím sa zabezpečí jeho anonymita. Estónske riešenie umožňuje voličom prihlásiť a hlasovať toľkokrát, koľko chcú počas stanoveného obdobia pred hlasovaním. Keďže každé ďalšie voličovo hlasovanie zruší to posledné, volič má do uzavretia stanoveného obdobia vždy možnosť zmeniť svoj hlas. Vďaka i-hlasovaniu bolo v posledných estónskych voľbách ušetrených 11 000 pracovných dní. Technológia blockchain sa využíva na odhalenie prípadnej manipulácie s volebnými hlasmi a výsledkami volieb.[31]

Zameranie: Fond sociálneho zabezpečenia / Krajina: Čína

Popis: Podľa vyjadrení podpredsedu Národnej rady pre sociálne zabezpečenie sa technológia Blockchain

[29] https://www.rik.ee/en/e-land-register
[30] https://www.rik.ee/en/international/court-information-system
[31] https://e-estonia.com/category/i-voting/

bude používať v čínskom systéme sociálneho zabezpečenia kvôli uľahčeniu obchodovania, realizácie priamych transakcií bez použitia sprostredkovateľa, zníženiu transakčných nákladov, ako aj cenným aplikáciám v oblasti investovania a správy fondov sociálneho zabezpečenia. Technológia blockchain sa plánuje využiť v oblasti sociálneho poistenia. Vzhľadom k tomu, že technológia blockchain je málokedy používaná v takto veľkom meradle, t. j. služba by bola využívaná 1,4 biliónom používateľov, tento krok by zásadne zmenil odvetvie zdravotnej starostlivosti. Táto iniciatíva by znamenala celosvetový prelom, ktorý by potvrdil skutočnú hodnotu technológie blockchain, jej zmysluplné využitie a benefity.[32]

Zameranie: Overovanie dokumentov prostredníctvom blockchain technológie v meste Viedeň / Krajina: Rakúsko

Popis: Blockchain technológia je kľúčovým prvkom iniciatívy Viedne v oblasti digitalizácie, ktorý umožňuje zvýšenie transparentnosti, efektívnosti a bezpečnosti údajov. Táto iniciatíva je súčasťou projektu DigitalCity.Wien. Projekt umožňuje obyvateľom overovať dátum a pravosť dokumentov, ako sú dopravné trasy, vlakové poriadky a výsledky hlasovania. Cieľom projektu je zjednodušiť a automatizovať administratívne procesy (podávanie správ v oblasti energetiky a schvaľovanie a overovanie registrácie podnikov, ktoré je potrebné často aktualizovať). Okrem toho blockchain technológia napomáha zlepšiť bezpečnosť uvedených informácií. Od spustenia projektu v decembri 2017 bolo do verejného blockchainu pridaných cca 400 dokumentov. S využitím blockchainu môžu zamestnanci mesta, obyvatelia alebo vývojári aplikácií sledovať zmeny v údajoch, takže ak niekto zmení trasu autobusu, ktorá je prepojená s mapovými aplikáciami, dôjde k odoslaniu upozornenia. Technológia taktiež umožňuje vydávanie notársky overených dokumentov mesta Viedeň a plánované je rozšírenie na všetky údaje Portálu rakúskej vlády. V budúcnosti sa očakáva spolupráca IT spoločností a mesta Viedeň s cieľom podporiť Viedeň ako smart city a hotspot pre digitálny priemysel.[33], [34]

Zameranie: Smart kontrakty v meste Rotterdam / Krajina: Holandsko

Popis: Mesto Rotterdam môže uložiť daň osobám, ktoré v ňom oficiálne nežijú, ale v určitý čas pobývajú (napr. turisti). Turistická daň vyplýva z využívania zariadení a služieb mesta. Príjmy plynúce z tohto turistického poplatku umožňujú mestu Rotterdam udržiavať a zlepšovať zariadenia a služby.

Vďaka technológii blockchain niektoré činnosti zamestnancov mesta Rotterdam pri výbere turistických daní už nie sú potrebné. Výber turistických daní sa realizuje prostredníctvom smart kontraktov. Hlavnou úlohou zamestnancov mesta Rotterdam tak zostáva len vytvorenie noriem a pravidiel.[35]

Zameranie: e-identity / Krajina: Estónsko

Popis: Na rozdiel od mnohých iných krajín má každý obyvateľ Estónska štátnu digitálnu identitu. Vďaka tomu je Estónsko niekoľko rokov pred krajinami, ktoré sa stále usilujú o to, ako overiť identitu občanov

[32] https://cointelegraph.com/news/china-to-use-blockchain-technology-in-tax-collection-and-electronic-invoice-issuance

[33] http://cityofblockchain.org/

[34] https://www.ey.com/en_gl/news/2018/08/ey-and-city-of-vienna-collaborate-on-public-blockchain-networks

[35] https://www.unlock-bc.com/news/2018-02-20/government-of-denmark-implements-35-blockchain-use-cases-and-number-grows

bez fyzického kontaktu. Estónsko má zďaleka najviac rozvinutý národný systém preukazov totožnosti na svete. Preukaz neslúži len ako identifikačný doklad s fotografiou, ale taktiež poskytuje digitálny prístup k všetkým elektronickým službám Estónska. V Estónsku sa každá osoba môže bezpečne identifikovať a poskytnúť digitálny podpis pomocou svojho preukazu totožnosti, mobilnej identifikácie alebo Smart-ID a tým používať elektronické služby. Čip na preukaze totožnosti obsahuje údaje, ktoré zabezpečuje 2048-bitové šifrovanie. Preukaz totožnosti sa pravidelne používa ako cestovný doklad pre občanov Estónska cestujúcich v rámci EÚ, karta zdravotného poistenia, prostriedok na identifikáciu pri prihlasovaní na bankové účty, digitálny podpis, i-Voting, prostriedok na prezeranie zdravotných záznamov, podávanie daňových priznaní a pod. Tento digitálny preukaz totožnosti má 98 % Estónčanov a 67 % z nich ho využíva pravidelne. Mobilná identifikácia umožňuje občanom používať mobilný telefón ako formu zabezpečeného digitálneho preukazu totožnosti. Podobne ako preukaz totožnosti, môže byť použitá na prístup k zabezpečeným elektronickým službám a na digitálny podpis dokumentov. Okrem toho má ďalšiu výhodu, že nevyžaduje čítačku kariet. Systém je založený na špeciálnej SIM karte, ktorú si zákazník musí vyžiadať od mobilného operátora. Súkromné kľúče spolu s aplikáciou poskytujúcou autentifikačné a podpisové funkcie sú uložené na SIM karte. Mobilnú identifikáciu využíva 12,2 % obyvateľov. Smart-ID je pohodlná mobilná aplikácia, ktorá funguje ako identifikačné riešenie pre každého, kto nemá v inteligentnom zariadení (smartfón, tablet) SIM kartu, ale musí online bezpečne preukázať svoju identitu. Pomocou Smart-ID je možné prihlásiť sa do elektronických služieb finančného sektora a potvrdiť transakcie, zmluvy a pod. K vykonaniu transakcie prostredníctvom Smart-ID postačuje 5 kilobajtov. Technológia blockchain zabezpečuje integritu údajov.[36]

Zameranie: e-Residency / Krajina: Estónsko

Popis: V decembri 2014 sa Estónsko stalo prvou krajinou, ktorá otvorila svoje digitálne hranice, aby umožnila komukoľvek na svete požiadať o získanie prístupu k národnej digitálnej identite a stať sa e-rezidentom. Estónska e-Residency je v podstate komerčná iniciatíva. Elektronický identifikačný doklad vydávaný e-rezidentom umožňuje držiteľom komerčné aktivity s verejným a súkromným sektorom, t. j. e-rezidenti majú prístup k podnikateľskému prostrediu EÚ a môžu využívať verejné elektronické služby prostredníctvom svojej digitálnej identity. Tento doklad nepredstavuje občianstvo v jeho tradičnom zmysle a nie je cestovným dokladom. V mnohých ohľadoch je však medzinárodným „pasom" do virtuálneho sveta. E-Residency je významnou zmenou aj vzhľadom na skutočnosť, že prostredníctvom technológie blockchain môžu e-rezidenti využívať notárske služby. Aplikácia blockchain technológie do e-Residency má potenciál zásadne zmeniť spôsob, akým sú údaje o identite overované a kontrolované. Hlavným dôvodom, prečo záujemcovia využívajú e-Residency, je založenie podnikania online v dôveryhodnej lokalite (EÚ) s možnosťou jeho rozšírenia do celého sveta. E-rezidenti majú možnosť založiť dôveryhodnú EÚ spoločnosť online z akéhokoľvek miesta na svete za jeden deň, spravovať túto spoločnosť v plnom rozsahu online, požiadať o podnikateľský bankový účet a zabezpečiť bezpečné elektronické bankovníctvo, zabezpečiť si prístup k poskytovateľom medzinárodných platobných služieb (Paypal, Braintree a pod.), digitálne podpisovať a zasielať dokumenty a priznávať dane online. E-rezidenti obdržia digitálnu identifikačnú kartu s dvoma PIN kódmi kvôli zabezpečeniu digitálnej autentifikácie a digitálnych podpisov. Takto zabezpečené digitálne podpisy sú právne ekvivalentné rukopisnému podpisu v rámci Estónska, ako aj u partnerov z celého sveta, ktorí túto formu podpisu akceptujú. O e-

[36] https://e-estonia.com/solutions/e-identity/id-card/

Residency zatiaľ požiadalo 50 tisíc ľudí zo 160 krajín sveta.[37]

Zameranie: Identita utečencov / Krajina: Fínsko

Popis: Úsilím v rámci celej Európy je aj riešenie problému totožnosti utečencov. Fínsko tento problém vyriešilo a na zaznamenávanie údajov o nových obyvateľoch využíva technológiu blockchain. V rámci svojho záväzku podporovať žiadateľov o azyl, Fínsko poskytuje utečencom namiesto hotovosti predplatenú debetnú kartu a ukladá totožnosť držiteľov kariet do blockchainu. Vzhľadom k použitej technológii už neexistuje problém s tzv. silne overenou totožnosťou. Tieto karty sú produktom miestneho startupu a fungujú ako jednoduchý nástroj na vykonávanie platobných operácií. Prostredníctvom vydávania a používania kariet sú fínske orgány schopné sledovať výdavky aj totožnosť používateľa. Výhodou tohto systému je finančné začlenenie a najmä pomoc ľuďom z rozvojových krajín. Pridanou hodnotou blockchainu je integrita údajov.

Zameranie: Zvýšenie transparentnosti grantov / Krajina: Kanada

Popis: Kanadská vláda začala skúšobný proces v rámci využívania technológie blockchain s cieľom transparentnejšieho využívania vládnych grantov v oblasti výskumu a poskytovania informácií vo vzťahu k verejnosti. Národná rada pre výskum (NRC) využíva Catena Blockchain Suite, kanadský produkt postavený na blockchaine Ethereum, na publikovanie informácií o Programe pomoci pre priemyselný výskum (NRC IRAP) a jeho financovaní v reálnom čase. Keď NRC vytvorí alebo zmení grant, príslušné informácie sa ukladajú do blockchainu Ethereum a uverejnia sa v online databáze, ktorú si môže prehliadať i verejnosť. Tieto informácie je možné filtrovať podľa peňažnej hodnoty, dátumu, prijímateľa a regiónu. Informácie o grantoch si môžu tiež overiť kliknutím na identifikačný link transakcie, ktorý ich privedie do jedinečného záznamu o transakciách v online transakčnej databáze Etherscan.io. NRC si vybrala Ethereum z niekoľkých dôvodov. Jedná sa o jednu z najetablovanejších blockchain technológií, ktorá momentálne existuje a na rozdiel od blockchainu, na ktorom je prevádzkovaná kryptomena Bitcoin, Ethereum umožňuje prevádzkovať inteligentné kontrakty, čo mu dáva oveľa väčší význam. Zvýšením transparentnosti prostredníctvom blockchain technológie môže Kanada vybudovať dôveru verejnosti a potenciálne zvýšiť zapojenie obyvateľov do tohto procesu. Napríklad obyvateľ si môže všimnúť, že určitá časť výskumu je zanedbávaná a upozorniť o tejto problematike príslušných zástupcov.[38]

Zameranie: Doklady o akademickom vzdelaní / Krajina: Malta

Popis: Ministerstvo školstva a zamestnanosti uzavrelo dohodu s blockchainovým startupom Learning Machine Technologies o vytvorení prototypovej platformy, ktorá umožní používateľom bezpečne ukladať a zdieľať svoje doklady o akademickom vzdelaní. Systém je postavený na otvorenom štandarde Blockerts, ktorý bol vyvinutý Learning Machine Technologies a MIT Media Lab v roku 2016. Blockerts slúži na vytváranie aplikácií, ktoré vydávajú a verifikujú oficiálne záznamy ukladané v blockchaine. Môžu zahŕňať certifikáty, vysokoškolské diplomy, odborné licencie a pod. Blockerts pozostáva z knižníc, nástrojov a mobilných aplikácií s otvoreným zdrojovým kódom, ktoré umožňujú využívať decentralizovaný ekosystém orientovaný na používateľov, ako aj dôveryhodnú verifikáciu

[37] https://e-resident.gov.ee/

[38] https://globalnews.ca/news/3977745/ethereum-blockchain-canada-nrc/

prostredníctvom technológie blockchain.

Blockcerts umožňuje používateľom prijímať, overovať, ukladať a zdieľať svoje doklady o akademickom vzdelaní v blockchaine a prostredníctvom digitálnej peňaženky vydávať kľúče, ktoré umožňujú bezpečný prístup k týmto dokladom.[39]

Zameranie: Rodný list / Krajina: Spojené štáty americké

Popis: Inštitúcie verejného sektora zohrávajú dôležitú úlohu pri rozvoji akéhokoľvek ekosystému digitálnej totožnosti. Totožnosť obyvateľa nie je len základným atribútom pre možnosť využívania služieb verejného sektora, ale aj základom dôvery a legitímnosti. Blockchainová iniciatíva Illinois, ktorej hlavným úsilím je skúmať vplyv a využitie technológie blockchain vo verejnom sektore, spolupracuje so spoločnosťou Evernym na bezpečných riešeniach v oblasti digitálnej totožnosti. Hlavnou úlohou tohto konceptu je vytvorenie zabezpečenej totožnosti pre občanov štátu Illinois počas procesu registrácie po narodení. Bez závislosti na centralizovanom úložisku môže byť takáto totožnosť efektívne a bezpečne overená subjektami, ktoré ju vyžadujú. Vládne inštitúcie, resp. matriky overia údaje uvedené v rodnom liste a kryptograficky zapíšu atribúty totožnosti, ako sú meno a priezvisko, dátum narodenia, pohlavie a pod. Poverenia na prezeranie a zdieľanie týchto údajov sú ukladané prostredníctvom jednoznačného identifikátora, každý údaj je kryptograficky zabezpečený a prístupný iba s výslovným súhlasom držiteľa totožnosti, resp. v prípade novorodenca, jeho zákonného zástupcu. Verejné inštitúcie, ako aj subjekty súkromného sektora, budú môcť overiť údaje o občanovi tým, že požiadajú o šifrovaný prístup k týmto údajom. To minimalizuje potrebu, aby subjekty vytvárali, prevádzkovali a spoliehali na svoje vlastné databázy údajov o totožnosti občanov.[40]

4.5 Potenciálne kľúčové úlohy a rola štátu pri adopcii blockchain technológie

Nasledujúci zoznam uvádza niektoré kľúčové úlohy štátu pri adopcii nových revolučných technológií akou je aj blockchain:

- Vzdelávanie, popularizácia, šírenie osvety a vyvracanie mýtov o blockchaine medzi verejnosťou a štátnymi zamestnancami,
- Analyzovať súlad s legislatívou a v prípade potreby odstrániť rozpory, vypracovať a zverejniť potrebné vysvetlenia a stanoviská,
- Zaviesť štandardy pre blockchainové riešenia v štátnej správe,
- Zrealizovať prvé vzorové blockchain projekty – napríklad niektorý z jednoduchších projektov uvedených ďalej v tejto štúdii,
- Aktívne sa zapojiť do prichádzajúcich EÚ cezhraničných blockchain projektov.

Úloha štátu	Hlavné činnosti
Byť medzi prvými v nasadzovaní technológie („early adopter")	Podporovať vývoj ako zákazník. Nasadiť technológiu na prvých projektoch.

[39] https://www.coindesk.com/maltas-government-putting-academic-certificates-blockchain/

[40] http://www.govtech.com/data/Illinois-Announces-Key-Partnership-in-Birth-Registry-Blockchain-Pilot.html

Úloha štátu	Hlavné činnosti
Vytvoriť víziu nasadzovania technológie	Vytvoriť víziu ako môže blockchain zlepšiť služby štátu občanom.
Investovať do vývoja technológie Vývoj a prototypovanie prvých príkladov použitia	Vytvárať partnerstvá s odbornou verejnosťou a komunitou vývojárov.
Vytvoriť regulačný rámec	Zaviesť regulačný rámec pre implementáciu blockchainu a jeho aplikácie.
Nastaviť štandardy pre bezpečnosť a ochranu súkromia.	Spolu s akademickými inštitúciami a odbornou verejnosťou potvrdiť že sú vytvorené vyhovujúce štandardy pre integritu, bezpečnosť a súkromie.
Vybudovať dôveru a interoperabilitu	Vytvoriť medzištátnu komunitu s cieľom rozvinúť potenciálne prípady použitia. Implementovať politiky, ktoré podporujú výskum a vývoj a inovácie v technológii blokov.
Vytvoriť partnerstvá s technologickými firmami a združeniami	Vytvoriť partnerstvá s technologickými firmami a priemyselnými združeniami pre širokú akceptáciu blockchain technológie. Spoluvytváranie inovatívnych aplikácií na zlepšenie služieb obyvateľstvu a zvýšenie bezpečnosti.
Dôraz na zdieľanie informácií a spoločné plánovanie	Zabezpečiť transparentnú výmenu spôsobilostí a kritických údajov na identifikáciu príležitostí na vytváranie hodnôt. Spoločné plánovacie zasadnutia s cieľom diskutovať o vývoji potrieb podnikov a posúdiť vplyv tejto technológie na podnikanie.

Tabuľka 9: Úloha štátu pri adopcii technológie blockchain

4.6 Blockchain na Slovensku

Na Slovensku vznikla silná komunita okolo zameraná na technológiu blockchain. Vzniklo viacero firiem špecializovaných na blockchain a mnoho tradičných IT firiem podporuje a dodáva takéto riešenia. Existuje mnoho nadšencov, ale aj IT špecialistov na blockchain. Mnoho firiem aktívne skúma možnosti tejto technológie a experimentuje s možným nasadením v praxi. Zavádzanie technológie blockchain na Slovensku sa dotýka mnohých subjektov. Nasledujúci zoznam uvádza hlavné kategórie dotknutých subjektov (stakeholders):

- Orgány štátnej správy v SR,
- Miestne orgány,
- Agentúry na podporu výskumu a vývoja,
- Slovenské vysokoškolské a výskumné inštitúcie,
- Startup spoločnosti špecializujúce sa na blockchain,
- Tradiční dodávatelia IT riešení,
- Štátni zamestnanci,
- Verejnosť, súkromné a právnické osoby ako používatelia riešenia založeného na blockchain,
- Európska komisia a ostatné štáty EÚ v prípade blockchain projektov cezhraničnej spolupráce,
- Priemyselné asociácie a klastre,

- Regionálne inovačné centrá,
- Občianske združenia,
- Odborná verejnosť.

Projekt: Blockchain na finančnej správe

V máji 2018 na konferencii GLOBSEC prezident finančnej správy SR prezentoval zámer využiť blockchain vo svojich procesoch pre naplnenie cieľa zefektívnenia výberu daní. Taktiež bol prezentovaný zámer zaviesť blockchain pri asignácii 2 % (3 %) dane. Očakávané je zvýšenie dôvery klientov a ochrana ich údajov, zvýšenie transparentnosti procesov, zníženie administratívnej záťaže a zníženie nákladov[41].

O ďalších projektoch využívajúcich blockchain vo verejnej správe na Slovensku nevieme.

Štúdium blockchain na vysokých školách

Podľa získaných informácii v čase prípravy štúdie (november 2018), blockchain nie je samostatným študijným odborom na žiadnej vysokej škole na Slovensku a ani neevidujeme samostatný predmet zameraný len na blockchain. Základy technológie blockchain sú však vyučované v rámci iných predmetov napríklad na FIIT STU BA.

Záujmové združenia

Občianske združenie Blockchain Slovakia.

Konferencie a workshopy

Dňa 10. októbra sa v Bratislave pod záštitou Úrady vlády SR a Európskej komisie uskutočnila konferencia BLOCKWALKS 2018 zameraná na využitie blockchainu vo verejnom sektore.

V priebehu ostatných dvoch rokov sa v SR realizovalo aj množstvo ďalších konferencií a workshopov, ktoré sa zaoberajú problematikou fintech, kryptomien, blockchain a vo všeobecnosti decentralizáciou údajov a elektronických služieb alebo aj inak zameraných eventov, ktorých súčasťou sú aj prednášky venujúce sa technológii blockchain. Je pritom možné pozorovať postupný pozitívny posun od tém, v ktorých sa blockchain spája čisto s kryptomenami k témam pojednávajúcim o využití tejto technológie v podnikových riešeniach a riešeniach pre verejnú správu.

[41] www.financnasprava.sk/_img/pfsedit/Dokumenty_PFS/Pre_media/Tlacove_spravy/Rok_2018/2018.05.21_TS_Blockchain.pdf

5 Blockchain v prostredí eGovernmentu na Slovensku

5.1 Prehľad vývoja informatizácie verejnej správy na Slovensku

Od roku 2003 sa v Slovenskej republike na národnej úrovni prijalo množstvo strategických dokumentov spojených s rozvojom informatizácie, elektronizácie, ale aj digitalizácie verejnej správy. Rozvoj moderných informačných a komunikačných technológií má ďalekosiahle dopady na každý aspekt moderného života. Tieto technológie predstavujú dôležitý nástroj a stimul rozvoja ekonomickej a sociálnej oblasti.

Informatizácia verejného sektora prostredníctvom prijímania ambicióznych plánov sa stala jednou z politických priorít. Mnohé plány, prijímané stratégie a koncepcie rozvoja zostali len v deklaratívnej polohe a ich realizácia zaostávala za očakávaniami, čo priznávajú aj aktuálne dokumenty v oblasti informatizácie.

V SR sa so zavádzaním elektronizácie verejnej správy stretávame v polovici deväťdesiatych rokov. Rozvoj sa odštartoval prijatím *zákona č. 261/1995 Z. z. o štátnom informačnom systéme*, ktorý stanovil podmienky správy štátneho informačného systému, ako aj práva a povinnosti úradov, resp. orgánov v štátnom informačnom systéme.

V roku 1999 bola prijatá stratégia reformy verejnej správy SR, ktorá predstavovala snahu o spoluprácu v oblasti informatizácie verejnej správy. Ďalším stimulom pre rozvoj elektronizácie verejnej správy v SR bolo prijatie *zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám*. V tom istom roku bola vypracovaná *Koncepcia decentralizácie a modernizácie verejnej správy*, ktorej cieľom bolo spracovanie kľúčových problémov informatizácie verejnej správy na Slovensku.

V roku 2001 bola vypracovaná *Politika informatizácie spoločnosti v SR*, ktorá vyplýva z iniciatívy eEurope+ a jedným z jej cieľov je vytvorenie a presadzovanie dlhodobej Stratégie informatizácie spoločnosti v SR.

Zákon č. *215/2002 Z. z. o elektronickom podpise* znamenal uvedenie dôležitého nástroja, na základe ktorého dochádza k identifikácii občana prostredníctvom internetu. V tom istom roku sa tiež prijal *zákon č. 428/2002 Z. z. o ochrane osobných údajov*.

Zjednodušenie získavania informácií zo strany občanov vo vzťahu k verejnej správe prinieslo v roku 2003 vytvorenie verejného informačného portálu www.občan.sk.

V januári 2004 bola prijatá *Stratégia informatizácie spoločnosti v podmienkach SR* a z nej vychádzajúce *Akčné plány*. Dokumenty obsahujú nielen strategické ciele, ale aj konkrétne a záväzné harmonogramy činností súvisiacich s procesom informatizácie spoločnosti. Zmyslom prijatia stratégie a akčného plánu bolo rozpracovanie predchádzajúceho dokumentu *Politika informatizácie spoločnosti v SR* na prioritné oblasti s časovým harmonogramom pri plnení a realizácii procesu informatizácie.

Ďalším východiskovým dokumentom budovania informatizácie z roku 2005 je *Stratégia konkurencieschopnosti SR do roku 2010*, ktorá je slovenskou verziou Lisabonskej stratégie z roku 2000. Značná časť sa zaoberala IKT ako nástrojmi na zvýšenie konkurencieschopnosti. Táto stratégia definovala hlavné oblasti a kroky politiky SR, ktoré by prispeli k naplneniu Lisabonskej agendy.

Z uvedenej stratégie vznikli akčné plány známe pod pojmom Minerva, ktoré určovali konkrétne kroky pre implementáciu politík Stratégie konkurencieschopnosti Slovenska do roku 2010.

Na základe Stratégie informatizácie spoločnosti v SR bola v roku 2005 vypracovaná *Cestovná mapa zavádzania elektronických služieb verejnej správy*. Ide o ucelený návrh, ako zavádzaním elektronických služieb koncepčne vybudovať elektronickú verejnú správu na Slovensku. Obsahom je aj časový harmonogram implementácie činností, ktoré budú v budúcnosti ponúkané občanom, podnikateľom alebo verejnej správe v elektronickej forme.

V roku 2006 bol portál www.občan.sk nahradený ústredným portálom verejnej správy SR (www.portal.gov.sk).

Stratégia informatizácie verejnej správy bola schválená vo februári 2008 ako zásadný strategický dokument, ktorý slúžil k riadeniu informatizácie verejnej správy, ktorý definoval strategické ciele informatizácie verejnej správy ako zvýšenie spokojnosti občanov, podnikateľov a ostatnej verejnosti s verejnou správou, elektronizácia procesov verejnej správy, efektívnejšia a výkonná verejná správa a zvýšenie kompetentnosti verejnej správy.

Zo Stratégie informatizácie verejnej správy vychádza *Národná koncepcia informatizácie verejnej správy*, ktorá bola schválená v máji 2008. Venuje sa princípom budovania eGovernmentu a zavádzania elektronických služieb na Slovensku. Stanovuje architektúru integrovaných informačných systémov verejnej správy a navrhuje koncepciu ich budovania tak, aby na základe dodržiavania štandardov boli informačné systémy nezávislé na technologických platformách, aby bola zabezpečená bezproblémová interoperabilita a bolo tak možné jednoduché prepojenie a vzájomná spolupráca všetkých systémov verejnej správy.

V roku 2008 bola schválená *Národná stratégia Slovenskej republiky pre digitálnu integráciu*, ktorá vyzýva štátnu správu, územné samosprávy, organizácie tretieho sektora na riešenie a realizáciu konkrétnych krokov a opatrení v problematike digitálnej integrácie. Hovorí aj o digitálnom začlenení občanov, ktorí sú ohrození digitálnym vylúčením z informačnej spoločnosti.

V tom istom roku bola prijatá *Národná stratégia pre informačnú bezpečnosť*. Ide o hlavný dokument, ktorý sa zaoberá oblasťou informačnej bezpečnosti. Dokument má tri základné úrovne. Prvá úroveň popisuje strategické ciele v tejto oblasti s dlhodobým charakterom. Druhá je zameraná na popis strategických priorít a tretia úroveň hovorí o najdôležitejších problémoch informačnej bezpečnosti.

V roku 2009 bola zriadená Národná agentúra pre sieťové a elektronické služby (NASES). Predmetom jej činnosti je realizácia aplikácie projektov a informačných systémov z oblastí informatiky a informatizácie spoločnosti, vypracúvanie koncepcií a štandardov informačných systémov verejnej správy, zabezpečovanie ich realizácie a vypracúvanie odborných stanovísk. Kľúčovými kompetenciami NASES je prevádzka a rozvoj siete GOVNET, Ústredného portálu verejnej správy, prevádzka sTESTA pre SR, rozvoj infraštruktúry širokopásmového internetu, poradenská, konzultačná, sprostredkovateľská a školiaca činnosť v oblasti informatiky, informačných sietí, elektronických komunikačných sietí, výpočtovej techniky.

Koncepcia využívania softvérových produktov vo verejnej správe bola schválená v roku 2009 a jej účelom bolo definovať rámcovú stratégiu pre obstaranie, nasadzovanie a prevádzkovanie softvérových produktov v prostredí verejnej správy, vychádzajúc z cieľov informatizácie verejnej správy v najbližších rokoch v súlade s požiadavkami a odporúčaniami EÚ.

V roku 2009 bola prijatá *Stratégia informatizácie spoločnosti na roky 2009 – 2013*, ktorá je vrcholovým strategickým dokumentom. Jej cieľom je aktualizovať stratégiu budovania informačnej spoločnosti na Slovensku a stanovuje hlavné oblasti rozvoja, ako aj priority SR nasledovne: budovanie

širokopásmových pripojení, informačná bezpečnosť a štandardy, elektronická verejná správa (eGovernment), elektronické zdravotníctvo (eHealth), digitálna gramotnosť a elektronické vzdelávanie (eEducation), znižovanie energetickej náročnosti a zvýšenie energetickej účinnosti. Tento dokument nahrádza pôvodnú Stratégiu informatizácie spoločnosti a zameriava sa najmä na tie oblasti, ktoré sa v skutočnosti vyvíjali pomalšie ako sa očakávalo.

V roku 2010 prijala SR *Stratégiu Európa 2020*, ktorá sa snažila o podporu pri implementácii a využívaní IKT. Jednou zo základných oblastí Stratégie Európa 2020 je Digitálna Agenda pre Európu (DAE) v podmienkach SR, ktorá sa zameriava na vymedzenie kľúčovej úlohy, ktorú zohrávajú IKT. Koordináciu aktivít, ktoré vyplývajú pre Slovensko z DAE na seba prevzalo MF SR, ktoré 13.4.2011 predložilo vláde SR iniciatívny materiál Digitálna agenda pre Európu v podmienkach SR.

Kritickejší pohľad na vývoj elektronizácie verejnej správy v SR reflektuje *Revízia budovania eGovernmentu* schválená v roku 2011. Materiál nenahrádza existujúce schválené strategické dokumenty, ale hodnotí najmä praktickú rovinu implementácie projektov a naznačuje potrebu revidovať koncepčné východiská v strednodobom horizonte.

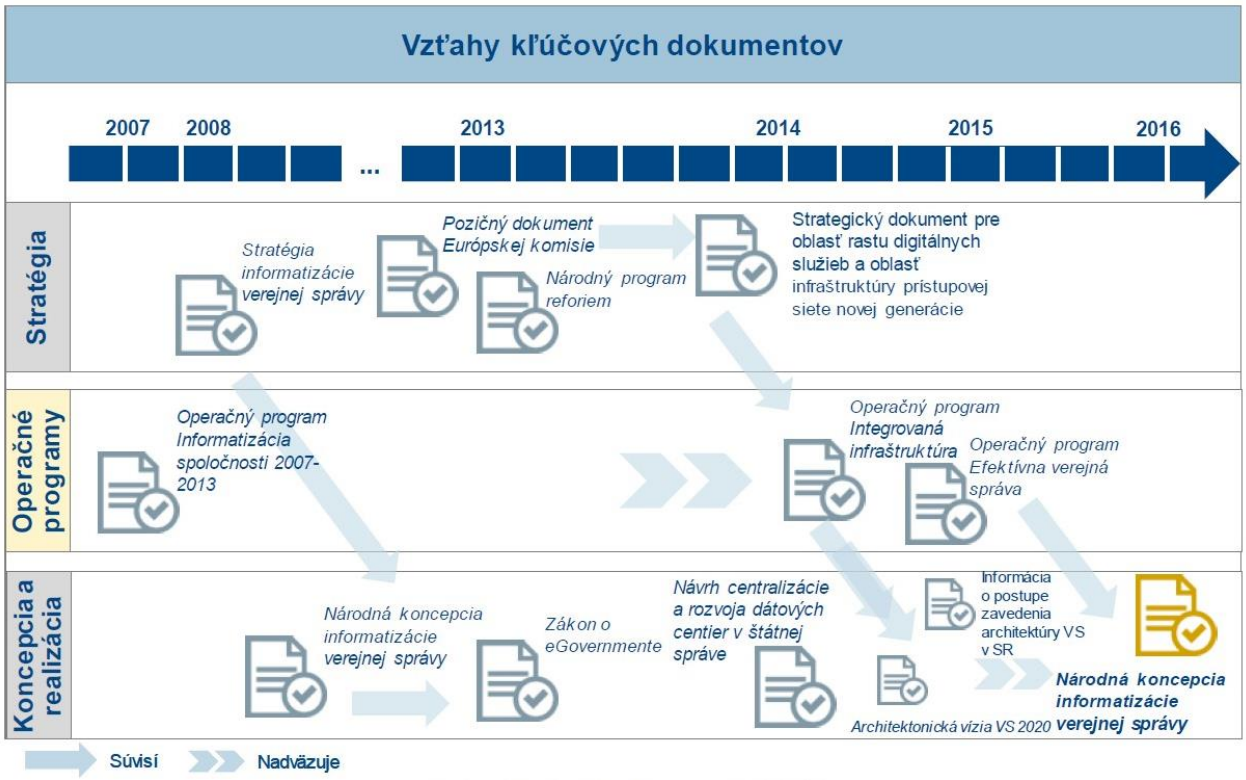
V roku 2014 bol prijatý Vládou SR *Návrh centralizácie a rozvoja dátových centier v štátnej správe*. Cieľom dokumentu je centralizácia všetkých dátových centier do dvoch hlavných – jedného v pôsobnosti Ministerstva financií SR a druhého v pôsobení Ministerstva vnútra SR, ktoré budú zamerané na poskytovanie cloudových služieb štátnym úradom a inštitúciám.

Strategický dokument pre oblasť rastu digitálnych služieb a oblasť infraštruktúry prístupovej siete novej generácie (2014-2020) definuje stratégiu ďalšieho rozvoja digitálnych služieb a infraštruktúry prístupovej siete novej generácie na Slovensku a zameriava sa na splnenie ex ante kondicionalít, prostredníctvom ktorých EÚ posudzuje pripravenosť členských štátov realizovať zvolené investičné priority.

Vláda SR dňa 28. 9. 2016 prijala strategický dokument *Národná koncepcia informatizácie verejnej správy (2016)*, ktorý definuje princípy budovanie eGovernementu na Slovensku. Dokument nadväzuje na Národnú koncepciu informatizácie verejnej správy prijatej v roku 2008. V dokumente sa prezentuje aktuálny stav architektúry integrovaného informačného systému verejnej správy, ako aj realizované rozvojové projekty a uskutočnené aktivity, no zároveň sa venuje novým princípom vyplývajúcich zo súčasných trendov a skúseností. Za východisko pre Národnú koncepciu informatizácie verejnej správy možno považovať aj nasledovnú legislatívu: zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy, zákon č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a Výnos MF SR č. 55/2014 Z. z. o štandardoch pre informačné systémy verejnej správy.

Na obrázku nižšie je uvedený prehľad a vzťahy kľúčových dokumentov slúžiacich na budovanie informatizácie v SR[42]:

[42] Národná koncepcia informatizácie verejnej správy (2016)



Obrázok 13: Prehľad a vzťahy kľúčových dokumentov

Ústredný portál verejnej správy (ÚPVS) zabezpečuje centrálny a jednotný prístup k informačným zdrojom a službám verejnej správy na internetovej stránke www.slovensko.sk. Portál zabezpečuje fyzickým a právnickým osobám služby ako: elektronické služby centrálneho elektronického priečinka, centrálnej ohlasovne, národnej evidencie vozidiel, elektronických občianskych preukazov, osvedčení o evidencii vozidla, ďalej elektronické služby registra adries a mnohé ďalšie. V rámci informačného systému pre platby a evidenciu správnych a súdnych poplatkov sa vytvoril systém, ktorý zabezpečil plnohodnotný prechod z pôvodných kolkov na elektronický bezhotovostný styk, tzv. e-Kolky.

Bol sprevádzkovaný Integrovaný informačný systém a administratívny informačný systém finančnej správy. Integrovaný informačný systém pokrýva celú šírku procesov daňových úradov (od vedenia daňového registra, cez spracovanie všetkých typov daňových priznaní a iných vstupných dokumentov, prepojenie na Štátnu pokladnicu, kompletné účtovanie a rozpočtovanie, vymáhanie pohľadávok, daňové kontroly, až po rôzne obslužné procesy typu správa poplatkov či generovanie korešpondencie). Administratívny informačný systém zabezpečuje podporu administratívnych procesov realizovaných v rámci finančnej správy.

Informačný systém Integrovaných obslužných miest (IOM) umožnil využívanie elektronických služieb verejnej správy s vysokou dostupnosťou pre obyvateľov SR. K hlavným službám, ktoré IOM zabezpečujú, je prístup k elektronickým službám verejnej správy povinných osôb (najmä podávanie návrhov, žiadostí a iných podaní) a získanie výstupu zo spracovania podania, prípadne iných dokumentov, potvrdení alebo informácií.

V septembri 2017 bola prijatá novela *zákona o e-Governmente*. Cieľom novely bolo najmä zjednotiť používané nástroje, zjednodušiť využívanie elektronických služieb a zaviesť mechanizmus kontroly

dodržiavania povinností. Medzi oblasti úpravy patrí napríklad zavedenie povinnosti používania centrálnej elektronickej podateľne, zjednodušenie „podpisovania" elektronických podaní, inštitucionalizácia vládneho cloudu a zavedenie sankcií za porušenie zákona. Najzásadnejší dopad predstavuje zavedenie centrálneho úradného doručovania, ktorého cieľom je znížiť administratívnu záťaž a zaviesť kontrolné mechanizmy. Ďalším kľúčovým opatrením je sprístupnenie online platby kartou, ktoré umožňuje používateľom elektronických služieb platiť za správne, súdne a iné poplatky.

Akčný plán informatizácie verejnej správy na obdobie 2017 až 2020 bol schválený v novembri 2017 Radou vlády SR pre digitalizáciu verejnej správy a jednotný digitálny trh. Výsledkom materiálu bude implementácia kľúčových projektov informatizácie, ako aj riešenia 25 životných situácií, ktoré budú úrady schopné riešiť podľa princípu jedenkrát a dosť. Tieto služby by mali byť spustené postupne, rovnako ako online platby štátu cez platobnú kartu a prihlasovanie s podpisovaním pomocou smartfónu. Aktivity sú zoskupené do štyroch vedných oblastí – „Lepšie dáta" a „Lepšie služby" sú zamerané na zlepšenie poskytovaných služieb pre občanov a podnikateľov. „Zdieľané služby (hybridného) vládneho cloudu" sú zamerané na zvyšovanie efektívnosti verejnej správy a „Prierezové aktivity" na posilnenie informatizácie z pohľadu legislatívy, ochrany osobných údajov a pod.

V roku 2018 vstúpil do platnosti *zákon č. 177/2018 Z. z. o niektorých opatreniach na znižovanie administratívnej záťaže využívaním informačných systémov verejnej správy a o zmene a doplnení niektorých zákonov (zákon proti byrokracii)*. Cieľom novely je zavedenie princípu jedenkrát a dosť, teda zrušenie povinnosti predkladať orgánom verejnej moci listinné výpisy, ktoré si orgány verejnej moci vedia preveriť. Pôjde o výpisy z listu vlastníctva, z obchodného registra, zo živnostenského registra a výpisy z registra trestov.

Dňa 25. 5. 2018 nadobudol účinnosť *zákon č. 18/2018 Z. z. o ochrane osobných údajov*. Týmto zákonom sa slovenský právny poriadok harmonizuje s nariadením č. 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov a smernicou európskeho parlamentu a rady (EÚ) 2016/680 o ochrane fyzických osôb pri spracúvaní osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií a o voľnom pohybe takýchto údajov a o zrušení rámcového rozhodnutia Rady 2008/977/SVV3.

Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov upravuje organizáciu, pôsobnosť a povinnosti orgánov verejnej moci v oblasti kybernetickej bezpečnosti, národnú stratégiu kybernetickej bezpečnosti, jednotný informačný systém kybernetickej bezpečnosti, organizáciu a pôsobnosť jednotiek pre riešenie kybernetických bezpečnostných incidentov a ich akreditáciu, postavenie a povinnosti prevádzkovateľa základnej služby a poskytovateľa digitálnej služby, bezpečnostné opatrenia, systém zabezpečenia kybernetickej bezpečnosti, kontrolu nad dodržiavaním tohto zákona a audit.

Jedným z kľúčových cieľov rozvoja slovenskej spoločnosti je pokrok v oblasti informatizácie verejnej správy a v oblasti poskytovania kvalitných elektronických služieb občanom. V podmienkach SR sa tento cieľ realizuje s využitím európskej finančnej pomoci, ako aj z domácich zdrojov. V programovom období 2007-2013 bol hlavným zdrojom financovania Operačný program Informatizácia spoločnosti (OPIS). Finančné prostriedky boli využité hlavne na zriaďovanie modernej verejnej správy a digitálneho obsahu a môžeme sem zaradiť nasledovné projekty: Elektronická zbierka zákonov (Slov-Lex), elektronické služby zdravotníctva (eHealth), elektronické služby národnej evidencie vozidiel, elektronický archív MV SR (eArchív), centrálny informačný systém matrík, elektronické služby katastra nehnuteľností, elektronické služby NKÚ SR, elektronické služby MPSVaR SR, digitálne školstvo (eVzdelávanie), rozvoj elektronických

služieb súdov (eJustice), elektronizácie občianskych preukazov (eID karta), elektronická poštová schránka (ePOBox), dátové centrum eGovernmentu, elektronická služba Sociálnej poisťovne (eSlužba Sociálnej poisťovne), elektronické služby Slovenskej pošty (integrované obslužné miesto občana), elektronický kolok (e-Kolok), elektronické služby Štatistického úradu, elektronické služby Generálnej prokuratúry SR a pod.

Zdrojom financovania v programovom období 2014-2020 sú Operačný program Integrovaná infraštruktúra (OPII) a Operačný program Efektívna verejná správa (OPEVS). V OPII pokrýva oblasti informatizácie prioritná os 7 s alokáciou 927 155 226 EUR (zdroje EÚ + štátny rozpočet).

Modernizovanie verejnej správy prostredníctvom OPII a OPEVS a preukázanie optimálnosti riešenia je potrebné prostredníctvom vypracovania reformného zámeru. Ku koncu roka 2018 bolo schválených 56 reformných zámerov v celkovej výške takmer 850 miliónov EUR (z toho OPII 575,6 mil. EUR a OPEVS 270,9 mil. EUR).

5.1.1 Potreby eGovernment riešení adresovateľné blockchainom

Táto kapitola sa snaží popísať niektoré všeobecné problémy, obmedzenia, nedostatky a požiadavky eGovernment riešení, kde blockchain môže prispieť k zlepšeniu. Keďže sa nám nepodarilo nájsť oficiálny ucelený a jednoznačný zoznam takýchto problémov, obmedzení a nedostatkov, snažili sme sa ich zozbierať z rôznych zdrojov a tiež využiť poznatky získané na stretnutiach zo zainteresovanými stranami. Konkrétne problémy, požiadavky a prínos blockchainu sú potom uvedené v kapitole 5.3 a 5.4 v rámci popisov jednotlivých navrhovaný príkladoch použitia.

Z takzvaného OPIS obdobia budovania e-Governmentu v rokoch 2010 až 2015 je možné identifikovať nasledovné nedostatky eGovernmentu najmä v týchto oblastiach:

- nedostatočný dôraz na systematické a holistické riadenie programu,
- nie vždy optimálne koordinačné a prioritizačné rozhodnutia spôsobené aj nedostupnosťou autentických a relevantných údajov pre podporu tohto rozhodovania (tiež nestálosť kľúčových východiskových údajov, napr. opakované neúspešné snahy o stabilizáciu tzv. číselníka životných situácií ako základného indikátora dopytu po službách eGovernmentu),
- problematické riadenie projektov budovania eGovernmentu tradičnými metódami,
- nedostatky pri riadení veľmi komplexných projektov a reťazcov dodávateľov projektových výstupov (dodávateľsky reťazec projektových výstupov reprezentuje za stranu verejnej správy typicky: riadiaci orgán, sprostredkovateľský orgán a prijímateľ a za podnikateľskú sféru okrem hlavného dodávateľa častokrát veľmi komplikovaná sieť mnohých špecializovaných subdodávateľských firiem),
- veľké množstvo čiastkových projektových produktov, veľké množstvo vzájomne sa podmieňujúcich súvislosti,
- veľká obťažnosť identifikovať reťaz príčin a dôsledkov pri sírení projektového incidentu a neskôr problému a jednoznačne priradiť zodpovednosť, vyvodiť dôsledky a zjednať nápravu,
- príkladmi takýchto komplexných projektov (a pritom z hľadiska budovania eGovernmentu ťažiskových), ktoré dodnes neboli uspokojivo ukončene a trpia mnohými problémami a komplikáciami sú napríklad projekt Elektronické služby Katastra nehnuteľnosti (ESKN), projekt Elektronické služby zdravotníctva (eHealth) alebo projekty implementácie viacerých základných

komponentov eGovernmentu a špeciálne spoločných modulov UPVS (podľa pôvodnej NKIVS z roku 2008),

- komplikácie spojené s integrovaním a zaistením interoperability individuálnych riešení eGovernmentu – typicky agendových systémov jednotlivých inštitúcii verejnej správy (pozri tiež časť 3.3.4),
- nedôvera verejnosti spôsobovaná nedostatočnou transparentnosťou procesov budovania eGovernmentu (od verejného obstarávania hlavného dodávateľa cez realizáciu projektu) ale aj elektrizovaných procesov v už modernizovaných agendových systémoch eGovernmentu (schopnosť na jednom mieste si komplexne overiť proces vybavenia "svojej" agendy a pod.)

Nedostatky uvedené vyššie je možne aspoň čiastočne adresovať použitím technológie blockchain opierajúc sa o vlastnosti popisované v tejto štúdii v kapitole 2.13 (Kľúčové vlastnosti, výhody a nevýhody), 3.2 (Blockchain a informačná bezpečnosť) a 5.3 a 5.4 (Prínosy v konkrétnych projektoch).

Niektoré ďalšie všeobecné požiadavky, ktoré môže adresovať zavedenie technológie blockchain, sumarizuje tabuľka nižšie, 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

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 10: Požiadavky na eGovernment riešenia

Aj keď existuje množstvo strategických dokumentov, akčných plánov, projektov, ako aj permanentná snaha napredovať v oblasti informatizácie verejnej správy, SR je v porovnaní s ostatnými krajinami EÚ ešte v pozadí, respektíve na zadných priečkach. Tu je však potrebné uviesť, že za ostatné roky

sa vykonalo viacero relevantných opatrení, ktoré mali v úmysle eGovernment posunúť smerom vpred. Nové technológie ako blockchain ponúkajú riešenia, ktoré by mohli zefektívniť oblasť informatizácie verejnej správy. Pri študovaní dokumentov uvedených vyššie vidíme značný prienik medzi uvádzanými prioritami a požiadavkami a základnými vlastnosťami blockchain vysvetlenými v tejto štúdii. Niektoré princípy a možný prínos blockchain je naznačený v tabuľke nižšie:

Oblasť	Názov	Referencia	Potenciál pre využitie blockchain
Dátové princípy	Údaje sú aktíva	NKIVS 2016, časť 3.2.2	vysoký
	Údaje sú dostupné a zdieľané	NKIVS 2016, časť 3.2.2	vysoký
	Údaje sú zrozumiteľné	NKIVS 2016, časť 3.2.2	stredný
	Otvorenosť údajov	NKIVS 2016, časť 3.2.2	vysoký
Bezpečnostné princípy	Bezpečnosť údajov	NKIVS 2016, časť 3.2.5	vysoký
	Pravosť údajov	NKIVS 2016, časť 3.2.5	vysoký
	Transparentnosť	NKIVS 2016, časť 3.2.5	vysoký
	Auditovateľnosť	NKIVS 2016, časť 3.2.5	vysoký
Predstavenie priorít informatizácie verejnej správy	Multikanálový prístup	NKIVS 2016, časť 6.2	stredný
	Integrácia a orchestrácia	NKIVS 2016, časť 6.2	stredný
	Riadenie údajov a big data	NKIVS 2016, časť 6.2	vysoký
	Otvorené údaje	NKIVS 2016, časť 6.2	vysoký
	Komunikačná infraštruktúra	NKIVS 2016, časť 6.2	stredný

Tabuľka 11: Niektoré princípy NKIVS 2016 a blockchain

Ako vysvetľujeme v kapitole 3.3.4, blockchain má tiež potenciál stať sa middlewarom pri prepájaní rôznych informačných systémov v rámci eGovernmentu. Po zaregistrovaní sa do spoločného middleware, ktorý využíva technológiu blockchain si môžu jednotlivé ISVS posielať medzi sebou správy veľmi bezpečným spôsobom. Samotná technológia blockchain problém vzájomného prepájania ISVS nevyrieši, avšak môže byť významným prínosom k jeho riešeniu.

Blockchain, ako je vysvetlené v kapitole 3.2.3 má tiež veľký potenciál stať sa nástrojom prevencie rôznych typov podvodov potenciálne uskutočňovaných aj v procesoch verejnej správy.

Blockchain tiež môže byť zdrojom spoľahlivých a nemenných údajov pre ďalšie spracovanie, interpretáciu a využitie pri strojovom učení a big data analýzach.

Vzhľadom na súčasný stav informatizácie na Slovensku, je však potrebné veľmi citlivo pristupovať k zavádzaniu nových riešení s dôrazom na nákladnosť investícií a zefektívnenie ponúkaných služieb. Niektoré ďalšie problémy a požiadavky eGovernment riešení a možný prínos technológie blockchain pri ich riešení sú uvedené v kapitolách vyššie:

- eID a eIDAS v kapitole 3.4.3,
- Ochrana osobných údajov v kapitole 3.4.1,
- Blockchain ako nástroj prevencie podvodov v kapitole 3.2.3,
- Správa informačných aktív a konfigurácií v kapitole 3.3.2,
- Riadenie identít a prístupov v kapitole 3.3.3,

- Ochrana údajov na účtovných dokladoch v kapitole 3.4.2

Požiadavky vyplývajúce z informačnej bezpečnosti a prínos technológie blockchain sú detailne popísané v kapitole 3.2.1 a v Tabuľka 7: Vlastnosti blockchain vs ciele informačnej bezpečnosti.

Niektoré ďalšie požiadavky na eGovernment riešenia a prínos špecifických vlastností technológie blockchain sú uvedené v nasledujúcej matici:

Niektoré požiadavky na eGovernment (nižšie) a vlastnosti blockchainu (vpravo) ktoré ich adresujú	Transparentnosť a sledovateľnosť	Možnosť verejnej kontroly	Integrita dát	Zníženie nákladov a komplexnosti	Trvalé a nemeniteľné digitálne zaznamenávanie	Redundancia uložených dát	Nastolenie dôvery	Schopnosť prepájať rôzne informačné systémy	Smart kontrakty
Jedenkrát a dosť				x				x	
Rozšírenie dostupnosti		x	x			x		x	
Zvýšenie dôveryhodnosti	x	x			x		x		x
Rozširovanie informatizácie na ďalšie oblasti				x	x			x	
Zníženie nákladov				x					x
Zvýšenie efektivity a efektívnosti				x	x			x	x
Dostupnosť dát						x	x		
Prevencia podvodov	x	x			x		x		x
Lepšia integrácia systémov			x					x	
Lepšia auditovateľnosť projektov	x								

Tabuľka 12: Niektoré požiadavky na eGovernment a vlastnosti blockchainu

5.2 Všeobecné odporúčania a odhadovaný časový rámec realizácie

Ku každému z prípadov použitia technológie blockchain (aplikácii) spomínaných nižšie odporúčame najprv vypracovanie štúdie uskutočniteľnosti daného implementačného projektu, ktorá bude obsahovať minimálne nasledovné časti:

- Súčasný stav,
- Problémy súčasného riešenia,
- Zoznam zainteresovaných subjektov (stakeholders),
- Legislatívny rámec a identifikovanie potrebných zmien,
- Očakávania zainteresovaných strán,
- Analýzu vhodnosti pre blockchain,
- Popis alternatívnych riešení a ich porovnanie,
- Detailný popis navrhovaného riešenia,
- Analýzu nákladov a prínosov,

- Odhadovaný časový rámec realizácie.

Zoznam prípadov použitia uvedený nižšie vznikol na základe súčasných poznatkov a skúseností, nasadenia v zahraničí a stretnutí so zainteresovanými stranami počas prípravy tejto štúdie. Tento zoznam nie je kompletný, očakávame identifikovanie ďalších a ďalších možných využití blockchainu v budúcnosti. Tak isto je možné, že niektoré projekty javiace sa na prvý pohľad ako vhodné, budú neskôr po detailnej analýze vyradené ako nevhodné z rôznych dôvodov. Popis projektov je len veľmi stručný a pred ich realizáciou bude nutné hlbšie skúmanie danej problematiky napríklad formou štúdie (ako je uvedené vyššie).

Harmonogram a postup realizácie jednoduchšieho projektu:

Fáza	Činnosť	Hlavné činnosti	Trvanie [týždňov]
I.	Štúdia uskutočniteľnosti, analýza, špecifikácia	Verené obstarávanie	8
		Dodávka, realizácia	8
II.	Dodávka, vývoj, testovanie, nasadzovanie, školenia	Verené obstarávanie	8
		Vývoj	13
		Testovanie, školenia, nasadzovanie	4
III.	Manažment projektu, dohľad na kvalitou	Verené obstarávanie	8 (súbežne s II.)
		Manažment a dohľad	(podľa II.)
SPOLU			41

Tabuľka 13: Harmonogram realizácie jednoduchého projektu

Harmonogram a postup realizácie stredne zložitého projektu:

Fáza	Činnosť	Hlavné činnosti	Trvanie [týždňov]
I.	Štúdia uskutočniteľnosti, analýza, špecifikácia	Verené obstarávanie	8
		Dodávka, realizácia	16
II.	Dodávka, vývoj, testovanie, nasadzovanie, školenia	Verené obstarávanie	8
		Vývoj	32
		Testovanie, školenia, nasadzovanie	8
III.	Manažment projektu, dohľad na kvalitou	Verené obstarávanie	8 (súbežne s II.)
		Manažment a dohľad	(podľa II.)
SPOLU			72

Tabuľka 14: Harmonogram realizácie stredného projektu

Harmonogram a postup realizácie väčšieho projektu:

Fáza	Činnosť	Hlavné činnosti	Trvanie [týždňov]
I.	Štúdia uskutočniteľnosti, analýza, špecifikácia	Verené obstarávanie	8
		Dodávka, realizácia	24
II.	Dodávka, vývoj, testovanie, nasadzovanie, školenia	Verené obstarávanie	12
		Vývoj	45
		Testovanie, školenia, nasadzovanie	12
III.	Manažment projektu, dohľad na kvalitou	Verené obstarávanie	8 (súbežne s II.)
		Manažment a dohľad	(podľa II.)
SPOLU			101

Tabuľka 15: Harmonogram realizácie väčšieho projektu

Poznámka: harmonogramy predpokladajú využitie existujúceho blockchainu, nezahŕňajú prípadný vývoj a nasadenie nového blockchainu.

5.2.1 Predpoklady a zdroje pre vývoj a nasadenie blockchain aplikácií

Cieľom tejto kapitoly je vysvetliť štruktúru a naznačiť odhadované náklady na vývoj, nasadenie a prevádzku distribuovaných a decentralizovaných aplikácií (d-App) využívajúcich blockchain. Odhady nákladov sú len orientačné a to z niekoľkých dôvodov:

- Blockchain a jeho využitie v komerčných alebo eGovernment riešeniach je zatiaľ veľmi mladá disciplína a napriek mnohým ohláseným zámerom je zrealizovaných len málo aplikácií (nie prototypov), ktoré využívajú technológiu blockchain a teda aj informácií o skutočných nákladoch je málo.
- K prípadom použitia blockchain diskutovaným v tomto dokumente neboli zatiaľ vypracované detailné špecifikácie na ich funkcionalitu, údaje, interakcie a požadovanú integráciu s inými systémami.

Presnejší odhad nákladov konkrétneho projektu bude vyžadovať ďalšiu komunikáciu so zainteresovanými stranami (stakeholdermi), zmapovanie súčasného stavu, problémov, očakávaní, legislatívneho rámca a ďalších súvislostí ako uvádzame v kapitole 5.2. Napriek vyššie uvedenému sa pokúsime naznačiť možné ekonomické modely fungovania, odhad nákladov a vysvetliť ich štruktúru.

Nasledujúca tabuľka uvádza hlavnú štruktúru nákladov na riešenie využívajúce blockchain. Pri modelovaní nákladov je potrebné oddeliť náklady na blockchain od nákladov na samotnú aplikáciu. Potom môžeme zvažovať varianty blockchainov a náročnosť ich implementácie. Náklady na samotnú aplikáciu sú porovnateľné, či využíva blockchain, centralizovanú databázu alebo databázu v cloude. Z toho vyplýva, že blockchain riešenie nemusí byť drahšie než tradičné a v istých prípadoch môže byť dokonca lacnejšie – z hľadiska celkových prevádzkových nákladov a zvlášť pri započítaní prínosov z vyššej informačnej bezpečnosti (viď. aj časť 3.2.3). Niektoré náklady, napríklad na údržbu a správu d-aplikácie, však môžu byť vyššie kvôli rizikám uvedeným v kapitole 3.2.2.

Skupina	Typ nákladu	Príklad nákladu
1 Blockchain	1.1 Jednorazové náklady	zriadenie uzlov, kúpa a inštalácia uzlov, vývoj/zakúpenie blockchain platformy
	1.2 Prevádzkové náklady	poplatky za zápis transakcie, prevádzka uzlov siete (el. energia, pripojenie do siete, servis, housing, cloud poplatky)
2 distribuovaná a decentralizovaná aplikácia (d-App)	2.1 Jednorazové náklady	analýza, návrh, vývoj, testovanie, integrácia do blockchain, nasadenie aplikácie
	2.2 Prevádzkové náklady	administrácia, údržba, zmeny aplikácie, podpora používateľov aplikácie (ročne typicky 10-20% z investičných nákladov 2.1)
3 Integrácia s existujúcimi systémami	3.1 Jednorazové náklady	analýza, návrh, vývoj, testovanie, nasadenie interfejsu s existujúcimi systémami (napr. podnikový ERP alebo IS verejnej správy)
	3.2 Prevádzkové náklady	administrácia, údržba, zmeny, atď. interfejsu (ročne typicky 10-20% z investičných nákladov 3.1)
4 Iné náklady	4.1 Jednorazové náklady	inštalácia u používateľov, školenia, propagácia
	4.2 Prevádzkové náklady	správa používateľov a ich prístupov

Tabuľka 16: Štruktúra nákladov riešenia využívajúceho technológiu blockchain

Jedno z kľúčových rozhodnutí je, aký typ blockchain technológie použijeme. Existujú dva hlavné smery: využiť existujúci verejný blockchain (napr. Ethereum) alebo budovať vlastný. Jednoduché odporúčanie a jednoznačné správne riešenie neexistuje, oba varianty majú svoje výhody a nevýhody, ktoré vyplývajú z popisu v kapitole 2 a 3 a tiež iný ekonomický prevádzkový model. Nasledujúca tabuľka sumarizuje niektoré hlavné vlastnosti oboch variantov:

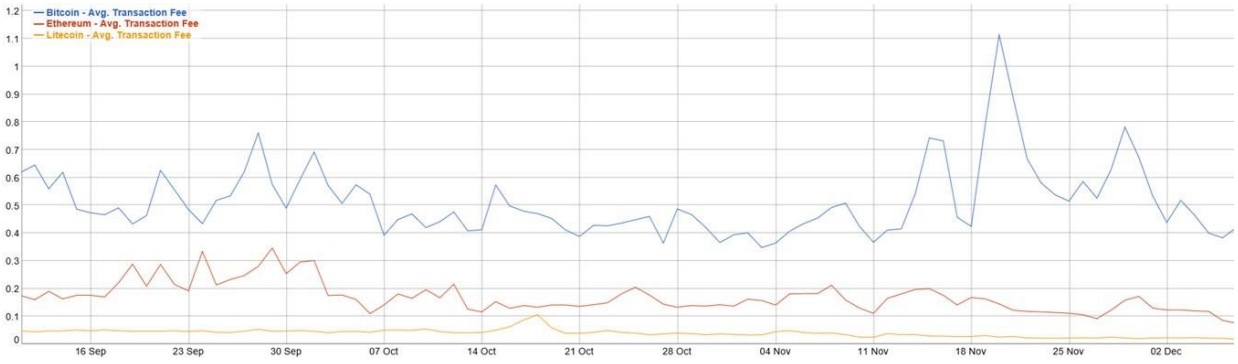
Predmet	Existujúci blockchain	Nový, vlastný blockchain
Dostupnosť (čas realizácie)	Ihneď	týždne (exist. platforma) - mesiace (upravená platforma, pripadne nová)
Možnosť úpravy na mieru, implementácia špeciálnych požiadaviek	žiadna, len výber najvhodnejšieho z dostupných blockchainov	vysoká
Investičné náklady	žiadne	stredné (exist. platforma, cloud, exist HW) až vyššie (vlastná platforma, fyzické uzly na novom HW)
Prevádzkové náklady	obyčajne nižšie, podľa objemu zapísaných transakcií	stredné, podľa počtu a spôsobu prevádzky uzlov
Volatilita prevádzkových nákladov	vyššia - väčšinu času sú nízke, ale v istom období sa môžu skokovo zvýšiť (viď napr. BTC v r. 2017)	malá
Riziká	viď kapitola 3	viď kapitola 3
Možnosť zmeny	jednoduchšia (neinvestovali sme, žiaden záväzok používania)	nákladnejšia (investície, HW)

Predmet	Existujúci blockchain	Nový, vlastný blockchain
Možnosť privátneho, neverejného riešenia	minimálna (kryptovanie)	vysoká

Tabuľka 17: Porovnanie existujúci a nový blockchain

Blockchain, ako každá iná SW a HW infraštruktúra, nie je zdarma. Prevádzkovatelia uzlov potrebujú investovať do HW, tento HW musí byť niekde umiestnený, niekto ho musí nainštalovať, musí byť napájaný elektrickou energiou, chladený, pripojený k Internetu a tiež niekým spravovaný a servisovaný. Všetko to vyžaduje náklady a prevádzkovateľ uzla musí byť niečím motivovaný, aby investoval a prevádzkoval uzol siete. Naviac, sieť blockchain z princípu preferuje čo možno najvyšší počet uzlov a ich rozmanitosť: umiestnených na geograficky rôznych miestach, nezávisle spravovaných, nezávisle napájaných a nezávisle pripojených k Internetu. V ďalšej časti sú naznačené možné prevádzkové a odmeňovacie modely.

Asi najznámejším modelom je model bežný u kryptomien, a to odmena vo forme kryptomeny pridelená uzlu ktorý vytvára nový blok. Napr. v Bitcoine získa uzol vytvárajúci nový blok odmenu 12,5 BTC (súčasný stav, približne o dva roky klesne na 6,25 BTC) za každý nový blok a približne 0,05 – 0,5 EUR za transakciu. Odmena za nový blok je nie je hradená používateľmi, ale sú to novo-emitované BTC. Používateľ požadujúci zápis transakcie platí len poplatok za samotnú transakciu. V sieti Ethereum je odmena za nový blok približne 500 EUR a bežná cena za transakciu 0,05 – 0,2 EUR. Maximálna cena transakcie sa dostala na asi 4 USD na veľmi krátky čas v januári 2018 a júli 2018. Cena v moderných blockchain sieťach sa pohybuje len okolo 0,01 – 0,05 EUR za uloženú transakciu, v závislosti od jej veľkosti. Pri využití verejného blockchainu nie je potrebné investovať do budovania siete, stačí využiť existujúcu sieť a platiť len poplatky za transakcie. Tieto sú obyčajne nízke, aj keď je isté riziko, že na krátky čas v prípade nepredvídateľných udalostí môže cena transakcie vzrásť. Vývoj priemerných poplatkov za transakciu v Bitcoin, Ethereum a Litecoin je zobrazený v grafe nižšie:[43]



Obrázok 14: Cena transakcie v období september až december 2018

Pri konzorčných alebo privátnych blockchainoch nemusia byť uzly odmeňované za validovanie bloku alebo zaradenie transakcie. Účastníci konzorcia (napr. štátne inštitúcie, notári, firmy z dodávateľského reťazca a pod.) sa môžu dohodnúť na zriadení a prevádzkovaní blockchainu bez poplatkov – každý bude benefitovať z prínosov riešenia a prijme za to záväzok prevádzkovať uzol siete požadovaných parametrov. V prípade štátneho blockchainu tiež prichádza do úvahy nariadenie vybudovania

[43] https://bitinfocharts.com/comparison/transactionfees-btc-eth-ltc.html#3m

a prevádzkovania týchto uzlov zo zákona, resp. príslušných vykonávacích predpisov. Tento model je možný iba ak nehrozí nadspotreba alebo zneužívanie siete.

V prípade budovania vlastnej blockchain siete sú nutné investície do zriadenia uzlov. Obstaranie samotného servera predstavuje jednorazový náklad od približne 1000 EUR vyššie podľa konfigurácie. Ďalej je potrebná inštalácia a obvyklá prevádzka (napájanie, chladenie, pripojenie do siete, housing, servis). Náklady je potrebné samozrejme vynásobiť počtom uzlov. Poplatky za transakciu nám odpadnú.

Ďalšou možnosťou je zriadiť uzly siete blockchain v cloudovom riešení. Odpadnú nám investičné náklady na zriadenie uzlov a zjednoduší sa prevádzka za cenu pravdepodobne vyšších prevádzkových nákladov. Výhodou je tiež jednoduchá škálovateľnosť – pridávanie uzlov a ich rozširovanie.

Poznámka: Pri zriaďovaní uzlov siete blockchain v cloude je potrebné dbať na to, aby aj v tomto prípade jednotlivé uzly „patrili" vzájomne nezávislým – logicky oddeleným prevádzkovateľom. Je potrebné vyhnúť sa lákavej myšlienke zveriť prevádzku uzlov v cloude jednej inštitúcii – tá by sa totiž stala „vlastníkom" celého blockchainu (administrátor zamestnaný touto inštitúciou by dokázal manipulovať s kópiu blockchain databázy na všetkých uzloch súčasne). Podobne je potrebné zamyslieť sa nad dôveryhodnosťou poskytovateľa cloudových služieb a tiež, či disponuje dostatočnými kontrolnými mechanizmami, pomocou ktorých dokáže zaistiť anonymitu "čo a na ktorom fyzickom serveri sa nachádza" a zabrániť tak, aby sa administrátor tohto cloudu mohol vôbec pokúsiť zmocniť sa viacerých cloudových uzlov tej istej siete blockchain. Máme za to, že cloudové služby známych – tzv. veľkých komerčných poskytovateľov túto podmienku spĺňajú, čo však nemusí byť prípad menších – lokálnych dátových centier (aj keď s prívlastkom „cloudové").

Výhodnou architektúrou siete blockchain tiež môže byť hybridný model – časť uzlov fyzických na rôznych miestach a časť virtuálnych v cloude, resp. ešte lepšie u rôznych poskytovateľov cloudových služieb.

Pre naplnenie očakávaní od blockchainu a minimalizáciu rizík uvedených v kapitole 3.2.2. by mali byť uzly čo najrôznorodejšie, spravované rôznymi entitami a umiestnené na geograficky rôznych miestach. Pri budovaní vlastnej – národnej siete blockchain je teda zváženie vhodného logického a fyzického „rozmiestnenia" uzlov, z hľadiska budúcej dôveryhodnosti tejto siete, kľúčové a robenie kompromisov s cieľom znížiť úvodnú investíciu tu nie je na mieste.

Ďalej je nutné rozhodnúť sa, ktoré sú požadované vlastnosti blockchainu podľa zamýšľanej aplikácie, resp. aplikácií a plánov do budúcna. Hlavné vlastnosti sú uvedené nižšie, podrobnejšie sú vysvetlené (včítane výhod a nevýhod) v kapitole 2 a 3:

- Konsenzuálny algoritmus,
- Možnosť smart kontraktov,
- Prevádzkový model – motiváciu validátorov,
- Požadovaný prístup: verejný, konzorčný alebo súkromný blockchain,
- Požadovanú kapacitu a odozvu.

Pri rozhodovaní sa o špecifikácii, vlastnostiach a zvažovaní nákladov treba brať do úvahy, že jedna infraštruktúra blockchain bude zrejme využívaná mnohými aplikácie (čím viac tým lepšie pre zaistenie návratnosti investície do tejto infraštruktúry), t. j. mala by vyhovovať aj ďalším zamýšľaným projektom, jej náklady sa budú deliť medzi viac projektov a očakávame tiež prínosy z viacerých projektov. O prínosoch blockchainových riešení pojednáva kapitola 2.13.

Nasledujúca tabuľka uvádza odhadované náklady na vývoj blockchain aplikácií, ktorých základná

špecifikácia vychádza z príkladov použitia uvedených v kapitole 5.3 a 5.4. Odhady sa tiež opierajú o dostupné informácie o nákladoch na predchádzajúce eGovernment riešenia, konzultácie s dodávateľmi IT riešení, ktorí majú skúsenosti s vývojom blockchain riešení a o prístup k modelovaniu nákladov pomocou Use Case Points[44] (UCP). UCP je technika na modelovanie a predpovedanie nákladov na vývoj SW.

Pri rámcových pracovných prepočtoch sme do UCP modelu príslušnej triedy (veľkosti) projektu (distribuovanej aplikácie) nahrali aj odhady o počte a zložitosti funkčných scenárov (use case) a typov a náročnosti používateľov daného projektu ako aj odhadli jednotlivé faktory technickej komplexnosti (TCF) a faktory komplexnosti prostredia (ECF), pričom vyššie hodnoty z titulu použitia technológie blockchain sme prisúdili týmto faktorom:

- TCF - Distribuovaný systém,
- TCF - Efektívnosť pre používateľa,
- TCF - Komplexnosť vnútorných procesov (u niektorých stredných a väčších projektov),
- TCF - Jednoduchosť používania,
- TCF - Jednoduchosť zmeny,
- EFC - Skúsenosti s implementáciou,
- EFC - Schopnosť vedúcich analytikov,
- EFC – Motivácia.

Ako dennú sadzbu sme použili 750 EUR/deň (s poznámkou, že pre projekty vývoja aplikácií využívajúcich blockchain je v súčasnosti potrebné uvažovať s o niečo vyššou cenou práce ako je tomu pri tzv. tradičných prístupoch k vývoju softvéru – vyššia atraktivita pre kvalitných vývojárov a zároveň vyššie projektové riziká spojené s novou technológiou).

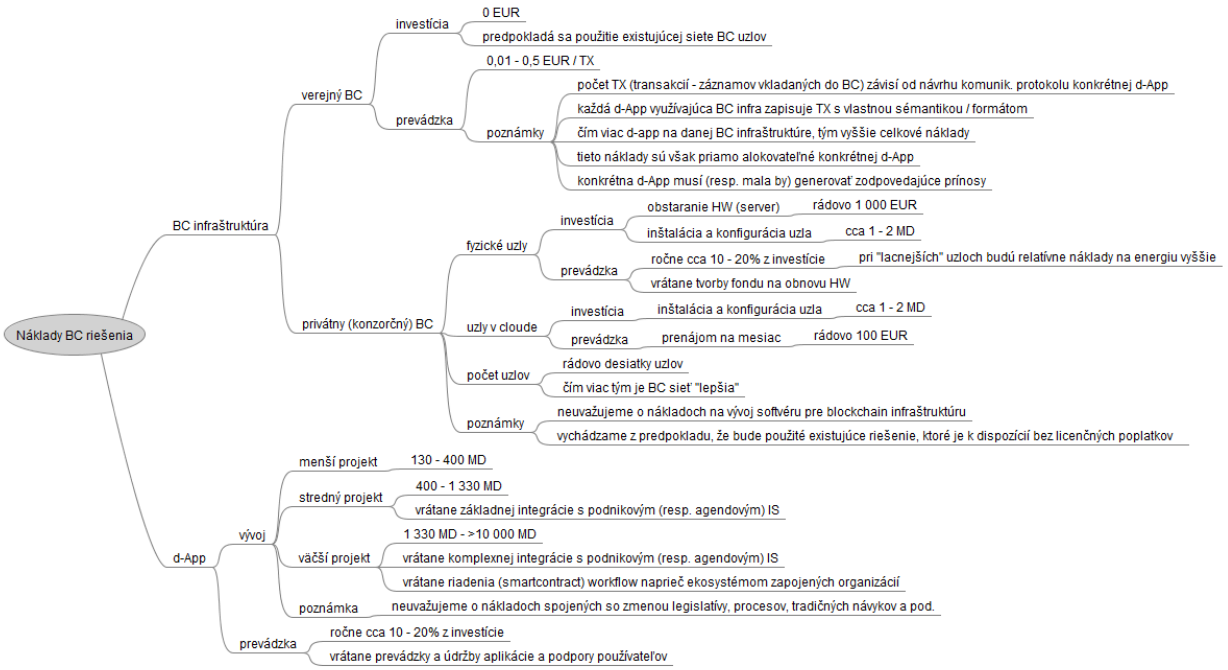
Ako sme už uviedli vyššie, keďže nevychádzame z presnej špecifikácie požiadaviek na dané riešenie, sú uvádzané odhady len orientačné. Pre zjednodušenie uvádzame tri kategórie projektov:

Predmet	Charakteristika	Príklad	Odhadovaný náklad (EUR bez DPH)
Menší projekt	nie je potrebná integrácia, nie sú otázky GDPR, ochranu obdobných údajov, jednoduché riešenie	"quick-wins" projekty 5.3.1, 5.3.3	100 000 – 300 000
Stredný projekt	stredne zložité procesy, požadovaná istá integrácia s exist. systémami,	5.4.1, 5.4.4	300 000 – 1 000 000
Väčší projekt	komplexné procesy, otázky súvisiace s ochranou osobných údajov, mnoho subjektov, integrácia s mnohými systémami	5.4.6, 5.4.9	1 mil. – 10 mil. a viac

Tabuľka 18: Porovnanie odhadovaných nákladov

Zjednodušený nákladový model blockchain riešenia podľa preferovaného architektonického rozhodnutia a zložitosti aplikácií je znázornený na nasledujúcej schéme (Obrázok 15).

44 https://en.wikipedia.org/wiki/Use_Case_Points



Obrázok 15: Zjednodušený nákladový model blockchain riešenia

Pred obstaraním realizácie finálneho projektu je možné rýchlo (rádovo týždne) a s relatívne nízkymi nákladmi zrealizovať funkčný prototyp riešenia, na ktorom je možné demonštrovať a testovať hlavné vlastnosti riešenia. Prototyp môžu testovať používatelia, môžu sa ňom overiť prevádzkové vlastnosti, jednoduchosť používania, funkčnosť apod. Pre fungovanie prototypu je možné okamžite využiť niektorý z verejných blockchainov alebo použiť testovací privátny blockchain len s niekoľkými uzlami, napr. aj v cloude bez dočasného oddelenia „vlastníctva" jednotlivých uzlov siete.

Vzhľadom na vyššie uvedené, odporúčame vybrať na realizáciu niektorý z „quicks wins" projektov uvedených v kapitole 5.3 alebo niektorý z jednoduchších projektov z kapitoly 5.4. Pred realizáciou jednoznačne odporúčame vykonať analýzu podľa bodu 5.2 a zvážiť možnosť overenia na prototype. Odhadované časové rámce realizácie sú uvedené tiež v kapitole 5.2.

5.3 Jednoduché „quick wins" prípady použitia

V tejto časti uvádzame výber prípadov použitia technológie blockchain, ktoré môžu aj významne zlepšiť niektoré aspekty poskytovania služieb verejnej správy, resp. významne zvýšiť dôveru verejnosti v štát a samosprávu. Zložitosť a cena ich implementácie pritom nemusí byť vysoká. Pre implementáciu „quick wins" je tiež dôležité aby kvôli nim, podľa možnosti, nemusela byť menená legislatíva ani existujúce procesy (t.j. „veci" sa budú robiť podľa rovnakých pravidiel ale trochu inak – lepšie). U týchto projektov očakávame žiadne alebo len minimálne súvislosti a nadväznosti na iné projekty.

Poznámka: Vzhľadom na uprednostnenie relatívne nižšej náročnosti implementácie sa v uvedených prípadoch nejedná o opatrenia, ktoré zásadným spôsobom odstránia nedostatky v budovaní eGovernmentu, o ktorých píšeme v predchádzajúcich častiach.

5.3.1 Transparentná verejná správa – hash zverejňovaných dokumentov v blockchaine

Problém: Určité dokumenty sú zverejňované na webových stránkach štátnej správy a samosprávy. Existuje však riziko, že tieto dokumenty budú dodatočne zmenené (náhodne alebo úmyselne – napr. v dôsledku hackerského útoku). Takéto prípady zneisťujú verejnosť a môžu spôsobiť stratu dôvery vo verejnú správu.

Navrhované riešenie a prínos využitia blockchain: Pri zverejnení dokumentu by bol vypočítaný aj hash dokumentu a tento by bol uložený do blockchainu. Verejnosť by si následne kedykoľvek mohla overiť, že dokument nebol neskôr pozmenený. Z blockchainu je tiež zrejmé, kedy bol hash uložený a teda najneskorší možný čas kedy bol vypočítaný. Takéto riešenie by bolo jednoducho, ľahko a rýchlo realizovateľné. Výhodou tiež je, že nenarážame na problémy s ochranou osobných údajov, GDPR, šifrovaním a pod. Podobný projekt zrealizovalo koncom roka 2017 Mesto Viedeň spolu s EY.[45]

Predmet	Ciele	Harmonogram	Zdroje, predpoklady a súvislosti s inými projektami
Transparentná verejná správa - hash zverejňovaných dokumentov v blockchaine	Zvýšiť dôveryhodnosť zverejnených dát zamedzením spätného zmenenia	41 týždňov v zmysle kapitoly 5.2	Ekonomické modely fungovania blockchain projektov sú načrtnuté v kapitole **Error! Reference source not found.**, presnejšie odhady potrebných zdrojov a súvislosti s inými projektami ukáže štúdia uskutočniteľnosti daného projektu

Tabuľka 19: Zverejňovanie dokumentov – Blockchain „quick win“

5.3.2 Transparentné riadenie samosprávy

Problém: Problematiku spomenutú v časti 5.3.1, je možné zúžiť na konkrétne agendy samosprávy (a konkrétneho mesto alebo obec) a metaúdaje o udalostiach, ktoré sú generované počas spracúvania týchto agend.

Navrhované riešenie a prínos využitia blockchain: Spoľahlivým a autentickým (autor, čas) zápisom vybraných metaúdajov o udalosti, resp. úkone vykonanom samosprávou (viď. tiež časť 3.3.1 Log udalostí) do verejného blockchainu sa môže dosiahnuť významné zvýšenie elektronizácie, dostupnosti, auditovateľnosti a transparentnosti postupov samosprávy. Záujem o ad-hoc alebo pravidelný prístup k takýmto, v podstate okamžite viditeľným, údajom môže mať nielen verejnosť ale aj orgány štátnej správy, prípadne orgány riadiace a kontrolujúce poskytovanie pomoci z EÚ fondov. K údajom o udalosti zaznamenávanej do blockchainu je možné podľa potreby pridať aj hash elektronického dokumentu, ktorý dopĺňa kontext tejto udalosti, pričom samotný dokument môže byť uložený „off-chain“ (viď. časť 2.10).

Základný návrh tém, ktoré je možné použiť na ďalšiu diskusiu a s cieľom definovať konkrétne udalosti a úkony samosprávy, metaúdaje ktorých má zmysel ukladať do verejného blockchainu:

- školy a materské školy: plánovanie kapacít, férové prideľovanie miest a prijímanie žiakov,
- stavebné úrady: sledovanie základných míľnikov pri územnom a stavebnom konaní,
- miestne oznamy: udalosti, plány, zmeny, nariadenia, vyhlásenia a pod. (časť 5.3.1),

[45] https://www.ey.com/en_gl/news/2018/08/ey-and-city-of-vienna-collaborate-on-public-blockchain-networks

- rozpočet (a verejný kontroling): príprava, schvaľovanie, čerpanie (plánované, mimoriadne),
- zmluvy s tretími stranami: výberové konanie, príprava zmlúv, plnenie zmlúv (sledovanie plnenia SLA a penalizácia), dodatkovanie zmlúv,
- iné dôležité témy samosprávy ako zdravotná starostlivosť, dopravené služby a pod.

Technické poznámky k implementácii v režime „quick win":

- Záznam vo verejnom blockchaine obsahuje len základné atribúty o udalosti: kedy, kto, čo, komu, kde, prečo, v akej hodnote a pod. a zaisťuje ich autenticitu, integritu a dostupnosť,
- Všetky údaje sú viditeľné pre všetkých, t.j. je nutné voliť len také atribúty, ktoré môžu byť zverejnené.
- Zapisovať je možné len pomocou špeciálnej verzie distribuovanej aplikácie (prístupná pre zapisujúcich úradníkov) ale predovšetkým záznam je podpísaný súkromným kľúčom úradníka alebo spoločným súkromným kľúčom úradu (samosprávy). Platnosť záznamu je možné overiť pomocou príslušného verejného kľúča voľne dostupného a riadne zabezpečeného v tom istom blockchaine (t.j. aj keď sa do blockchain pokúsi zapísať udalosť neautorizovaný používateľ, jeho zápis bude možné jednoducho odhaliť a ignorovať).
- Úradník zapisuje údaje manuálne, t.j. nepredpokladá sa integrácia na zdrojový informačný systém samosprávy. Okrem času zápisu do blockchain (automaticky a spoľahlivo generované blockchainom) bude úradník zapisovať aj údaj o čase, kedy daná udalosť nastala (pred zápisom do blockchain).
- Súčasťou riešenia (distribuovanej aplikácie) budú len základné nástroje na vyhľadávanie a získavanie (download) údajov z blockchainu. Nástroje na komplexné analyzovanie a reporting sa budú vytvárať dodatočne podľa potrieb konkrétneho „čitateľa".
- Preddefinované budú základné typy zapisovaných udalostí, resp. úkonov. Riešenie však bude otvorené pre dopĺňanie ďalších typov udalostí podľa reakcie a dopytu „čitateľov". Ďalšie typy udalostí by malo byť možné dopĺňať bez zásadného (prípadne žiadneho) programátorského zásahu.

Predmet	Ciele	Harmonogram	Zdroje, predpoklady a súvislosti s inými projektami
Transparentné riadenie samosprávy	Zvýšiť dôvery vo férové prideľovanie zdrojov a hospodárne využívanie financií samosprávou	41 týždňov v zmysle kapitoly 5.2	Ekonomické modely fungovania blockchain projektov sú načrtnuté v kapitole **Error! R eference source not found.**, presnejšie odhady potrebných zdrojov a súvislosti s inými projektami ukáže štúdia uskutočniteľnosti daného projektu

Tabuľka 20: Transparentné riadenie samosprávy – Blockchain „quick win"

5.3.3 Transparentné otváranie obálok s cenovými ponukami

Problém: Z obavy (či už odôvodnenej alebo nie), že cenová ponuka uchádzača môže byť vyzradená, napr. v prospech iného uchádzača, ešte pred oficiálnym „otváraním obálok" (papierových alebo elektronických), uchádzači typicky zdržiavajú odoslanie cenových ponúk do posledného možného momentu.

Navrhované riešenie a prínos využitia blockchain: Každý uchádzač uloží do termínu odovzdávania ponúk do verejnej blockchainovej databázy len hash svojej cenovej ponuky (hash elektronického dokumentu, ktorý reprezentuje cenovú ponuku). Samotnú cenovú ponuku prinesie až na oficiálne „otváranie obálok" kde sa stretne s ostatnými uchádzačmi. Až tu uchádzač prvýkrát predstaví svoju cenovú ponuku, pričom umožní každému inému uchádzačovi a výberovej komisii, aby si vypočítali hash jeho ponuky a porovnali ho s pôvodným hashom v blockchaine.

Poznámky:

- Zavedenie tohto opatrenia do praxe verejnej správy by zrejme vyžiadalo malú zmenu zákona o verejnom obstarávaní, čo však nemusí byť „jednoduché“ a môže tento prípad použitia vyradiť zo zoznamu „quick wins“.
- Tento prípad použitia blockchain je možné analogicky a veľmi jednoducho použiť v mnohých iných situáciách, napr. pri potrebe zaistenia nespochybniteľného náhodného výberu (napr. pri výbere kontrolovaného subjektu alebo štátneho úradníka zodpovedného za vykonanie určitého úkonu – sudca či exekútor) alebo pri rôznych lotériách a stávkach a pod.

Predmet	Ciele	Harmonogram	Zdroje, predpoklady a súvislosti s inými projektami
Transparentné otváranie obálok s cenovými ponukami	Zvýšiť dôveryhodnosť procesov verejného obstarávania	41 týždňov v zmysle kapitoly 5.2	Ekonomické modely fungovania blockchain projektov sú načrtnuté v kapitole **Error! R eference source not found.**, presnejšie odhady potrebných zdrojov a súvislosti s inými projektami ukáže štúdia uskutočniteľnosti daného projektu

Tabuľka 21: Transparentné otváranie cenových ponúk – Blockchain „quick win“

5.3.4 Potvrdenie o návšteve školy

Problém: Jedno z najpoužívanejších tlačív na Slovensku je Potvrdenie o návšteve školy. Rodič musí toto potvrdenie získať v škole a následné doručiť na Úrad práce, sociálnych vecí a rodiny, zamestnávateľovi, zdravotnej poisťovni a sociálnej poisťovňa. Dokladovať návštevu školy je v týchto prípadoch samozrejme potrebné, avšak chodenie s lístočkom je neefektívne a je stratou času.

Navrhované riešenie a prínos využitia blockchain: Škola by mohla do blockchainu zapísať údaje žiaka, rodič by si tento zápis mohol overiť a každá inštitúcia alebo zamestnávateľ by si v blockchaine overil, že dieťa navštevuje školu. V prípade ukončenia dochádzky by škola o tom vložila ďalší záznam.

Predmet	Ciele	Harmonogram	Zdroje, predpoklady a súvislosti s inými projektami
Potvrdenie o návšteve školy	Odbremeniť rodičov od dokladovania návštevy školy v zmysle pravidla jedenkrát a dosť	41 týždňov v zmysle kapitoly 5.2	Ekonomické modely fungovania blockchain projektov sú načrtnuté v kapitole **Error! R eference source not found.**, presnejšie odhady potrebných zdrojov a súvislosti s inými projektami ukáže štúdia uskutočniteľnosti daného projektu

Tabuľka 22: Potvrdenie o návšteve školy – Blockchain „quick win“

5.3.5 Register dosiahnutého vzdelania

Problém: Potreba nezmeniteľného a dôveryhodného záznamu o dosiahnutom vzdelaní a získaných akademických titulov.

Navrhované riešenie a prínos využitia blockchain: Škola s príslušným právom by po dosiahnutí vzdelania alebo udelení titulu uložila záznam do blockchainu. Blockchain by zabezpečil nemennosť a dôveryhodnosť tohto záznamu a tiež dôveryhodný záznam o období získania titulu. Zamestnanec by nemusel dokladovať dosiahnuté vzdelanie pri nástupe do práce, zamestnávateľ by mal vysokú istotu o uvádzanom dosiahnutom vzdelaní. Tento projekt spĺňa väčšinu znakov vhodnosti využitia blockchainu: mnoho účastníkov, potreba nastolenia dôvery, potreba dôveryhodného zdieľania histórie transakcií, potreba

zjednodušeného riešenia sporov.

Predmet	Ciele	Harmonogram	Zdroje, predpoklady a súvislosti s inými projektami
Register dosiahnutého vzdelania	Zaistiť nezmeniteľné a dôveryhodné záznamy o dosiahnutom vzdelaní a získaných akademických titulov.	41 týždňov v zmysle kapitoly 5.2	Ekonomické modely fungovania blockchain projektov sú načrtnuté v kapitole **Error! Reference source not found.**, presnejšie odhady ukáže štúdia uskutočniteľnosti daného projektu

Tabuľka 23: Register dosiahnutého vzdelania – Blockchain „quick win“

5.4 Ďalšie prípady použitia

5.4.1 Proces a dokumenty verejného obstarávania

Problém: Riziko popísané v časti 5.3.1 sa zvlášť týka dokumentácie procesu verejného obstarávania. Rôzne súvisiace dokumenty, resp. ich časti, ktoré neobsahujú „príliš“ citlivé informácie, sa už dnes zverejňujú na rôznych webových sídlach (elektronické vestníky, centrálny register zmlúv alebo stránky jednotlivých inštitúcii verejnej správy). Pre zvýšenie dôvery podnikateľov a občanov v procesy verejného obstarávania je vhodné chrániť integritu týchto dokumentov (autenticitu a nepopierateľnosť, čas vzniku a nemennosť).

Navrhované riešenie a prínos využitia blockchain: Podobne ako v časti 5.3.1 by u všetkých zverejňovaných dokumentov (zadanie, verejné údaje o ponuke uchádzačov, rozhodnutie, vyhlásenie výsledkov a zmluva) by bol vypočítaný ich hash a tento by bol uložený do verejného blockchainu spolu s ďalšími metaúdajmi popisujúcimi vykonaný úkon. Verejnosť by mohla následne kedykoľvek overiť, že hash bol uložený v danom čase a že dokument nebol neskôr zmenený a je autentický.

5.4.2 Rozšírenie viditeľnosti v dodávateľských reťazcov

Podpora riadenia dodávateľských reťazcov je jedným z často diskutovaných prípadov použitia technológie blockchain. Blockchain tu môže slúžiť nielen ako univerzálny technický interfejs medzi ľubovoľným počtom účastníkov dodávateľského ekosystému ale najmä ako prostriedok pre odstránenie oneskorení a šumu, ktoré spôsobuje šírenie informácie medzi dvojicami zadávateľ – dodávateľ (hra na detský telefón) a tiež ako prostriedok pre zlepšenie kolaborácie a v konečnom dôsledku aj prijímania spontánnych, a z hľadiska celého ekosystému, efektívnych rozhodnutí (a to bez nutnosti, aby bol tento ekosystém niekým vlastnený).

Dodávateľsko-odberateľské vzťahy pritom vytvárajú nielen komerčné firmy navzájom a ich zákazníci ale analogicky aj inštitúcie verejnej správy navzájom a ich zákazníci (občania a podnikatelia), resp. kombinovane – komerčné firmy spolu s IVS.

Takýmto dodávateľským reťazcom je napr. aj:

- systém inštitúcií verejnej správy, ktoré spolupracujú pri „dodávke“ služby eGovernmentu v rámci riešenia životnej situácie občana alebo podnikateľa (viď. tiež časť 3.3.4 Komunikačný middleware),
- IVS a komerčné firmy spolupracujúce pri realizácií zložitého projektu implementácie informačného systému verejnej správy (viď. tiež časť 5.4.3),

- ale aj klasický dodávateľský reťazec tovarov a služieb, ktorý kombinuje IVS a komerčné firmy (napr. služby MHD, do ktorých je zapojené mesto, dopravný podnik ale aj MV SR a MDV SR a množstvo firiem zabezpečujúcich technické prostriedky a podmienky MHD).

Dodávateľský reťazec podporovaný komunikačným riešením na báze technológie blockchain môže spoľahlivo slúžiť veľkému množstvu entít a vytvoriť medzi nimi prostredie dôvery bez potreby centrálnej autority. Čím viac účastníkov sa pripojí (typicky dobrovoľne), tým väčší objem údajov môže byť použitý v prospech efektívneho fungovania celého ekosystému. Samozrejme je potrebné zvážiť, ktoré informácie ukladať v otvorenej podobe, ktoré šifrovať a ktoré neukladať vôbec, aby sa účastníci necítili ohrození.

5.4.3 Rozšírenie viditeľnosti v komplexných projektoch

Použitie technológie blockchain pri riadení komplexných projektov s veľkým množstvom subdodávateľov je v podstate analógiou prípadu popísaného v časti 5.4.2.

Napr. namiesto udalostí typu:

- odoslanie / (ne)akceptovanie objednávky a odoslanie / prijatie / (ne)akceptovanie dodávky, by v prípade riadenia projektu mohli byť v blockchaine zdieľané udalosti typu:
- zadanie / (ne)prevzatie pracovného balíka a dodanie / otestovanie / (ne)prevzatie projektového produktu a pod.

Autentické, spoľahlivé, včasné a podľa možnosti „celoplošné“ šírenie požiadaviek, inštrukcií, rizík, incidentov, ponaučení a iných projektových informácií považujeme za kľúčový predpoklad úspechu pri riadení komplexných projektov, ktoré sú súčasťou budovania eGovernmentu (veľa projektových produktov, komplikované súvislosti a veľké celospoločenské dopady).

Takýchto projektov sa zúčastňuje viacero IVS (okrem realizátora – typicky prijímateľa pomoci z EÚ fondov aj ďalšie spolupracujúce IVS ako aj riadiaci orgán a sprostredkovateľský orgán príslušného operačného programu) a za podnikateľskú sféru okrem hlavného dodávateľa častokrát veľmi zložitá sieť mnohých špecializovaných subdodávateľských firiem.

Vybrané projektové údaje uložené v blockchaine môžu významne prispieť aj k identifikovaniu zreťazenia príčin a dôsledkov pri šírení incidentu a neskôr problému a umožňujú tak priradiť zodpovednosť, vyvodiť dôsledky a zjednať nápravu a v konečnom dôsledku tak aj predchádzať opakovaniu minulých chýb.

5.4.4 Registrácia áut a prejdených kilometrov

Tento register v určitej podobe existuje už teraz (www.rpzv.sk). Takzvané „stáčanie“ kilometrov stále predstavuje obrovský problém (dopad v krajinách EÚ sa odhaduje na 5,6 až 9,6 mld. EUR ročne[46]). Blockchain by mohol priniesť vyššiu transparentnosť a všeobecnú dôveru k záznamom o „meraniach“ stavu km, ktoré pomôžu prípadné stáčanie odhaliť. Keďže autá sa často dovážajú zo zahraničia, táto databáza by mala byť celoeurópska a teda tento projekt by mohol by byť kandidátom na cezhraničnú spoluprácu v rámci European blockchain partnership.

Poznámka: Merania o stave km môžu byť odčítané a do blockchainu zapísané popri iných úkonoch (napr. kontrolách EK/TK/KO, iných servisných úkonoch, poistných udalostiach, policajných kontrolách alebo aj

[46] http://www.europarl.europa.eu/news/en/headlines/society/20180525STO04312/fighting-mileage-fraud-on-used-cars

náhodnom styku obsluhy auto umyvárne, či hotelovej služby s vozidlom a pod.). Jednoduchá kontrola dvojice časovo nadväzujúcich záznamov potom spoľahlivo odhalí, ak v danom období došlo k stáčaniu km a zo štatistického hľadiska zameria pozornosť na typické „body", v ktorých k stáčaniu dochádza. Dôležité je, že jednoducho dostupná možnosť (najmä pre potenciálneho záujemcu o ojazdené vozidlo) overiť si stáčanie km, má potenciál úplne zlikvidovať tento typ podvodu (zanikne po ňom dopyt). Samozrejme v tomto prípade je potrebné ošetriť dôvernosť jednoznačného identifikátora vozidla (tzv. VIN číslo), ktorého sa záznam o prejdených km týka. T.j. odpoveďou na dotaz, či k stáčaniu došlo alebo nie, bude zrejme len konštatovanie "áno" alebo "nie" a nie samotný naposledy zapísaný stav km pre dané vozidlo.

5.4.5 Voľby a referendá

Problém: Potreba zabrániť a predchádzať podvodom pri voľbách a referendách.

Navrhované riešenie a prínos využitia blockchain: Blockchain by zabránil viacnásobnej a neautorizovanej voľbe, tiež zabezpečil nespochybniteľnosť výsledkov a umožnil neskoršiu auditovateľnosť a overenie výsledkov (každý si môže samostatne a v ľubovoľnom čase prepočítať výsledky volieb).

5.4.6 Kataster nehnuteľností

Problém: Záznamy o vlastníctve, prevodoch nehnuteľností a ďalšie súvisiace záznamy uložené v centrálnej databáze.

Navrhované riešenie a prínos využitia blockchain: Projekt katastra nehnuteľností je často uvádzaný ako vzorový príklad nasadenia blockchainu. Spĺňa väčšinu atribútov riešenia vhodného pre nasadenie blockchainu: mnoho účastníkov, potreba dôvery, charakter transakcií, potreba zdieľania histórie transakcií, zjednodušené riešenie sporov. Je možné aj zmysluplné nasadenie smart kontraktov. Projekt katastra nehnuteľností bol realizovaný alebo prebieha realizácia vo viacerých krajinách, viď podkapitolu 4.4. Tento projekt však rozhodne nie je z kategórie „quick-wins", je veľmi komplexný, problémy by mohli nastať v súvislosti s množstvom vstupných dát, overovaním vstupov, ochranou osobných údajov atď. a preto odporúčame pred prípadnou realizáciou dôkladnú špecifikáciu, štúdiu uskutočniteľnosti, prípadne projekt realizovať až neskôr, v druhej vlne projektov.

5.4.7 Poľnohospodárske dotácie evidované cez blockchain

V tejto oblasti vnímame silnú verejnú požiadavku 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. Tiež je spomínaný register užívateľov pôdy, ktorý by mohol byť realizovaný cez blockchain.

5.4.8 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.

5.4.9 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.

5.4.10 Register zmeniek

Blockchain by mohol povinne uchovávať zoznam vystavených zmeniek a tým by sa predišlo následným sporom o pravosť zmenky alebo sporom o dátume jej vystavenia. Zamedzilo by sa tiež „prekvapeniam" v podobe novoobjavených zmeniek a pochybnostiach o ich pravosti.

5.4.11 Register notársky overených podpisov

Záznam o notárskom overení podpisu by sa mohol ukladať do blockchainu. Tým by sa predišlo falšovaniu notársky overených podpisov, druhá strana by si ľahko mohla overiť pravosť overenia podpisu a tiež dátum zápisu overenia.

5.4.12 Register notársky overených splnomocnení

Záznam o udelení splnomocnenia by bol vždy uložený do blockchainu. Tým by sa predišlo falšovaniu splnomocnení, druhá strana by si ľahko mohla overiť pravosť splnomocnenia a dátum zápisu.

5.4.13 Zúčtovanie využívania vládneho cloudu

Využívanie služieb vládneho cloudu by mohlo byť monitorované cez blockchain. Ľahko by sa potom dalo sledovať a reportovať minulé využitie a tiež plánovať budúci rozvoj. Mohla by sa využiť tokenizácia aktív – kapacita a/alebo výpočtový výkon by bol tokenizovaný, inštitúcia by ho mohla využívať len do výšky vlastnených tokenov, inštitúcie by mohli podľa plánovaného využitia nakupovať/vymieňať/predávať tokeny. V prípade vyšších požiadaviek a navýšenia kapacity by boli vydané dodatočné tokeny v príslušnom množstve.

5.4.14 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.

5.4.15 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.

5.4.16 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.

5.4.17 Central bank digital currency (CBDC)

CBDC je idea vydávania virtuálnej kryptomeny centrálou bankou ako náhrada klasickej (FIAT) meny. Úspech virtuálnych mien inšpiruje a priťahuje vlády a centrálne banky a tiež nabáda k otázke, či by štáty a centrálne banky nemohli vydávať vlastnú kryptomenu ako bezpečnú, dostupnú a efektívnu alternatívu, prípadne až náhradu, klasickej meny. CBDC je možné vnímať ako potenciál na inováciu a mohlo by byť ďalším míľnikom v vývoji peňazí.

Ako výhody zavedenia CBDC sú uvádzané najčastejšie:

- Potenciál na zníženie transakčných nákladov,
- Bezpečnejší, dostupnejší a spoľahlivejší platobný systém,
- Pružnejší a odolnejší platobný systém,
- Finančná inklúzia,
- Technologická efektívnosť,
- Väčšia transparentnosť a spätná sledovateľnosť transakcií môže uľahčiť a skvalitniť dohľad centrálnej banky,
- Uľahčenie alebo umožnenie vzniku nových služieb, procesov a podnikateľských modelov založených na digitálnych menách,
- Lepšia spolupráca medzi aktérmi transakcií a možné zmierňovanie kurzovej volatility,
- Zlepšenie boja proti AML/CFT.

Väčšina centrálnych bánk v súčasnosti skúma možnosť vydávania kryptomien, aj keď existuje stále mnoho otvorených otázok. Základnou otázkou je, kto by mal mať prístup k tejto mene ako prvý – komerčné banky, finančné inštitúcie, podniky alebo aj obyvateľstvo? Aká by mala byť úloha centrálnej banky? Mala by centrálna banka vôbec ponúkať nové formy peňazí? Kto bude zodpovedný za vydávanie virtuálnych peňaženiek (wallets)? Malo by byť riešenie centralizované alebo decentralizované? Kto by mal prevádzkovať uzly siete? Ako by bolo možné realizovať off-line platby? Mala by byť hotovosť úplne zrušená? Aká by mala byť miera anonymity? Mali by mať prístup k takejto mene aj subjekty zo zahraničia?

Niektoré z verejne ohlásených zámerov sú uvedené nižšie:

- Austrália[47],

[47] https://www.rba.gov.au/speeches/2017/sp-gov-2017-12-13.html

- Bahamy[48],
- Brazília[49],
- Čína[50],
- Dánsko[51],
- Kanada[52],
- Nórsko[53],
- Rusko[54],
- Spojené kráľovstvo[55],
- Švédsko[56],
- Izrael[57].

Problematika CBDC musí byť dôsledne preskúmaná – dotýka sa každého, projekt ma mnohé nepreskúmané ekonomické a sociálne dôsledky. Kroky smerujúce k spusteniu CBDC musia byť preto dôkladne zvážené. Je potrebné preskúmať vplyv na úrokové sadzby, štruktúru sprostredkovania, finančnú stabilitu a finančný dohľad. Vplyv na pohyby výmenných kurzov a ceny ostatných aktív je tiež neznámy a vyžaduje ďalšie skúmanie. Práce na skúmaní zavedenia CBDC prebiehajú a zatiaľ nie sú ukončené. Počiatočné prieskumy ukazujú možné riešenia a realizovateľnosť, avšak jednoznačne je nutné ďalšie skúmanie tejto problematiky.

5.4.18 Námety pre ďalšie prípady použitia

- Tokenizácia aktív na kapitálovom trhu,
- Register exekučných konaní,
- CMDB databáza konfigurácii v blockchaine,
- Register obyvateľov, narodení, úmrtí (elektronická matrika),
- Evidencia udalostí na úseku zbraní a streliva,
- Register súdnych rozhodnutí,
- Register znalcov,

---

48 https://www.bahamas.gov.bs/wps/portal/public/gov/government/news/digital%20currency%20to%20be%20introduced%2C%20says%20dpm

49 https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20180718/Pages/Programme.aspx

50 https://www.ccn.com/crucial-issue-central-bank-cryptocurrency-asap-pboc/

51 http://www.nationalbanken.dk/en/publications/Pages/2017/12/Central-bank-digital-currency-in-Denmark.aspx

52 https://www.bankofcanada.ca/2018/12/staff-working-paper-2018-58/

53 http://www.nationalbanken.dk/en/publications/Pages/2017/12/Central-bank-digital-currency-in-Denmark.aspx

54 https://www.ethnews.com/draft-of-cryptoruble-bill-submitted-to-russian-parliament

55 https://www.bankofengland.co.uk/research/digital-currencies

56 https://www.riksbank.se/en-gb/payments--cash/e-krona

57 https://www.boi.org.il/en/NewsAndPublications/PressReleases/Pages/6-11-18.aspx

- Register rozhodnutí o registrácii liekov,
- Register obyvateľov,
- Register bytov,
- Prideľovanie a registrácia sociálnych dávok,
- Register vydaných certifikátov,
- Register patentov a žiadostí o registráciu patentu,
- Transparentná správa štátneho majetku – prenájom, privatizácia,
- Obchodovanie s emisnými povoleniami na CO2,
- Register domácich zvierat s čipom, doma chovaných nebezpečných zvierat, prípadne poľnohospodárskych zvierat,
- Transparentné nakladanie a verejnými financiami na úrovni štátneho rozpočtu, miestnych rozpočtov,
- Zápočtové listy pre výpočet dôchodku ukladané do blockchainu,
- Pôvod a certifikácia potravín alebo iných produktov,
- Register trestov,
- Register dronov,
- Register vlastníctva cenných papierov,
- e-Health v blockchaine,
- PKI (Public Key Infractructure) bez centrálnej autority s využitím blockchain.

Ďalšie námety prípadov použitia, v ktorých sa môže vhodne uplatniť technológia blockchain je možné nájsť v časti 3.3 Blockchain ako kontrolný mechanizmus.

6 Fintech

6.1 Fintech všeobecne

Finančné inovácie, ako aj riešenia založené na technológii blockchain sú nástrojom, ktorého využitie môže zmeniť spôsob vykonávania finančných operácií. Fintech inovácie poskytujú možnosti pre rozvoj existujúcich služieb bánk, poisťovní a obchodníkov s cennými papiermi, zapojenie tzv. tretích strán a vývoj nových inovatívnych služieb. Jedná sa hlavne o zjednodušenie prístupu k službám a produktom na finančnom trhu pri zachovaní vysokého stupňa bezpečnosti a ochrany klientov.

Fintech možno charakterizovať ako nový finančný sektor, ktorý aplikuje technológie na zlepšenie finančných aktivít. Fintech predstavuje nové aplikácie, procesy, produkty alebo obchodné modely v odvetví finančných služieb, ktoré pozostávajú z jednej alebo viacerých doplnkových finančných služieb a sú poskytované ako koncový proces prostredníctvom internetu. Fintech zmenil tradičný spôsob poskytovania bankových a finančných služieb. Fintech spoločnosti predstavujú začínajúce spoločnosti (startupy), ako aj etablované finančné a technologické spoločnosti, ktoré sa snažia nahradiť alebo zvýšiť využívanie finančných služieb poskytovaných existujúcimi finančnými inštitúciami. Mnohé existujúce finančné inštitúcie implementujú riešenia a technológie Fintech spoločností s cieľom zlepšiť a rozvíjať svoje služby, ako aj získať konkurenčnú výhodu.

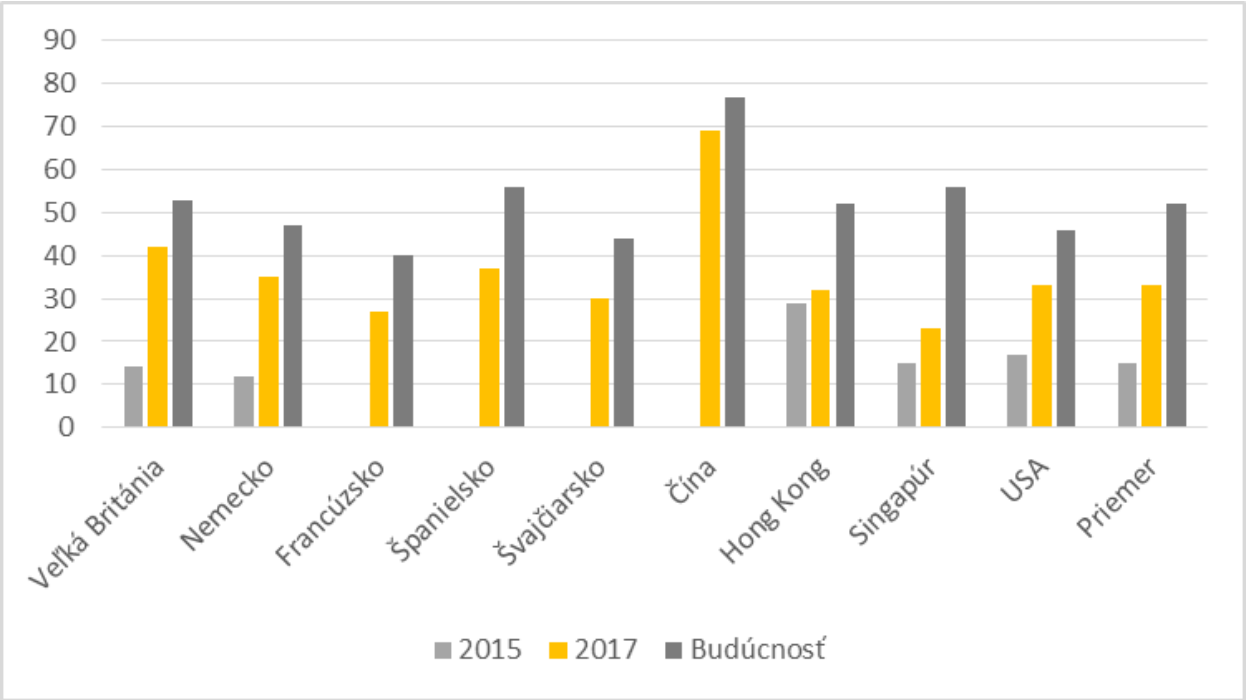
Zatiaľ čo technologické inovácie v oblasti financií nie sú nové, investície do nových technológií sa v posledných rokoch podstatne zvýšili a tempo inovácií je exponenciálne. Príkladom technológií zameraných na sprístupnenie finančných služieb širokej verejnosti je napr. využívanie mobilného bankovníctva prostredníctvom inteligentných telefónov, vykonávanie platieb a investovanie pomocou rôznych nástrojov, používanie kryptomien a pod.

O dynamickom rozvoji v tejto oblasti pojednáva aj množstvo prieskumov a analýz. Podľa publikácie spoločnosti EY „EY FinTech Adoption Index 2017“[58] sa v blízkej budúcnosti celosvetovo očakáva podiel využívania Fintech riešení v priemerne 52% z celkového trhu reprezentovaného Fintech aj tzv. tradičnými riešeniami (riešeniami implementovanými finančnými inštitúciami). Z nasledovného grafu (Obrázok 16), ktorý je uvedený v spomenutej publikácii možno vidieť porovnanie minulého, súčasného a očakávaného budúceho používania Fintech riešení podľa vybraných krajín. Graf ukazuje ako boli Fintech spoločnosti prijaté trhmi v jednotlivých krajinách v roku 2015 (ak je údaj k dispozícii), v roku 2017 a očakávané prijatie v budúcnosti ako to naznačujú respondenti prieskumu z roku 2017.

Poznámky:

- Nakoľko je publikácia "EY FinTech Adoption Index 2017" vydávaná v dvojročnom cykle a posledné vydanie bolo z roku 2017, v čase prípravy tejto štúdie nebolo možné uviesť aktuálnejšie údaje. Cieľom uvedenia týchto údajov v štúdii bolo prezentovať trend rastu významu Fintech riešení. Na tieto účely boli údaje uvedené v publikácii postačujúce.
- Táto kapitola je spracovaná na základe verejne dostupných zdrojov, údajov Centra pre finančné inovácie MF SR (CFI) a využitia publikácií a poznatkov spoločnosti EY v tejto oblasti. Rozsah tejto časti je taktiež limitovaný celkovým zameraním dokumentu a relatívnym významom tejto kapitoly v rámci jeho rozsahu.

[58] https://www.ey.com/Publication/vwLUAssets/ey-fintech-adoption-index-2017/$FILE/ey-fintech-adoption-index-2017.pdf



Obrázok 16: Vývoj prijatia Fintech riešení v jednotlivých krajinách

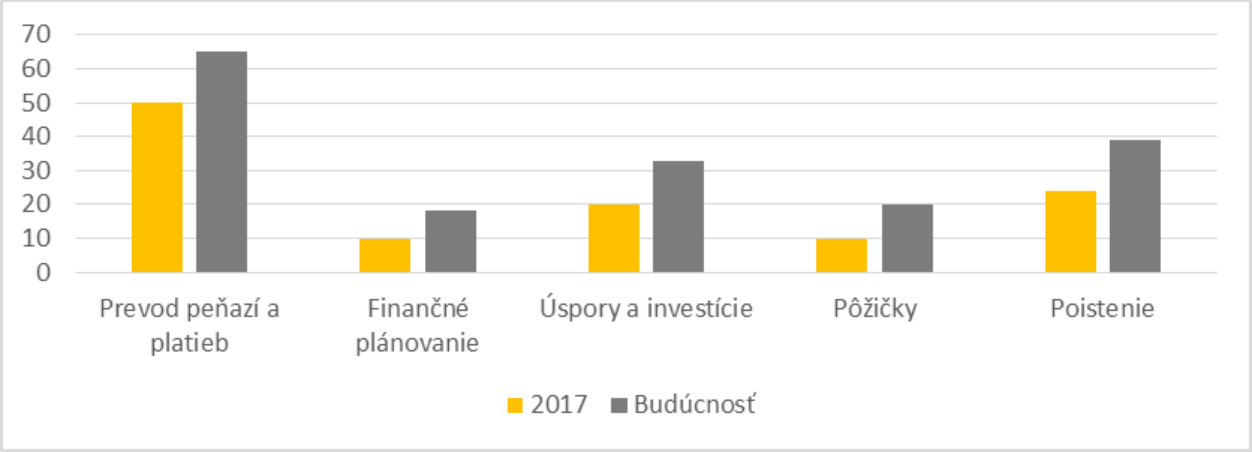
Umelá inteligencia, sociálne siete, strojové učenie, mobilné aplikácie, blockchain, cloud computing a BigData analýza priniesli nové služby a obchodné modely zo strany zavedených finančných inštitúcií a nových účastníkov na trhu. Všetky tieto technológie môžu byť prínosom pre spotrebiteľov, ako aj pre spoločnosti tým, že umožnia väčší prístup k finančným službám, ponúknu širší výber a zvýšia efektívnosť operácií. Taktiež môžu prispieť k znižovaniu národných bariér a zvýšeniu hospodárskej súťaže v takých oblastiach, ako je napr. on-line bankovníctvo, on-line platby a transferové služby, poskytovanie pôžičiek, investičné poradenstvo a služby. Fintech predstavuje podstatne nižšie prekážky pre vstup do finančného sektora a zmenu kľúčových charakteristík, ktoré definujú poskytovateľov finančných služieb.

Blockchain aj Fintech majú potenciál zmeniť spôsob, akým v súčasnosti fungujú finančné inštitúcie a rôzne odvetvia. Je potrebné si uvedomiť, že Blockchain a Fintech nie je to isté. Blockchain je technológia, ktorá zohráva kľúčovú úlohu v inováciách spoločností Fintech. Je dôležité mať na pamäti, že Blockchain je len jednou z najnovších Fintech inovácií, ktoré zmenili tvár finančného sektora. Avšak tentoraz by to mohol byť posledný krok, ktorý je potrebný na to, aby sa svet stal spravodlivejším, inkluzívnejším a smeroval k prosperujúcej spoločnosti, čo bude prospešné pre nás všetkých.

6.2 Prehľad Fintech riešení vo svete

Vo svete sa Fintech spoločnosti usadili ako významní poskytovatelia produktov finančných služieb najmä v oblasti bankovníctva, ale aj poisťovníctva a správy majetku. Či už ide o nový obchodný model, nový produkt alebo službu, spoločnosti Fintech demonštrujú úspech v oblasti inovácií a formujú budúcnosť odvetvia finančných služieb. Známymi priekopníkmi v oblasti platobných systémov sú Alipay, Android Pay, Apple Pay, M-Pesa, PayPal and Samsung Pay. Podľa publikácie spoločnosti EY „EY FinTech Adoption Index

2017“ je porovnanie súčasného a predpokladaného budúceho používania Fintech riešení podľa kategórií, resp. oblastí nasledovné:



Obrázok 17: Porovnanie súčasného a očakávaného používania Fintech riešení podľa kategórií

Ako je možné vidieť z obrázku spotrebiteľská ochota používania Fintech riešení je pozitívna vo všetkých piatich uvedených kategóriách služieb Fintech. V oblasti poskytovania pôžičiek a finančného plánovania bol zaznamenaný najväčší pomerný rozdiel medzi súčasným a očakávaným používaním služieb.

V celosvetovom meradle možno spomenúť nasledujúce úspešné Fintech spoločnosti, ktoré sa zaoberajú rôznymi oblasťami finančného sektora:

Platby

- **Ant Financial** (Čína) je najväčšia Fintech spoločnosť na svete. Pod Ant Financial spadajú spoločnosti Alipay, Ant Fortune, Yu'e Bao, Zhima Credit, MYbank and Ant Financial Cloud.
- **Revolut** (Veľká Británia) je alternatíva digitálneho bankovníctva, ktorá umožňuje používateľom vykonávať platby v rôznych menách bez poplatkov. Aplikácia tiež umožňuje používateľom sledovať výdavky a investovať do kryptomien a iných finančných produktov.
- **Compass** (USA) je platforma používajúca BigData a špičkové algoritmy poskytujúce najpresnejšie ceny nehnuteľností a najefektívnejšiu cestu predaja za najvyššiu cenu.
- **Stripe** (USA) ponúka spôsob akceptovania platieb online a prostredníctvom mobilných aplikácií pomocou bankových účtov.

Pôžičky

- **JD Finance** (Čína) využíva svoje odborné znalosti v oblasti elektronického obchodu na financovanie siedmich vertikálnych oblastí vrátane spotrebiteľských financií, crowdfundingu a platobných služieb.
- **Sofi** (USA) ponúka širokú škálu služieb v oblasti poskytovania úverov a správy majetku.
- **Lufax** (Čína) je spoločnosť obchodujúca s finančnými aktívami online, využívajúca BigData na analýzu rizika.
- **ACORN Oaknorth Holdings** (Veľká Británia) sa špecializuje na poskytovanie úverov pre malé a stredné podniky prostredníctvom svojej dátovej a technologickej platformy ACORN.

Investovanie/Správa majetku

- **Robinhood** (USA) je maklérska spoločnosť, ktorá umožňuje zákazníkom nakupovať a predávať cenné papiere kótované v USA na burze s nulovou províziou.
- **51 Credit Card Manager** (Čína) prevádzkuje aplikáciu, ktorá môže inteligentne spravovať účty kreditnej karty jedným kliknutím a používateľom pomáha lepšie spravovať vlastné záväzky.
- **WealthSimple** (Kanada) je online investičný manažér, ktorý umožňuje jednoduché, nákladovo efektívne a dostupné investovanie.
- **QUOINE** (Japonsko) poskytuje novú generáciu finančných služieb a obchodovania s využitím technológie blockchain.

Poistenie

- **Oscar Health** (USA) sa snaží radikálne transformovať zdravotné poistenie prostredníctvom technológií.
- **Clover Health** (USA) je spoločnosť pôsobiaca v oblasti zdravotného poistenia zameraná na znižovanie nákladov prostredníctvom vyžívania údajov a analýzy.
- **Policybazaar** (India) bol pôvodne založený ako informačný portál zaoberajúci sa vzdelávaním o poistení. V súčasnosti je lídrom digitálneho poisťovníctva v Indii.

Neo-bankovníctvo

- **Nubank** (Brazília) je brazílska neo-banka, ktorá vydala viac ako 5 miliónov kreditných kariet a 2,5 miliónov digitálnych platobných účtov.
- **Atom Bank** (Veľká Británia) je prvou čisto digitálnou retailovou bankou vo Veľkej Británii.
- **Monzo** (Veľká Británia) je digitálna banka zameraná na vytvorenie bežných účtov bez poplatkov, založených a spravovaných prostredníctvom mobilných zariadení.
- **N26** (Nemecko) ponúka aplikáciu pre mobilné bankovníctvo, prostredníctvom ktorej je možné vykonávať finančné operácie bez poplatkov.

Multi odvetvové zameranie

- **Grab** (Singapúr) využíva údaje a technológie na zlepšenie viacerých oblastí, od dopravy až po platby.
- **Baidu** - Du Xiaoman Financial (Čína) poskytuje krátkodobé úverové a investičné služby s využitím umelej inteligencie.

6.3 Prehľad Fintech riešení v SR

V rozšírení bezhotovostných terminálových operácií patrí Slovensko k svetovým lídrom. Počet platieb na POS platobných termináloch na Slovensku presiahol objem výberov z bankomatov už v roku 2007. Rýchlemu rastu napomáha aj otvorenosť obchodníkov zavádzať čo najviac riešení umožňujúcich bezhotovostný platobný styk, ako aj ochotou klientov používať inovatívne produkty, ktoré zjednodušujú spôsob realizácie platby. Pre banky a technologické spoločnosti je Slovensko často trhom, v rámci ktorého testujú svoje riešenia. Rozvoju Fintech spoločností napomáha aj smernica PSD2, podľa ktorej platby za tovar, poskytovanie úverov či elektronické obchodovanie už nebudú výhradne doménou etablovaných bankových inštitúcií.

Medzi úspešné riešenia a spoločnosti, ktoré sa už na trhu presadili patrí sprostredkovateľ online služieb

TrustPay alebo aplikácia Papaya, umožňujúca vyrobiť z mobilu či tabletu pokladňu s funkciami objednávok, platieb a skladového hospodárstva. Na trhu je už etablovaná služba platieb na mobilné telefónne číslo VIAMO, či platobný systém pre e-shopy Besteron.

V rámci Slovenska Fintech spoločnosti prevažne kopírujú celosvetový trend a zameriavajú na nasledovné oblasti: prevod peňazí a platieb, pôžičky peer-to-peer, POS obchodovanie, Big Data, marketing a správanie zákazníkov, podnikové procesy, neo-bankovníctvo, crowdfunding/crowdinvesting, správa majetku, účtovníctvo a služby pre malé a stredné podniky. Podľa oblastí pôsobenia môžeme medzi Fintech spoločnosti pôsobiace na Slovensku zaradiť:

Prevod peňazí a platieb

- **Besteron** je platobná brána, ktorá poskytuje spoločnostiam elektronického obchodu všetky formy bezhotovostnej platby, umožňujúca prijímať finančné prostriedky z transakcií v reálnom čase.
- **TrustPay** patrí medzi prvé finančné inštitúcie v rámci regiónu, ktoré zabezpečujú bezpečný platobný styk v rámci EHP. Členstvo v certifikáciách VISA Europe, MasterCard, Union Pay a PCI DSS Level 1 umožňuje klientom poskytovať cezhraničné B2B platobné služby.
- **Piano** poskytuje softvér založený na cloudovej technológii, ktorý pomáha mediálnym spoločnostiam zvyšovať online príjmy a spravovať používateľské práva na platformách a kanáloch.
- **VIAMO** je jednoduchá mobilná aplikácia, ktorá umožňuje posielať mikroplatby prostredníctvom telefónu priamo na slovenské telefónne číslo. Aplikácia je podporovaná bankovými inštitúciami ako Tatrabanka a Všeobecná úverová banka.
- **Everifin** je B2C platforma zameraná na správu bankových účtov v rámci jednej aplikácie.
- **By square** umožňuje prostredníctvom QR kódu rýchlo a pohodlne zaplatiť faktúru bez nutnosti prepisovania údajov.

Pôžičky peer-to-peer

- **Zinc Euro** je peer-to-peer služba zameraná na poskytovanie úverov s rezervným fondom zameraným na ochranu finančných prostriedkov investora.
- **Žltý melón** je peer-to-peer úverová služba, prostredníctvom ktorej sú pôžičky prístupnejšie a investície sú výhodnejšie ako u tradičných bankových inštitúcií.

POS obchodovanie

- **Payowallet** je aplikácia, ktorá konsoliduje všetky zľavové karty (resp. karty odmien) na jednom mieste a šetrí finančné prostriedky, ak sú produkty zakúpené priamo z aplikácie.
- **Papaya** je mobilné POS riešenie založené na technológii cloud, určené pre zariadenia so systémom Android, ktoré pomáhajú malým a stredným firmám zlepšiť procesy a zvýšiť predaj.

Big Data

- **Datatree** pomáha bankovým inštitúciám zavádzať pokročilé prediktívne algoritmy a extrahovať množstvo informácií z transakčných údajov.
- **Knoyd** ponúka riešenia v oblasti údajov pre podniky akejkoľvek veľkosti alebo odvetvia na mieru. Ide o poradenstvo, ktoré umožňuje efektívne využívať veľké množstvo údajov.

- **Pygmalios** je technologická spoločnosť, ktorá poskytuje softvér a služby pre analýzu skúseností zákazníkov s obchodmi.

Marketing a správanie zákazníkov

- **Dateio** je spoločnosť zameraná na business intelligence, ktorá poskytuje podnikom marketingové riešenia pre zvýšenie lojality zákazníkov prostredníctvom personalizovaných marketingových ponúk na základe údajov z platobných kariet zákazníkov.
- **Mindworx** spája odborníkov v oblasti správania sa zákazníkov, ktoré efektívne kombinuje so zručnosťami z marketingu, ľudských zdrojov, presnej analýzy dát a ich aplikovanie na dosiahnutie cieľov klientov.
- **Market Locator** je nástroj na cielený mobilný marketing a analýzu populácie. Umožňuje prilákať nových zákazníkov s cielenými geolokačnými SMS správami a analyzovať, kde potenciálny zákazníci trávia čas a kde by bolo vhodné otvoriť novú prevádzku.

Podnikové procesy

- **Minit** je softvér, ktorý automaticky analyzuje procesy a poskytuje zrozumiteľné vizuálne náhľady s cieľom nárastu výnosov, úspor a zvýšenia efektívnosti.
- **GoodAI** je spoločnosť pôsobiaca v oblasti výskumu a vývoja umelej inteligencie, ktorá uplatňuje svoje riešenia v oblasti finančných služieb.

Crowdfunding/Investovanie

- **Finnest** je platformou pre investovanie do úspešných stredných podnikov. Zameriava sa na financovanie etablovaných spoločností, ktoré sú z dlhodobého hľadiska úspešné a vytvárajú miliónové obraty.
- **Crowdberry** je nový spôsob spájania súkromného kapitálu s inovatívnymi spoločnosťami. Crowdberry je investičná platforma, ktorej základnou podstatou je prepojenie siete súkromných investorov s dynamickými podnikateľskými nápadmi. Cieľom je získať kapitál od rôznych investorov výmenou za majetkové účasti v spoločnostiach.
- **Finax** – ide o poradenskú platformu, ktorej cieľom je vytvoriť spravodlivý, moderný a výkonný investičný produkt. Finax sprístupňuje inteligentné investovanie širokej verejnosti za rovnakých podmienok a výhod.
- **Hithit** je platformou pre tvorivé nápady. Spája umelcov, dizajnérov, vývojárov s darcami, ktorí ich chcú finančne podporovať. Darcovia sú za svoje príspevky odmeňovaní rôznymi stimulmi.

Neo-bankovníctvo

- **365 bank** je inteligentná banka pre retail zákazníkov, ktorá pracuje s BigData. Je určená pre používateľov mobilov a poskytuje bezproblémové založenie online účtu a jeho používanie v každodennom živote.

Správa majetku

- **Rapid Data** vytvára riešenia pre správu majetku a pri poskytovaní komplexnej starostlivosti o klientske portfólio. V rámci jedného nástroja ponúka reportovanie, optimalizáciu portfólia, simulovanie a stresové testovanie.

Účtovníctvo a služby pre malé a stredné podniky

- **Datamolino** je aplikácia, ktorá automaticky extrahuje kľúčové informácie z pokladničných bločkov, došlých a odoslaných faktúr a údaje bezodkladne odosiela priamo do účtovných systémov Xero alebo Sage One.
- **Archiles** je platforma pre automatizáciu založená na cloudovom prostredí, ktorá poskytuje technológiu extrakcie a komplexný nástroj pre riešenie manuálnej a ťažkopádnej práce s účtovnými dokladmi.
- **iDoklad** je jednoduchý nástroj pre živnostníkov a malé podniky na vystavovanie faktúr a sledovanie finančného zdravia spoločnosti.
- **SuperFaktúra** je online aplikácia pre podnikateľov a malé podniky na vystavovanie faktúr a organizovanie výdavkov, objednávok a získavanie odhadov o finančnom stave podnikania.

6.4 Nástroje podpory Fintech a ich porovnanie

Vlády štátov sa snažia podporovať inovácie v snahe zefektívniť vlastnú činnosť a vytvoriť stimuly pre rast finančného trhu, ako aj celého hospodárstva. Vytvárajú a implementujú stratégie a konkrétne opatrenia na podporu inovácií, informatizácie a digitalizácie. Medzi rozšírené nástroje na podporu Fintech spoločností patria:

- **Inovačný hub**, resp. centrum inovácií je inštitucionálne usporiadanie, v ktorom regulované alebo neregulované subjekty (t. j. spoločnosti bez povolenia) komunikujú s príslušným orgánom s cieľom prediskutovať otázky týkajúce sa finančných technológií (výmena informácií a názorov atď.) a snažia sa získať vysvetlenie, pokiaľ ide o súlad obchodných modelov s regulačným rámcom alebo o regulatórne či licenčné požiadavky (t. j. individuálne usmernenia spoločnosti o výklade platných pravidiel).
- **Regulatórny Sandbox** je experimentálne regulačné prostredie, ktoré poskytuje finančným inštitúciám a nefinančným spoločnostiam kontrolovaný priestor, v rámci ktorého si môžu na istý čas vyskúšať inovatívne riešenia založené na finančných technológiách s podporou orgánu (t. j. regulátora, ktorý prostredie vytvára), čo im umožňuje potvrdiť a otestovať ich obchodný model v bezpečnom prostredí.
- **RegTech** je novou oblasťou odvetvia finančných služieb, ktorá využíva informačné technológie na posilnenie regulačných procesov. Osobitný dôraz kladie na regulačné monitorovanie, podávanie správ a súlad s právnymi predpismi. Cieľom RegTech je zvýšiť transparentnosť, konzistentnosť a štandardizovať regulačné procesy, poskytnúť spoľahlivé interpretácie nejednoznačných nariadení a tým zabezpečiť vyššiu úroveň kvality pri nižších nákladoch.

6.5 Prehľad nástrojov podpory Fintech vo svete a SR

V tejto časti dokumentu je uvedený prehľad nástrojov podpory Fintech vo svete a SR. Výber jednotlivých krajín bol zameraný hlavne na krajiny, ktoré sú spravidla lídrami v tejto oblasti. Kapitola vychádza prevažne z dokumentu „Fintech Best Practice“, ktorého autorom je Centrum pre finančné inovácie (CFI) Ministerstva financií SR. Tento dokument bol vypracovaný CFI a konzultovaný s ďalšími zainteresovanými stranami a jeho obsah pokladáme ho za veľmi kvalitný a konzistentný. Štruktúrovaným a vyčerpávajúcim spôsobom vhodne charakterizuje situáciu v tejto oblasti v analyzovaných krajinách. Ďalšie analýzy a poznatky z iných zdrojov potvrdzovali obsah z tohto referencovaného dokumentu. Do tejto štúdie boli prevzaté podstatné časti tohto dokumentu. Autori dokumentu taktiež absolvovali pracovné stretnutie s CFI ohľadom tejto problematiky.

6.5.1 Európska únia

Európska komisia venuje zvýšenú pozornosť možnostiam využitia príležitostí, ktoré ponúkajú technologické inovácie v oblasti finančných služieb. EÚ má ambíciu stať sa globálnym centrom finančných technológií, kde spoločnosti a investori z EÚ môžu čo najlepšie využívať výhody, ktoré ponúka jednotný trh. Na uvedené nadväzujú aj nové pravidlá, ktoré pomôžu platformám kolektívneho financovania (crowdfunding) rásť v rámci jednotného trhu EÚ.

EÚ prijala Akčný plán pre finančné technológie: Za konkurencieschopnejší a inovatívnejší európsky finančný sektor, ktorý umožní finančnému sektoru využívať pokrok v oblasti nových inovatívnych technológií, ako blockchain, umelá inteligencia, cloudové služby a pod. Akčný plán je súčasťou úsilia o vytvorenie únie kapitálových trhov (CMU), jednotného trhu s finančnými službami pre spotrebiteľov a vytvorenie jednotného digitálneho trhu. Akčný plán stanovuje kroky, ktorými sa umožní a zjednoduší rozvoj inovačných obchodných modelov, podpora šírenia nových technológií, zvýšenie kybernetickej bezpečnosti a integrity finančného systému, ako sú:

- Laboratórium EÚ v oblasti finančných technológií, v ktorom sa budú európske a vnútroštátne orgány stretávať s poskytovateľmi technológií v neutrálnom a nekomerčnom priestore,
- Monitorovacie stredisko a fórum EÚ pre technológiu blockchain, ktorého úlohou je informovať o výzvach a možnostiach kryptoaktív. Zároveň pracuje na komplexnej stratégii pre technológiu distribuovanej databázy transakcií a blockchain,
- Verejná konzultácia na tému ako najlepšie podporiť digitalizáciu informácií zverejnených kótovanými spoločnosťami v EÚ, a to aj prostredníctvom využitia inovačných technológií na prepojenie národných databáz,
- Pracovné semináre s cieľom zlepšiť výmenu informácií v oblasti kybernetickej bezpečnosti,
- Predloženie plánu s osvedčenými postupmi týkajúcimi sa regulatórnych sandboxov.

Súčasťou akčného plánu je aj návrh nariadenia o európskych poskytovateľoch kolektívneho investovania a návrh novely smernice Európskeho parlamentu a Rady 2014/65/EÚ o trhoch s finančnými nástrojmi, ktorou sa mení smernica 2002/92/ES a smernica 2011/61/EÚ, ktorých cieľom je umožniť lepší prístup k financovaniu, a to najmä pre začínajúce podniky a iné malé podniky. V súčasnosti je pre mnohé platformy ťažké expandovať do iných krajín EÚ. Práve preto je kolektívne financovanie v EÚ v porovnaní s ostatnými veľkými svetovými ekonomikami menej rozvinuté a trh EÚ je fragmentovaný. Jednou z najväčších prekážok je absencia spoločných pravidiel v celej EÚ. Táto situácia značne zvyšuje náklady na dodržiavanie predpisov a prevádzkové náklady a bráni platformám kolektívneho financovania v expanzii do zahraničia.

Tento návrh uľahčí platformám ponúkanie služieb v celej EÚ a spoločnostiam, ktoré potrebujú finančné prostriedky a zlepší prístup k tejto inovatívnej forme financovania. Navrhované nariadenie po schválení v Európskom parlamente a Rade umožní platformám požiadať o značku EÚ na základe jednotného súboru pravidiel. Táto značka umožní ponúkanie služieb v celej EÚ. Investori budú v rámci platforiem kolektívneho financovania chránení jasnými pravidlami pre zverejňovanie informácií, pravidlami týkajúcimi sa správy a riadenia rizík a jednotného prístupu k dohľadu.

Oblasť platobných služieb na trhu EÚ spadá od 13. 1. 2018 pod smernicu Európskeho parlamentu a Rady (EÚ) 2015/2366, ktorá je známa pod skratkou PSD2 (Payment Services Directive 2). PSD2 bola prijatá v kontexte stratégie Európa 2020. Smernica zahŕňa zmeny v oblasti regulovania poskytovania služieb prostredníctvom Fintech spoločností a taktiež upravuje zvýšenie bezpečnosti a ochrany spotrebiteľa. Cieľom je prispieť k jednotnému harmonizovanému trhu elektronických platieb v rámci celého

paneurópskeho priestoru, v súlade s rozvojom digitálnych platieb a inováciami.

Cieľom prvej smernice o platobných službách PSD1 (smernica EÚ 2007/64/ES) bolo vytvoriť univerzálny, moderný a zrozumiteľný súbor pravidiel, ktoré by sa vzťahovali na všetky platobné služby v EÚ a EHP. PSD1 otvorila platobný trh, posilnila tým jeho konkurencieschopnosť a umožnila, aby boli cezhraničné platby jednoduché, efektívne a rovnako spoľahlivé ako platby v rámci jedného členského štátu EÚ. Navyše poskytla aj potrebnú legislatívnu podporu platformy pre jednotnú oblasť platieb v eurách.

Smernica PSD2 prehlbuje dosah a rozsah PSD1. Rozširuje jej pôsobnosť na všetky meny a platby, teda aj na tie prípady, keď sa v rámci EÚ/EHP nachádza len jeden poskytovateľ. Okrem iného zavádza striktné bezpečnostné požiadavky na iniciovanie a spracovanie elektronických transakcií, ako aj na ochranu klientskych dát. Tiež zavádza povinnosť získania licencie pre nových trhových hráčov, tzv. tretie strany. Ide o tri typy poskytovateľov:

- poskytovateľa platobných služieb vydávajúceho platobné nástroje viazané na kartu,
- poskytovateľa platobných iniciačných služieb,
- poskytovateľa služieb informovania o účte.

Hlavným cieľom smernice PSD2 je posilniť transparentnosť a možnosť rýchlejšieho prijímania inovácií v oblasti platobných služieb, a tým prispieť k účinnému a efektívnemu trhu s platbami.

PSD2 zavádza minimálny štandard nazývaný silná klientska autentifikácia, inak povedané aj dvojfaktorová klientska autentifikácia (2FA). Koncept silnej klientskej autentifikácie bol zavedený už v roku 2014 v rámci usmernení EBA (finálne usmernenia týkajúce sa bezpečnosti internetových platieb). Tieto usmernenia sa týkali platieb cez internet, PSD2 však rozšírila priestor pre aplikovanie silnej klientskej autentifikácie aj na také prípady, keď platiteľ: a) pristupuje k platobnému účtu on-line, b) iniciuje elektronickú platobnú transakciu alebo c) vykonáva akúkoľvek akciu cez vzdialený kanál, ktorá by mohla predstavovať riziko platobného podvodu alebo iného zneužitia.

Poskytovatelia platobných iniciačných služieb sú podľa PSD2 novým licencovaným poskytovateľom platobných služieb. Banky majú na základe PSD2 mandát na umožnenie platby z účtu platiteľa prostredníctvom aplikačných programových rozhraní (API – Application Programming Interface) tohto poskytovateľa. Táto metóda umožňuje limitovaný prístup do vnútorného prostredia internet bankingu len k tým informáciám, na poskytovanie ktorých dal klient svoj súhlas. Jej hlavnou úlohou je zabezpečiť, na základe výslovného súhlasu platiteľa, iniciovanie platobného príkazu prostredníctvom on-line prístupu k platobnému účtu. Poskytovateľ platobných iniciačných služieb podľa PSD2 nesmie uchovávať citlivé platobné údaje, nemá vo vlastníctve finančné prostriedky platiteľa, je zodpovedný za správne predloženie platobného príkazu a nesmie byť diskriminovaný zo strany banky.

Otázkam súvisiacim s PSD2 sa venuje Európska centrálna banka, Európska komisia a aj Európsky orgán pre bankovníctvo (European Banking Authority – EBA). EBA má za cieľ zadefinovať regulačné technické štandardy, implementačné technické štandardy a usmernenia. Tieto opatrenia sa týkajú najmä bezpečnosti, štandardov komunikácie, transparentnosti a poskytovania informácií. Boli vytvorené pracovné skupiny expertov, ktorí majú za úlohu analyzovať dopad PSD2 a regulačných technických štandardov EBA týkajúcich sa silnej klientskej autentifikácie a bezpečnej komunikácie na API v paneurópskom priestore.

6.5.2 Slovenská republika

Ministerstvo financií SR vo februári 2018 zriadilo Centrum pre finančné inovácie (CFI). Hlavným cieľom

CFI je vytvoriť pre relevantné orgány štátnej správy, subjekty trhu a záujmové združenia platformu umožňujúcu pravidelnú výmenu informácií a skúseností. Prioritnou aktivitou CFI je zmapovanie prostredia ovplyvňujúceho zavádzanie nových technológií v oblasti finančného trhu, identifikácia nedostatkov alebo možností na zlepšenie tohto prostredia a aktívne odstraňovanie bariér pre vznik a pôsobenie Fintech spoločností na Slovensku. CFI zriadilo tri pracovné skupiny:

- Platobné služby a bankovníctvo,
- Crowdfunding, kapitálový trh a Poisťovníctvo,
- Virtuálne meny a blockchain.

V rámci pracovných skupín za účasti zástupcov Ministerstva financií SR, Národnej banky Slovenska, Úradu podpredsedu vlády SR pre investície a informatizáciu, vysokých škôl, záujmových združení a samotných účastníkov trhu sú prediskutované možnosti aplikácie podporných mechanizmov v SR, nové trendy v platobných službách, PSD2 a API, nástroje podpory Fintech v SR, skúsenosti účastníkov trhu so zavádzaním nových inovatívnych riešení v podmienkach SR, crowdfunding, daňové opatrenia, virtuálne meny a blockchain.

Národná banka Slovenska spolu s Ministerstvom financií SR v konzultácii so Slovenskou bankovou asociáciou spolupracovali na transpozícii smernice PSD2 do národného zákona v zmysle novelizačného zákona č. 281/2017 Z. z., ktorým sa mení a dopĺňa zákon č. 492/2009 Z. z. o platobných službách a o zmene a doplnení niektorých zákonov v znení neskorších predpisov. Na Slovensku bol zverejnený novelizačný zákon o platobných službách v Zbierke zákonov SR s účinnosťou od 13. 1. 2018. Na základe tohto kroku sa vytvorili právne podmienky na to, aby sa Slovensko zaradilo medzi tie členské štáty EÚ, ktoré včas implementovali všetky potrebné opatrenia na poskytovanie platobných služieb v súlade s PSD2.

Na účely zabezpečenia otvoreného prístupu k účtu mnohé banky pôsobiace na slovenskom trhu implementovali aplikačné programové rozhranie (API). Problematike rozhraní sa venuje aj Slovenská banková asociácia, ktorá vydala jednotný nepovinný štandard – Slovak Banking API Standard[59]. Tento štandard je od 1. 12. 2017 publikovaný na webovej stránke Slovenskej bankovej asociácie.

PSD2 prináša povinnosť licencie a regulácie dvoch typov poskytovateľov: poskytovateľa platobných iniciačných služieb a poskytovateľa služieb informovania o účte. Na základe ustanovení zákona č. 492/2009 Z. z. o platobných službách a zmene a doplnení niektorých zákonov v znení neskorších predpisov Národná banka Slovenska vedie zoznam (register podľa PSD2). Národná banka Slovenska zabezpečuje technické riešenie zoznamu (registra podľa PSD2) prostredníctvom technickej aplikácie subjekty finančného trhu.

6.5.3 Veľká Británia

Veľká Británia (VB) sa dlhodobo považuje za najinovatívnejšiu ekonomiku sveta, ktorá dlhodobo podporuje zavádzanie inovácií vo finančnom sektore. Podpora inovatívnych technológii vo finančnom sektore začala systematicky zo strany vlády VB v roku 2010. V roku 2017 predstavila vláda v rámci Industrial Strategy: building a Britain fit for the future[60] stratégiu VB byť najinovatívnejšou ekonomikou na svete. Súčasťou tejto snahy je aj stratégia Fintech Sector Strategy: Securing the Future of the UK Fintech[61], ktorá predstavuje výhľad na kroky, ktoré je potrebné prijať na upevnenie pozície UK ako finančného trhu

[59] https://www.sbaonline.sk/ProjectDetail?name=slovak-banking-api
[60] https://www.gov.uk/government/publications/industrial-strategy-building-a-britain-fit-for-the-future
[61] https://www.regulationtomorrow.com/eu/hm-treasury-fintech-sector-strategy/

otvoreného inováciám.

Najvýznamnejšie nástroje na podporu Fintech:

Inovačný hub – FCA Innovate

V roku 2014 vytvoril orgán dohľadu v UK – Financial Conduct Authority (FCA) – inovačnú iniciatívu FCA Innovate[62]. Súčasťou iniciatívy bolo vytvorenie Inovačného hubu a Regulatórneho Sandboxu. Ide o hlavné projekty, ktoré pomáhajú Fintech spoločnostiam spĺňať regulačné požiadavky. Hlavnou činnosťou Inovačného hubu je poskytovanie poradenstva a vydávanie podporných dokumentov pre spoločnosti, ktoré majú záujem sa uchádzať o licenciu alebo zaviesť nový inovatívny produkt.

Regulatórny Sandbox

Regulatórny Sandbox predstavuje podporu Fintech spoločností najmä v rámci predlicenčnej fázy. Inovatívne spoločnosti si v kontrolovanom prostredí môžu otestovať svoj nový produkt a docieliť jeho súlad s reguláciou. Takéto opatrenie znižuje náklady spoločností a zlepšuje ich prístup k financovaniu. Projekt globálneho sandboxu, v rámci ktorého by bolo možné otestovať cezhraničné pôsobenie a hľadať riešenia na regulačné obmedzenia je vo fáze skúmania možností a bilaterálnych spoluprác.[63]

Podpora RegTech

Do konca roka 2018 plánuje FCA pripraviť regulácie, ktoré by mali byť splniteľné pomocou automatizovaného softvérového čítania, čo má smerovať k rozvoju RegTech odvetvia a odbúrať tak náklady spojené so spĺňaním regulácie.

V roku 2015 FCA vytvorila nový dohliadací orgán pre platobné systémy[64]. Payment System Regulator (PSR) sa stal novým nezávislým regulátorom, ktorý má funkčnú a rozhodovaciu samostatnosť v oblasti platobného styku. Cieľom PSR je zabezpečiť dostatočný rozvoj a dostupnosť platobných systémov pre všetkých účastníkov trhu.

UK rozšírilo prístup k zúčtovacím účtom v rámci expresného systému hrubého zúčtovania (RTGS) aj na nebankových poskytovateľov platobných služieb – platobné inštitúcie a inštitúcie elektronických peňazí.[65] Nebankové spoločnosti tak získali možnosť zúčtovania s peniazmi centrálnej banky a nemusia sa spoliehať na služby komerčných bánk.

V roku 2016 Bank of England zriadila akcelerátor, ktorý vytvára priestor pre spoluprácu s technologickými firmami na účely uplatnenia inovácií v oblasti centrálneho bankovníctva.

Vo VB sa nastaveniu Open banking štandardu zaoberala CMA (Competition and Markets Authority), ktorá

[62] https://www.fca.org.uk/firms/fca-innovate
[63] https://www.fca.org.uk/firms/regulatory-sandbox/global-sandbox
[64] https://www.psr.org.uk/
[65] https://www.bankofengland.co.uk/news/2018/april/non-bank-psp-access-to-the-payments-system-announcement; https://www.bankofengland.co.uk/-/media/boe/files/markets/other-market-operations/accessfornonbankpaymentserviceproviders.pdf?la=en&hash=19DEFEB783364B8B79245628043B69FC1DB8B0FE

rozhodla, že RBSG, LBG, Barclays, HSBCG, Nationwide, Santander, Danske, BoI a AIBG vytvoria spoločný API štandard pomocou, ktorého bude možné zdieľať dáta s ostatnými poskytovateľmi a tretími stranami.[66] Cieľom tejto iniciatívy je rozšíriť jednotný API štandard aj na ostatné bankové inštitúcie.

6.5.4 Francúzsko

Aktivity smerujúce k zlepšeniu Fintech prostredia vo Francúzsku zastrešujú orgány dohľadu – ACPR (Orgán pre obozretný dohľad a rezolúciu – Autorité de contrôle prudentiel et de résolution) a AMF (Orgán pre finančné trhy – Autorité des marchés financiers). ACPR zriadilo spolu s AMF Fintech fórum, ktoré sa spolu s ostatnými zainteresovaným rezortmi stretáva na polročnej báze.

Najvýznamnejšie nástroje na podporu Fintech:

Crowdfunding

Vo Francúzsku existujú tri typy platformy: zhromažďovanie darcov (získavanie finančných prostriedkov na konkrétnom účte určenom na realizáciu projektu, službu môžu prevádzkovať iba akreditovaní poskytovatelia služieb), uzatváranie pôžičiek (sprostredkovateľ pôžičiek musí byť právnickou osobou a musí byť zaregistrovaný v registri ORIAS ako sprostredkovateľ crowdfundingu), upisovanie cenných papierov (platforma musí mať povolenie ako poradcu pre finančné investície, poskytovateľa investičných služieb alebo viazaného agenta).

French Tech Ticket[67]

Francúzsko vytvorilo ročný program pod názvom „French Tech Ticket", ktorého cieľom je zvýšiť medzinárodnú účasť na francúzskom startupovom trhu. Vybraní účastníci programu získajú: grant, zrýchlený proces získania povolenia na pobyt, program na podporu rastu startupu, 12 mesiacov vo vybraných inkubátoroch, pomoc pri administratívnych procesoch a balík na zjednodušenie presťahovania.

Podpora inkubátorov

Francúzska vláda s cieľom podporiť rozvoj inkubátorov vytvorila s pomocou verejnej investičnej banky Bpifrance fondy pod názvami „French Tech Acceleration Fund" a „Large Venture Fund". Výhodnejšími úvermi alebo grantmi tak podporuje inkubátory, akcelerátory a startupy.

6.5.5 Nemecko

Nemecko v súčasnosti nemá ucelenú definíciu koncepcie Fintech spoločností. Fintech spoločnosti sú posudzované individuálne ako začínajúce podniky, ktoré poskytujú špecializované finančné služby s použitím inovatívnych technologických postupov[68]. V prípade určitých podnikateľských modelov Fintech

[66] https://assets.publishing.service.gov.uk/media/57ac9667e5274a0f6c00007a/retail-banking-market-investigation-full-final-report.pdf
[67] https://www.frenchtechticket.com
[68] https://www.bundesfinanzministerium.de/Web/EN/Issues/Featured/FinTech/Supervision-and-regulation/supervision-and-regulation.html

spoločnosti spadajú pod licenčné a dohľadové právomoci nemeckého dohľadového orgánu BaFin (Bundesanstalt fur Finanzdienstleistungsaufsicht)[69]. Ostatné Fintech spoločnosti musia iba spĺňať požiadavky „Hospodárskeho zákonníka". V roku 2016 BaFin vytvoril pracovnú skupinu, ktorej úlohou bolo preskúmať možnú podporu Fintech prostredia v Nemecku. Táto skupina sa neskôr pretransformovala na interný odbor BaFin.

Najvýznamnejšie nástroje na podporu Fintech:

Podpora pre startupy

Podporné programy pre startupy, ktoré majú formu verejných pôžičiek na rozvoj s priaznivými úrokovými sadzbami, dlhými splatnosťami a v mnohých prípadoch počiatočnými obdobiami odkladu pred splatením záväzkov splácania poskytuje Nemecká vláda, špeciálny fond ERP a nemecké spolkové krajiny.

FinCamp – DE

Ministerstvo financií usporadúva podujatia „FinCamp", ktoré sú zamerané na podporu dialógu s nemeckými finančnými spoločnosťami. Na podujatiach sa zúčastňujú zástupcovia Fintech spoločností, bankových inštitúcií a združení, zamestnanci ministerstva financií, Nemeckej centrálnej banky a BaFin.

6.5.6 Švajčiarsko

Švajčiarsko podporuje inovácie hlavne v oblasti zdaňovania pre startupy a inovatívne spoločnosti. Švajčiarsko v súčasnosti nemá reguláciu v oblasti Fintech a uplatňuje rovnaké pravidlá pre všetky spoločnosti bez ohľadu na to, či využívajú tradičné alebo inovatívne podnikateľské modely. Vo Švajčiarsku je orgánom zodpovedným za dohľad Swiss Financial Market Supervisory Authority. Orgán je taktiež zodpovedný za vydávanie povolení, resp. autorizácií na vykonávanie jednotlivých činností.

Švajčiarsko monitoruje technologický vývoj a skúma potenciálny dopyt po úprave regulácie, ktorej výsledkom by bolo zníženie zbytočnej administratívnej záťaže.

Najvýznamnejšie nástroje na podporu Fintech:

Sandbox exemption

Sandbox exeption je prístupná pre všetky spoločnosti. Podľa tejto výnimky, na akceptovanie vkladov od verejnosti do výšky 1 mil. CHF nebude potrebné spĺňať licenčné podmienky určený bankovým zákonom.

Nové licencie

V rámci nových licencií pre spoločnosti akceptujúce vklady od tretích strán do výšky 100 mil. CHF došlo k významnému zníženiu minimálnych kapitálových požiadaviek, požiadaviek na likviditu, nárokov na účtovníctvo a audit a absencií poskytovania garancií za vklady.

[69] Dňa 1. mája 2002 sa Federálny bankový dozorný orgán zlúčil s Federálnym dozorným úradom pre cenné papiere a Úradom pre dohľad nad federálnymi poisťovňami, aby sa stal Federálnym orgánom pre dohľad nad finančným trhom („BaFin"). Jeho hlavným cieľom je zabezpečiť správne fungovanie, stabilitu a integritu nemeckého finančného systému.

6.5.7 Estónsko

Pri aplikovaní finančných inovácií patrí Estónsko v rámci Európy k najprogresívnejším štátom a je významným hráčom v oblasti alternatívneho financovania a startupov používajúcich inovatívne technológie. Niektoré Fintech spoločnosti založené v Estónsku majú v súčasnosti celosvetové pôsobenie v rámci P2P platforiem pre nezabezpečené spotrebiteľské úvery. Aktivity v oblasti alternatívnych platobných služieb, poskytovania alternatívneho financovania a poskytovaní nových technológií vo finančnom sektore vykonáva viacero inovatívnych firiem.

Najvýznamnejšie nástroje na podporu FinTech:

Opatrenia národnej banky a orgánu dohľadu na podporu Fintech spoločností

Centrálna banka vypracovala v roku 2017 stratégiu na roky 2018-2022, ktorej jedným z hlavných cieľov je podpora Fintech. Centrálna banka zohráva aktívnu rolu vo Fintech pracovnej skupine, ktorá je zriadená na FSA (Estónsky orgán dohľadu), hodnotí možné vplyvy na fungovanie finančného sektora a na stabilitu biznis modelov založených na alternatívnych technológiách, vedie diskusie s Fintech spoločnosťami, s ministerstvom financií a FSA pracuje na vytvorení vhodného legislatívneho prostredia pre finančné inovácie.

FSA je orgánom dohľadu, ktorý zohráva významnú úlohu pri finančných inováciách, monitoruje oblasť finančných inovácií, reaguje na možné riziká a prijíma opatrenia, vymieňa si informácie s Fintech spoločnosťami, napomáha spolupráci medzi orgánmi dohľadu a Fintech spoločnosťami a pomáha vyriešiť prípadné prekážky vytvorené komplexnosťou právneho rámca pri zavádzaní inovatívnych riešení do praxe.

Konkrétna pomoc zo strany FSA inovatívnym spoločnostiam

FSA poskytuje Fintech spoločnostiam pomoc v oblasti právneho rámca, získaní autorizácie na poskytovanie služieb a taktiež priamy kontakt so špecialistom, ktorý pomáha nájsť odpovede na potenciálne otázky spojené s biznis plánom.

6.5.8 Litva

Litva v posledných rokoch vytvorila komplexný systém na podporu inovatívneho podnikania, a to vo všeobecnosti pre akúkoľvek podnikateľskú iniciatívu a špecificky pre podnikateľov prinášajúcich inovatívne produkty. Celú iniciatívu podpory inovatívneho podnikania v Litve zastrešuje spoločnosť Invest Lithuania založená a vlastnená litovským ministerstvom hospodárstva. Cieľom je prilákať potenciálnych investorov z domáceho a najmä zahraničného prostredia. Atraktivitu zabezpečuje najmä „tailor made" poradenstvom pre jednotlivé spoločnosti alebo investičné zámery, podporou v oblasti daňových zvýhodnení, naberania zamestnancov a rýchlym založením spoločnosti.

Nositeľom inovatívneho prístupu vo finančnej oblasti je Litovská centrálna banka (LCB), ktorá vytvorila fungujúci ekosystém procesov a nástrojov na podporu zakladania, licencovania a fungovania inovatívnych poskytovateľov finančných služieb.

Najvýznamnejšie nástroje na podporu FinTech:

Skrátené licenčné konanie

LCB deklaruje, že licenčný proces pre platobné inštitúcie a inštitúcie elektronických peňazí trvá len 3 mesiace. Pre banky je to 6 mesiacov. Podmienkou pre takto expresne posúdenú a schválenú licenciu je kvalitná príprava podkladov, tvoriacich súčasť žiadosti o licenciu. LCB vytvorila používateľsky priateľskú webovú stránku, ktorá je prispôsobené priamo pre žiadateľov o licencie v oblasti finančného trhu. Stránka obsahuje najčastejšie kladené otázky pre jednotlivé sektory, spolu s podpornými dokumentmi a informáciami o podmienkach licencovania subjektov.

Konzultačné nástroje – Newcomer programme

Newcomer Programme[70] (NP) sa zameriava na predprípravnú fázu v oblasti definovania podnikateľského zámeru a predlicenčných konzultácií s pracovníkmi LCB. Konzultácie sa týkajú najmä súladu zamýšľanej činnosti so zákonnými požiadavkami na vykonávanú činnosť a predbežnú kontrolu dokumentov, ktoré sú súčasťou žiadosti o licenciu. Web stránka zároveň ponúka prehľad rozdielov licencií a licencovaných činností jednotlivých inštitúcií a zoznam najčastejšie kladených otázok.

Priamy prístup do SEPA prostredníctvom účtu vedeného v LCB

LCB povoľuje aj nebankovým subjektom využívať systém CentroLink[71], ktorý umožňuje vykonávanie SEPA transakcií, prostredníctvom prideleného IBAN a SWIFT BIC kódu a napojením na Európske platobné systémy STEP 2 a RT1 (EBA Clearing), t. j. vykonávanie transakcií bez potreby sprostredkovateľa (bankovej inštitúcie).

Sandbox režim (pripravovaný)

LCB plánuje zaviesť sandbox pre finančné inštitúcie. Režim by mal umožniť začínajúcim spoločnostiam alebo spoločnostiam zavádzajúcim nový produkt jeho nasadenie do reálneho prostredia v obmedzenom rozsahu a na presne stanovený čas (pravdepodobne jeden rok).

Rozvoju Fintech v Litve prispieva aj základná regulácia peer-to-peer a crowdfunding platforiem.

6.5.9 Poľsko

V roku 2017 poľský orgán dohľadu Kimisja Nadzoru Finansowego[72] (KNF) spolu s Ministerstvom financií poľskej republiky (MF PL) a Ministerstvom pre digitalizáciu[73] (MD PL) založili špeciálnu pracovnú skupinu, ktorá sa venuje identifikácii právnych, regulatórnych a dohľadových prekážok pre rozvoj finančných inovácií[74]. Pracovná skupina vypracovala správu o stave finančných inovácií, prekážkach ich zavádzania na poľskom finančnom trhu a krokoch potrebných na ich odstránenie.

Najvýznamnejšie nástroje na podporu Fintech:

Akčný plán podpory inovácií

[70] http://www.lb.lt/en/newcomer-programme
[71] https://www.lb.lt//en/centrolink#ex-1-1
[72] https://www.knf.gov.pl/
[73] http://archiwum.mc.gov.pl/en/the-areas-of-our-activity
[74] https://www.knf.gov.pl/en/MARKET/Fintech/Special_Task_Force_for_Financial_Innovation

Správa Fintech in Poland – barriers and opportunities[75] identifikovala zoznam bariér a popis krokov, ktoré už boli alebo majú byť uskutočnené na odstránenie prekážok. Výsledkom je zriadenie Inovačného hubu, zriadenie Fintech dedikovaného tímu KNF, detailnejšia a prehľadnejšia komunikácia KNF voči dohliadaným subjektom alebo podnikateľom, ktorí chcú vstúpiť na trh, vypracovanie zoznamu legislatívnych zmien v oblasti outsourcingu, identifikácie a reportingu.

Inovačný hub

KNF založila Inovačný hub na podporu nových inovatívnych spoločností a podporu existujúcich účastníkov finančného trhu, ktorí zavádzajú inovatívne produkty alebo služby. Inovačný hub slúži na výmenu informácií o regulačných povinnostiach spoločností pri zavádzaní inovácií a nových produktov.

KNF za účelom zlepšenia komunikácie s účastníkmi trhu zriadila webovú stránku s informáciami potrebných k príprave na licenčný proces spoločnosti.

Sandbox

MD PL vyhodnocuje možnosti vytvorenia virtuálneho sandboxu, v prostredí ktorého by mohli inovatívne spoločnosti testovať svoje produkty a služby. KNF zároveň uvažuje o možnosti zriadenia regulatórneho sandboxu, ako pokračovanie Inovačného hubu. Za hlavnú prekážku zavedenia regulatórneho sandboxu KNF v súčasnosti považuje nedostatok formalizovaných postupov pri výkone dohľadu.

6.5.10 Maďarsko

Účastníci trhu a Fintech spoločnosti v čoraz väčšej miere spolupracujú s finančnými inštitúciami na zlepšovaní ponúkaných služieb (v oblasti bankovníctva, platobných služieb, poisťovníctva a pod.). V roku 2017 sa Maďarská centrálna banka uskutočnila verejnú konzultáciu so zameraním na regulačnú podporu pre Fintech inovácie a následne rozhodla o zavedení opatrení pre podporu Fintech spoločností.

Najvýznamnejšie nástroje na podporu Fintech:

Inovačný hub

Cieľom Inovačného hubu je podporovať inovácie a napomáhať vzniku inovatívnych riešení. V rámci hubu môžu účastníci trhu získavať informácie, ako postupovať pri aplikácii ich inovatívnych riešení v rámci existujúceho ekonomického prostredia. Inovačný hub je zameraný na podporu nových, ako aj existujúcich spoločností, ktoré sa podieľajú na vývoji alebo implementácií Fintech riešení do praxe. Orgán dohľadu v rámci tejto platformy odpovedá na otázky účastníkov trhu, ktoré súvisia s finančnými inováciami. Taktiež im pomáha porozumieť legislatívnemu prostrediu a identifikuje legislatívne opatrenia, ktoré účastníci trhu musia spĺňať.

Regulatórny sandbox

V rámci sandboxu by bola účastníkom trhu, ktorí sa zameriavajú na finančné inovácie, udelená dočasná výnimka na plnenie regulačných požiadaviek. Testovacia fáza pre inovatívne firmy by bola na obdobie pol

[75] http://fintechpoland.com/en/projects/barriers-and-opportunities-for-fintech-innovation-in-poland-report/

roka.

6.5.11 Singapur

V Singapure taktiež neexistujú žiadne špecifické predpisy na úpravu vykonávania podnikateľských aktivít Fintech spoločností. Fintech spoločnosti musia dodržiavať existujúcu legislatívu, ktorá reguluje odvetvie finančných služieb.

Udržateľný, neinflačný hospodársky rast prostredníctvom primeranej tvorby menovej politiky a úzkeho makroekonomického dohľadu nad vznikajúcimi trendmi a možnými zraniteľnosťami podporuje Monetary Authority of Singapur („MAS"). MAS je taktiež dozorným orgánom nad všetkými finančnými inštitúciami a úzko spolupracuje s inými vládnymi agentúrami a finančnými inštitúciami.

Najvýznamnejšie nástroje na podporu Fintech:

Fintech Sandbox

Hlavným cieľom sandboxu je poskytnúť Fintech spoločnostiam priestor s obmedzením trvaním na experimentovanie s produktmi a službami.

Financial Technology & Innovation Group

V roku 2015 MAS založil Financial Technology & Innovation Group („FTIG"). Cieľom je podporenie iniciatívy inteligentného finančného centra. V rámci FTIG boli zriadené tri úrady - Payments & Technology Solutions Office, Technology Infrastructure Office a Technology Innovation Lab, ktoré sú zodpovedné za formulovanie regulačných politík, vypracovanie stratégií na uľahčenie využívania technológií a inovácií, na lepšie riadenie rizík, zvýšenie účinnosti a posilnenie konkurencieschopnosti vo finančnom sektore.

Úrad Fintech

V roku 2016 MAS založil Úrad pre Fintech, ktorý slúži ako jednorazová virtuálna entita pre všetky záležitosti týkajúce sa Fintech spoločností. Členovia Úradu pre Fintech sú: Rada pre hospodársky rozvoj v Singapure, Infocomm Investments, Informačný komunikačný úrad pre rozvoj médií, Národná výskumná nadácia, SPRING Singapur.

6.5.12 Hongkong

Hongkong je dlhodobo svetovým finančným centrom. Previazanosť ekonomiky s finančným trhom a finančnými službami je dlhodobo vysoká. Na trend zavádzania inovácií reaguje aj vláda a finanční regulátory.

V apríli 2015 bola zriadená pracovná skupina pre finančné technológie[76] (Fintech Facilitation Office). Hlavným cieľom je podporiť trvalo udržateľný rozvoj Fintech odvetvia v Hongkongu a propagovať Fintech služby v očiach verejnosti pri plnení vysokých nárokov na kybernetickú bezpečnosť a bezpečnosť osobných údajov. Pre Fintech spoločnosti v Hongkongu neexistuje žiadna špecifická regulačná schéma

[76] http://www.hkma.gov.hk/eng/key-functions/international-financial-centre/fintech-facilitation-office-ffo.shtml

a podliehajú už existujúcej legislatíve v oblasti finančných trhov. Fintech spoločnosti vykonávajúce regulované činnosti musia získať licenciu od Hong Kong Securities and Futures Commission[77].

Najvýznamnejšie nástroje na podporu Fintech:

Fintech Facilitation Office

Hongkonský orgán dohľadu Hong Kong Monetary Authority[78] (HKMA) plní aj úlohu dohľadu nad finančnými inováciami. Pre zabezpečenie rozvoja Fintech ekosystému v Hongkongu a na podporu Hongkongu ako globálneho FinTech centra HKMA zriadil Fintech facilitation Office („FFO"), ktorý plní úlohu platformy na výmenu nápadov Fintech iniciatív a realizáciu aktivít zameraných na rozvoj, vytvára prepojenie medzi účastníkmi trhu a regulačnými orgánmi v rámci HKMA, iniciuje výskum v oblasti potenciálneho použitia, prínosov a rizík Fintech riešení, sprostredkúva spoluprácu medzi vzdelávacími inštitúciami a podnikateľmi.

Fintech Supervisory Sandbox

V roku 2016 HKMA spustila iniciatívu Fintech Supervisory Sandbox[79] („FFS"), ktorá umožňuje bankám a ich partnerským technologickým spoločnostiam realizovať pilotné testy Fintech iniciatív bez potreby dodržiavania požiadaviek dohľadu HKMA.

Bankovým inštitúciám a technologickým spoločnostiam umožňuje sandbox zhromažďovať údaje a spätnú väzbu používateľov na zdokonaľovanie nových produktov a služieb.

6.6 Analýza Fintech riešení

Z doposiaľ známych informácií je možné prostredníctvom SWOT analýzy uviesť nasledovné porovnanie Fintech riešení voči tradičným riešeniam:

Výhody	Nevýhody
▸ zjednodušenie prístupu k službám pre konečného používateľa ▸ využívanie produktov a služieb na diaľku bez potreby návštevy finančnej inštitúcie ▸ zníženie nákladov klienta, t. j. možnosť výberu lacnejšej služby alebo produktu ▸ rýchlosť a pohodlie pri realizácií transakcií, schvaľovaní úverov a pod. ▸ prístup k štatistickým a agregovaným dátam ▸ užívateľsky priateľské aplikácie ▸ zvýšenie personalizácie produktov a služieb pre klienta	▸ strata osobného kontaktu s klientom ▸ vylúčenie zákazníkov, ktorí nevedia používať internet alebo zariadenia (počítače, smartfóny a tablety) ▸ slabá štruktúra a skúsenosti začínajúcich spoločností, v mnohých prípadoch neschopnosť dotiahnuť riešenia „do konca"

[77] http://www.sfc.hk/web/EN/index.html
[78] http://www.hkma.gov.hk/eng/
[79] http://www.hkma.gov.hk/eng/key-functions/international-financial-centre/fintech-supervisory-sandbox.shtml

Výhody	Nevýhody
▸ odbúranie manuálnej práce	
Príležitosti	**Hrozby**
▸ zefektívnenie činnosti bánk a iných finančných inštitúcií ▸ väčší výber produktov a služieb a s tým spojené zvýšenie konkurencie na finančnom trhu ▸ vývoj technológie a inovatívnych produktov a služieb ▸ zefektívnenie manuálnych a rutinných činností ▸ osveta používateľov	▸ bezpečnostné riziko spojené s novou technológiou ▸ vyššie riziko úniku osobných údajov a finančných dát klientov ▸ výkon rýchlych a unáhlených rozhodnutí zo strany klientov ▸ IT gramotnosť používateľov a ochota klientov prijať nové technológie ▸ národné legislatívne prekážky, ako aj absencia spoločných pravidiel v EÚ a s tým spojená náročnosť expandovania platforiem do iných krajín EÚ a zvýšených nákladov na dodržiavanie predpisov

Tabuľka 24: SWOT analýza Fintech riešení

6.7 Odporúčané nástroje podpory Fintech na Slovensku

Podľa publikácie Finance for Fintech[80] očakávaný celosvetový nárast Fintech spoločností v nasledujúcich troch rokoch bude predstavovať 80 %. Rapídny rast sa očakáva najmä v Nemecku (o 284 %). Taktiež významný rast sa očakáva vo Veľkej Británii, Austrálii, Spojených štátoch amerických, Singapure a Hong Kongu.

Etablované finančné inštitúcie investujú do Fintech inovácií (či už interne alebo prostredníctvom partnerstiev s novými inovatívnymi spoločnosťami) a snažia sa aktívne vyvíjať nové produkty a služby. Finančné inštitúcie zavádzajú inovácie na popredné miesta svojich stratégií a v nasledujúcich troch až piatich rokoch plánujú výrazne zintenzívniť investície do tejto oblasti.

Záujem o Fintech riešenia nie je pod drobnohľadom len finančných inštitúcií. Dopytu sa prispôsobili aj významné technologické spoločnosti, ktoré sa výrazne angažujú napr. v oblasti platieb. Otvárajú sa nové obchodné príležitosti a na trh vstupujú netradičný účastníci. Zvýšenie dynamiky rozvoja finančných služieb na Slovensku a zlepšenie konkurencieschopnosti slovenského prostredia je aj snahou SR.

CFI prostredníctvom zriadenia pracovných skupín zložených zo zástupcov relevantných orgánov štátnej správy, subjektov trhu a záujmových združení, umožnilo zintenzívnenie výmeny informácií a skúseností v oblasti finančných technológií. V tejto snahe je potrebné pokračovať a nadviazať ďalšími krokmi.

Vzhľadom k intenzívnemu vývoju technológií a veľkému počtu začínajúcich spoločností, ktoré majú záujem sa tejto problematike venovať by bolo vhodné zaviesť Inovačný hub, v rámci ktorého by Fintech spoločnosti mali možnosť komunikovať s príslušnými orgánmi a prediskutovať otázky týkajúce

[80] www2.londonstockexchangegroup.com/Finance-For-Fintech

sa finančných technológií. Jednalo by sa najmä o vysvetlenie všeobecných regulatórnych a licenčných požiadaviek, ako aj individuálnych usmernení. Inovačný hub by mal spĺňať najmä funkciu informačnej databázy, komunikačného kanálu a platformy na podporu v legislatívnej oblasti).

Ďalším nástrojom, ktorého využitie by bolo potrebné analyzovať je Regulatórny Sandbox, t. j. vytvorenie bezpečného experimentálneho prostredia regulátorom, v rámci ktorého by bolo možné inovatívne riešenia založené na finančných technológiách otestovať. V rámci EÚ už viaceré krajiny (napr. Veľká Británia, Holandsko) regulatórny sandbox založili a ich skúsenosti je možné využiť v prostredí slovenského trhu.

Začínajúce Fintech spoločnosti spravidla nemajú dostatok vedomostí o legislatíve, licencovaní/registrovaní a podmienkach vstupu na finančný trh. Inovatívne produkty a služby zo sebou prinášajú otázky, ktoré ešte neboli zodpovedané. Vzhľadom k tomu by okrem platformy inovatívneho hubu ako pomocný nástroj mohla slúžiť používateľsky priateľská webová stránka. Stránka by obsahovala odpovede na najčastejšie kladené otázky, spolu s podpornými dokumentmi a informáciami o podmienkach licencovania/registrovania subjektov, príslušnej legislatíve a aktuálnych témach v oblasti finančných technológií. Tento súbor informácií by umožnil žiadateľom kvalitnú prípravu na licenčné/registračné konanie a zorientovanie sa v príslušnej legislatíve. Webová stránka by taktiež obsahovala kontakty na relevantné orgány štátnej správy, ktoré by odpovedali na otázky záujemcov, prípadne poskytovali konzultácie.

V neposlednom rade je dôležitá osveta a vzdelávanie v oblasti finančných technológií. CFI, ako aj zainteresované orgány štátnej správy, prispievajú účasťou na rôznych platformách, čím zvyšujú povedomie o tejto oblasti v rámci odbornej aj laickej verejnosti.

Dôležitým aktérom je aj Národná banka Slovenska ako orgán dohľadu nad finančným trhom. Nakoľko finančné technológie sa rýchlo rozvíjajú a dynamicky vstupujú do každodenného života, význam NBS a nezanedbanie úloh roly dohľadového orgánu ako aj proaktivita vo vzťahu k Fintech riešeniam a ich podpore je nezastupiteľná.

Zo strany orgánov štátnej správy by bolo vhodné vytvoriť akčný plán, v rámci ktorého budú identifikované najmä prekážky vstupu spoločnosti Fintech na slovenský a globálny finančný trh a návrh krokov na ich odstránenie vrátane časového harmonogramu.

Hlavnou prekážkou rozvoja Fintech spoločností sú však financie. Vo všeobecnosti spoločnosti získavajú financie zo súkromných alebo verejných zdrojov. Častou formou financovania Fintech spoločností sa stáva crowdfunding, čo je alternatívna forma financovania, ktorá spája tých, ktorí sú ochotní požičať alebo investovať finančné prostriedky priamo s tými, ktorí potrebujú financovanie pre konkrétny projekt. V súčasnosti aj v SR pôsobia spoločnosti ako Crowdberry, Hithit a Finnest. Taktiež v rámci ekosystému 365 vzniká 365.fintech, čo je platforma na investovanie do startupov a zameriava sa na spoločnosti primárne z oblastí finančných technológií a BigData.

Z verejných zdrojov je možné financovanie zabezpečiť prostredníctvom vytvorenia štátneho fondu, finančných nástrojov alebo Európskych štrukturálnych a investičných fondov (EŠIF). V rámci EŠIF nenávratnú finančnú pomoc poskytuje Operačný program Integrovaná infraštruktúra (OPII).

Finančné prostriedky je možné zacieliť na spracovanie štúdií, hodnotení, analýz, strategických a metodických dokumentov (PO 8 OPII). V rámci prioritnej osi 8 OPII – Technická pomoc je alokovaných 102 352 942 EUR (zdroje EÚ + štátny rozpočet). K novembru 2018 bolo v rámci prioritnej osi 8 OPII – Technická pomoc zazmluvnených 48 486 566,16 EUR (zdroje EÚ + štátny rozpočet).

Podpora Fintech projektov z prioritnej osi 7 OPII - Informačná spoločnosť je otázna vzhľadom na nastavenie operačného programu, charakter projektov a žiadateľov, merateľné ukazovatele a udržateľnosť projektu.

Veľkou výzvou zostáva nastavenie regulácie peer-to-peer a crowdfunding platforiem, jednoduchšie zakladanie spoločností, daňové zvýhodnenia nových, ako aj existujúcich inovatívnych spoločností a nastavenie rozumných hraníc medzi bankami a novo licencovanými poskytovateľmi služieb, ktoré zaručia adekvátnu úroveň bezpečnosti a zároveň nebudú brániť rozvoju a inováciám.

Prípadné zvýhodnenie daňového zaťaženia Fintech spoločností voči ostatným subjektom je na zvážení gestora daňových zákonov. Daňové zvýhodnenie by však mohlo viesť k určitej forme skrytej štátnej pomoci, ktorá by mohla byť v rozpore s platnou legislatívou.

Výsledkom podpory spoločností Fintech by malo byť zvýšenie dynamiky rozvoja finančných služieb v SR a zlepšenie konkurencieschopnosti slovenského podnikateľského ekosystému na európskom i globálnom trhu.

7 Odporúčania pre UPVII

Nasledujúce odporúčania predstavujú navrhovaný zoznam aktivít na realizáciu a podporu zo strany ÚPPVII počas najbližšieho obdobia. Zoznam nepredstavuje akčný plán implementácie ďalších eGovernment projektov, len návrh niektorých odporúčaní identifikovaných počas prípravy tejto Štúdie. Keďže je však problematika blockchain pomerne komplexná a neustále rozširujúca sa téma, nie je možné na obmedzenom priestore, ktorý poskytuje táto štúdia, jej úplné pokrytie. Väčšinu týchto odporúčaní je možné začať realizovať ihneď, odhadovaný minimálny časový harmonogram pre realizáciu jednoduchšieho aj komplexnejšieho projektu je uvedený v kapitole 5.2 Všeobecné odporúčania a odhadovaný časový rámec realizácie.

1. Zaviesť štandardy pre blockchainové riešenia a blockchainy v štátnej správe tak, aby si každá organizácia nevytvárala vlastné riešenia, nekompatibilné s inými.
2. Vzdelávanie a popularizácia medzi štátnymi zamestnancami a verejnosťou. Podporiť konferencie, zrealizovať prvé pilotné projekty a široko ich spopularizovať v médiách, vytvoriť dedikovanú web stránku o blockchaine a ďalšie. Pri popularizácii a vzdelávaní je možne použiť aj texty z tejto Štúdie.
3. Zrealizovať prvé blockchain projekty. Môže ísť aj o niektorý z jednoduchších projektov uvedených vyššie v tejto štúdii. Do diskusie o projekte zapojiť odbornú verejnosť, využiť takýto projekt na popularizáciu a získavanie cenných skúseností do budúcna.
4. Analyzovať a v prípade potreby upraviť regulácie pre blockchain a Fintech projekty, vypracovať a zverejniť vysvetlenia a stanoviská.
5. Zvážiť spustenie vládneho blockchain (prípadne dvoch): jeden konzorčný pre komunikáciu medzi štátnymi inštitúciami a druhý verejný pre aplikácie štát-verejnosť.
6. Intenzívne priebežné sledovanie vývoja technológie a jej využitia. Jednou z možností je zrealizovať slovenské blockchain pozorovateľské fórum na podobnom princípe ako EU Blockchain Observatory and Forum na obdobie napr. dvoch rokov, pravidelné stretnutia, štvrťročné reporty o vývoji vo svete blockchainu či o projektoch na Slovensku atď.
7. Aktívne sa zapojiť do prichádzajúcich EÚ cezhraničných blockchain projektov. Navrhnúť blockchain projekty vhodné pre EÚ cezhraničnú spoluprácu, pridať sa do schválených pilotných projektov už počas prípravy, navrhovať riešenia a ponúkať spoluprácu pri realizácii.
8. Fintech odporúčania: Analyzovať možnosti zavedenia inovačného hubu, regulatórneho sandboxu, nastavenie regulácie peer-to-peer a crowdfunding platforiem, vytvorenia webovej stránky a ostatných nástrojov na zvýšenie povedomia v tejto oblasti.
9. Sledovať a aktívne skúmať problematiku CBDC. V tejto oblasti prebieha intenzívny výskum v mnohých krajinách, vychádzajú štúdie, objavujú sa nové zistenia a prichádzajú pilotné projekty, toto všetko odporúčame priebežne a aktívne sledovať. Potrebná je spolupráca NBS, CFI MF SR a ÚPPVII. Zvážiť vypracovanie štúdie na túto tému na Slovensku.

EY | Audit | Dane | Transakcie | Poradenstvo

Informácie o EY

EY patrí medzi najvýznamnejšie celosvetové firmy poskytujúce odborné poradenské služby v oblasti auditu a daňového, transakčného a podnikového poradenstva. Našimi názormi a kvalitou služieb prispievame k budovaniu dôvery v kapitálové trhy a ekonomiky celého sveta. Podporujeme rozvoj popredných lídrov, ktorých spája dôraz na kvalitu poskytovaných služieb vo vzťahu k všetkým zainteresovaným skupinám. V tom je náš hlavný prínos k lepšie fungujúcemu svetu pre našich ľudí, klientov a širšiu komunitu.

Označenie EY sa vzťahuje na celosvetovú organizáciu spoločností, ktorej riadiacou spoločnosťou je britská Ernst & Young Global Limited. Každá členská spoločnosť je nezávislým právnym subjektom. Ernst & Young Global Limited neposkytuje služby priamo klientom. Ďalšie informácie nájdete na našich webových stránkach ey.com.

ey.com/sk