VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

NÁVRH VYUŽITÍ TECHNOLOGIE BLOCKCHAIN VE FIREMNÍM PROSTŘEDÍ
IMPLEMENTATION OF BLOCKCHAIN TECHNOLOGY

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — **Bc. Kristína Dzurdzíková**
AUTHOR

VEDOUCÍ PRÁCE — **Ing. Lukáš Novák, Ph.D.**
SUPERVISOR

BRNO 2020

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav informatiky
Studentka:	**Bc. Kristína Dzurdzíková**
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Informační management
Vedoucí práce:	**Ing. Lukáš Novák, Ph.D.**
Akademický rok:	2019/20

Ředitel ústavu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů a se Studijním a zkušebním řádem VUT v Brně zadává diplomovou práci s názvem:

Návrh využití technologie Blockchain ve firemním prostředí

Charakteristika problematiky úkolu:

Úvod
Vymezení problému a cíle práce
Teoretická východiska práce
Analýza problému a současné situace
Vlastní návrhy řešení
Závěr
Seznam použité literatury
Přílohy

Cíle, kterých má být dosaženo:

Hlavním cílem této práce je zpracovat návrh využití technologie Blockchain na vybraném firemním procesu a doporučit vhodné platformy pro realizaci daného návrhu. Dílčím cílem je seznámení s danou problematikou a srovnání vybraných Blockchain platforem.

Základní literární prameny:

BASHIR, Imran. Mastering Blockchain: Distributed ledger technology, decentralization, and smart contracts explained. Birmingham: Packt Publishing, 2018. ISBN 978-1788839044.

DRESCHER, Daniel. Blockchain Basics: A Non-Technical Introduction in 25 Steps. New York: Apress, 2017. ISBN 978-1484226032.

MOUGAYAR, William a Vitalik BUTERIN. The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology. New Yersey: Wiley, 2016. ISBN 978-1119300311.

TAPSCOTT, Don a Alex TAPSCOTT. Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World. London: Portfolio Penguin, 2016. ISBN 978-0241237854.

VIGNA, Paul. The Truth Machine: The Blockchain and the Future of Everything. New York: St. Martin's Press, 2018. ISBN 978-1250114570.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2019/20

V Brně dne 29.2.2020

L. S.

doc. RNDr. Bedřich Půža, CSc. ředitel	doc. Ing. et Ing. Stanislav Škapa, Ph.D. děkan

Abstrakt

Táto diplomová práca sa zaoberá vytvorením návrhu využitia technológie blockchain vo firemnom prostredí. Hlavným cieľom práce je vytvoriť návrh pre vybraný firemný proces a jeho implementácia v konkrétnej blockchainovej platforme. Analýza súčasného stavu popisuje aktuálny proces a požiadavky spoločnosti na funkcionalitu novej technológie. V návrhovej časti práce som realizovala porovnanie vybraných blockchainových platforiem. Následne som vybrala to najvhodnejšie riešenie a implementovala v ňom svoj návrh. Táto kapitola ďalej obsahuje návrh postupu ako overiť, či je daný proces vhodný na implementáciu blockchain technológie alebo nie. Ďalej popisuje ako postupovať pri výbere vhodného riešenia a vyzdvihuje jeho kľúčové faktory.

Abstract

This diploma thesis deals with the creation of a design for the utilization of blockchain technology in a corporate environment. The main goal of this work is to create a proposal for a business process and its implementation in a specific blockchain platform. The analysis of the current state of the process describes current process and company's requirements for the functionality of new technology. In the design part of the work, I compared specific blockchain platforms. As a result of this part I chose the most suitable solution for the implementation of my proposal. This chapter further includes the design of a methodology for verifying whether the process is suitable for the implementation of a blockchain technology or not. Moreover, it describes how to proceed when choosing a suitable solution and highlights its key factors.

Kľúčové slová

blockchain technológia, blockchain as a servis, distribuovaná účtovná kniha, peer to peer sieť, konsenzus mechanizmus, smart kontrakt

Key words

blockchain technology, blockchain as a servis, distributed ledger, peer to peer network, consensus mechanism, smart contract

Bibliografická citácia

DZURDZÍKOVÁ, Kristína. *Návrh využití technologie Blockchain ve firemním prostředí.* Brno, 2020. Dostupné také z: https://www.vutbr.cz/studenti/zav-prace/detail/119617. Diplomová práce. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky. Vedoucí práce Lukáš Novák.

Čestné prehlásenie

Čestne prehlasujem, že predložená diplomová práca je pôvodná a spracovala som ju samostatne. Prehlasujem, že citácia použitých prameňov je úplná, že som vo svojej práci neporušila autorské práva (v zmysle Zákona č. 121/2000 Sb., o práve autorskom a o právach súvisiacich s právom autorským).

V Brne dňa 10. mája 2020

.....

podpis študenta

Poďakovanie

Chcela by som poďakovať vedúcemu svojej práce Ing. Lukášovi Novákovi, Ph.D. za pomoc a cenné rady pri spracovaní tejto diplomovej práce.

OBSAH

ÚVOD

Žijeme v dobe, kedy sa nové technológie vyvíjajú a menia rýchlosťou svetla. To, čo bolo ešte pred nedávnom najnovším technologickým výdobytkom, sa stáva veľmi rýchlo zastaraným. Čoraz častejšie sa stretávame s pojmami, ktoré súvisia so svetom kryptomien. Každý, kto pozná hlbší význam pojmu kryptomena, nepochybne vie, čo sa skrýva za slovom Bitcoin. Čo však stojí za touto úspešnou kryptomenou, ktorá neustále narastá na popularite? Je to práve Blockchain, ktorý je synonymom pre technológiu „distribuovanej účtovnej knihy“, ktorú si môžeme predstaviť ako decentralizovanú databázovú štruktúru. Ako už je z názvu zrejmé, ide o „reťaz blokov“, ktorá pracuje s transakciami.

Napriek tomu, že doposiaľ najznámejšie využitie Blockchainu je práve v prípade Bitcoinu, nemožno poprieť jeho ďalšie všestranné využitie. V súčasnosti sa teší popularite, čo sa týka jeho využitia v podnikových procesoch. Mnohé spoločnosti, ktoré sú dlhodobými lídrami na trhu ICT produktov a služieb v súčasnosti investujú značné finančné obnosy práve do výskumu tejto technológie. Odborníci predpokladajú svetlú budúcnosť a všestranné vyžitie tejto technológie v podnikovej sfére. Veľké spoločnosti investujú do vývoja tejto technológie a zároveň sa sami stávajú jej užívateľmi. Svoje uplatnenie momentálne nachádza najmä vo finančnom a bankovom sektore, no jej úspešné implementácie nájdeme aj v sektore globálneho obchodovania, dodávateľského reťazca a mnohé ďalšie.

Niet pochýb o tom, že táto technológia má perspektívu a mnohé silné stránky. Vďaka spoľahlivým kryptografickým mechanizmom, ktoré využíva, je zárukou poskytovania vysokého stupňa bezpečnosti a spoľahlivosti. Má zmysel najmä tam, kde nachádzame viacero organizácií, ktoré sú vo vzájomnej interakcii a potrebujú medzi sebou zdieľať a upravovať dáta. Úzko súvisí s pojmom smart kontrakt, ktorý by mohol čoskoro úplne nahradiť klasický papier. V dnešnej dobe máme už niekoľko platforiem a hotových riešení, ktoré umožňujú organizáciám implementáciu tejto technológie.

CIEĽ A METODIKA PRÁCE

Hlavným cieľom tejto práce je spracovať návrh využitia technológie Blockchain na vybranom firemnom procese a odporučiť vhodné platformy pre realizáciu daného návrhu. Dielčím cieľom je zoznámenie s danou problematikou a porovnanie vybraných Blockchainových platforiem.

Vybraný firemný proces bol spracovaný podľa reálneho objednávkového procesu. Poznatky pre teoretickú časť práce som čerpala najmä z vedeckých článkov a odborných kníh. Podkladom pre analýzu súčasného stavu boli konzultácie priamo s účastníkmi procesu a lídrom objednávkového tímu, ktorý mi dodal všetky potrebné informácie pre pochopenie celkovej problematiky a princípu tohoto procesu. V návrhovej časti práce som vytvorila návrh nového riešenia v konkrétnom produkte, ktorý najviac zodpovedal požiadavkám procesu.

1 TEORETICKÉ VÝCHODISKÁ

Nasledujúca kapitola obsahuje súhrn teoretických poznatkov potrebných pre pochopenie základných princípov blockchain technológie a s ňou súvisiacich procesov.

1.1 Blockchain a jeho pôvod

Blockchain je druh distribuovanej decentralizovanej databázy, ktorá vďaka svojím vlastnostiam zabezpečuje kontrolu nad všetkými transakciami vykonanými v danej blockchainovej sieti a vysoký stupeň bezpečnosti. Kontrola je udržiavaná za pomoci zdieľanej účtovnej knihy, ktorá je verejne prístupná všetkým účastníkom siete. Kniha obsahuje všetky transakcie, ktoré boli v sieti realizované, takže o nich majú prehľad všetci užívatelia. Mechanizmus blockchainovej sieť pracuje na princípe schvaľovania väčšiny, prostredníctvom čoho je udržiavaná synchronizácia a overovanie obsahu účtovných kníh, ktoré sú replikované u všetkých účastníkov (7).

Napriek tomu, že jeho pôvod sa viaže ku technológiám, ktoré boli predstavené pred niekoľkými desiatkami rokov, svoju popularitu nadobudol až v roku 2008, pri svojom doposiaľ najznámejšom využití - Bitcoine. V tomto roku anonymný jednotlivec (alebo skupina ľudí – tento fakt doteraz nie je známy) pod pseudonymom Satoshi Nakamoto uverejnil štúdiu, kde predstavil Bitcoin - blockchainovú digitálnu menu. Bitcoin je prvým príkladom digitálnej meny, ktorá disponuje riešením na problém dôvery v decentralizovaných systémoch (7).

Bitcoin

Bitcoin je kryptomena, ktorá je fungujúcim príkladom využitia technológie blockchain vo finančnom sektore. bitcoinový blockchain je decentralizovaná účtovná kniha, ktorá obsahuje časové známky a chronologicky zaznamenáva všetky transakcie v sieti. Kniha je verejne prístupná všetkým účastníkom siete, ktorí sú označovaní ako *peers*. Môžu to byť buď jednotlivci alebo anonymné uzly, ktoré fungujú bez ľudského zásahu. Transakcie sa vysielajú do siete a ich platnosť je overiteľná jednotlivými účastníkmi nezávisle na sebe. Platné transakcie sa ukladajú do blokov, ktoré sú kryptograficky zašifrované. Okrem účastníkov označovaných ako peers, existuje ďalšia skupina

účastníkov, ktorí sú nazývaní ako *miners* alebo vo všeobecnosti *voters*. Títo medzi sebou navzájom súťažia aby vyťažili nový blok, ktorý nadväzuje na posledný blok súčasného reťazca, pričom musí byť zachované chronologické poradie blokov v reťazci. Súťaž je založená na relatívnej výpočtovej sile každého minera s ohľadom na celkovú výpočtovú silu všetkých aktívnych minerov v sieti (7).

1.1.1 Vývoj Blockchain technológie

Táto kapitola popisuje niekoľko generácií blockchain technológie, ktoré sa vyvinuli od časov jeho vzniku.

Blockchain v 1.0

Táto verzia blockchainu bola predstavená pri vzniku bitcoinu a využíva sa najmä pri kryptomenách. Keďže Bitcoin bol prvým prípadom využitia a implementácie kryptomeny, dáva zmysel vymedzovať prvú generáciu blockchainu týmto spôsobom. Bitcoin a všetky alternatívne kryptomeny spadajú do tejto kategórie. Patria sem zároveň všetky aplikácie, ktoré súvisia s kryptomenami a finančnými transakciami (25).

Blockchain v 2.0

Blockchain generácie 2.0 je využívaný v sektore finančných služieb. V tejto generácií sa prvýkrát predstavili smart kontrakty. Spadajú sem menové, finančné a marketingové aplikácie, ktoré narábajú s finančnými aktívami (napríklad opcie, dlhopisy, swapy a ďalšie (25).

Blockchain v 3.0

Tretia generácia technológie blockchain sa využíva na implementáciu aplikácií mimo sektor finančných služieb. Využíva sa na všeobecnejšie účely ako sú napríklad vládny sektor, zdravotníctvo, média, či právny sektor. Veľkú popularitu nadobudli aj mnohé obchodné riešenia a firemné aplikácie, ktoré túto technológiu postupne implementujú do svojich firemných procesov (25).

1.2 Druhy blockchainu

Vo všeobecnosti môžeme definovať tri rôzne druhy blockchainu. Rozlišujeme blockchain súkromný, verejný a konzorcium blockchain. Verejný a súkromný blockchain majú mnoho podobných vlastností:

- obe sú decentralizované siete typu peer to peer, kde každý účastník siete uchováva repliku zdieľanej účtovnej knihy, ktorá obsahuje digitálne podpísané transakcie
- oba typy sieti udržiavajú repliky synchronizované prostredníctvom protokolu označovaného ako konsenzus protokol
- oba poskytujú určité záruky na nemeniteľnosť zdieľanej knihy, a to aj v prípade, že by sa niektorí účastníci siete mohli stať potencionálnymi útočníkmi (17).

Hlavný rozdiel medzi verejným a súkromným blockchainom súvisí s tým, kto má povolenú účasť v sieti, kto vykonáva konsenzus protokol a kto udržiava zdieľanú účtovnú knihu (17).

Verejný blockchain

Verejný blockchain je úplne otvorený a platí, že ktokoľvek sa môže zapojiť do siete a byť jej účastníkom. Sieť má zvyčajne určitý druh stimulačného mechanizmu. Jeho úlohou je povzbudiť čo najväčší počet účastníkov, aby sa zapojili do činnosti v sieti. Bitcoin je dnes jednou z najväčších verejných blockchainov (17).

Vo verejnom blockchaine sú účastníkmi anonymné uzly. Všetky anonymné uzly sa spolu podieľajú na udržiavaní transakčnej účtovnej knihy prostredníctvom algoritmu konsenzu (3).

Jednou z hlavných nevýhod verejného blockchainu je značné množstvo výpočtového výkonu, ktoré je potrebné na udržiavanie distribuovanej knihy a synchronizácie v sieti. Hlavným dôvodom je, že dosiahnutie konsenzu vyžaduje, aby každý uzol v sieti vyriešil komplexný kryptografický problém, ktorý je náročný na výpočtové zdroje. Ďalšou nevýhodou tohto typu siete je otvorenosť verejného blockchainu, ktorá pre transakcie predstavuje pomerne málo súkromia a s tým spojenú nižšiu úroveň celkovej bezpečnosti siete (17).

Súkromný blockchain

V súkromnom blockchaine sa účastníkmi môžu stať len autorizovaní užívatelia. Vytvorenie nového bloku a udržiavanie účtovnej knihy sa realizuje na základe pravidiel preddefinovaných v konkrétnom sieťovom mechanizme - algoritme konsenzu. Typické algoritmy konsenzu, ktoré sa v sieťach tohto typu využívajú sú Proof of Work (PoW) a Proof of Stake (PoS) (3).

Ak chceme pridať nového užívateľa do súkromného blockchainu, musí byť do siete najskôr prizvaný správcom siete alebo iným účastníkom, ktorý má na to dostatočné právomoci. Následne musí sieťový mechanizmus overiť, či užívateľ spĺňa pravidlá a politiku danej siete. V prípade podnikov, ktoré prevádzkujú súkromnú blockchainovú sieť, spravidla platí, že využívajú sieť s povoleniami, takzvaný *permissioned blockchain*. Takáto sieť má vopred definované pravidlá prístupu, povolenia na správu transakcií a vykonávanie iných operácií. Sieťový mechanizmus zabezpečuje aby boli účastníkom pridelené odpovedajúce stupne prístupu ku konkrétnym transakciám. Mechanizmus kontroly prístupu sa môže meniť. Existujúci účastníci v súkromnej sieti majú právo pozmeniť podmienky účasti pre budúcich účastníkov. Akonáhle sa nový užívateľ pripojí k existujúcej sieti, bude súčasťou systému udržiavania blockchainu decentralizovaným spôsobom (17).

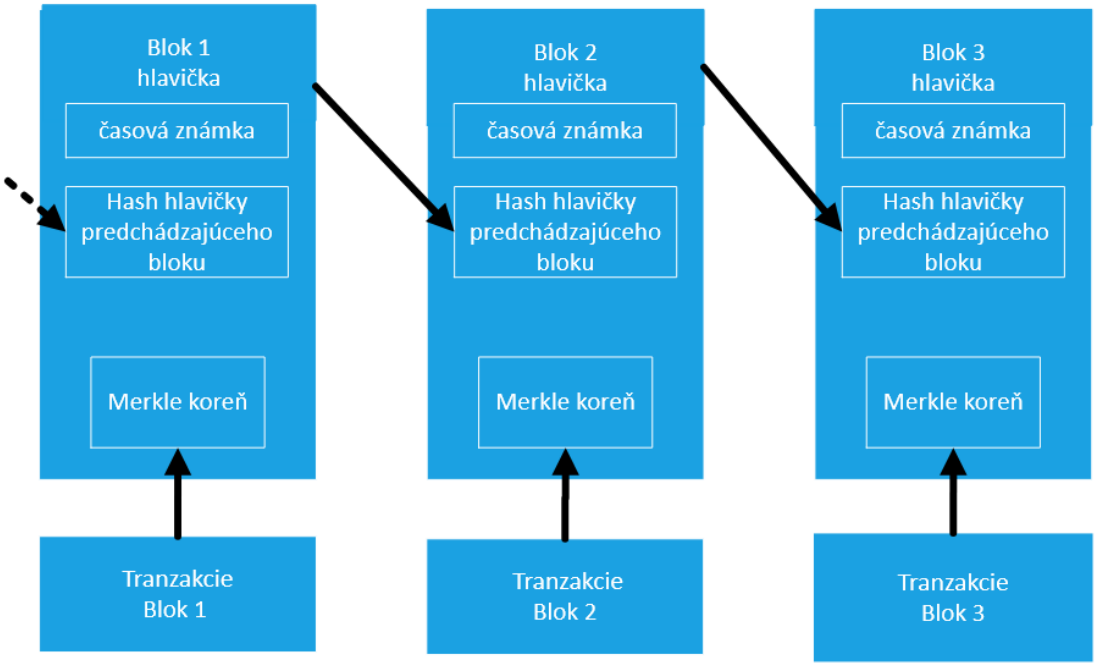
Konzorcium Blockchain

Konzorcium blockchain je hybridný model, ktorý je kombináciou funkcií verejného a súkromného blockchainu. V blockchainovej sieti typu konzorcium účastníci vopred vyberajú skupinu uzlov, ktoré môžu riadiť proces konsenzu a sú tak určitým spôsobom nadradené ostatným (28).

Tento typ siete udržiava distribuovanú štruktúru a zároveň posilňuje bezpečnosť prostredníctvom kontrolovania prístupu užívateľov. V závislosti od mechanizmu konsenzu, je vhodný pre vládne agentúry alebo finančné inštitúcie, ktoré vyžadujú dohodu medzi účastníkmi (32).

1.3 Štruktúra blockchainu

Blockchain je distribuovaná dátová štruktúra, zložená z blokov, ktoré tvoria súvislý reťazec. Každý blok v reťazci obsahuje záznam o transakcii a je identifikovaný šifrovacím hashom. Zároveň uchováva údaj o hashi bloku, ktorý mu predchádza. Výnimkou z tohto je len prvý blok reťazca označovaný ako genesis blok. Každý blok ďalej obsahuje časovú známku a koreň merkle, ktorého význam je bližšie popísaný v kapitole číslo 1.8, ktorá sa zaoberá kryptografickými technikami (8).



Obrázok č. 1: Štruktúra bloku
(Zdroj: Vlastné spracovanie podľa: 8)

Genesis blok

Genesis blok je spoločný predchodca všetkých blokov. Je zakódovaný v klientskom softvéri a nemôže byť nijakým spôsobom upravovaný. Všetky uzly vždy vedia hash a štruktúru genesis bloku, ktorý je bezpečnostným koreňom siete (16).

Genesis blok býva niekedy označovaný ako blok nula - *zero block*. To znamená, že nasledujúci blok, ktorý bude do reťazca pridaný za ním, bude označený ako blok číslo jedna. Číslo používané na označenie poradia jednotlivých blokov je známe ako *block height number*. Je to vždy kladné číslo typu integer väčšie ako nula (22).

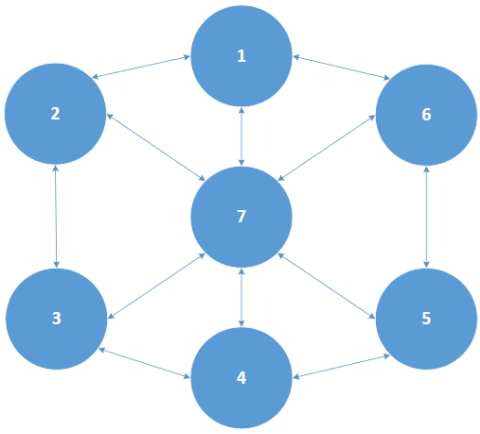
Nodes - Uzly

Ako už bolo spomínané, blockchain si môžeme predstaviť ako reťazce dát. Je nutné však zadefinovať ďalší dôležitý pojem a to je *node.* Nodes sú sieťové uzly, ktoré tvoria chrbticu blockchainovej siete. Bez nich by sieť nebola plne funkčná a neplnila by svoju úlohu. Keďže blockchainová sieť je druh peer to peer siete (viď kapitola 1.4), uzol môže byť považovaný za rovnocenného práve vtedy, keď je schopný pripojiť sa a komunikovať s ostatnými uzlami v sieti. Z technického hľadiska je blockchainovým uzlom akýkoľvek počítač, ktorý má nainštalovaného blockchainového klienta a je schopný prevádzkovať plne funkčnú kópiu distribuovanej knihy. Keď sa chcú užívatelia pripojiť ku sieti, robia to prostredníctvom týchto uzlov (12).

Základné úlohy blockchainového uzla sú:

1. pripojenie k blockchainovej sieti,
2. zachovávanie aktuálnej verzie distribuovanej účtovnej knihy,
3. monitorovanie transakcií,
4. zdieľanie platných transakcií v sieti,
5. monitorovanie novo pridaných blokov v sieti,
6. overovanie novo pridaných blokov - potvrdzovanie transakcií,
7. vytváranie a zdieľanie nových blokov (12).

Node plní funkciu malého servera, ktorý slúži ako úložisko pre bloky dát. Nemusí to byť teda len počítač, môže to byť akýkoľvek druh zariadenia. Nodes tvoria infraštruktúru blockchainu. Všetky sú vzájomne prepojené a neustále si navzájom vymieňanú aktuálne blockchainové dáta aby zachovali vzájomnú synchronizáciu. Uskladňujú, rozširujú a uchovávajú dáta. *Full node* je zariadenie, ktoré obsahuje kompletnú kópiu všetkých vykonaných transakcií (23).



Obrázok č. 2: Rozloženie uzlov v blockchainovej sieti
(Zdroj: Vlastné spracovanie podľa: 23)

Distribuovaná účtovná kniha

Blockchainová účtovná kniha je dátová štruktúra, ktorá pozostáva z usporiadaného zoznamu transakcií. Môžu byť do nej zaznamenané transakcie peňažných prostriedkov alebo výmena tovaru či iného aktíva medzi viacerými stranami. V blockchainovej sieti sa kniha replikuje u všetkých uzlov. Okrem toho sú transakcie ukladané do blokov, ktoré sa neskôr navzájom spájajú. Blockchainová sieť začína s určitým počiatočným stavom, pričom kniha zaznamenáva celú históriu operácií a transakcií, ktoré boli vzhľadom na počiatočný stav v sieti vykonané. Systém môže mať jednu alebo viacero kníh, ktoré môžu byť navzájom prepojené. Veľké podniky môžu napríklad vlastniť viacero účtovných kníh, jednu pre každé z jeho oddelení: inžinierstvo, starostlivosť o zákazníkov, dodávateľský reťazec, mzdové účtovníctvo atď. Vlastníctvo môže byť buď úplne verejné, alebo naopak striktne súkromné pod kontrolou jednej skupiny. Bitcoin je napríklad úplne verejný a v dôsledku toho si vyžaduje nákladný protokol konsenzu, ktorý musí určiť, kto môže knihu aktualizovať a vykonávať v nej zmeny (11).

1.4 Peer to peer sieť

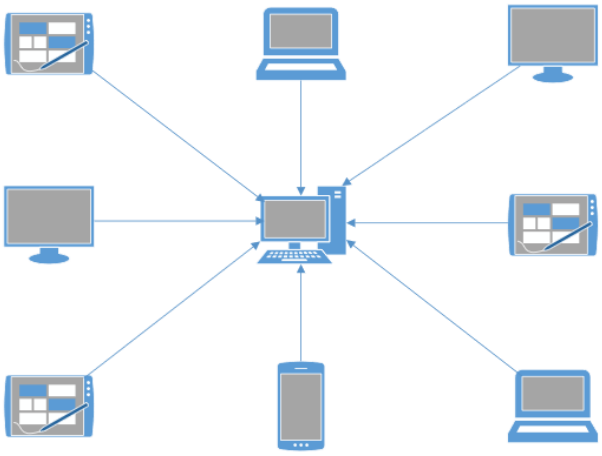
Využitie siete peer to peer (P2P) v technológií blockchain je jedným z dôvodov prečo je táto sieť tak pevná a bezpečná. Peer to peer sieť, ako už názov napovedá, je sieťová topológia, vďaka ktorej môžu všetky uzly v sieti navzájom komunikovať. Môžu si navzájom medzi sebou odosielať a prijímať správy (25).

Uzly spolu komunikujú priamo bez potreby centrálneho servera na výmenu informácií. V tomto modeli nie sú žiadne špeciálne uzly ani hierarchia a každý uzol požaduje informácie priamo od príslušných uzlov. Siete peer-to-peer sú preto decentralizované a otvorené. Blockchain je preto jednoducho súborom uzlov, ktoré prevádzkujú sieťový blockchainový protokol, pričom hlavným princípom je decentralizácia riadenia. Uzly v tradičnej blockchainovej sieti preberajú rôzne úlohy v závislosti od svojich príslušných funkcií v blockchaine. Blockchainová sieť má najmä za úlohu preposielať informácie medzi uzlami, spravovať databázu kde sa informácie ukladajú, vykonávať ťažobné úlohy a udržiavať službu používateľského rozhrania, napr. služba krypto peňaženky. Z tohto dôvodu môže každý uzol v blockchaine zastávať rôzne úlohy (ako napríklad minner, peňaženka či smerovací uzol). Všetky uzly vykonávajú smerovacie funkcie, aby sa mohli efektívne zúčastňovať na blockchaine (26).

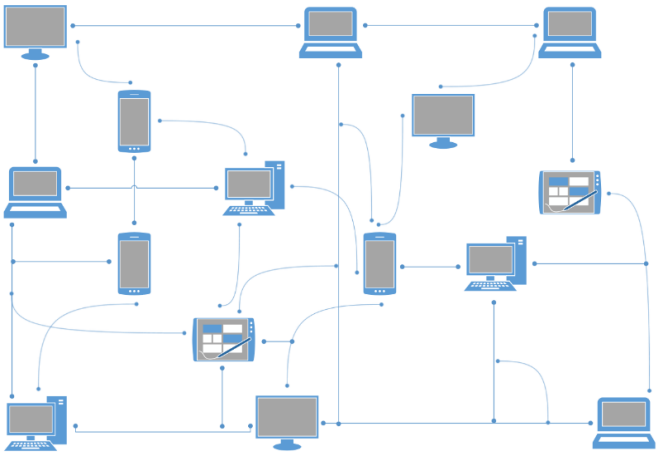
Schollmeier definuje sieť typu peer-to-peer ako architektúru distribuovanej siete, kde účastníci taktiež zdieľajú časť svojich vlastných hardvérových zdrojov, ako je napríklad výpočtová kapacita alebo úložisko. Tieto zdieľané zdroje sú potrebné na poskytovanie služieb a obsahu ponúkaného danou sieťou (napr. zdieľanie súborov, ukladanie alebo kolaboratívne zdieľané pracovné plochy) a sú priamo prístupné iným uzlom bez toho, aby museli byť spravované sprostredkovateľskými subjektmi či vyžadovali nejaké ďalšie povolenia (24).

Každá zmena, ktorá v sieti nastane, vytvára reťaz komunikácie medzi uzlami. Každý uzol je však nezávislý od ostatných uzlov a môže pokračovať v činnosti nezávisle na ostatných uzloch. Z hľadiska bezpečnosti, vzhľadom na decentralizovanú povahu sietí typu peer to peer, môžeme považovať neprítomnosť centrálneho servera za určitú výhodu. Dôvodom je to, že sťažuje útoky v sieti, ako sú napríklad DoS útoky alebo iné útoky týkajúce sa architektúr klient/server (26).

Nasledovné obrázky zachytávajú schému komunikácie uzlov siete typu peer to peer a centralizovanej siete:



Obrázok č. 3: Centralizovaná sieť
(Zdroj: Vlastné spracovanie podľa: 15)



Obrázok č. 4: Peer to peer sieť
(Zdroj: Vlastné spracovanie podľa: 15)

1.5 Mechanizmus blockchainovej siete

Blockchainová sieť je množina uzlov, ktoré pracujú v jednej sieti. Uzol môže všeobecne slúžiť ako vstupný bod pre niekoľko rôznych užívateľov do danej siete. V blockchainovej sieti platia nasledovné pravidlá :

1. Interakcia medzi užívateľmi siete a blockchainom je realizovaná prostredníctvom dvojice kľúčov - súkromný a verejný kľúč. Súkromný kľúč užívatelia používajú na podpisovanie svojich vlastných transakcií, a verejný kľúč je používaný na adresáciu transakcií v sieti. Využíva sa tu asymetrická

kryptografia, ktorá zabezpečuje autentifikáciu, integritu a nemennosť siete. Každá podpísaná transakcia je vysielaná daným uzlom k jeho užívateľom. Pred iniciovaním ďalšieho prenosu sa susedný užívatelia najskôr presvedčia o platnosti prichádzajúcej transakcie. V prípade, že je transakcia neplatná, je zlikvidovaná. Po úspešnom potvrdení jej platnosti, je transakcia vysielaná do celej siete (8).

2. Transakcie, ktoré boli usporiadané a potvrdené v sieti pomocou vyššie uvedeného algoritmu v rámci dohodnutého časového intervalu, sú zoradené a umiestnené do kandidátneho bloku s časovou značkou. Tento proces sa nazýva *mining* - ťaženie. Uzol, ktorý tento blok vyťažil, rozpošle tento blok naspäť do siete. Voľba ťažiaceho uzla a obsahu bloku závisia od konsenzového mechanizmus, ktorý je v sieti preddefinovaný (8).

3. Uzly overia, či navrhovaný blok obsahuje platné transakcie a či odkazuje na hash predchádzajúceho bloku v reťazci. Ak overenie prebehlo úspešne, blok je pridaný do reťazca. Ak overenie nebolo úspešné, prebehne zlikvidovanie navrhovaného bloku, a tým sa ukončí aktuálny cyklus (8).

Pre bezproblémové fungovanie blockchainovej siete je nutné aby boli predom definované pravidlá fungovania. Tieto pravidlá sú naprogramované v každom blockchain klientovi, ktorý potom na základe nich rozhoduje, či je daná prichádzajúca transakcia platná alebo naopak a súčasne rozhodne, či by mala byť do siete pridaná alebo nie (8).

Obrázok č. 5: Proces pridania transakcie do blockchainu
(Zdroj: Vlastné spracovanie podľa: 28)

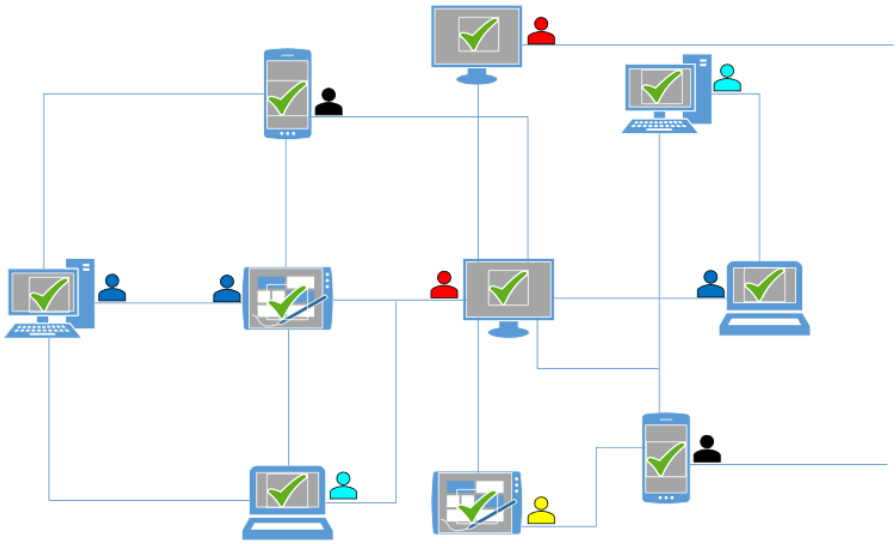
1.6 Konsenzus mechanizmus

Konsenzus protokoly sú jedným z najdôležitejších a revolučných aspektov blockchainovej technológie. Tieto protokoly vytvárajú nevyvrátiteľný systém dohody medzi rôznymi zariadeniami v distribuovanej sieti a zároveň zabraňujú zneužívaniu systému. Vďaka využitiu konsenzových protokolov v blockchainovej sieti, zostávajú

všetky uzly v sieti synchronizované. Protokol je definovaný ako súbor pravidiel, ktoré opisujú spôsob komunikácie a prenosu dát medzi elektronickými zariadeniami. V prípade blockchainovej siete hovoríme o uzloch. Tieto pravidlá je potrebné definovať na úplnom začiatku. V pravidlách je podrobne opísané, ako budú informácie štruktúrované a ako ich jednotlivé zariadenie bude vysielať a prijímať (15).

Termínom "konsenzus" rozumieme, že uzly v sieti sa musia zhodnúť na jednotnom závere a sú schopné proces kontrolovať samostatne. Ide o kľúčový aspekt blockchain technológie, ktorý vykonáva dve podstatné funkcie. Prvou je, že konsenzové protokoly umožňujú aktualizáciu blokov, pričom súčasne zabezpečujú, aby bol každý blok v reťazci pravdivý. Druhým aspektom je, že zabraňuje akémukoľvek neoprávnenému jednotlivcovi kontrolovať alebo pozmeniť blokový systém a obsah (15).

Konsenzus je teda výpočtový mechanizmus, ktorý sa využíva aby zabezpečil pravidlá uzatvárania dohôd na základe jednotnej verzie pravdy všetkými uzlami v sieti (25).



Obrázok č. 6: Schéma komunikácie v konsenzus mechanizme
(Zdroj: Vlastné spracovanie podľa: 15)

Existujú dva druhy konsenzových mechanizmov:

1. Proof - based/ leader – based (alebo tiež Nakamoto konsenzus) kde je zvolený vodca, ktorý následne navrhne výslednú hodnotu (25).
2. Byzantine fault tolerance – čo je tradičnejší prístup, ktorý je založený na výsledkoch hlasovania vybraných uzlov (25).

Pravidlá konsenzového protokolu

Pravidlá konsenzu sú špecifickým súborom pravidiel. Kľúčovou požiadavkou na dosiahnutie konsenzu je jednomyseľná zhoda uzlov v sieti na jednej dátovej hodnote, dokonca aj v prípade, že niektoré z uzlov zlyhajú alebo nie sú považované za dostatočne spoľahlivé. Keďže blockchain technológia sa nespolieha na centrálny orgán pre bezpečnosť, používatelia nemajú žiadne predchádzajúce znalosti o tom, ktorá verzia záznamu je platná. Účastníkom siete, ktorí udržiavajú blockchain, poskytujú protokoly konsenzu odmeny ako motiváciu, aby v tom pokračovali. Tieto odmeny prichádzajú vo forme kryptomien alebo žetónov. Konsenzové protokoly sú navrhnuté tak, aby sa dali ťažko napodobňovať alebo replikovať. To znamená, že je časovo náročné vykonať požadované výpočtové procesy. Metódy konsenzu sa líšia v závislosti od blockchainu, v rámci ktorého overujú bloky a existujú rôzne formy konsenzu (15).

1.7 Druhy konsenzových mechanizmov

Existuje mnoho rôznych algoritmov konsenzu, pričom výber konkrétneho konsenzového mechanizmu v danej sieti je realizovaný na základe základnej štruktúry blockchainu. Jedná sa o vyššie spomínane formy blockchainu - verejný, súkromný alebo konzorcium blockchain. Všetky spomínané formy blockchainu majú jednotný cieľ, ktorým je aby zabezpečili uchovávanie a udržiavanie jednotnej a integrovanej verzie pravdy. Problém dvojitého vynakladania prostriedkov, ktorý je v súčasnej dobe vážnym problémom pre hodnotné transakcie, je možné vyriešiť prostredníctvom blockchainového konsenzového mechanizmu. Existujú rôzne mechanizmy konsenzu, ktoré sú funkčné na rôznych blockchainových platformách, ale všetky z nich riešia prevažne problémy toho istého druhu. Príkladom problému je, že niektoré mechanizmy konsenzu musia vynaložiť značné množstvo výpočtovej sily a energie aby boli schopné docieliť dohodu konsenzu. Niektoré ďalšie mechanizmy konsenzu majú rozličný stupeň bezpečnosti, ktorý sa mení v závislosti od daného typu blockchainovej siete (28).

Practical Byzantine Fault Tolerance

V prípade mechanizmu PBFT platí, že všetky uzly v sieti blockchain vlastnia verejný kľúč. Akonáhle je iniciovaná a vysielaná správa o transakcii, uzly preposielajú informácie spolu s verejným kľúčom na vykonanie operácie. Každý uzol v sieti

vykonáva operáciu na základe inštrukcií v transakcii. Keď operácia skončí a jednotlivý uzol má výsledné rozhodnutie, zdieľa ho v rámci siete. Konsenzus sa dosiahne na základe rozhodnutí všetkých uzlov. V procese kolektívneho konsenzu sa sieť zapája do kolektívnych rozhodnutí uzlov pre všetky transakcie. Tento protokol využíva napríklad Hyperledger Fabric (28).

Proof of Work

Ďalším mechanizmom je Proof of Work – (PoW). V tomto prípade sú zúčastnené uzly zapojené do intenzívnej výpočtovej a matematickej výpočtovej práce, výsledkom ktorej je dosiahnutie konsenzu. PoW nevyžaduje účasť všetkých uzlov, namiesto toho využíva jedinečný hash kód určitej veľkosti. Uzol, ktorý vyrieši matematickú hádanku a vygeneruje hashový kód, ju odošle do siete. Neskôr ostatné uzly overujú informáciu, po jej úspešnom overení sa vytvorí nový blok a pridá sa do blockchainu. Dôvodom použitia hashovacej funkcie je to, že ju nemožno spätne dešifrovať, čo znamená, že falošné návrhy sú odhalené a nezarátavajú sa do finálneho rozhodnutia. Ďalším faktom je že PoW funguje ako náhodný proces len s veľmi nízkou pravdepodobnosťou na úspech. To znamená, že predtým, ako akékoľvek uzly vygenerujú platný dôkaz, je realizovaných veľa procesov typu pokus a omyl. PoW je využívaný v bitcoine a platí, že uzol, ktorý dokáže ako prvý predložiť dôkaz, ktorý je po overení vyhodnotený ako platný, získava nárok na odmenu vo forme niekoľkých bitcoinov. V blockchaine založenom na PoW je určité pracovné zaťaženie, ktoré bolo odsúhlasené sieťou. Toto zaťaženie je úmerné s dĺžkou blockchainového reťazca (28).

Proof of Stake

V PoS mechanizme majú uzly zapojené do vytvárania a pripájania nového bloku viac-menej finančný záujem - získanie odmeny. PoS nahradzuje hash funkciu digitálnym podpisom. Sieť náhodne vyberie jeden zúčastnený uzol na základe jeho pomerného podielu v sieti pokiaľ ide o schvaľovanie transakcií. To znamená, že sieť podnecuje vznik lotériového systému a zapája jednotlivé uzly v závislosti od ich prispievaného podielu v sieti. V súčasnosti tento mechanizmus využívajú napríklad Blackcoin alebo Bitshares (28).

V tabuľke nižšie, môžeme vidieť prehľad základných funkcionalít konsenzových mechanizmov, pričom platí: **+++** - najviac priaznivé, **+** - najmenej priaznivé.

Tabuľka č. 1: Prehľad vlastností mechanizmov konsenzu
(Zdroj: Vlastné spracovanie podľa: 30)

	Porovnanie charakteristík			
	Základné vlastnosti	Efektívnosť nákladov	Výkon	Flexibilita
Proof-of-work	+++	+	+	+
Proof-of-stake	++	++	++	+++
Practical Byzantine Fault Tolerance	+	+++	+++	+

1.8 Blockchain a kryptografia

V tejto kapitole definujem niektoré dôležité pojmy kryptografie, ktoré sa týkajú technológie blockchainu. Patrí sem napríklad kryptografia s verejným kľúčom, hashovanie a Merkle stromy.

Kryptografia je veda o vývoji protokolov, ktoré bránia tretím stranám v prístupe ku súkromným údajom. Moderná kryptografia kombinuje disciplíny z matematiky, informatiky, fyziky, strojárstva a ďalších. Niektoré dôležité pojmy sú definované nižšie:

- **šifrovanie:** kódovanie textu do nečitateľného formátu
- **dešifrovanie:** vyhradenie šifrovania - prevádzka neusporiadanej správy do jej pôvodnej podoby
- **šifra:** Algoritmus na vykonávanie šifrovania alebo dešifrovania, zvyčajne dobre definovaná sada krokov, ktoré je možné nasledovať (27).

Blockchainové systémy používajú niekoľko kryptografických techník, aby zabezpečili integritu účtovných kníh a celej siete. Integritou je v tomto prípade myslená schopnosť detegovať možnú manipuláciu s údajmi uloženými v blockchaine. Táto vlastnosť je nevyhnutne potrebná najmä vo verejných prostrediach, kde neexistuje žiadna vopred nastavená dôvera. To isté platí aj v prípade súkromných blockchainov, kde je integrita rovnako dôležitá (11).

V blockchainovej sieti existuje niekoľko úrovní zabezpečenia integrity. Patrí sem nemennosť, ktorá je zabezpečovaná prostredníctvom hashového stromu *Merkle tree*,

ktorého koreňový hash je uložený v bloku. Akákoľvek zmena stavu má teda za následok zmenu v koreňovom hashi. Druhá úroveň ochrany integrity súvisí s históriou blokov. Tá je chránená, vďaka tomu, že bloky sú po ich pripojení do blockchainového reťazca nemenné. Ďalšou kľúčovou technikou je prepájanie blokov prostredníctvom kryptografických hashov. Každý blok obsahuje hash z predchádzajúceho bloku, takže modifikácia v bloku okamžite zruší platnosť všetkých nasledujúcich blokov. Kombináciou týchto techník poskytuje blockchain bezpečný a efektívny dátový model, ktorý sleduje všetky historické transakcie a vykonané zmeny (11).

Bezpečnostný model Blockchainu tiež využíva kryptografiu s verejným kľúčom. Identita vrátane totožnosti jednotlivých užívateľov a transakcie sú odvodené na základe certifikátov verejného kľúča. Existuje mnoho nových systémov (niektoré sú zatiaľ len predmetom výskumu), ktoré rozširujú pôvodný mechanizmus blockchainu o nové a komplexnejšie kryptografické protokoly. Ich cieľom je zlepšiť bezpečnosť a výkon pomocou nových techník (11).

Asymetrická kryptografia

Kryptografia s verejným kľúčom (nazývaná tiež asymetrická kryptografia) je kryptografický systém, ktorý používa pár kľúčov - verejný kľúč a súkromný kľúč. Blockchain využíva asymetrickú kryptografiu na autentifikáciu, autorizáciu a overovanie transakcií bez odhalenia totožnosti používateľov. Asymetrická kryptografia je realizovaná prostredníctvom dvoch rôznych kľúčov: verejného a súkromného. Každý užívateľ disponuje svojím vlastným súkromným kľúčom. Druhý – verejný kľúč je dostupný v sieti blockchain. Tieto kľúče sa využívajú na prácu s funkciami zasielania správ ako je šifrovanie a dešifrovanie. Verejný kľúč sa použije ako adresa odosielateľa, keď odosielateľ iniciuje vyslanie správy o transakcii. Správa zvyčajne obsahuje dve časti. Prvou časťou je správa a druhou časťou je zašifrovaný digitálny podpis správy – formou hashu, ktorý je podpísaný súkromným kľúčom. Adresát musí vytvoriť hashovú hodnotu správy, a potom dešifrovať správu použitím odosielateľovho verejného kľúča. Keď sa obe hashové hodnoty zhodujú, transakcia je schválená (28).

Digitálny podpis

Digitálne podpisy sú jedným z hlavných aspektov zaistenia bezpečnosti a integrity údajov, ktoré sa zaznamenávajú do blockchainu. Sú štandardnou súčasťou väčšiny blockchainových protokolov. Používajú sa predovšetkým na zabezpečenie transakcií, blokov, na prenos citlivých informácií, riadenie inteligentných zmlúv a podobne. Ide najmä o udalosti a situácie kedy je nevyhnutné odhaliť a zabrániť vonkajšiemu neoprávnenému zásahu. Digitálne podpisy využívajú asymetrickú kryptografiu, čo znamená, že informácie môžu byť zdieľané s každým prostredníctvom verejného kľúča. Digitálne podpisy poskytujú tri kľúčové výhody ukladania a prenosu informácií pomocou blockchainu. Hlavnou výhodou je, že zaručujú integritu. Odosielané šifrované dáta nemôžu byť pozmenené. Ak sa to stane, podpis by sa tiež zmenil, čím by sa stal neplatný. Digitálne podpísané údaje preto nielenže nemajú viditeľný obsah, ale dokážeme odhaliť, či boli pozmenené alebo poškodené. Digitálne podpisy zaisťujú nielen bezpečnosť údajov, ale aj identitu odosielateľa. Vlastníctvo digitálneho podpisu je vždy viazané na určitého používateľa, takže si môžeme byť istí, že komunikujeme s tým, s kým zamýšľame. Napokon skutočnosť, že súkromné kľúče sú prepojené jednotlivými používateľmi, dáva digitálnym podpisom vlastnosť nepopierania. To znamená, že ak je niečo digitálne podpísané používateľom, môžeme to považovať za právne záväzné a spojené s touto osobou (15).

Kryptografické hashovanie

Hashovanie je ďalšou základnou technológiou blockchainu a je priamo zodpovedné za vytvorenie nemeniteľnosti - jedna z najdôležitejších funkcií blockchainu. Hashovanie je pojem počítačovej vedy, ktorý znamená že zoberieme vstupný reťazec ľubovoľnej dĺžky a vytvoríme z neho výstup pevnej dĺžky. Nezáleží na tom, či je vstup do určitej hashovacej funkcie dlhý na 3 znaky alebo 100 znakov, výstup bude mať vždy rovnakú dĺžku. Kryptografické hashovacie funkcie sú hashovacie funkcie, ktoré majú tieto kľúčové vlastnosti:

- **Determinovanosť:** bez ohľadu na to, koľkokrát dáme funkcii konkrétny vstup, vždy bude mať rovnaký výstup
- **Návratnosť:** nie je možné určiť vstup z výstupu funkcie

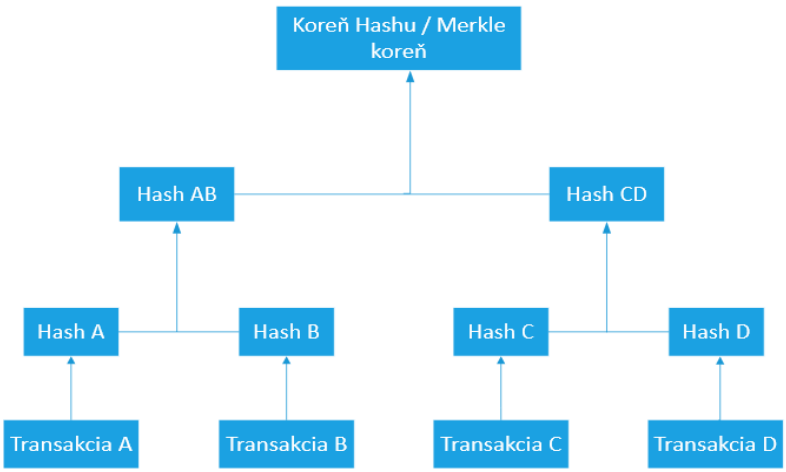
- **Odolnosť proti kolízii:** žiadne dva vstupy nemôžu mať rovnaký výstup (15).

Ďalšou dôležitou vlastnosťou kryptografických hashovacích funkcií je to, že zmena ľubovoľného množstva údajov na vstupe značne zmení výstup. Napríklad hash výstupy 111111 a 111112 by boli úplne jedinečné a nemali by k sebe žiaden vzťah (27).

Hlavným princípom hashovania blockchain technológie je, že každý nový blok údajov obsahuje hashový výstup všetkých údajov v predchádzajúcom bloku. Je možné si to predstaviť ako blockchain, ktorý práve pridal jeho 1000. blok. Dáta z bloku 999 existujú v bloku 1000 ako výstup funkcie hash. Do údajov bloku 999 sú však zahrnuté hodnoty hash údajov z bloku 998, ktoré obsahujú hodnoty hash údajov z bloku 997. Ak by sa zmenil len 1 bit údajov v akomkoľvek predošlom bloku, došlo by k zmene hashového výstupu týchto blokov, ale zároveň aj každého ďalšieho bloku za ním (27).

Hashové stromy - Merkle Trees

Merkle strom (alebo hashovací strom) je strom, ktorý využíva kryptografické hashovacie funkcie na ukladanie hashových výstupov namiesto nespracovaných údajov v každom uzle. Každý listový uzol pozostáva z kryptografického hashu svojich pôvodných dát a každý rodičovský (nadradený) uzol je hash kombinácie svojich hashov dcérskych (podradených) uzlov. Koreň Merkle stromu je jednoducho koreňový (hlavný) uzol stromu Merkle, čo znamená, že predstavuje hashový výstup kombinovaných hashov ľavého a pravého pod-stromu. Schéma stromu Merkle so 4 listovými uzlami je uvedené nižšie na obrázku č.7 (27).



Obrázok č. 7: Merkle strom
(Zdroj: Vlastné spracovanie podľa: 27)

Každý listový uzol predstavuje hash dát pre transakcie A, B, C a D. Hash A a hash B sa spoja a hashujú, čím vzniká hash AB, pričom hash CD sa vytvára rovnakým spôsobom. Nakoniec sa hash AB a hash CD spoja a hashujú tak, aby vytvorili koreň stromu Merkle. Použitím koreňa Merkle a aplikáciou kryptografických hashovacích funkcií, môžeme rýchlo zistiť, či boli transakcie v danom bloku neoprávnene pozmenené alebo či bola narušená niektorá transakcia. Ak sa pozmení nejaká transakcia v už potvrdenom bloku, platí že koreň Merkle by sa vo výsledku úplne líšil od toho „správneho“ koreňa Merkle a manipulácia by bola očividná. Merkle stromy tiež umožňujú používateľom overiť, či bola ich transakcia zaradená do bloku bez stiahnutia celého blockchainu. Procesy, ako napríklad zjednodušené overenie platby, môžu kontrolovať jednotlivé vetvy merkle stromu a overiť, či sa do tohto stromu hashovala nejaká transakcia. Táto úroveň účinnosti technológie blockchain by bola nemožná ak by v každom bloku nebol zahrnutý Merkle koreň (27).

1.9 Smart kontrakty

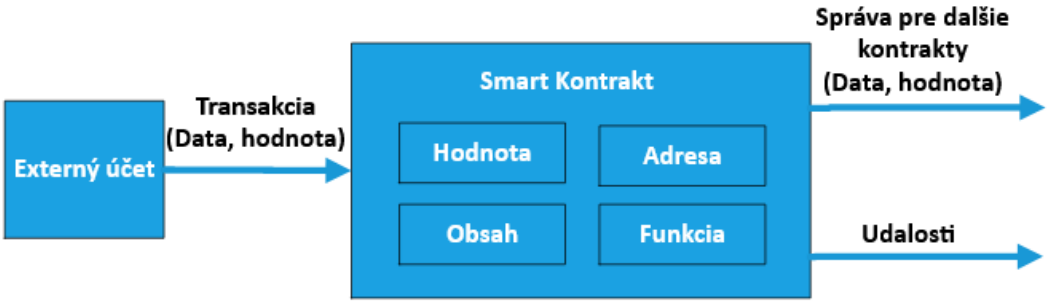
Vo všeobecnosti sú smart kontrakty (inteligentné zmluvy) definované ako počítačové protokoly, ktoré v digitálnej sfére spravujú, overujú a uvádzajú do platnosti zmluvy uzavreté medzi dvoma alebo viacerými stranami v blockchainovej sieti (2).

Smart kontrakt je počítačový program s mechanizmom, ktorý zabezpečuje svoje vlastné overovanie, je samostatne realizovateľný a odolný proti manipulácii v snahe o pozmenenie či falšovanie jej obsahu. Tento koncept prvýkrát navrhol Nick Szabo v roku 1994. Vstupom je konkrétna transakcia na základe ktorej sa realizujú preddefinované príkazy a výstupy. Integrácia blockchainu a smart kontraktov poskytuje väčšiu flexibilitu vo vývoji, dizajne a implementácii niektorých problémov z reálneho sveta. Realizácia prebieha efektívnejšie, rýchlejšie a s nižšími nákladmi, pričom nie je nutná účasť ďalších prostredníkov či tretích strán. Integrácia smart kontraktov a blockchainu sa stala dôležitou oblasťou záujmu a rozvoja, pretože umožňuje peer to peer transakcie a databáza môže byť udržiavaná verejne a bezpečným spôsobom v dôveryhodnom prostredí. Smart kontrakty sú nemenné a jednoducho sledovateľné. Všetky informácie o transakciách sú prítomné v tele smart kontraktu a sú realizované automaticky. Na implementáciu smart kontraktov sa používa programovací

jazyk Solidity v rôznych blockchainových platformách ako sú napríklad Ethereum, Eris DB, Zeppelin alebo Counterparty (5).

Vlastnosti smart kontraktu môžeme zhrnúť nasledovne:

- smart kontrakt je strojovo čitateľný kód, ktorý beží na blockchainovej platforme
- smart kontrakty sú súčasťou jedného aplikačného programu
- smart kontrakty sú programom riadené udalosti
- smart kontrakty sú nezávislé, akonáhle sú vytvorené, nie je potrebné ich monitorovanie
- smart kontrakty sú distribuované (5).
- smart kontrakt môže mať svoje vlastné kryptomeny alebo iné digitálne aktíva, s ktorými môže disponovať za predom definovaných podmienok (2).



Obrázok č. 8: Štruktúra smart kontratku
(Zdroj: Vlastné spracovanie podľa: 5)

1.10 Príklady využitia Blockchainu

Táto kapitola popisuje niektoré konkrétne príklady využitia technológie blockchain v reálnom prostredí.

Zásobovací reťazec

Systém dodávateľského reťazca pozostáva z rôznych úrovní transakcií. V systéme dodávateľského reťazca je zapojených viacero podsystémov. Zastrešujú jednotlivé odvetvia dodávateľského reťazca ako je napríklad oddelenie spracovania potravín, sektor dopravy či prepravný systém. Vo všetkých týchto prípadoch platí, že využitie blockchain technológie a zdieľanej účtovnej knihy, zachováva tento systém viac

transparentný, spoľahlivý a bez nutnosti zásahu tretej strany. Blockchain zabezpečuje v odvetví dodávateľského reťazca spoľahlivosť a dôvernosť, pričom všetky dáta sú dostupné v otvorenom distribuovanom systéme. Ak sa spolu s blockchainom používa aj inteligentná zmluva, potom sa systém stáva celkovo autonómnym a bezpečným. Využívanie inteligentných zmlúv v dodávateľských reťazcoch napomáha zjednodušiť pohyb tovaru a obnoviť dôveru v obchodovaní (5).

Systém zdravotnej starostlivosti

S rastúcou technologickou úrovňou zároveň rastie úroveň štandardu životnej úrovne. Novodobé zdravotné zariadenia a podporná technológia umožňujú sledovať zdravotný stav z pohodlia domova. Existuje veľa zariadení, ktoré sú vyvinuté tak, aby boli schopné čítať rôzne atribúty v tele človeka. Tieto dáta je možné zhromažďovať pomocou koncových zariadení, pričom rýchle spracovanie dát umožňuje rýchle získanie informácií. Blockchain technológia pomáha udržiavať súkromie pacientov a uchováva údaje vo formáte digitálnych kníh. Smart kontrakt môže byť v tomto systéme použitý, aby bol systém spoľahlivejší a automatizovaný. Pomocou smart kontraktu ľudia môžu spísať podmienky a stavy, ktoré by sa mali dodržať, pri práci so zhromaždenými údajmi (5).

Internet vecí – IoT

Internet vecí je jednou z perspektívnych oblastí výskumu. Ako uvádza správa od spoločnosti CISCO, počet zariadení IoT pripojených k rôznym aplikáciám už prekračuje počet celkovej populácie sveta. Blockchain implementovaný do technológii inteligentný domov, inteligentných miest, inteligentnej dopravy, inteligentného monitorovania a aplikácie v oblasti životného prostredia je už záležitosťou bežného výskumu a rozvoja. Ak by sa koncepcia smart kontraktu úspešne integrovala s blockchainom, potom sa IoT stane viac autonómnejším (5).

Poisťovníctvo

V tradičnom systéme poistenia trvá veľmi dlho spracovanie jednotlivých požiadaviek, pričom existuje veľa nejednoznačností medzi rôznymi zainteresovanými stranami počas spracovania. Inteligentný zmluvný systém môže zjednodušiť proces a vďaka využívaniu technológie blockchain môže byť všetko transparentné, bezpečné a realizované bez

zásahu tretej strany. Vždy, keď sú splnené podmienky inteligentnej zmluvy, spustia sa príslušné udalosti (5).

Finančný systém

Blockchain technológia vynájdená spolu s kryptomenou Bitcoin bola pôvodne používaná len pre finančné systémy. Tradičné bankové systémy zahŕňajú účasť nejakej tretej strany, ktorá prevedie peniaze z jedného účtu na iný účet. Pričom ako už bolo zmienené, v blockchainovom systéme ide o takzvanú transakciu peer to peer, ktorá nevyžaduje žiadne centrálne ukladanie. Použitím inteligentných zmlúv a blockchain technológie môže finančný sektor výrazne prosperovať, ale stále je potrebné vykonať veľa výskumov na implementáciu inteligentných zmlúv (5).

Nehnuteľnosti

Tradičný systém správy nehnuteľnosti zahŕňa veľa možných rizík a taktiež je časovo náročný. Musí prejsť rôznymi úrovňami právneho konania, ku ktorému sú potrebné mnohé podpisy a veľa ručného overovania dokumentov. Implementácia technológie blockchain a inteligentných zmluvu môže vyriešiť problém spojený so sektorom nehnuteľností. Centralizovaný systém môže umožniť nákup ako aj predaj nehnuteľností bez účasti tretej strany. Dokument je tiež overený a uznaný digitálne pričom všetky dokumenty sú uložené v digitálnej účtovnej databáze ku ktorej má prístup každý účastník (5).

1.11 Blockchainové platformy

Okrem jednej z najznámejších platforiem Bitcoin, sa v posledných rokoch objavilo niekoľko alternatívnych platforiem. Napriek tomu, že tieto platformy prebrali od Bitcoinu základný mechanizmus, odlišujú sa niekoľkými kľúčovými vlastnosťami. Pravidlá prístupu tzv. *access policies* u každej platformy definujú, kto sa môže do siete pripojiť a využívať ju. Verejné blockchainy umožňujú pripojenie komukoľvek k informáciám uloženým v reťazci blokov, ku ktorým je možné pristupovať prostredníctvom internetu. Súkromný blockchain povoľuje prístup iba vybraným uzlom. Politika overenia pravosti alebo tzv. "validation policy" definuje, kto sa medzi uzlami môže podieľať na vytváraní konsenzu a zavádzať inteligentné zmluvy.

Blockchainy bez možnosti nastavenia takýchto povolení umožňujú každému uzlu vykonávať oboje. Blockchainy s možnosťou nastavenia povolení obmedzujú tieto možnosti iba na špeciálne uzly, napríklad kvalifikované prostredníctvom priamej pozvánky (10).

Medzi najznámejšie blockchainové platformy patria nasledovné:

- Bitcoin - (bitcoin.org), prvá platforma blockchainu
- Ethereum - (ethereum.org), platforma, ktorá prvýkrát zaviedla inteligentné zmluvy
- Hyperledger Fabric - súkromná povolená platforma, ktorú organizuje Nadácia Linux a podporuje viac ako 200 vedúcich pracovníkov v odvetví
- Corda - súkromná, schválená platforma konzorcia viac ako 200 finančných inštitúcií a technologických firiem (10).

1.11.1 Hyperledger Fabric

Hyperledger Fabric je open source DLT (Distibuted Ledger technology) platforma, navrhnutá na použitie v podnikových kontextoch, ktorá poskytuje niektoré kľúčové rozlišovacie schopnosti oproti iným populárnym platformám distribuovanej knihy alebo blockchainu. Hyperledger bol založený v rámci Linux Foundation, ktorá sama o sebe má dlhú a veľmi úspešnú históriu realizácie open source projektov v rámci otvoreného riadenia, ktoré rozvíja silné spoločenstvá a prosperujúce ekosystémy. Má vývojovú komunitu, ktorá sa od svojich prvých záväzkov rozrástla na viac ako 35 organizácií a takmer 200 vývojárov. Hyperledger Fabric má vysoko modulárnu a konfigurovateľnú architektúru, ktorá umožňuje inováciu, univerzálnosť a optimalizáciu pre široké spektrum prípadov priemyselného použitia vrátane bankovníctva, financií, poisťovníctva, zdravotnej starostlivosti, ľudských zdrojov, dodávateľského reťazca a dokonca aj poskytovania digitálnej hudby. Je to prvá distribuovaná platforma na podporu inteligentných kontraktov napísaných vo viacúčelových programovacích jazykoch ako Java, Go a Node. Z toho vyplýva, že väčšina podnikov už má potrebné zručnosti na vypracovanie inteligentných zmlúv (21).

1.11.2 Blockchain as a Service

Blockchain as a service je komplexné cloudové riešenie, ktoré umožňuje vývojárom, podnikateľom a podnikom vyvíjať, testovať a implementovať aplikácie blockchain a inteligentné zmluvy, ktoré sú hostované na platforme BaaS. Platformy BaaS okrem toho poskytujú všetku potrebnú infraštruktúru a prevádzkovú podporu, aby sa zabezpečilo hladké fungovanie aplikácií. Užívatelia si tak môžu pomerne rýchlo a jednoducho vytvoriť sieť podľa vlastných potrieb (35).

2 ANALÝZA SÚČASNÉHO STAVU

Nasledujúca kapitola popisuje spoločnosť IBM, pre ktorú som sa rozhodla spracovať návrh využitia technológie Blockchain, na vybranom firemnom procese. Obsahuje základné informácie o spoločnosti, jej organizačnú štruktúru a požiadavky spoločnosti na funkcionalitu a prevádzkovanie novej technológie. Opisuje súčasný stav objednávkového procesu a jeho jednotlivé fázy. Ďalej približuje štruktúru objednávkového tímu, ktorý v súčasnosti riadi proces objednávania. Identifikuje všetky externé organizácie, ktoré sú do tohto procesu určitým spôsobom zahrnuté. Ako proces funguje som mala možnosť diskutovať priamo s lídrom objednávkového tímu, ktorý mi dodal všetky potrebné materiály pre komplexné pochopenie celého systému.

2.1 Informácie o spoločnosti

Spoločnosť IBM (International Business Machines Corporation) bola založená v roku 1911 a v súčasnej dobe je jednou z popredných spoločností v oblasti informačných technológií vo svete. Počas svojej existencie priniesla niekoľko jedinečných inovácií, ktoré doslova ovplyvnili celý svet a sú využívané v každodennom živote. Príkladom takýchto inovácií sú ATM bankomaty, technológia magnetického pásiku na platobných kartách, čiarové kódy, diskety, pevné disky a mnoho ďalších vynálezov nielen v sektore informačných technológií. Spoločnosť má v súčasnosti viac ako 375 tisíc zamestnancov a je jednou z najväčších spoločností v Spojených štátoch amerických (36).

Pobočka IBM v Brne

Pobočka IBM Service Delivery Centrum Brno, ktorá bola založená v roku 2001 je nákladové stredisko, ktoré je definované ako organizačná jednotka, ktorá nevytvára priamy zisk, ale poskytuje hlavne interné služby bez kontaktu s externým trhom. Momentálne má táto pobočka približne 4500 zamestnancov v zastúpení národností z celého sveta. Organizačná štruktúra spoločnosti je maticová. Zamestnanci sú radení do jednotlivých oddelení podľa pracovného zamerania. Zodpovedajú sa svojmu funkčnému manažérovi, ktorý zodpovedá za kvalitu vykonanej práce, a zároveň prvému líniovému manažérovi (36).

2.2 IBM a Blockchain

IBM je jednou z popredných spoločností, ktoré investujú do technológie Blockchain. Vedie niekoľko výskumov a investuje do vývoja tejto technológie. Výsledkom toho je, že má vo svojom portfóliu už niekoľko Blockchainových riešení v rozličných odvetviach. Nižšie môžeme vidieť zoznam všetkých odvetví, pre ktoré spoločnosť poskytuje blockchainové produkty:

- Potravinársky priemysel
- Globálne obchodovanie
- Finančné obchodovanie
- Cezhraničné platby
- Ochrana identity
- Automobilový priemysel
- Bankovníctvo a finančné servisy
- Zdravotníctvo
- Vládny sektor
- Poisťovníctvo
- Média a zábava
- Maloobchodný a spotrebný tovar
- Cestovanie a preprava (35).

IBM Blockchain platforma

Spoločnosť taktiež prevádzkuje vlastnú blockchainovú platformu. IBM Blockchain platforma poskytuje kompletný balík blockchain *as a service* (BaaS), ktorý ponúka služby v prostredí podľa vlastného výberu. Zákazník si môže zvoliť prevádzkovanie vrátane IBM cloudu, alebo cloudu od nejakých iných spoločností. Tento produkt umožňuje členom rozvíjať, riadiť, prevádzkovať a rozširovať vlastnú blockchainovú sieť. Produkt IBM Blockchain Platforma, využívajúci technológiu Hyperledger Fabric,

umožňuje prevádzkovanie distribuovanej obchodnej siete založenej na zásadách dôvery a súkromia (34).

2.3 Popis procesu na implementáciu

Spoločnosť by chcela vypracovať návrh na inováciu interného objednávkového procesu, ktorý by napomohol zlepšeniu celkovej efektivity spracovania objednávok. Proces má momentálne niekoľko nedostatkov. Inováciou za použitia vhodnej technológie by bolo možné slabé stránky eliminovať.

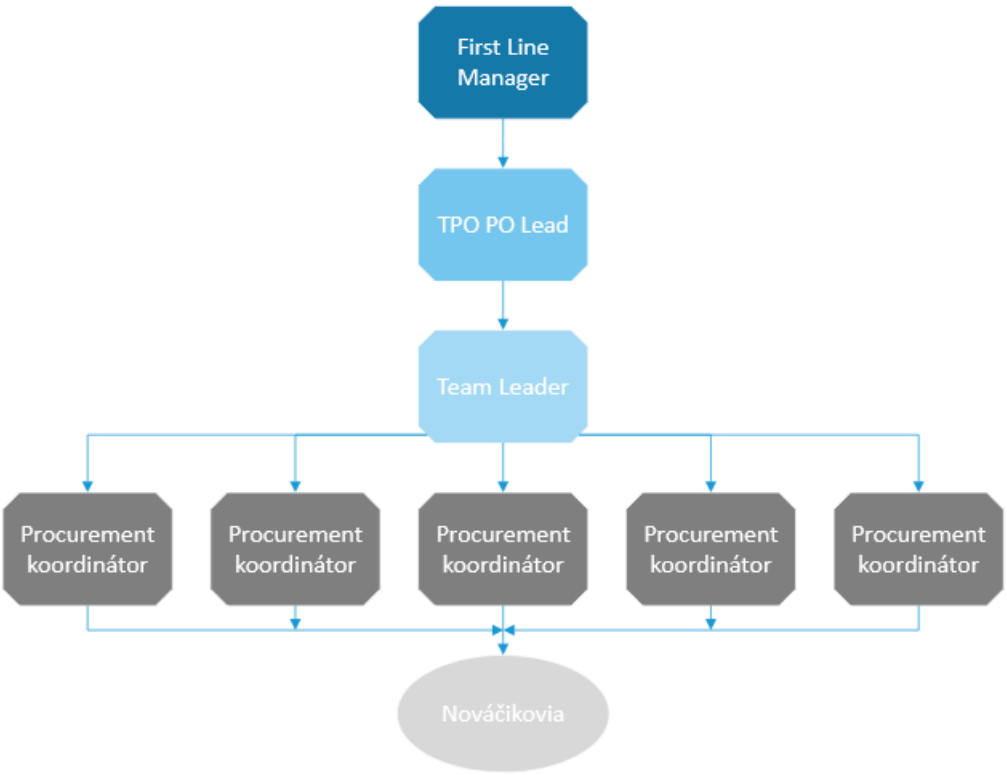
Dôvodom, prečo by sa mal proces inovovať práve využitím technológie blockchain je fakt, že do celého procesu zasahuje aj niekoľko externých organizácií, s ktorými spoločnosť spolupracuje a zdieľa dáta. Všetky tieto externé organizácie potrebujú prístup ku objednávkovým dátam a zároveň ich potrebujú upravovať. V súčasnej dobe, má spoločnosť s každou z týchto spoločností nastavený individuálny spôsob komunikácie a zdieľania dát.

V prípade, že by sa v tomto procese implementovalo blockchainové riešenie a zapojili do neho všetky organizácie, zjednotil by sa tak nielen spôsob komunikácie, ale dáta a transakcie by boli transparentné a prístupné pre všetkých na jednom mieste.

Objednávkový tím a organizačná štruktúra

Objednávkový proces má na starosti samostatný špecializovaný tím, ktorý je kategorizovaný ako poskytovateľ služieb v oblasti projektového manažmentu. Tím spadá pod oddelenie projektového riadenia. Jeho interný názov je TPS PO team. Má svoj servisný katalóg, ktorý obsahuje zoznam všetkých poskytovaných služieb. Vo všeobecnosti však môžeme povedať, že ponúka podporu v oblasti služieb týkajúcich sa projektového riadenia.

Počet pracovníkov procurement tímu závisí na objeme aktuálneho počtu objednávok. V priemere však môžeme povedať, že má do 10 členov. Na čele tímu je líder, ktorý zabezpečuje chod tímu po administratívnej stránke, rozhoduje o spolupráci s novými aj súčasnými klientami a určuje vnútornú stratégiu tímu. Pozná detailne celý objednávkový proces. Na obrázku č. 9 nižšie, môžeme vidieť organizačnú štruktúru tímu.



Obrázok č. 9: Organizačná štruktúra objednávkového tímu
(Zdroj: Vlastné spracovanie)

2.3.1 Interné tímy zapojené do objednávkového procesu

Okrem procurement tímu, ktorý ma na starosti spracovanie objednávok, je do procesu zapojených ešte mnoho ďalších pracovníkov, ktorí objednávku musia schváliť alebo zrevidovať. Nižšie môžeme vidieť zoznam všetkých tímov, ktoré sú v procese zahrnuté:

- **Projektový tím**

Spadajú sem všetci členovia, ktorí sa zúčastňujú na danom projekte. Sú to projektoví manažéri, výkonní predstavitelia daného projektu (delivery project executive a project executive), koordinátori projektového riadenia, finanční analytici a ďalší.

- **Tím architektov**

Ide o tím technikov, ktorí kontrolujú požadovaný produkt po technickej stránke a skúmajú vhodnosť navrhnutého riešenia a jeho prípadne obmeny.

- **Sklad**

Tento tím kontroluje, či je požadovaný produkt dostupný na sklade so zánovným hardvérom.

- **Tím softvérových analytikov**

Softvéroví analytici kontrolujú dostupnosť a vhodnosť požadovaných softvérov a komunikujú detaily s poskytovateľom.

- **Predkupný tím**

Tento tím je do objednávkového procesu zahrnutý od úplného začiatku až po jeho koniec. Na začiatku nahráva objednávku do systému a kontroluje cenovú ponuku. Neskôr sa k nemu objednávka ešte párkrát vráti. Sú zodpovední za vytváranie nákupnej karty a jej nahrávanie do systému.

- **Finančný tím**

Tento tím kontroluje dostupnosť finančných prostriedkov a uvoľňuje financie z rozpočtu.

- **Tím nákupcov**

Nákupcovia na základe nákupnej karty vytvárajú výsledné objednávkové číslo, ktoré sa zasiela dodávateľovi.

2.3.2 Externé organizácie zapojené do objednávkového procesu

Jedným z hlavným princípov technológie Blockchain je, že ide o riešenie, ktoré má zmysel v prípade, že sú určité dáta zdieľané a upravované medzi viacerými organizáciami. Preto je nutné identifikovať všetky organizácie, ktoré nejakým spôsobom ovplyvňujú objednávkový proces. Okrem vyššie vymenovaných interných tímov, je však dôležité identifikovať aj všetky externé organizácie, ktoré sú do procesu zapojené. Spadajú sem nasledovné organizácie:

- **Klientska organizácia**

V prvom rade je to organizácia zákazníka, ktorý si u spoločnosti IBM objednal nejakú službu alebo produkt. Zákazník komunikuje priamo s projektovým manažérom

spoločnosti, ktorý sa stará o bezproblémové doručenie dohodnutého servisu. Prvotná požiadavka na nový hardvér alebo servis teda príde priamo od klienta. V prípade, že by sa počas objednávkového procesu čokoľvek zmenilo, projektový manažér musí komunikovať všetky zmeny s klientom, ktorý ich musí odsúhlasiť alebo navrhnúť prípadné zmeny. Častou situáciu sú drobné zmeny v cenách či konfigurácii. Preto je nutné, aby mal klient prístup k objednávke počas celého procesu a mohol tak kontrolovať a odsúhlasovať prípadné zmeny.

- **Dcérske spoločnosti, ktoré dodávajú časť produktu alebo služby**

Spoločnosť IBM má dcérske spoločnosti, ktoré majú na starosti zabezpečovanie a poskytovanie určitého typu alebo časti produktov. Príkladom môžu byť platformy či rôzne licencie. V prípade, že je niektorý z týchto produktov súčasťou balíka, ktorý si klient objednal, musí byť táto dcérska spoločnosť od začiatku zahrnutá do objednávkového procesu. Spoločnosť potrebuje mať prístup k detailom požadovaného riešenia, aby vedela dodať svoju časť. Neskôr počas celého vývoja objednávkového procesu potrebuje byť informovaná, v akom štádiu sa objednávka nachádza, aby si vedela odvodiť predbežný dátum doručenia. Keď je objednávka na konci a nákupca vytvorí objednávkové číslo, je odoslané dcérskej spoločnosti na spracovanie a dodanie výsledného produktu. Z toho dôvodu, je dôležité aby bola táto organizácia zahrnutá do procesu počas celej doby trvania.

- **Externý dodávatelia**

Keďže spoločnosť IBM ponúka nielen vlastné riešenia, ale aj mnohé produkty a služby formou outsourcingu, komunikuje a zdieľa dáta s mnohými externými dodávateľmi, ktorí poskytujú požadované produkty. Títo dodávatelia tak potrebujú byť informovaní a zahrnutí do procesu. Čo je však ešte dôležitejšie, spoločnosť s nimi realizuje určité finančné transakcie, ktoré vyžadujú vysoký stupeň bezpečnosti a prístup k potrebnej dokumentácií.

- **Doručovacie spoločnosti**

Ďalšia externá organizácia, ktorá sa zúčastňuje objednávkového procesu, je doručovacia spoločnosť. Ak je obsahom objednávky nejaký hardvér, musí byť fyzicky doručený do požadovaného dátového centra alebo klientskej lokality. Doručované produkty

sa vyrábajú vo fabrikách po celkom svete a tak isto sú doručované na adresy po celom svete, keďže IBM je nadnárodná spoločnosť. Je dôležité aby boli objednávky sledovateľné počas celej doby doručenia. Nielen klient, ale aj všetci ostatní účastníci procesu musia vedieť aký je približný odhadovaný čas doručenia. Častokrát dochádza ku oneskoreniam, alebo dodaniam na nesprávnu adresu, a následne je veľmi náročné informovať o tom všetky príslušne strany, či komunikovať prípadne oneskorenia doručenia projektu. Tie majú za následok nedodržanie podmienok zmluvy a s tým spojené pokuty.

2.4 Súčasný objednávkový proces

Súčasný objednávkový proces je veľmi komplexný a časovo náročný. Na úplnom začiatku procesu je požiadavka na zaobstaranie nového hardvéru, softvéru či služby, podľa daných potrieb jednotlivých projektov. Požiadavka prichádza od klientskej spoločnosti. Tá je pridelená projektovému manažérovi, ktorý je prostredníkom medzi klientskou organizáciou a interným objednávkovým tímom. Požiadavka na novú objednávku je zadaná objednávkovému tímu. Ten ju prevezme, a skontroluje či projektový manažér dodal všetky potrebné vstupy. V prípade že áno, vybraný člen procurement teamu iniciuje začatie objednávky.

V prvom kroku je nutné rozhodnúť, o aký typ objednávky ide, a na základe toho pokračovať podľa príslušných predpisov pravidiel spracovania prislúchajúcich tomuto typu objednávky. Proces sa delí na dve vetvy. Musíme rozlíšiť, či ide o hardvérovú alebo softvérovú objednávku.

Proces objednávania HW

V prípade, že je objednávaný produkt hardvér, je celková doba objednávky dlhšia o približne 3 až 4 týždne v porovnaní so softvérovou objednávkou. Objednávka musí prejsť viacerými štádiami schválenia. Keďže sa jedná o hardvér, je potrebné získať aj technické schválenie od architektov, ktorí overujú, či je vybrané hardvérové riešenie naozaj to najvhodnejšie pre potreby daného projektu. Taktiež overujú dostupnosť obdobných substitútov, či zánovného hardvéru, ktorý sa nachádza momentálne na sklade a je pripravený na použitie.

V ďalšom kroku sa overuje a určuje cena objednávky. Tím, ktorý má na starosti toto schválenie, musí overiť aká je momentálna cenová ponuka pre požadovaný produkt. Je nutné rozlišovať, či ide o produkt od externého dodávateľa alebo o interný produkt, ktorého výrobu si spoločnosť zabezpečuje sama. Na základe aktuálnej ceny zhotovia výsledný konfiguračný súbor, ktorý bude slúžiť počas celého procesu ako objednávacia kvóta. Obsahuje detailné položky produktu spolu s príslušnými cenami a dátum platnosti kvóty. Tie sú platné v priemere niekoľko mesiacov.

V prípade, že objednávame produkt od externého dodávateľa, overujeme platnosť predloženej cenovej ponuky. Taktiež musí obsahovať dátum platnosti a detailný popis jednotlivých objednávaných položiek. Môže nastať ešte tretia situácia, a to v prípade, že je požadovaný hardvér dostupný na sklade spoločnosti. Túto skutočnosť overuje ďalší tím. Ak je produkt k dispozícii, tím predloží cenovú ponuku a konfiguráciu dostupného hardvéru. V ďalšom štádiu tohto procesu je nutné overiť typ kontraktu. Niektoré kontrakty majú totiž väčšiu prioritu než iné. Kontrakty s väčšou prioritou majú poopravený objednávkový proces, to znamená, že by mali prejsť celým procesom rýchlejšie.

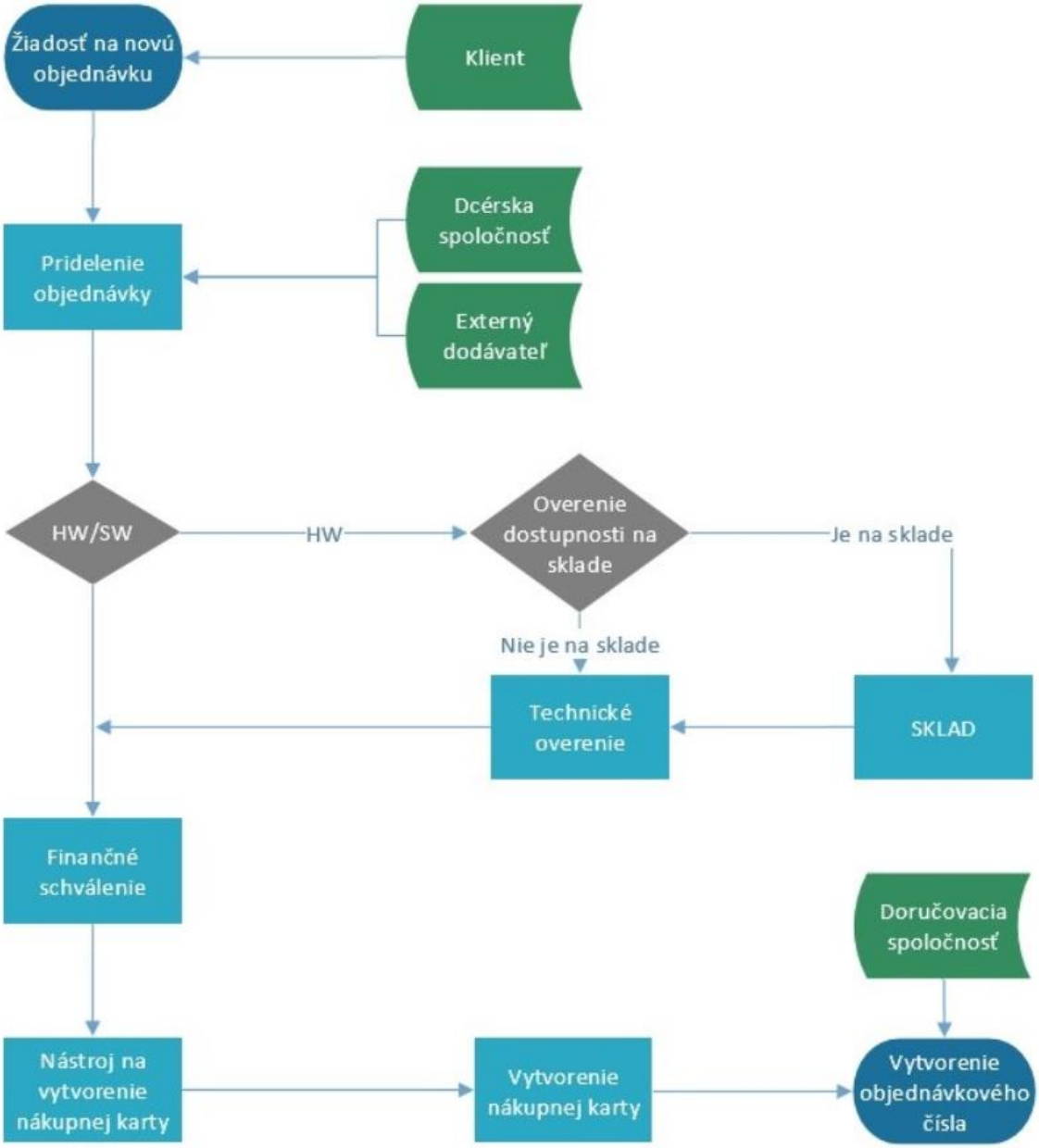
Proces objednávania SW

V prípade, že objednávame softvérový produkt, nie je nutné technické schválenie ani kontrola dostupnosti na sklade. Objednávka je priamo presmerovaná do webovej aplikácie, ktorá má na starosti finančné schválenie. Po dodaní všetkých potrebných dokumentov a splnení všetkých požiadaviek, je žiadosť zaradená do schvaľovacieho procesu, ktorý môže trvať niekoľko dní až týždňov. Ak je finančné overenie úspešné, objednávka je presmerovaná do ďalšej webovej aplikácie, kde sa zadáva žiadosť na vytvorenie nákupnej karty, na základe ktorej sa neskôr vytvára objednávkové číslo. Rovnako ako v prípade hardvérových nástrojov na technickú kontrolu a overenie dostupnosti na sklade, aj v tomto štádiu je nutné predložiť všetku potrebnú dokumentáciu. Vytvorí sa nová žiadosť, do ktorej sa vyplnia všetky informácie a detaily objednávaného produktu, prípadne požiadavky na dodatočnú správu a údržbu servisu, a všetky finančné údaje. Overí sa platnosť predloženej cenovej ponuky a jej obsah sa nahrá do systému. Keď je žiadosť vytvorená, je zaslaná na kontrolu a schválenie pôvodnému zadávateľovi. Následne musí prejsť celým schvaľovacím cyklom, ktorý je

tvorený softvérovými administrátormi, objednávkovým tímom, ktorý vytvára nákupné karty, ďalej finančným tímom a tímom, ktorý sa stará a vytvorenie výsledného objednávkového čísla na konci celého procesu. Toto číslo, je na konci úspešného objednávkového procesu zaslané externému alebo internému dodávateľovi, ktorý podľa neho vytvorí a dodá požadovaný produkt.

Diagram objednávkového procesu

V nasledujúcej schéme môžeme vidieť procesný diagram súčasného objednávkového cyklu. Ako možno vidieť, objednávkový cyklus začína žiadosťou od projektového manažéra (ktorá prišla pôvodne od klienta). Postupne žiadosť prechádza všetkými úrovňami schválenia, pričom celý proces sa delí na dva cykly v závislosti od druhu objednávky. Bloky, ktoré sú zvýraznené zelenou farbou, predstavujú externé organizácie a moment, kedy vchádzajú do procesu.



Obrázok č. 10: Diagram objednávkového procesu
(Zdroj: Vlastné spracovanie)

Technické schválenie

Technické overovanie hardvérových objednávok je realizované v samostatnej databázovej aplikácií, v ktorej je nutné vytvoriť pre každú objednávku individuálnu žiadosť. Zadávanie žiadostí do systému a ich spracovanie je v tomto prípade vykonávaná členmi objednávkového tímu, ktorí v prípade potreby spolupracujú s projektovými manažérmi. Technická kontrola objednávok je vykonávaná tímom architektov. Tí rozhodujú o vhodnosti daného riešenia na základe potrieb projektu

a zmluvných podmienok. V prípade, že s navrhnutým riešením nesúhlasia, predložia nový návrh. Ak je návrh schválený, je nutné vytvoriť novú konfiguráciu a taktiež novú cenovú ponuku, na základe ktorej bude pokračovať objednávkový proces. Bez tejto technickej revízie nie je možné pokračovať v objednávkovom procese. Po úspešnom absolvovaní technickej revízie, schváli príslušný architekt žiadosť v databázovej aplikácií a vytvorí o tom dokumentáciu, ktorá slúži počas celého procesu ako povinná príloha.

Finančné schválenie

Ďalšou veľmi dôležitou etapou objednávkového procesu je takzvaný CapEx – čo je skratka pre finančné schválenie. Táto revízia je vykonávaná obdobne ako technické schválenie. Je realizovaná v samostatnej databázovej aplikácií, kde členovia procurement tímu vytvárajú nové žiadosti pre jednotlivé objednávky. Pre každú objednávku musí byť vytvorená samostatná žiadosť. Dĺžka cyklu udelenia finančného schválenia je závislá na momentálnej situácii rozpočtu. Dôležitým vstupom pre vytvorenie tejto žiadosti je povinná dokumentácia, ktorá už bola vyššie spomínaná pri technickom schválení. Taktiež je nutné priložiť dokumentáciu o úspešnom absolvovaní technickej revízie. Proces finančného schválenia má na starosti samostatný tím, ktorý na pravidelnej báze skúma jednotlivé žiadosti. Výsledné schválenie žiadosti môže trvať až niekoľko týždňov.

Vytvorenie objednávkového čísla

Keď je úspešne vytvorená nákupná karta, je odoslaná na schválenie a kontrolu ďalšej skupine ľudí. Mnohí z nich už túto objednávku schválili predtým v predošlých aplikáciách. Keď karta dokončí celý schvaľovací cyklus, je uložená do systému. Vytvorí sa dokumentácia o jej vytvorení a tá je následne odoslaná poslednému tímu. Ide o takzvaných kupcov, ktorí podľa karty vytvoria interné objednávkové číslo. To je následne odoslané externému, respektíve internému dodávateľovi.

2.5 Nedostatky súčasného procesu

Po oboznámení sa s celým objednávkovým procesom a pochopení jeho komplexného fungovania, som identifikovala niekoľko nedostatkov, ktoré by bolo vhodné odstrániť,

aby tak spoločnosť mohla poskytovať svoje služby ešte efektívnejšie a rýchlejšie. Sú to slabé miesta, ktoré by v prípade úspešnej implementácie dokázal blockchain vyriešiť:

- V procese je zahrnutých niekoľko organizácií, pričom s každou z nich spoločnosť IBM zdieľa dáta a komunikuje iným spôsobom, nezávisle na ostatných organizáciách.
- Dáta sú ukladané do niekoľkých databáz a systémov, tie isté osoby schvaľujú proces niekoľkokrát, čo vedie k zdvojenej práci a neefektívnemu využívaniu zdrojov.
- Proces je časovo náročný, priemerný čas na dokončenie objednávky je 5 až 8 týždňov.
- Vznikajú oneskorenia, ktoré by mohli mať za následok dodatočné poplatky.
- Proces nie je dostatočne transparentný, objednávky sa občas zaseknú na určitom bode, pričom účastníci procesu nevidia aktuálneho vlastníka a dôvod prečo objednávka nenapreduje.
- Neúplný alebo nevhodne objednaný HW z dôvodu zlyhania ľudského faktoru pri manuálnom zadávaní údajov z kvóty.
- Veľa prostredníkov, ktorí musia proces overovať (niekedy viacnásobne).
- Objednávky môžu byť omylom zaslané na chybnú adresu / zadávateľ nemá dostatočný prehľad o tom kde sa aktuálne objednávka nachádza.
- Náročný audit.
- Náročná prehľadnosť historických transakcií.

2.6 Požiadavky spoločnosti na funkcionalitu novej technológie

V prípade, že by sa spoločnosť rozhodla zainvestovať do blockchainu a schválila by jeho implementáciu pre súčasný objednávkový proces, vznikol by interný projekt, ktorý bude vyžadovať dôkladnú analýzu súčasného stavu a prepracovaný návrh implementácie. Tak ako pre každý projekt, je nutné zadefinovať požiadavky na funkcionalitu a realistické podmienky úspechu, ktoré budú jasne merateľné.

Jedným z hlavných cieľov by bolo urýchliť celkový objednávkový proces, a zabezpečiť aby boli objednávky spracované rýchlejšie. Súčasný objednávkový proces trvá v priemere približne 40 dní. Aby bol projekt úspešný, malo by dôjsť k urýchleniu celkového procesu aspoň o 10 dní.

Ďalej požaduje zníženie finančných nákladov spojených s nasledovnými faktormi:

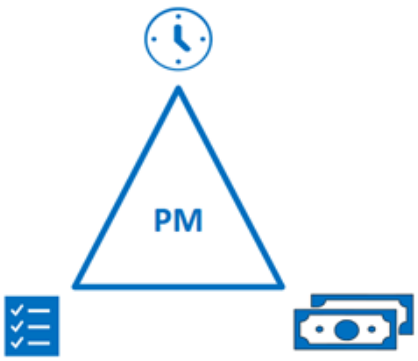
- **Kompresia procesu** - zníženie počtu ľudí, ktorí musia súčasný proces obsluhovať a udržiavať. Spoločnosť požaduje aby sa počet ľudských zdrojov, ktoré sa v procese účastina znížil aspoň o jednu tretinu.
- **Infraštruktúra** - zníženie nákladov na infraštruktúru. Spoločnosť požaduje, aby sa náklady na prevádzkovanie novej infraštruktúry znížili aspoň o 10%.
- **Oneskorenia** - zníženie počtu objednávok, ktoré neboli doručené včas. Spoločnosť požaduje zníženie počtu oneskorených objednávok aspoň na polovicu.
- **Chybovosť** - zníženie chybovostí v objednávkach. Spoločnosť požaduje zníženie chybových objednávok aspoň o 5%.

Spoločnosť požaduje zvýšenie spokojnosti zákazníkov. Úspech tejto požiadavky bude merateľný prostredníctvom dotazníku spokojnosti. Projekt bude úspešný, v prípade že budú výsledky dotazníku vykazovať zvýšenie kladných bodov aspoň o 10 %. V prípade že budú klienti spokojnejší, spoločnosť by mala zaznamenať nárast aj v počte nových prijatých objednávok a to aspoň o 5 %. V neposlednom rade by spoločnosť uvítala zvýšenie dôvernosti a bezpečnosti finančných transakcií, ktoré sú pri objednávaní realizované. Všetky tieto požiadavky a ich vyžadované hodnoty sú zhrnuté nižšie v tabuľke č.2.

Tabuľka č. 2: Požiadavky spoločnosti
(Zdroj: Vlastné spracovanie)

Definícia KPI	Požadovaná výsledná hodnota KPI			
	Jednotky KPI	Požadovaná zmena	Zmena/jednotka	Vplyv na celkový výsledok projektu
Dĺžka procesu	dni	zníženie	25%	Veľký
Ľudské zdroje	počet zamestnancov	zníženie	33%	Malý
Infraštruktúra	náklady v EUR	zníženie	10%	Stredný
Oneskorenia	počet objednávok	zníženie	50%	Veľký
Chybovosť	počet objednávok	zníženie	5%	Malý
Spokojnosť zákazníka	dotazník spokojnosti	zvýšenie	10%	Stredný

Na obrázku nižšie vidíme tri kľúčové faktory, ktoré podľa IBM metodológie pre riadenie projektov WWPMM ovplyvňujú úspešné dokončenie projektu. Čas, rozsah a náklady sú tri hlavné faktory, na ktorých je závislý celkový úspech projektu. Spoločnosť sa prostredníctvom vyššie zadefinovaných hodnôt KPI snaží nielen o to aby výsledná implementácia pozitívne ovplyvňovala samostatný objednávkový proces, ale aj takzvanú trojitú podmienku. Implementácia novej technológie by mala pozitívny vplyv na rozsah procesu, znížila by celkové náklady a urýchlila celý proces.



Obrázok č. 11: Trojitá podmienka
(Zdroj: Vlastné spracovanie)

2.7 Zhrnutie poznatkov analýzy

V tejto kapitole som bližšie popísala spoločnosť a priblížila som súčasný stav objednávkového procesu. Po osobnej konzultácií a pochopení komplexného systému a funkčnosti, som identifikovala niekoľko nedostatkov, ktoré by som odporučila z objednávkového procesu odstrániť, v záujme zlepšenia funkčnosti a aj zvýšenia spokojnosti zákazníkov.

Z výsledkov analýzy je zrejmé, že súčasný objednávkový proces je nielen časovo ale aj finančne náročný. Je náročný na zdroje a vyžaduje veľa prostredníkov. Inováciou vo forme vhodnej technológie, by sme mohli docieliť jeho efektívnejšiu realizáciu. Dôležitý činiteľ pri výbere vhodnej technológie zohráva fakt, že nejde o čisto interný proces, ale komplexný objednávkový systém, do ktorého sú zapojené aj ďalšie externé organizácie. Keďže ide o individuálne spoločnosti, voči ktorým spoločnosť nemá prirodzenú dôveru, je nutné zvoliť riešenie, ktoré tento problém vyrieši. Spoločnosť veľa investuje do výskumov blockchain technológie a tak má dostatok skúsených developerov a projektových manažérov, ktorí by sa mohli podujať na realizáciu tohto projektu. Spoločnosť zadefinovala konkrétne ciele a kritéria, ktoré musia byť splnené v prípade implementácie. Bol vytvorený zoznam KPI a ich požadované hodnoty, ktoré by mali byť dodržané pre úspešné dokončenie projektu

3 NÁVRH VLASTNÉHO RIEŠENIA

Táto kapitola je venovaná vytvoreniu návrhu využitia blockchain technológie na zvolenom firemnom procese. V prvej časti porovnávam vybrané blockchainové platformy a BaaS produkty. Ďalej odporúčam najvhodnejšie riešenie pre potreby vybraného objednávkového procesu a následne v ňom implementujem svoj návrh. Na základe vytvoreného návrhu som taktiež vytvorila zoznam prínosov, ktoré by táto implementácia mala na objednávkový proces pre všetky organizácie, ktoré sa procesu zúčastňujú.

V ďalšej časti som vytvorila návrh ako postupovať pri overení, či je zvolený firemný proces vhodný na implementáciu technológie blockchain a zároveň ako správne postupovať pri výbere vhodnej blockchainovej platformy. V neposlednom rade som zhodnotila návrh z ekonomického hľadiska.

3.1 Porovnanie platforiem

Táto kapitola je venovaná porovnaniu vybraných platforiem. Je rozdelená na dve časti. V prvej časti porovnávam 4 vybrané blockchainové platformy.

V druhej časti porovnávam produkty Blockchain as a servis. Ďalej som zvolila do užšieho výberu 2 konkrétne produkty, ktoré mali k dispozícií bezplatnú alebo cenovo dostupnú skúšobnú verziu svojho produktu, a vytvorila som v nich skúšobnú sieť.

Vybrané blockchainové platformy

V tejto podkapitole porovnávam blockchainové platformy a ich základné charakteristiky. Platformy som porovnávala na základe niekoľkých rovnakých kritérií. Jednotlivé platformy porovnávam z hľadiska funkcionality, transakčnej rýchlosti, programovacích jazykov, podporovaných protokolov a konsenzus mechanizmov.

Nižšie v tabuľke č.3 môžeme nájsť prehľad kľúčových parametrov a ich hodnôt. Ako možno vidieť, platformy sa výrazne líšia čo sa týka počtu a rýchlosti spracovania transakcií. Zatiaľ čo Bitcon spracuje jednu transakciu približne za 10 minút, Hyperledger a Corda to zvládnu takmer okamžite. Taktiež sa značne líšia hodnotou TPS, ktorá predstavuje počet spracovaných transakcií za sekundu, pričom opäť vedie

Hyperledger, ktorý dokáže spracovať až 3500 transakcií. Preto je vhodným kandidátom na implementáciu podnikových blockchainových riešení.

Tabuľka č. 3: Porovnanie platforiem
(Zdroj: Vlastné spracovanie)

Porovnávané atribúty	Názov platformy				
		Bitcoin	Ethereum	Hyperledger Fabric	Corda
	Kryptomena	Bitcoin	Ethereum	Neexistuje	Neexistuje
	Prístupová politika	Verejná	Verejná	Súkromná	Súkromná
	Validačná politika	Permissionless	Permissionless	Permissioned	Permissioned
	Konsenzus protokol	Proof of Work	Proof of Work (Proof of stake)	Hlasovací algoritmus	Overovací konsenzus/ Konsenzus jedinečnosti
	Priemerný čas spracovania transakcie	10 minút	15 sekúnd	Takmer okamžite	Takmer okamžite
	Maximálna frekvencia transakcií (TPS)	7 TPS	20 TPS	3500 TPS	170 TPS
	Jazyk Smart kontraktu	Bitcoin skript, BitML	Solidity, Serpent	Go	JVM jazyky (Java, Kotlin)

Blockchain as a service produkty

V tejto časti porovnávam elementárne vlastnosti hotových blockchainových riešení, ktoré ponúkajú spoločnosti ako službu. Znamená to, že zákazník má k dispozícii takmer hotové riešenie, ktoré môže prispôsobiť svojím potrebám. O celkovú infraštruktúru a prevádzkovanie siete sa pritom stará spoločnosť, ktorá túto službu prevádzkuje. V tabuľke porovnávam BaaS produkty od 5 rôznych spoločností - IBM, Microsoft, SAP, Amazon a Kompi Tech. Ako možno vidieť líšia sa navzájom protokolmi, ktoré

podporujú programovacími jazykmi a najmä konsenzus mechanizmom. Všetky tieto produkty disponujú možnosťou vytvárania smart kontraktov a následne aj aplikácií. Spoločnosť Kompi Tech a Microsoft ponúkajú možnosť otestovať svoje produkty bezplatne.

Tabuľka č. 4: Porovnanie BaaS produktov
(Zdroj: Vlastné spracovanie)

	Názov produktu				
	IBM Blockchain	Azure Blockchain service	Amazon managed Blockchain	SAP Blockchain	Kompi Tech Blockchain
Platforma	IBM Blockchain platforma	Azure Blockchain service platforma	Amazon Blockchain Platforma	SAP Cloud platforma	Kompi Tech platforma
Podporované protokoly	Hyperledger Fabric	Quorum (Ethereum)	Hyperledger Fabric /Ethereum	Hyperledger Fabric	Hyperledger Fabric
Skúšobná verzia	Áno - platená verzia	Áno - neplatená verzia	Áno - platená verzia	Áno - platená verzia	Áno - neplatená verzia
Tvorba Smart kontraktov a aplikací	Áno	Áno	Áno	Áno	Áno
Programovací jazyk	Java a Go jazyky	Solidity	Java, C++, C#, GO	Java	Go
Konsenzus mechanizmus	BFT	BFT	PoW, PoS	BFT	PoC

3.2 Porovnanie konkrétnych BaaS produktov

Do užšieho výberu som zvolila spoločnosti, ktoré majú vo svojom portfóliu blockchainových produktov službu *Blockchain as a service*. Ako už bolo spomenuté, nie všetky platformy poskytujú bezplatnú možnosť otestovania produktu. Z tohto dôvodu som vybrala len tie riešenia, ktoré boli cenovo dostupné. Tieto podmienky spĺňali produkty od spoločností Microsoft a Amazon. Porovnanie som realizovala testovaním jednotlivých produktov. Vytvorila som si členstvo formou skúšobnej verzie.

V oboch prípadoch som vytvorila skúšobnú blockchainovú sieť. Pri porovnávaní som sa zamerala na obdobné parametre každej siete ako je maximálny povolený počet členov a uzlov v sieti, podporované protokoly, bezpečnostný mechanizmus siete, tvorba smart kontraktov, aplikácií a doplnkové služby. Taktiež som porovnávala do akej mieri má spoločnosť prepracované podporné materiály na pomoc pri tvorbe siete, a ktoré ďalšie aplikácie od spoločnosti bude nutné nainštalovať. V neposlednom rade som zisťovala aké sú finančné predpoklady pre dané produkty.

3.2.1 Microsoft Azure Blockchain servise

Azure Blockchain Servise je produktom od Microsoftu a je to plne spravovaný servis technológie účtovnej knihy, ktorý ponúka spoločnostiam možnosť vytvoriť si vlastné blockchainové riešenia. V rámci tohto produktu si môže zákazník vytvoriť a prevádzkovať vlastnú sieť, využívať vstavaný konzorcium manažment systém a následne vytvárať smart kontrakty podľa vlastných potrieb.

Obrázok č. 12: Logo Azure
(Zdroj: 37)

Vytvorenie a správa siete môžu byť realizované niekoľkými spôsobmi. Prostredníctvom portálu Azure, Azure CLI alebo prostredníctvom programu Visual Studio code. Svoju skúšobnú sieť som vytvorila prostredníctvom portálu Azure. Pomenovala som ju Kristina_Blockchain a vytvorila som v nej niekoľko testovacích uzlov.

Name	Type
procurementnode (preview)	Azure Blockchain Service
Kristina_Blockchain	Resource group
Free Trial	Subscription

Obrázok č. 13: Vytvorenie siete
(Zdroj: Vlastné spracovanie)

Podporované protokoly

Produkt je navrhnutý tak, aby podporoval viaceré protokoly. V súčasnosti však zatiaľ podporuje len protokol Quorum za použitia IBFT konsenzus mechanizmu. Správa takejto siete nevyžaduje veľkú administratívu a je kompatibilná s mnohými open source produktmi, vďaka ktorým môžeme vytvárať aplikácie podľa vlastných potrieb.

Azure Blockchain Development Kit

Výhodou tohto produktu je, že ponúka jeho užívateľom k dispozícií pomocný nástroj Azure Blockchain Development Kit for Ethereum, ktorý nám poskytuje presný popis ako postupovať pri tvorbe siete, pri vytváraní jej členov a uzlov, pri tvorbe smart kontraktov a aplikácií všetkými dostupnými spôsobmi. Vďaka tomuto nástroju by mal byť schopný sieť vytvoriť aj užívateľ s nulovými skúsenostiam v danej problematike. Sama som podľa tohto návodu postupovala pri tvorbe mojej skúšobnej siete. Tento nástroj skontroluje, či má systém nainštalované všetky potrebné prerekvizity. V prípade, že nejaká chýba, informuje o tom užívateľa a poskytne mu odkaz, kde sa dajú stiahnuť.

Vytvorenie siete a úroveň poskytovaných služieb

Každý užívateľ si môže vytvoriť konzorcium a môže sieť nakonfigurovať podľa vlastných potrieb vo veľmi krátkom čase, o čom som sa sama presvedčila pri jej vytváraní. Pri vytváraní siete je nutná jej prvotná konfigurácia. Ak chceme vykonať dodatočné zmeny v konfigurácií, môžeme tak učiniť kedykoľvek neskôr pokiaľ to bude potrebné.

Nástroj Blockchain development Kit definuje niekoľko krokov, ako postupovať pri vytváraní blockchainového riešenia pre našu organizáciu:

1. Vytvorenie siete
2. Správa uzlov a ich „zdravia“
3. Výber Ledger technológie
4. Vytvorenie Smart kontraktu
5. Pripojenie uzlov
6. Manuálne vytvorenie účtovnej knihy
7. Zadefinovanie obchodnej logiky

8. Priradenie identity uzlom
9. Ustanovenie členov
10. Vytvorenie rolí pre uzly
11. Vytvorenie politiky siete
12. Prispôsobenie integrácie
13. Presadzovanie politiky
14. Správa povolení
15. Rozšírenie do ďalšej siete (37)

Pri tvorbe vlastnej siete som postupovala podľa týchto krokov. Výhodou je, že vytvorenie skúšobnej blockchainovej siete a jej prevádzkovanie je počas prvých 30 dní zadarmo .Zákazník ma k dispozícii počiatočný kredit vo výške 200 dolárov, z ktorého som neskôr financovala prevádzkovanie svojich uzlov. Po úspešnom vytvorení siete je vygenerovaný unikátny kód, ktorý označuje túto jedinečnú blockchainovú sieť. Ďalej som pokračovala tým, že som si vytvorila prvého člena pre nové konzorcium prostrednícvtom portálu Azure. Uzol som pomenovala procurementnode a nastavila mu potrebné parametre. Bude fungovať na protokole Quorum, kedže momentálne iné nie sú v tomto produkte k dispozicíi. Pri vytváraní musíme zvoliť akú úroveň služby požadujeme. V ponuke sú dve úrovne služieb:

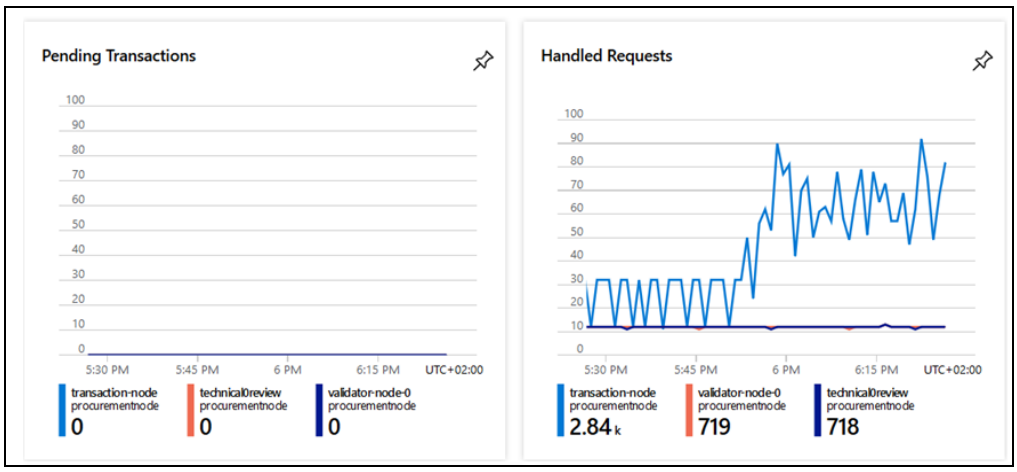
- **Základný balík**
- **Štandardný balík**

Ako môžeme vidieť na obrázku nižšie, tieto dve možnosti sa líšia výkonom, veľkosťou úložiska, počtom validačných a transakčných uzlov, dostupnosťou a v neposlednom rade finančnými nákladmi. Pri vytváraní svojej skúšobnej verzie som si vybrala prvú možnosť – štandardný balík. V rámci tohto balíku je teda možné prevádzkovať 2 transakčné uzly a máme k dispozícii úložisko veľkosti 5 GB. Môžeme vidieť predpokladané mesačné náklady, ktoré činia približne 215 dolárov.

	Basic Environment for dev/test	Standard Run production workloads
Compute	1 vCore	2 vCores
Storage [1]	5 GB	5 GB
Number of validator nodes	1	2
Number of transaction nodes [2]	2 (Add node)	1
Hybrid deployment support	N/A	Coming soon
High availability	N/A	99.9%
Estimated cost per month [3]	$214.58 71.42 per node	$897.58 299.09 per node

Obrázok č. 14: Balíky služieb
(Zdroj: Vlastné spracovanie)

Keď je nový člen konzorcia vytvorený, môžeme skontrolovať podrobnosti v sekcii *Overview*. V tejto sekcii môžeme ďalej sledovať aktivitu jednotlivých blokov a transakcií, ktoré boli vykonané alebo práve v sieti prebiehajú. Takisto možeme vidieť diagram, ktorý zobrazuje vybavené žiadosti. V každom grafe vidíme krivku priradenú jednotlivým uzlom. Uzly sú rozlíšené na transakčné a validačné.



Obrázok č. 15: Prehľad aktivity uzlov
(Zdroj: Vlastné spracovanie)

Členovia siete a pridelenie rolí

V závislosti od potrieb danej siete, môžeme do siete prizvať nových členov či už z vlastnej alebo nejakej inej organizácie. Pridanie nového člena do siete môže vykonať len administrátor. Nový užívatelia môžu byť pridaní na základe Azure subscription ID.

Je možné tak učiniť v sekcii *Access control* kde je zároveň k dispozícií niekoľko preddefinovaných rolí, ktoré je možno priradiť jednotlivým členom siete. V prípade potreby je možné vytvoriť aj vlastné užívateľské profily.

Smart kontrakty

Po vytvorení a nakonfigurovaní siete, je možné vytvoriť prvé Smart kontrakty. Možno postupovať podľa návodu Developement Kitu a pripojiť sa tak ku sieti prostredníctvom programu Visual Studio Code, kde je možné vytvárať, rozvíjať a realizovať smart kontraky prostredníctvom transakcií. Toto je však len jedna z možností. Obdobným spôsobom sa dajú smart kontrakty realizovať aj prostredníctvom ďalších nástrojov ako sú napríklad MetaMask v kombinácií s Remix nástrojom, či Truffle alebo Geth.

Blockchain data manager

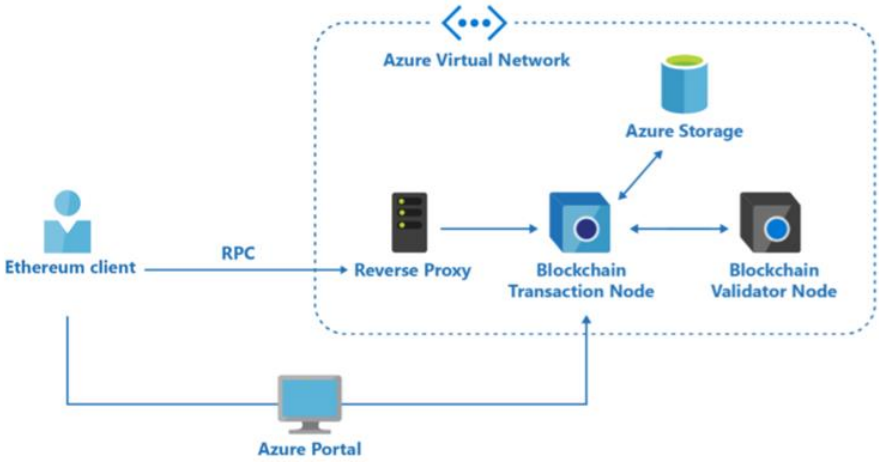
Azure Blockchain data manažér je možné nájsť a vytvoriť priamo prostredníctvom portálu Azure. Nájdeme ho ako samostatnú záložku v sekcii *Blockchain*. Je to nástroj, ktorý sa využíva na ukladanie dát blockchainových transakcií vykonaných v sieti do databázy Azure Cosmos DB. Pre plné využívanie tejto funkcionality som musela nainštalovať ešte instanciu Azure Event Grid Topics. Proces ukladania dát funguje tak, že Blocchain data manager ukladá, transformuje a doručí dáta z účtovnej knihy do Azure Event Gridu, odkiaľ sú následne prostredníctvom Azure Logic App konektoru (nástroj, ktorý napomáha automatizovaniu odosielania dát) uložené do dokumentu vytvorenom v Cosmos databáze.

Aplikácie

Priamo prostredníctvom portálu Azure je možné implementovať do siete nami naprogramovanú blockchainovú aplikáciu. Stačí pridať internetový odkaz na zdrojový súbor, ktorý obsahuje kód pre aplikáciu vytvorený vo Visual Studio.

Bezpečnosť siete

Služba Azure Blockchain servis využíva niekoľko Azure nástrojov na zabezpečenie a sprístupnenie údajov. Údaje sú zabezpečené pomocou izolácie, šifrovania, autentifikácie. Všetky zdroje sú izolované v súkromnej virtuálnej sieti. Každý transakčný a validačný uzol si môžeme predstaviť ako virtuálny stroj, pričom platí, že dva stroje z rôznych sietí nemôžu medzi sebou navzájom komunikovať (37).



Obrázok č. 16: Bezpečnostná schéma siete
(Zdroj: 37)

3.2.2 Amazon Managed Blockchain

Ďalším produktom, ktorý som testovala je Amazon Managed blokchain servis. Obdobne ako pri predchádzajúcom riešení aj tento produkt je plne spravovaný servis technológie účtovnej knihy, ktorý ponúka spoločnostiam možnosť vytvoriť si súkromnú blockchainovú sieť a to za využitia open source produktov. V rámci tohto produktu si môže zákazník vytvoriť a prevádzkovať vlastnú sieť a následne podľa potreby vytvárať smart kontrakty či obchodné a iné aplikácie. Aplikácie zachovávajú všetky hlavné princípy blockchain technológie. Môžu byť zdieľané medzi niekoľkými organizáciami, ktoré vďaka tomuto produktu môžu bezpečne a transparentne realizovať medzi sebou obchody a rôzne druhy transakcií, bez potreby vstupu prostredníkov či centrálnych autorít.

Obrázok č. 17: Logo Amazon
(Zdroj: 38)

Podporované protokoly

V prípade protokolov máme možnosť zvoliť si medzi dvoma druhmi open source frameworkov, ktoré budú použité pri vytváraní a prevádzkovaní novej siete. Momentálne je plne k dispozícií Hyperledger Fabric, ktorý som si zvolila pri vytváraní svojej skúšobnej siete. Druhou z možností je použitie Etherea, ktoré bude však plne dostupné až o niekoľko mesiacov. Produkt momentálne pracuje s verziou Hyperledger Fabric 1.2, pričom spoločnosť Amazon spravuje potrebné certifikačné autority Hyperlegder Fabric a peer uzly (38).

Amazon Management sprievodca

Pri tvorbe siete som postupovala podľa Amazon management návodu, ktorý vytvorili tvorcovia produktu tak, aby poskytoval detailnú inštruktáž a informácie ku celkovému konceptu tohto riešenia. Návod je dostupný na stránkach produktu a je možné ho stiahnuť vo forme PDF.

Ako postupovať pri vytváraní potrebného riešenia, definujú nasledovné kroky:

1. vytvorenie siete
2. vytvorenie prvého člena siete
3. nastavenie klienta
4. zapojenie sieťového administrátora
5. vytvorenie peer uzla
6. vytvorenie kanálu
7. spustenie kódu
8. prizvanie členov siete a vytvorenie kanálu (38).

Vytvorenie siete a úroveň poskytovaných služieb

V prvom kroku som si vytvorila účet. Po vytvorení som sa prihlásila do Amazon webovej konzoly AWS (Amazon Web Servis), odkiaľ majú užívatelia prístup ku všetkým službám a produktom, ktoré má spoločnosť aktuálne vo svojom produktovom portfóliu. Vytvorenie siete vyžaduje prvotnú konfiguráciu, voľbu

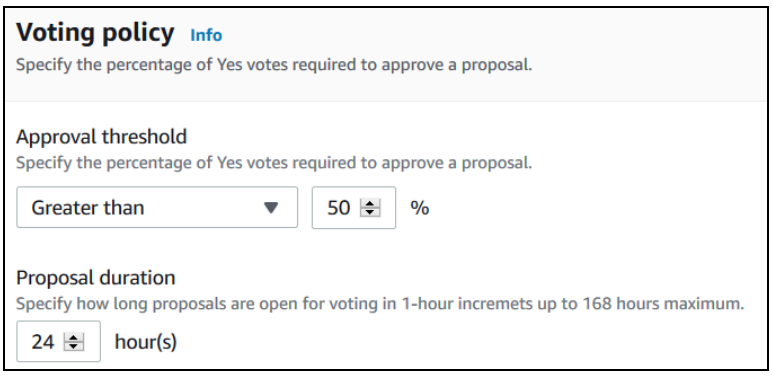
protokolu, nastavenie politiky hlasovania a vytvorenie prvého člena siete. Pri tvorbe siete máme k dispozícií dva druhy užívateľského plánu:

- **Starter Plán**

Tento plán je skôr vhodnejší pre malé alebo testovacie siete. Má obmedzenia čo sa týka počtu členov a uzlov. Môžeme mať maximálne 5 členov na sieť a 2 rovnocenné uzly na člena. Objednávacia služba poskytovaná v sieti Starter Edition má nižšiu priepustnosť a dostupnosť transakcií ako v sieti Standard Edition.

- **Standard Plán**

Je verzia vhodnejšia pre výrobné siete. Čo sa týka počtu členov a uzlov, opäť platia obmedzenia. Môžeme mať maximálne 14 členov na sieť a 3 rovnocenné uzly na člena. Objednávacia služba poskytovaná v sieti Standard Edition má vyššiu priepustnosť a dostupnosť transakcií ako v sieti Starter Edition. Pre svoju sieť som zvolila prvú môžnosť – Starter plan. Ďalej je potrebné nastaviť politiku hlasovania. Tá nám udáva minimálne percentuálne množstvo členov, ktorí musia schváliť návrh tak aby sa stal platným. Ponechala som prednastavených 50%. To znamená, že v prípade, že aspoň polovica účastníkov siete danú transakciu odsúhlasí, stane sa platným. V opačnom prípade sa stáva neplatným. Taktiež je možné nastaviť ako dlho je daný návrh otvorený a prístupný jednotlivým uzlom na hlasovanie.

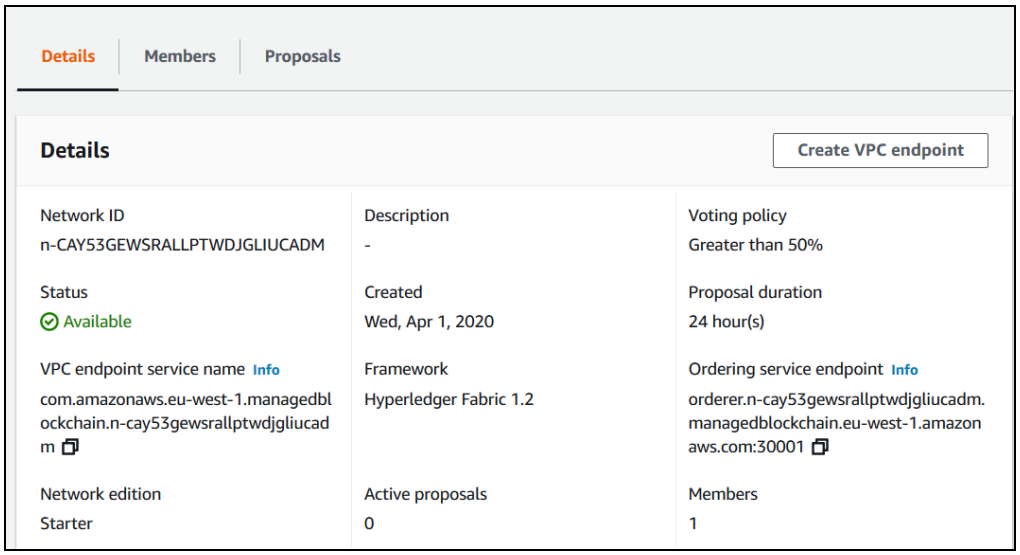


Obrázok č. 18: Politika hlasovania
(Zdroj: Vlastné spracovanie)

Týmto bola prvotná konfigurácia siete hotová a prešla som k ďalšiemu kroku, ktorým bolo vytvorenie prvého člena siete. Každá sieť musí mať minimálne jedného člena, ale podľa potreby danej organizácie ich môže byť aj viac. Keď je člen vytvorený, treba

vytvoriť peer node, ktorý mu bude prislúchať. Svojho člena som pomenovala member1. Meno jednotlivých členov v sieti musí byť vždy unikátne. V poslednom kroku je ešte nutné vytvoriť administrátora pre správu Hyperledger Fabric certifikačnú autoritu. Vytvorila som administrátora s menom *testadmin* a vytovrila mu heslo pre prístup.

Po vyplnení týchto údajov som bola presmerovaná na záverečnú kontrolu všetkých zadaných údajov. Po odsúhlasení sa vygejeruje nová sieť, čo trvá približne 15 minút. V detailoch môžeme nájsť unikátne sieťové ID. Toto ID jednoznačne identifikuje danú sieť a neskôr bude možné sa ku sieti pomocou neho pripojiť z nástrojov na tvorbu smart kontraktov a aplikácií.



Obrázok č. 19: Vytvorenie siete
(Zdroj: Vlastné spracovanie)

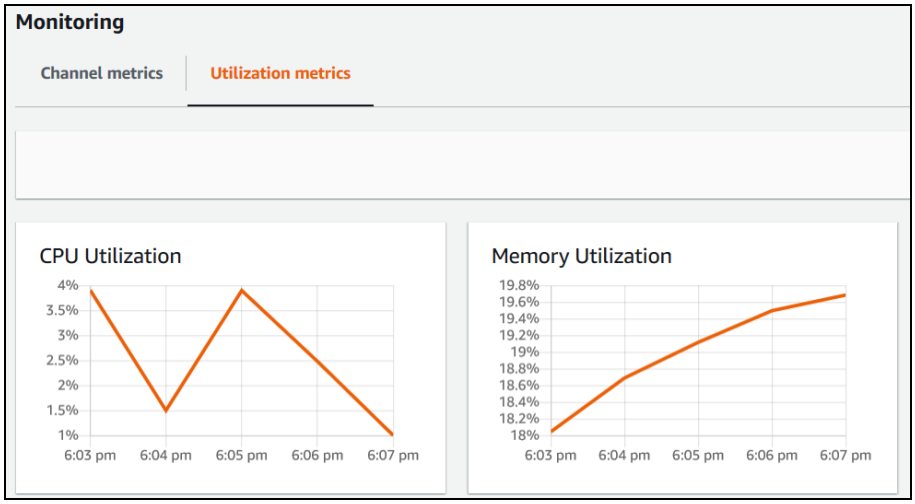
V tomto štádiu je ešte treba vytvoriť koncový bod a prideliť jednlotlivým členom siete užívateľské uzly. Každá takto vytvorená blockchainová sieť je považovaná za samostatný súkromný servis poskytovaný spoločnosťou Amazon. Z toho dôvodu produkt automaticky pri vytvorení novej siete vytvorí zároveň unikátny súkromný názov, podľa ktorého je možné sieť identifikovať. Každý člen tak musí mať koncový bod, ktorý bude odkazovať na tento súkromný servis. Prostredníctvom tohto koncového bodu sa budú môcť všetci členovia daného účtu pripojiť ku blockchainovým sieťovým zdrojom. Obdobný princíp platí aj v prípade objednávkového servisu, ktorý musí mať pridelený koncový bod.

Členovia siete a pridelenie rolí

Ako už bolo spomínané v predchádzajúcich krokoch, aby bol člen schopný vykonávať v sieti transakcie, je nutné vytvoriť a prideliť mu uzol. Pri tvorbe uzlu musíme zvoliť typ blockchainovej instancie. Môžme vybrať malú (2 v CPU, 2GB) alebo strednú (2 v CPU, 4GB). Potom ešte zvolíme zónu dostupnosti. Približne po 10 minútach sa vygeneruje nový uzol, ktorému sa automaticky vygeneruje unikátne ID a koncové body.

Overview management systém

Pre každý uzol v sieti môžeme prostredníctvom grafov v sekcii *Utilization metrics* sledovať jeho aktivitu. Môžeme sledovať vyťaženie procesoru a využívanú pamäť.



Obrázok č. 20: Prehľad aktivity v sieti
(Zdroj: Vlastné spracovanie)

Smart kontrakty

Smart kontrakty sú v prípade Hyperledger Fabric známe pod názvom „chaincode“. Produkt Managed Blockchain obsahuje verzie knižnice Fabric-shim. Táto knižnica poskytuje rozhranie kódov (chaincodes) medzi aplikáciami, uzlami a systémom Hyperledger Fabric pre aplikácie (38).

Bezpečnosť siete

Amazon Managed Blockchain ponúka plne spravované šifrovanie. Poskytuje zvýšenú bezpečnosť šifrovaním všetkých dát pomocou šifrovacích kľúčov. Ide o službu *AWS Key Management Service*. Táto funkcia pomáha znižovať prevádzkové zaťaženie

a zložitosť ochrany citlivých údajov. Ďalším bezpečnostným prvkom je Certifikačná autorita spoločnosti Hyperledger Fabric (CA), ktorá v každom členstve poskytuje certifikačnú autoritu na zabezpečenie komunikačných kanálov Hyperledger Fabric v sieti (38).

3.2.3 Odporučenie najvhodnejšieho riešenia

V predchádzajúcej kapitole som si vyskúšala dve BaaS riešenia od spoločností Amazon a Microsoft. Pri vytváraní a konfigurácií sietí som mala možnosť vidieť výhody a nevýhody každého produktu. Obe porovnávané riešenia pracujú na obdobnom princípe. Zákazník si môže vytvoriť vlastnú sieť, kde môže následne podľa potreby pozvať ďalších členov. V nasledujúcej časti popisujem silné a slabé stránky oboch produktov:

- **Amazon managed blockchain**

Za výhodu riešenia od spoločnosti Amazon považujem to, že pri tvorbe siete máme k dispozícií na výber dva rôzne protokoly. V súčasnosti môžeme zvoliť Hyperledger Fabric, pričom v dohľadnej budúcnosti by sa malo pridať aj Ethereum. Ďalšou výhodou tohto riešenia je možnosť nastavenia politiky hlasovania. Vlastník siete môže rozhodnúť o tom, aký percentuálny podiel je nutný, aby sa daná transakcia stala platnou. Táto funkcionalita môže byť u podnikových riešení kľúčová.

Za nevýhodu tohto produktu považujem, že neposkytuje až tak veľa možností pre škálovanie produktu a pomerne jednoduchú *overvirew* sekciu, kde možno pozorovať len elementárne metriky. Za menšiu nevýhodou tiež považujem, že nie je k dispozícií neplatená skúšobná verzia produktu.

Cena za hodinu prevádzkovania uzla je približne 0,67 centov a cena za 1 GB úložiska približne 0,10 centov.

- **Azure blockchain service**

Blockchainové riešenie od spoločnosti Microsoft je dostupné v skúšobnej neplatenej verzii, pričom zákazník môže prečerpať bonusový kredit vo výške 200 dolárov. Microsoft blockchain je kompatibilný s ďalšími instanciami a produktami, ktoré má spoločnosť vo svojom portfóliu, takže ich môžeme zakomponovať do návrhu v rámci

neplatenej verzie a škálovať návrh podľa vlastných potrieb. Je možné tak vytvoriť funkčnú sieť a neskôr nad jej obsahom využiť rôzne business inteligence a analytické nástroje pre podporu manažérskeho rozhodovania.

Za výhodu tohto produktu považujem nástroj *Azure Blockchain Developement Kit,* ktorý slúži ako podporný nástroj pre zákazníka. Je to integrovaný sprievodca, ktorý je nápomocný v prípade, že už máme vytvorenú sieť a chceme ďalej navrhovať a vytárať smart kontrakty a aplikácie. Celkovo je ku tomuto riešeniu dostupných pomerne veľa návodov a informácií, takže by mal byť dostupný aj pre bežných užívateľov, ktorý nemajú v tejto oblasti až tak veľa skúseností. Za ďalšiu výhodu považujem existenciu prehľadných nástrojov a dashboardov, kde je možné pozorovať aktivitu v sieti, prehľad transakcií, výpočtové metriky a stav úložiska.

Pokiaľ ide o finančné náklady, cena za hodinu prevádzkovania uzla je približne 0,71 centov a cena za 1 GB úložiska približne 0,05 centov.

Výsledný produkt

Na základe poznatkov, ktoré som nadobudla pri vytváraní oboch sietí, by som odporučila ako vhodnejšie riešenie produkt od spoločnosti Microsoft Azure Blockchain servise. Tento produkt ponuka možnosť vytvorenia siete typu konzorcium, ktorá je pre potreby objednávkového procesu ideálnou voľbou. Funkcionalita siete tak bude plne pod kontrolou vlastníka, a bude možné nastaviť rôzne úrovne prístupov.
Produkt je prepracovanejší čo sa týka dashboardov, sledovania aktivity v sieti a ďalších metrík. Je kompatibilný s mnohými open source nástrojmi, ktoré sa využívajú na vývoj potrebných blockchainových smart kontraktov a aplikácií. Naviac je kompatibilný s ďalšími produktmi od spoločnosti Microsoft a je možné ho škálovať podľa individuálnych potrieb. Je možne prepojiť ho s BI a analytickými nástrojmi pre podporu rozhodovania. V neposlednom rade je nutné poznamenať, že ku tomuto riešeniu existuje viacero dostupných prevádzkových a edukačných materiálov, ktoré môžu v prípade mnohých firiem bez interného developerského tímu zohrať kľúčovú rolu. Pokiaľ ide o finančnú stránku, produkty sú na tom cenovo približne rovnako. Cena za prevádzkovanie uzla je v prípade Azure Blockchain produktu o približne 0.05 centov vyššia, no na druhej strane poskytuje úložisko za polovičnú cenu ako produkt od

spoločnosti Amazon. V prepočte je tak výsledný cenový rozdiel len pár desiatok EUR mesačne.

3.3 Návrh nového objednávkového procesu pomocou blockchainu

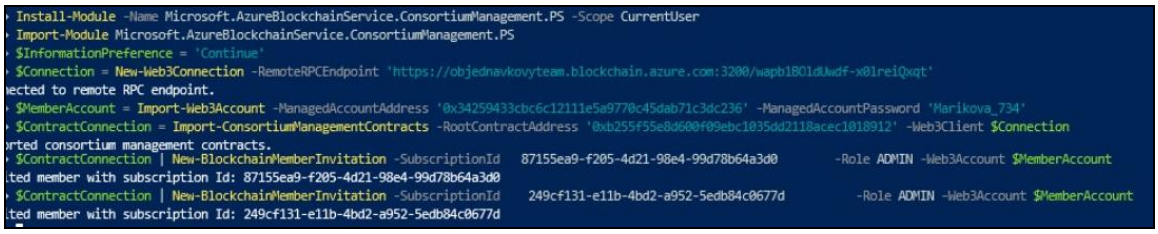
Táto kapitola je venovaná vytvoreniu návrhu pre nový objednávkový proces. Pre implementáciu som sa rozhodla použiť produkt od spoločnosti Microsoft - Azure Blockchain servise. V porovnaní, ktoré som realizovala v predchádzajúcej kapitole som dospela k záveru, že tento produkt má vo všeobecnosti viac výhod a užitočných funkcionalít. Zároveň lepšie zodpovedá požiadavkám objednávkového procesu. Pre implementáciu svojho návrhu do tohto produktu, som opäť využila bezplatnú verziu.

Vytvorenie siete v Azure Blockchain Service

V prvom kroku návrhu, som prostredníctvom portálu Azure vytvorila blockchainovú sieť typu konzorcium. Pomenovala som ju *Objednávkový proces.* Zároveň som vytrovila niekoľko členov, ktorí budú predstavovať jednotlivých účastníkov objednávkového procesu v zastúpení organizácie IBM. Keďže objednávkový proces tvorí niekoľko ďalších externých organizácií, vytvorila som pre ne užívateľské účty tak, aby mala každá organizácia svoj vlastný predplatený účet. Pod každým účtom som ďalej vytvárala konkrétnych členov danej organizácie.

Členovia konzorcia

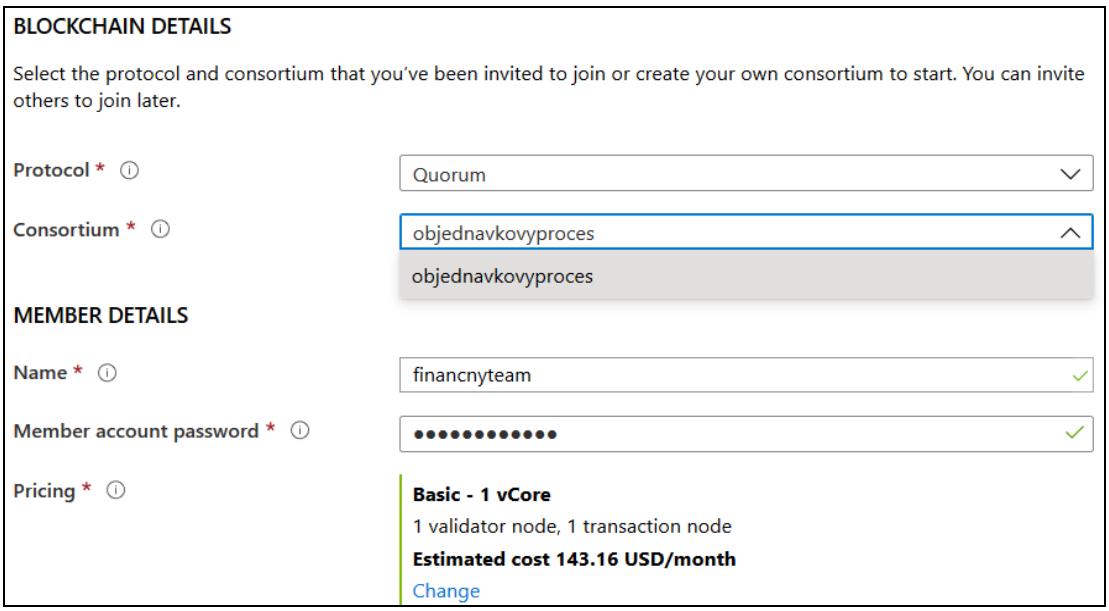
Pozvanie jednotlivých organizácií a jej členov do konzorcia som realizovala prostredníctvom príkazového riadka Power Shell. Najskôr bolo nutné pripojiť sa ku konzorciu prostredníctvom údajov *RootContractAddress* a *RemoteRPCEndpoint,* ktoré sú pre každé konzorcium jedinečné.



Obrázok č. 21: Pripojenie ku konzorciu
(Zdroj: Vlastné spracovanie)

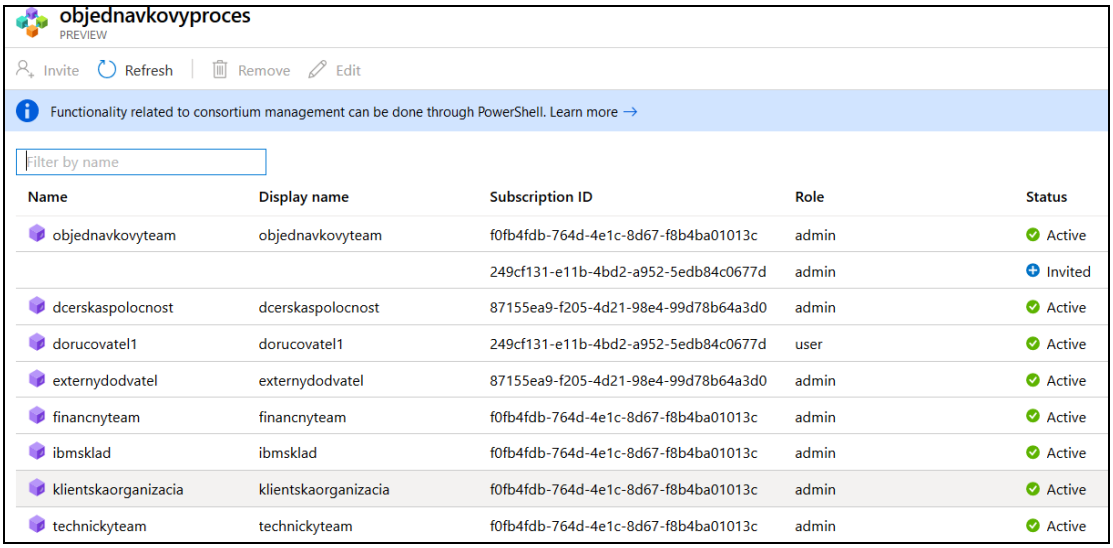
Po pripojení sa načíta zoznam aktuálnych členov konzorcia a je možné vykonávať ďalšiu správu členstva ako je pridávanie a mazanie členov, rozosielanie pozvánok novým členov, či priradenie členských rolí. Poslala som nové pozvánky pre všetky účty vytvorené pre externé organizácie.

Ak chce organizácia potvrdiť pozvánku a pripojiť sa do nového konzorcia, musí vytvoriť nový uzol, prostredníctvom ktorého bude v sieti vykonávať aktivitu. Prostredníctvom jedného uzla sa môžu pripojiť viacerí členovia. Po zaslaní pozvánky sa v sekcii na vytvorenie nového člena objaví v zozname názov konzorcia, ktoré danej organizácií poslalo pozvánku. Postupne som vytvorila nové uzly pre každú organizáciu prizvanú do konzorcia.



Obrázok č. 22: Vytvorenie nového člena
(Zdroj: Vlastné spracovanie)

V sekcii konzorcium môžeme vidieť všetkých účastníkov siete, vrátane ich aktuálnej pridelenej roly a statusu. Pokiaľ ešte nejaký člen neakceptoval pozvánku, vidíme jeho stav ako *Invited*. Na obrázku nižšie môžeme vidieť, že do vytvoreného konzorcia boli prizvané všetky organizácie a účastníci objednávkového procesu.



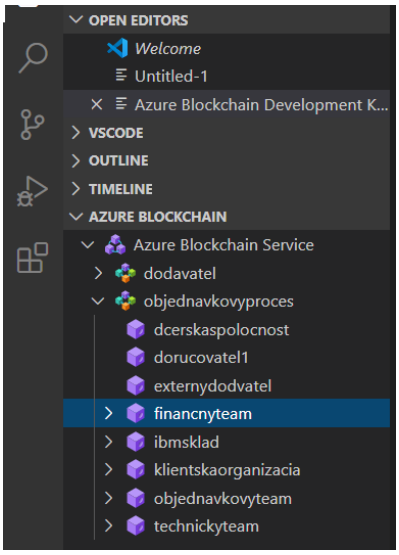
Obrázok č. 23: Objednávkový proces
(Zdroj: Vlastné spracovanie)

Blockchain data manager

Pre plné využívanie tejto funkcionality som musela nainštalovať ešte instanciu Azure Event Grid Topics. Proces ukladania dát funguje tak, že Blockchain data manager ukladá, transformuje a doručí dáta z účtovnej knihy do Azure Event Gridu, odkiaľ sú následne prostredníctvom Azure Logic App konektoru (nástroj, ktorý napomáha automatizovaniu odosielania dát) uložené do dokumentu vytvorenom v Cosmos databáze. Následne je možné tieto dáta analyzovať pomocou rôznych BI a analytických nástrojov a vytvárať tak reporty, prehľady a dashboardy pre podporu rozhodovania.

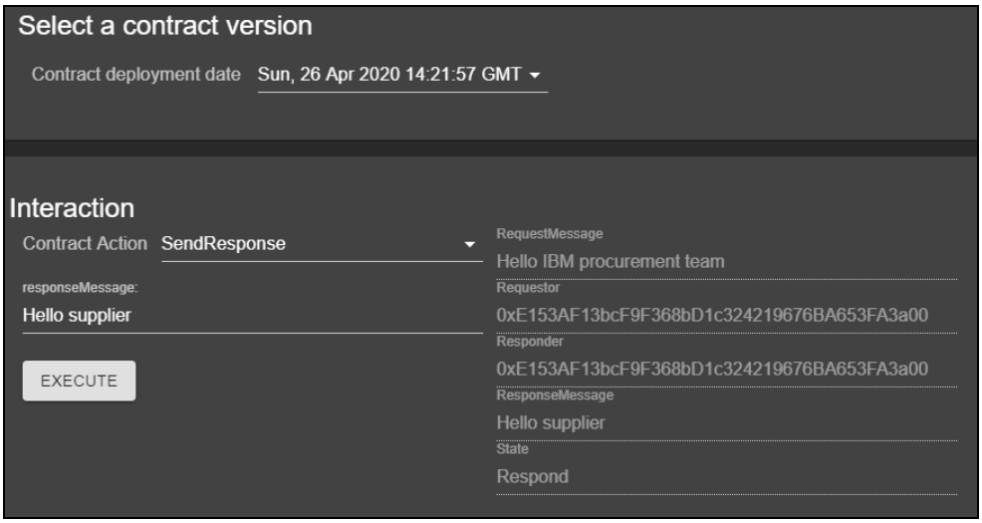
Smart kontrakt

V ďalšom kroku som pre novovytvorené konzorcium vytvorila jednoduchý smart kontrakt, ktorý umožňuje posielanie správ medzi účastníkmi siete. Spôsobov ako vytvárať a testovať smart kontratky a aplikácie je viacero. Ja som na vytvorenie kódu zvolila program Visual Sudio Code, aby som mohla zároveň otestovať funkčnosť doplnku *Azure Blockchain Developement Kit*, ktorý je potrebné stiahnuť a nainštalovať ako doplnok programu VS Code. Prostredníctvom príkazového riadku vo VS som sa pripojila ku svojmu konzorciu. Automaticky sa zobrazili všetci existujúci členovia siete:



Obrázok č. 24: Pripojenie ku konzorciu pomocou VS
(Zdroj: Vlastné spracovanie)

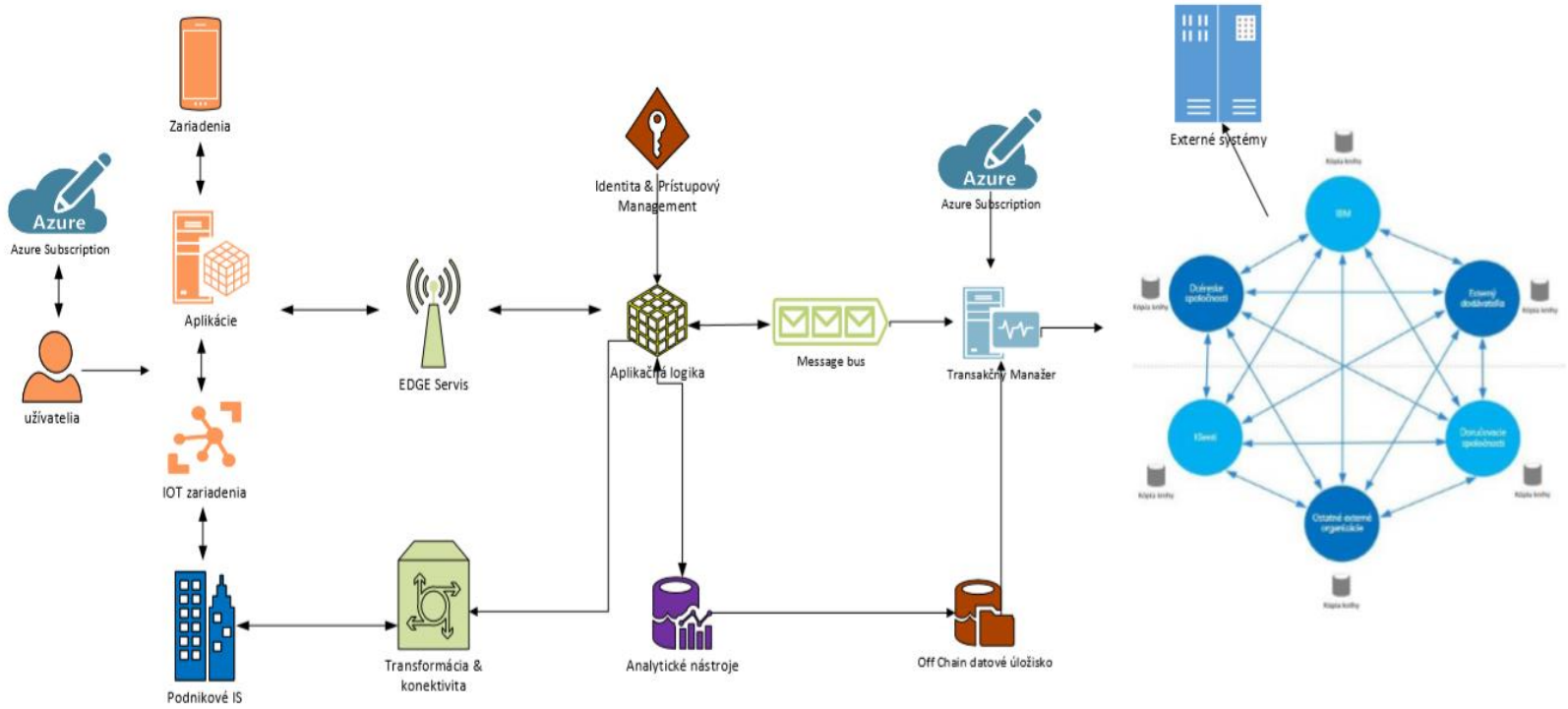
Následne som prostrednícvtom nového Solidity projektu vytvorila a spustila jednoduchý smart kontrak pre pre navrhnuté konzorcium. Tento jednoduchý kontrakt bol vytvorený na demonštráciu funkčnosti vytvoreného konzorcia. Bolo by možné prispôsobiť ho pre akúkoľvek sieť. Skúsený programátor by dokázal vytvoriť kompletný kód, ktorý by slúžil ako mechanizmus pre objednávkový proces.



Obrázok č. 25: Návrh Smart kontraktu
(Zdroj: Vlastné spracovanie)

Po vytvorení blockchainovej siete, som vytvorila návrh schémy, ako by vyzerala sieť a celkové riešenie v prípade implementácie novej technológie.

Schému môžeme vidieť nižšie na obrázku č. 26. Nové riešenie bude integrované a kompatibilné so súčasným podnikovým informačným systémom. Užívatelia budú mať k sieti prístup prostredníctvom svojich osobných zariadení, podnikových aplikácií a súčasťou budú aj IoT zariadenia. Dáta zo siete budú okrem primárneho úložiska odosielané aj do externých systémov (napríklad interných systémov organizácií zapojených do procesu), a zároveň do Off chain dátového úložiska spoločnosti IBM. Odtiaľ budú prístupné pre ďalšie spracovanie prostredníctvom rôznych analytických a business inteligencie nástrojov.



Obrázok č. 26: Schéma nového riešenia
(Zdroj: Vlastné spracovanie)

3.4 Prínosy nového návrhu v objednávkovom procese

V tejto časti som vytvorila zoznam potencionálnych prínosov, ktoré by mala implementácia vybraného blockchainového riešenia pre objednávkový proces a jeho účastníkov.

- **Prehľadné sledovanie a kontrola objednávok**

Výhodou implementácie novej technológie by bolo s ňou spojené prehľadnejšie sledovanie stavu objednávok. Každý účastník by mal prístup ku aktuálnym informáciám o priebehu objednávok a nemusel by tak vyhľadávať potrebné informácie manuálne v nástrojoch a aplikáciách. Všetko by bolo uložené na jednom mieste, eliminovala by sa mailová komunikácia spojená s týmto zisťovaním. Účastníci by mali dohľad na všetok tovar obsiahnutý v danej objednávke, videli by servisy súvisiace s objednávkou a konkrétne transakcie vrátane ich historického prehľadu. Taktiež by obsahovali detaily obchodu uzavretého medzi obchodnými partnermi.

- **Zavedenie inteligentných zmlúv**

Využitie Smart kontraktov v objednávkovom procese by vnieslo do objednávkového procesu určitú automatizáciu. Napomohlo by to ku dodržiavaniu požiadaviek zadaných zo strany klienta ale aj spoločnosti samotnej. Bolo by zabezpečované plnenie všetkých povinností, ktoré spoločnosti ukladá SLA (Service Level Agreement). Zároveň by boli prístupné všetkým účastníkom procesu. Na plnenie by dohliadal samotný sieťový mechanizmus.

- **Efektívnejšie využitie ľudských zdrojov**

Ďalším pozitívom by bolo viditeľné zvýšenie efektivity práce zúčastnených ľudských zdrojov. Vďaka tomu, že by sa eliminovala dvojitá komunikácia spojená so zisťovaním detailov a súčasného stavu objednávok, pracovníci by mohli získaný čas využiť na spracovanie ďalších objednávok alebo iných činností. Zároveň by sa vyhli vynakladaniu úsilia na viacnásobné schvaľovanie tej istej objednávky vo viacerých aplikáciách. Ak by totiž implementácia prebehla úspešne, stačilo by tú istú objednávku zrevidovať len jedenkrát.

- **Urýchlenie procesu**

Kladným dôsledkom predošlých opatrení by bolo celkové urýchlenie objednávkového procesu. Výsledný čas spracovania objednávky od úplného začiatku až do jej konečnej fázy by sa mohol znížiť až o polovicu. Vďaka tomu, že sa eliminujú dvojité náklady vynaložené na schvaľovanie tej istej objednávky a celý proces bude prebiehať na jednom mieste, bude celkový proces rýchlejší a požadovaný tovar alebo služba sa tak dostanú ku klientovi načas.

- **Dôvernejšie transakcie**

Okrem zrýchlenia a zjednodušenia platobných transakcií, bude mať implementácia za následok aj zvýšenie celkovej efektivity a bezpečnosti jednotlivých transakcií. Keďže blockchain je synonymom pre vysokú kryptografickú bezpečnosť, budú platobné transakcie zabezpečené a ich realizácia prebehne rýchlejšie. Celkovo sa stane overovanie dostupnosti prostriedkov a finančných zdrojov prístupnejšie a zjednodušené pre užívateľov.

- **Zjednodušuje procesy a zvyšuje jeho efektivitu**

Dielčie procesy, ktoré tvoria objednávkový systém budú nielen menej časovo náročné, ale bude ich aj jednoduchšie vykonávať, pretože všetky potrebné materiály a dokumenty o revízii budú dostupné na jednom mieste. Tým, že sa proces urýchli, bude celkový projekt ukončený rýchlejšie a efektivita objednávkového procesu sa tak zvýši.

- **Zlepšenie dodávateľského reťazca**

Zlepší sa celkový dodávateľský reťazec. Všetci účastníci procesu budú mať prehľad o tom, kde a v akom stave sa objednávka nachádza, aké akcie je nutné vykonať a kto za ne aktuálne nesie zodpovednosť. Vývoj objednávky bude sledovaný a zaznamenávaný na jednom mieste a samotný dodávateľ bude jeho súčasťou od úplného začiatku. Bude tak mať všetky potrebné informácie včas a doručenie produktu prebehne v rámci stanoveného dátumu.

- **Audity**

Vďaka tomu, že žiadna historická transakcia nemôže byť z blockchainu vymazaná, budú audity oveľa dôveryhodnejšie a spoľahlivejšie. Eliminujú sa nezrovnalosti a chyby

vzniknuté pri manuálnom zadávaní dát do systému. Práca samotného auditora bude vykonaná rýchlejšie, vďaka tomu, že všetky procesy vrátane dôležitej dokumentácie budú dostupné na jednom mieste.

- **Dôvera a autentifikácia užívateľov**

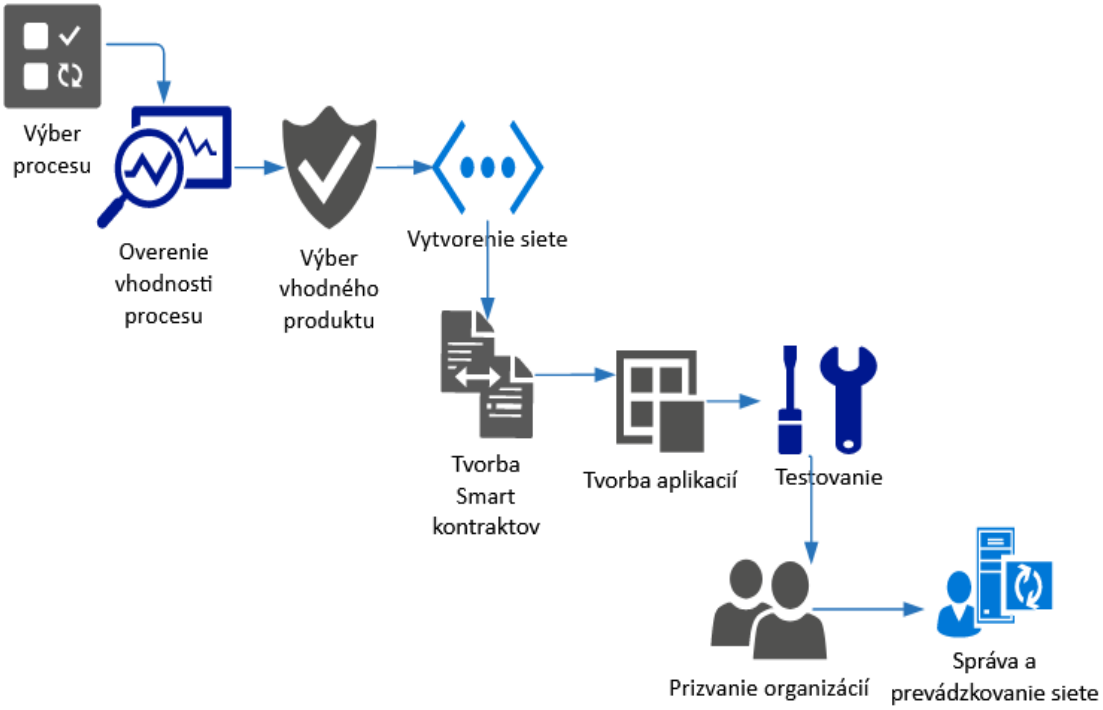
Systémy vybudované pomocou technológie blockchain sú považované vo všeobcnosti za veľlmi bezpečné a to vďaka kryptografickým nástrojom, ktoré táto technológia využíva. Autentifikácia a autorizácia užívateľov zahrnutých do procesu je veľmi spoľahlivá, vďaka využívaniu súkromných a verejných kľúčov. Nielen finančné transakcie realizované v objednávkovom procese sa tak stávajú bezpečnejšie a spoľahlivejšie.

3.5 Návrh všeobecného postupu implementácie

V nasledujúcej kapitole som vytvorila všeobecný návrh, ktorý obsahuje zoznam krokov ako postupovať v prípade, že chceme overiť, či je vybraný firemný proces vhodný na implementáciu technológie blockchain alebo nie. Ďalej popisujem ako by sme mohli realizovať výber vhodnej blockchainovej platformy pre potreby konkrétneho firemného procesu a na ktoré kľúčové faktory by sme sa pri výbere technológie mali zamerať.

3.5.1 Schéma implementácie

Vytvorila som jednoduchú schému, ktorá demonštruje ako postupovať pri implementácii blockchain technológie na vybranom procese. V prvom kroku vyberieme proces, pričom je nutné overiť, či sa na implementáciu hodí alebo nie. Ďalej pokračujeme k výberu vhodného produktu, v ktorom následne vytvoríme sieť. Pokračujeme tvorbou smart kontraktov a aplikácií, ktoré bude pred spustením nutné otestovať. Po úspešnom spustení prizveme do fungujúcej siete účastníkov a externé organizácie.



Obrázok č. 27: Postup implementácie blockchainu
(Zdroj: Vlastné spracovanie)

3.5.2 Vhodnosť procesu na implemetáciu blockchain technológie

Pred tým, než sa rozhodneme implementovať blockchain technológiu na akýkoľvek firmený proces, mali by sme zvážiť vhodnosť jej použitia. Existujú určité kritéria a podmienky, ktoré nám môžu toto rozhodnutie zjednodušiť.

V nasledujúcej kapitole definujem niekoľko kľúčových kritérií, ktoré by mal spĺňať každý proces pred tým, než sa rozhodneme pre investíciu a implementáciu tejto technológie. Ak teda projekt spĺňa nižšie uvedené kritéria, doporučuje sa využitie blockchain technológie. Paralelne demonštrujem príklad použitia na objednávkovom procese.

- **Na procese sa zúčastňuje niekoľko strán, ktoré zdieľajú spoločné dáta, vrátane externých organizácií:**
  - ✓ Na objednávkovom procese sa zúčastňuje veľa strán: klient, PM, dodávateľ, finančné oddelenie, technici, DPE, administrátori, nákupcovia, prostredníci pre prácu s aplikáciami a databázami, doručovacia spoločnosť, dcérske spoločnosti.

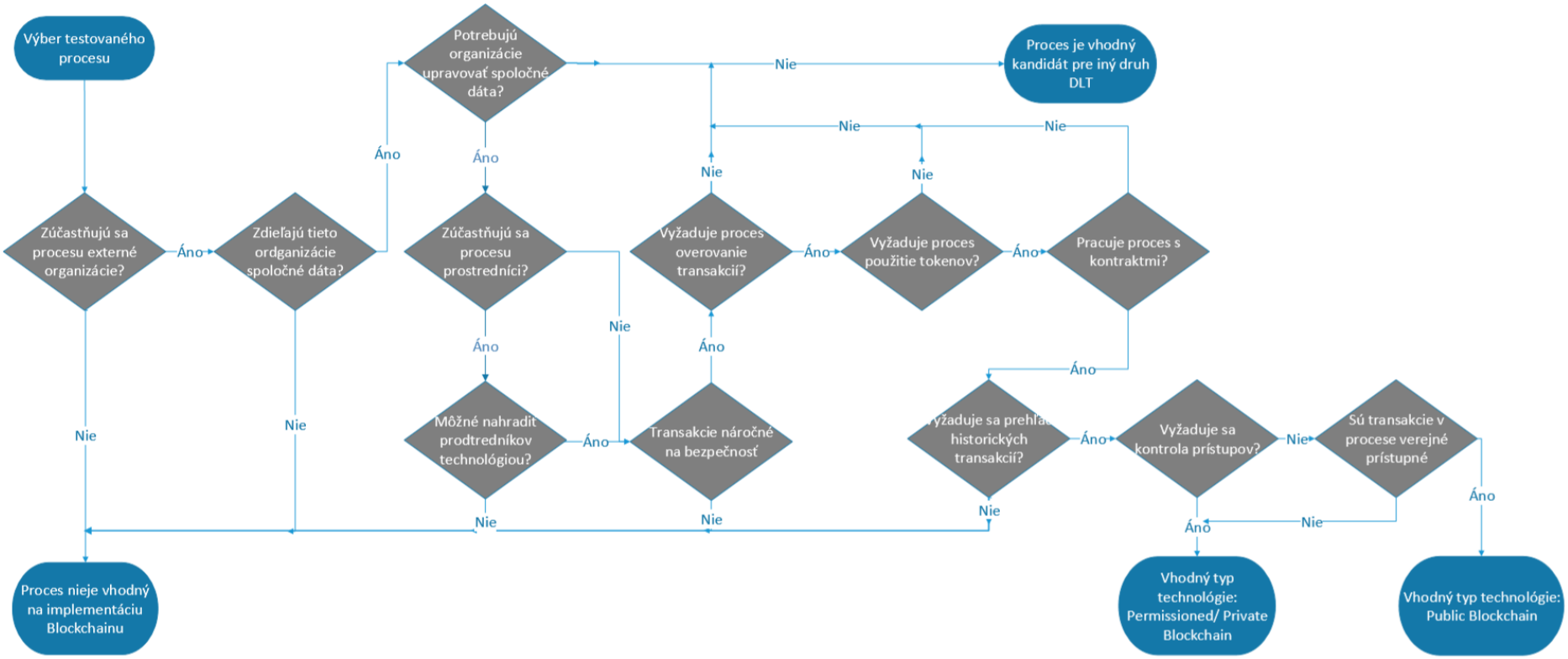
- **Proces vyžaduje verifikáciu**
  - ✓ V procese sú realizované finančné transakcie, je nutnosť autentifikácie a tiež overovanie obsahu a polohy objednávky, overovanie historických objednávok, ich kopírovanie, ďalej overovanie dostupnosti peňažných prostriedkov, potreba auditu atď.
- **Účastníkmi procesu sú viaceré strany, ktoré zdieľajú a upravujú spoločné dáta**
  - ✓ Pri objednávkovom procese vykonávajú zmeny niekoľké strany: klient, PM, dodávateľ, finančné oddelenie, technici, DPE, administrátori, nákupcovia, prostredníci pre prácu s aplikáciami a databázami, doručovacia spoločnosť, dcérske spoločnosti.
- **Proces je komplexný a vyžaduje účasť prostredníkov**
  - ✓ Objednávkový proces vyžaduje účasť externých certifikačných autorít a inštitúcií, ktoré vykonávajú finančné operácie. Pracuje s rozsiahlou sieťou databáz a aplikácií, ktoré vyžadujú značné množstvo pracovníkov nie len na obsluhovanie, ale aj fyzickú údržbu tohto komplexného systému.
- **Kľúčovým faktorom procesu je čas**
  - ✓ Táto podmienka platí v prípade objednávkového procesu dvojnásobne. Vzhľadom na to, že úspech projektov je závislý na včasnom dodaní objednávky, čas spracovania objednávky musí byť čo najkratší. V procese je realizovaných mnoho transakcií (nie len finančných), ktoré sú navzájom závisle a podliehajú časovej exspirácií. To znamená v prípade, že jedna operácia nie je vykonaná v požadovanom časovom rámci, platnosť transakcie, ktorá jej predchádzala môže vypršať a celý proces sa tak musí opakovať od začiatku.
- **Požaduje vysoký stupeň bezpečnosti**
  - ✓ V procese sú realizované finančné operácie, ktoré vyžadujú určitý stupeň bezpečnosti. Najviac sa pracuje s citlivými informáciami z kontraktu, ktoré by nemali byť prístupné neoprávneným osobám.

- **Proces pracuje s kontraktom**
  - ✓ Táto podmienka je splnená v prípade všetkých objednávok. Všetok HW a SW, ktorý sa objednáva, je predmetom nejakého kontraktu. Tie zvyčajne obsahujú detailný popis konfigurácie a funkcionality, ktoré boli zadefinované klientom. Táto zmluva sa tak používa počas celého procesu ako povinný dokument, ktorý prejde revíziou všetkých tímov.
- **Transakcie sú na sebe závislé**
  - ✓ Ako už sme spomínali v predchádzajúcom kroku, jednotlivé transakcie spolu súvisia a v prípade, že nie je dodržaná časová línia, môže sa stať že exspirujú všetky. Vytvorenie objednávky, tvorenie nákupných kariet, schvaľovacie procesy, tvorba PO čísel – všetky tieto operácie spolu navzájom súvisia.

Diagram na overenie vhodnosti procesu pre blockchain

V nasledujúcej časti, som na základe kritérií definovaných v predchádzajúcej kapitole vytvorila rozhodovací diagram, ktorý v prípade zodpovedania každého bloku pomôže rozhodnúť, či sa pre konkrétny proces odporúča implementácia blockchain technológie alebo nie.

Začiatok diagramu je v ľavom hornom roh. Stačí keď si zodpovieme na otázky v rozhodovacích blokoch (ÁNO/NIE) a budeme postupovať v smere príslušných šípok. Postupne sa dostaneme k jednému zo 4 možných výsledkov. Na konci diagramu by sme tak mali dostať odpoveď či sa nami zvolený proces na implementáciu blockchainu hodí alebo nie. V prípade, že dôjdeme k záveru, že je testovaný proces vhodným kandidátom na implementáciu, dostaneme výsledné odporučenie aký typ blockchainovej siete by bol vhodný.



Obrázok č. 28: Diagram overenia vhodnosti procesu

(Zdroj: Vlastné spracovanie)

3.5.3 Výber vhodnej Blockchainovej platformy

V prípade, že sa spoločnosť rozhodne pre implementáciu blockchain technológie do firemného procesu, mali by zvážiť, ako správne postupovať pri výbere toho najvhodnejšieho riešenia. Každá spoločnosť má individuálne potreby a špecifické procesy, a tak by mala postupovať aj pri výbere svojho riešenia.

Táto kapitola popisuje kľúčové faktory, ktoré treba zvýšiť pri výbere vhodnej blockchainovej platformy adekvátnej k potrebám vybraného podnikového procesu. Každý bod je treba podrobne zvážiť a prispôsobiť potrebám konkrétneho procesu.

- **Existujúce technológie a IS**

Pred zavedením novej technológie je nutné vykonať niečo ako analýzu súčasného stavu internej časti procesu. Bude potrebné identifikovať všetky súčasné technológie (ako sú napríklad umelá inteligencia, cloud, súčasný informačný systém atď.), ktoré aktuálny proces priamo využívajú (alebo svojou činnosťou ovplyvňuje - je s nimi v interakcii).

Ďalej treba definovať, ktoré funkcionality a vlastnosti týchto technológií musia byť zachované. Následne bude nutné vytvoriť návrh nového riešenia s ohľadom na to, aby tieto funkcionality boli kompatibilné s návrhom a funkčné aj po implementácií nového systému.

- **Dostupnosť schopností**

Pri výbere platformy musíme zvážiť, aký programovací jazyk toto riešenie podporuje. Odporučila by som voliť riešenie, ktoré umožňuje programovanie v takom jazyku, ktorý developerský team spoločnosti pozná a ovláda. V prípade, že organizácia momentálne developerský team ešte nemá a bude ho formovať až pre potreby zavedenia nového blockchainového návrhu, odporúčala by som spraviť dôkladný prieskum trhu. Odporučila by som zvoliť platformu, ktorá podporuje taký programovací jazyk, ktorý ovláda dostatočné množstvo programátorov. Nie v každom prípade však bude možné postupovať podľa tohto návodu. V prípade, že vyberieme riešenie, ktoré podporuje novší jazyk, ktorý zatiaľ nemá toľko používateľov, odporučila by som overiť dostupnosť potrebných učebných a vzorových materiálov, ktoré by boli nevyhnutné pre zaškolenie developerského tímu.

- **Súkromný a verejný blockchain**

Je dôležité správne určiť aký typ blockchainovej siete požadujeme. Existujú siete verejné a siete súkromné, v ktorých môžeme definovať editorské a prístupové práva. V prípade, že firemný proces realizuje transakcie, ktoré nemôžu byť prístupné verejnosti, odporúčam zvoliť súkromný blockchain. Toto bude platiť v drvivej väčšine podnikových procesov, keďže väčšina firiem klasifikuje svoje dáta ako dôverné, a okrem zamestnancov a klientov by nemali byť nikomu prístupné. Existujú však výnimky, kedy bude platiť opak. Pokiaľ sa firma vydá cestou súkromného blockchainu má niekoľko možností. Môže si zvoliť blockchain čisto súkromný, konzorcium alebo hybridné riešenie. Ak chceme aby bola správa siete čisto v rukách majiteľa firmy, ideálnym riešením je súkromný blockchain. Okrem majiteľa (alebo bez jeho povolenia) nemôže mať nikto iný prístup a editorské práva ku dátam v sieti. V prípade, že proces vyžaduje aby mali ku dátam prístup viacerí účastníci, no nechceme aby mali možnosť dáta upravovať, odporúčam použiť hybridné riešenie.

Ďalšou možnosťou je zvoliť riešenie typu konzorcium, ktoré nám umožňuje vytvoriť skupinu uzlov, ktoré budú mať v sieti väčšie práva ako tie ostatné. Môže to byť napríklad v situácií, kedy si chce majiteľ zachovať väčšinové hlasovacie právo ako jeho zamestnanci.

- **Dostupnosť podpory**

Pred výberom platformy by sme sa mali dostatočne informovať o situácií na trhu. V súčasnosti je dostupných už pomerne veľa produktov, ktoré sa zaoberajú problematikou blockchainu, no nie všetky z nich poskytujú dostatok dokumentácie a návodov ako postupovať pri tvorbe siete a riešení jej problémov. Je preto nutné vopred overiť, či spoločnosť takýmito materiálmi disponuje. Prijateľná úroveň podpory je rozhodujúca pre rozvoj a prevádzkovanie blockchainu.

- **Potreba tokenov a šifrovania**

Unikátnosť technológie blockchain spočíva v jej vysokej úrovni bezpečnosti a možnosti zavedenia tokenov. Avšak ak proces vyžaduje tokenizáciu, je potrebné si uvedomiť, že nie všetky blockchainové riešenia disponujú touto možnosťou. Platí to najmä v prípade, že chceme využiť hotové riešenie, ktoré poskytujú spoločnosti formou plne

spravovaných podnikových blockchainových platforiem. Mnohé z týchto produktov zatiaľ touto možnosťou nedisponujú.

- **Škálovateľnosť**

Existuje veľa druhov platforiem, pričom každá má svoje silnejšie a slabšie stránky. Preto je nutné pred jej výberom vymedziť parametre, ktoré budú pre potreby nášho procesu kľúčové. Musíme nadefinovať minimálne a maximálne požadované hodnoty. Ak už sa teda rozhodneme pre jednu platformu, mali by sme zvážiť do akej mieri spĺňa požiadavky, pričom by sme mali zvážiť aj potreby procesu do budúcna. Platformy totiž zatiaľ neposkytujú až také široké možnosti škálovateľnosti. Líšia sa najmä rôznou rýchlosťou spracovania transakcií. Tá sa zaznamenáva v jednotkách, ktoré sú označované ako TPS (transactions per second) a predstavujú počet spracovaných transakcií za sekundu. Niektoré platformy pracujú s rýchlosťou len približne 10 transakcií za sekundu, pričom iné za rovnaký čas dokážu spracovať aj 1000. Musíme teda zohľadniť, koľko transakcií a ako často bude v procese vykonávaných.

Ďalej musíme zvážiť, aký stupeň bezpečnosti bude riešenie požadovať. Je zrejmé, že procesy, ktoré pracujú s finančnými operáciami budú vyžadovať väčší stupeň bezpečnosti ako napríklad tie, ktoré realizujú finančné operácie len zriedka. Vo všeobecnosti teda platí, že ak spoločnosť alebo organizácia pracuje s citlivými informáciami, mala by voliť platformu s overenou históriou, spoľahlivým záznamom o udržiavaní bezpečnosti.

V prípade, že máme pri tvorbe návrhu pocit, že žiadna platforma nespĺňa naše požiadavky do uspokojivej miery, mali by sme zvážiť či je blockchain to pravé riešenie. Existuje totiž mnoho ďalších technológií tohto typu (distributed ledger technológií), ktoré poskytujú lepšie podmienky pre škálovateľnosti riešenia.

3.6 Ekonomické zhodnotenie

Nasledujúca kapitola je venovaná ekonomickému zhodnoteniu navrhnutého riešenia. Obsahuje celkové náklady na implementáciu nového procesu za pomoci technológie Blockchain. Náklady na nový proces porovnávam s odhadovanými nákladmi na súčasný proces.

Rozdelenie nákladov

Pri počítaní nákladov je nutné určiť, o aký typ blockchainového produktu ide a identifikovať dodatočné náklady spojené s jeho implementáciu a údržbou. V niektorých prípadoch, firmy platia len za sieť samotnú. Ďalej existujú riešenia, kedy zákazník požaduje len platformu alebo infraštruktúru, na ktorej bude sieť prevádzkovaná. Menšie spoločnosti bez developerského tímu požadujú aj služby programátora. V neposlednom rade máme k dispozícií plne spravované riešenia typu „*as a service*“, kde si zákazník toto všetko prenajme v jednom balíku a už je na ňom, ako si produkt prispôsobí vlastným potrebám. V mojom návrhu som zvolila implementáciu návrhu prostredníctvom balíku BaaS. Spravila som teda zhodnotenie finančných nákladov celkového riešenia v prepočte na jeden mesiac a rok prevádzkovania takejto siete. Náklady som rozdelila nasledovne:

- Náklady na vytvorenie a prevádzkovanie siete
- Náklady na prevádzkovanie uzlov
- Náklady na úložisko
- Náklady na vývoj Smart kontraktov a aplikácií
- Náklady na doplnkové služby

Náklady na vytvorenie a prevádzkovanie siete

Samotné vytvorenie blockchainovej siete je v tomto prípade zadarmo. Je však nutné, aby mal každý účastník, ktorý bude chcieť byť členom tejto siete, vytvorený Azure *pay-as -you go* účet. Následne bude jeho aktivita v sieti účtovaná prostredníctvom uzlov.

Náklady na prevádzkovanie uzlov

Hlavné náklady sú spojené s prevádzkovaním jednotlivých uzlov. Každý člen, ktorý chce v sieti vykonávať transakcie potrebuje minimálne jeden transakčný a jeden validačný uzol. Pre realizáciu návrhu odporúčam využitie balíku STANDARD, ktorý je určený pre produkčné prostredie. Pred samotným spustením siete bude však nutné prejsť vývojovou a testovaciu fázou, kde postačí balík BASIC. Na začiatok bude potrebných približne 8 členov a neskôr ich môžeme navýšiť podľa potrieb siete.

Tabuľka č. 5: Náklady na prevádzkovanie uzlov
(Zdroj: Vlastné spracovanie)

Druh užívateľského programu	Náklady na prevádzkovanie uzlov				
	Počet členov	Počet uzlov na člena	Počet hodín	Cena za hod (€)	Celková cena za mesiac (€)
Program BASIC (Vývoj)	2	2	1500	0.071	426.00 €
Program STANDARD (Produkcia)	8	3	750	0.229	4,122.00 €

Náklady na úložisko

Ďalej musíme počítať s nákladmi na úložisko. V tabuľke nižšie vidíme prepočet približných celkových nákladov. Vo vývojovej fáze bude mať každý člen k dispozícii 20 GB na testovacie účely. Neskôr v produkčnej fáze postačí 15 GB na člena.

Tabuľka č. 6: Náklady na úložisko
(Zdroj: Vlastné spracovanie)

Druh užívateľského programu	Náklady na úložisko				
	Počet členov	Počet uzlov na člena	Počet GB na člena	Cena za GB	Celková cena za mesiac (€)
Program BASIC (Vývoj)	2	2	20	0.05	4.00 €
Program STANDARD (Produkcia)	8	3	15	0.05	18.00 €

Náklady na vývoj Smart kontraktov, aplikácií a doplnkové služby

Po vytvorení siete bude nutné aby tím developerov naprogramoval smart kontrakty. Predpokladám, že odhadovaný čas na tento vývoj bude približne 335 hodín (približne dva mesiace). Ak počítame s priemernou hodinovou sadzbou developera (približne 12 eur/hod) dostaneme sumu približne 4000 EUR, čo však bude len jednorazová položka. Medzi doplnkové služby bude nutné započítať náklady na Blockchain data managera. Cena je počítaná za jednotlivé transakcie, pričom na jeden uzol bude treba

približne 370 tisíc transakcií za mesiac. Ďalšou službou bude podpora od spoločnosti Microsoft, ktorá činí približne 85 EUR na mesiac.

Tabuľka č. 7: Ostatné náklady
(Zdroj: Vlastné spracovanie)

Druh nákladov	Ostatné náklady			
	Jednotka	Cena (€)	Potrebný počeť	Celková cena za mesiac (€)
Blockchain data manager	Cena za 1 transakciu	0.0001	3000000	300.00 €
Developer	Cena za hodinu práce	12	335	4,020.00 €
Podpora	Cena za mesiac podpory	85	1	85.00 €

3.6.1 Porovnanie celkových nákladov na nový a starý proces

V predchádzajúcich tabuľkách sú zaznamenané všetky jednotlivé náklady, rozdelené podľa fáz implementácie. V prvej fáze bude prebiehať vývoj a spoločnosť môže využiť balík BASIC, ktorý bol vytvorený práve na tieto účely. Táto fáza je odhadovaná približne na 2 mesiace, čomu odpovedá aj prepočet nákladov v tabuľkách vyššie. Cenové sadzby sú počas vývojovej fáze nižšie. Druhou fázou implementácie bude spustenie produkcie. V tejto fáze bude musieť spoločnosť prejsť na program STANDARD, ktorý bol vytvorený pre produkčné prostredie. V tabuľke nižšie môžeme vidieť celkové výsledne náklady získané sčítaním všetkých položiek z prechádzajúcich tabuliek. Výsledné náklady sú rozdelené na počiatočné náklady a celkové ročné náklady. Počiatočné náklady predstavujú jednorázovú investíciu zo strany spoločnosti, a ich celková výška je približne 4,5 tis EUR. Ročné náklady zahŕňajú celkové náklady na prevádzkovanie a údržbu siete za jeden rok a predstavujú približne 54 tisíc EUR.

Tabuľka č. 8: Celkové náklady
(Zdroj: Vlastné spracovanie)

POČIATOČNÉ NÁKLADY - Jednorázová investícia	
Developer	4,020.00 €
Cena za úložisko počas vývoja	4.00 €
Blockchain data manager	100.00 €
Prevádzkovanie uzlov počas vývoja	426.00 €
CELKOVÉ POČIATOČNÉ NÁKLADY	4,550.00 €
ROČNÉ NÁKLADY - Prevádzkovanie a údržba	
Prevádzkovanie uzlov	4,122.00 €
Úložisko	18.00 €
Blockchain data manager	300.00 €
Podpora	85.00 €
Celkové mesačné náklady	4,525.00 €
CELKOVÉ ROČNÉ NÁKLADY	54,300.00 €

V ďalšej tabuľke môžeme vidieť približný odhad aktuálnych nákladov spojených s prevádzkovaním súčasného objednávkového procesu.

Tabuľka č. 9: Približné aktuálne náklady
(Zdroj: Vlastné spracovanie)

ODHADOVANÉ AKTUÁLNE NÁKLADY	
SW na tvorbu PO čísel	2,500.00 €
SW na tvorbu žiadostí o vytvorenie PO čísla	600.00 €
Databáza na finančné schválenie	400.00 €
Databáza na technické schválenie	400.00 €
SAP SW (10 licencií) - sledovanie objednávok	1,080.00 €
SW na tvorbu nákupných kariet	600.00 €
Podpora a obsluha nástrojov a aplikácií	1,500.00 €
Celkové mesačné náklady	7,080.00 €
CELKOVÉ AKTUÁLNE ROČNÉ NÁKLADY	84,960.00 €

Ako možno vidieť z výsledného porovnania v tabuľkách vyššie, ročné náklady na prevádzkovanie nového procesu by boli nižšie približne o 30 000 EUR. Firma by tak znížila svoje aktuálne náklady na prevádzkovanie o približne 36 %.

ZÁVER

Blockchain je technológia, ktorá má nepochybne sľubnú budúcnosť vo svete ICT technológií. Našla využitie v mnohých sektoroch a je zárukou bezpečnosť. Je však nutné podotknúť, že je zatiaľ stále predmetom výskumov a pilotných skúšobných projektov, ktoré majú síce perspektívne predpoklady, no nie sú vhodné pre každú spoločnosť či jednotlivca.

Vo svojej práci som vytvorila návrh uplatnenia a využitia tejto technológie pre reálny objednávkový proces. Realizovala som porovnanie rôznych platforiem a hotových produktov, ktoré sú momentálne dostupné na ICT trhu. Na základe výsledkov tohto zhodnotenia, som zvolila riešenie najviac vyhovujúce potrebám súčasného procesu. Dospela som k záveru, že najvhodnejším riešením pre daný proces je produkt *Blockchain as a service*. Pri tomto druhu riešenia sa klient môže priamo pustiť do budovania siete a nemusí sa starať o infraštruktúru a jej správu. Vzhľadom na to, že spoločnosť by zatiaľ chcela implementovať len tento pilotný proces, nebolo by pre ňu z finančného hľadiska výhodné vybudovať svoju vlastnú infraštruktúru.

Spoločnosť by touto implementáciou dosiahla rýchlejšie spracovanie objednávok, znížila chybovosť a to by malo za následok aj celkové zlepšenie dodávateľského reťazca a zlepšenie spokojnosti zákazníkov. Ďalším prínosom by bolo ušetrenie finančných nákladov, spojené nielen s urýchlením procesu, ale aj s jeho prevádzkovaním. Aby spoločnosť zabezpečila chod objednávkového procesu, musí v súčasnosti prevádzkovať niekoľko webových nástrojov a aplikácií, čo je náročné nielen na finančné ale aj ľudské zdroje. V prípade implementácie novej technológie, by bola väčšina týchto aplikácií a prostredníkov eliminovaná a všetko by prebiehalo na jednotnom zdieľanom úložisku – účtovnej knihe.

Na základe vykonaného ekonomického zhodnotenia som dospela k záveru, že implementácia procesu pomocou technológie blockchain by spoločnosti ušetrila ročne približne 36% aktuálnych nákladov spojených s prevádzkovaním objednávkového procesu.

.

ZOZNAM POUŽITÝCH ZDROJOV

(1) YU, Shitang, Kun LV, Zhou SHAO, Yingcheng GUO, Jun ZOU a Bo ZHANG, 2018. A High Performance Blockchain Platform for Intelligent Devices. *2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN)* [online]. IEEE, 2018, 260-261 [cit. 2020-04-25]. DOI: 10.1109/HOTICN.2018.8606017. ISBN 978-1-5386-4870-4. Dostupné z: https://ieeexplore.ieee.org/document/8606017/

(2) WANG, Shuai, Liwei OUYANG, Yong YUAN, Xiaochun NI, Xuan HAN a Fei-Yue WANG, 2019. Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends. *IEEE Transactions on Systems, Man, and Cybernetics: Systems* [online]. **49**(11), 2266-2277 [cit. 2020-04-25]. DOI: 10.1109/TSMC.2019.2895123. ISSN 2168-2216. Dostupné z: https://ieeexplore.ieee.org/document/8643084/

(3) KIM, Jun-Tae, Jungha JIN a Keecheon KIM, 2018. A study on an energy-effective and secure consensus algorithm for private blockchain systems (PoM: Proof of Majority). In: *2018 International Conference on Information and Communication Technology Convergence (ICTC)* [online]. IEEE, 2018 [cit. 2020-04-25]. DOI: 10.1109/ICTC.2018.8539561. ISBN 978-1-5386-5041-7. Dostupné z: https://ieeexplore.ieee.org/document/8539561/

(4) OGIELA, Marek R. a Michal MAJCHER, 2018. Security of Distributed Ledger Solutions Based on Blockchain Technologies. In: *2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA)* [online]. IEEE, 2018 [cit. 2020-04-25]. DOI: 10.1109/AINA.2018.00156. ISBN 978-1-5386-2195-0. Dostupné z: https://ieeexplore.ieee.org/document/8432358/

(5) MOHANTA, Bhabendu Kumar, Soumyashree S PANDA a Debasish JENA, 2018. An Overview of Smart Contract and Use Cases in Blockchain Technology. In: *2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)* [online]. IEEE,

2018 [cit. 2020-04-25]. DOI: 10.1109/ICCCNT.2018.8494045. ISBN 978-1-5386-4430-0. Dostupné z: https://ieeexplore.ieee.org/document/8494045/

(6) PECK, Morgen E., 2017. Blockchain world - Do you need a blockchain? This chart will tell you if the technology can solve your problem. *IEEE Spectrum* [online]. **54**(10), 38-60 [cit. 2020-04-25]. DOI: 10.1109/MSPEC.2017.8048838. ISSN 0018-9235. Dostupné z: http://ieeexplore.ieee.org/document/8048838/

(7) ASTE, Tomaso, Paolo TASCA a Tiziana DI MATTEO, 2017. Blockchain Technologies: The Foreseeable Impact on Society and Industry. *Computer* [online]. **50**(9), 18-28 [cit. 2020-04-25]. DOI: 10.1109/MC.2017.3571064. ISSN 0018-9162. Dostupné z: http://ieeexplore.ieee.org/document/8048633/

(8) CHRISTIDIS, Konstantinos a Michael DEVETSIKIOTIS, 2016. Blockchains and Smart Contracts for the Internet of Things. *IEEE Access* [online]. **4**, 2292-2303 [cit. 2020-04-25]. DOI: 10.1109/ACCESS.2016.2566339. ISSN 2169-3536. Dostupné z: http://ieeexplore.ieee.org/document/7467408/

(9) YU, Yong, Yannan LI, Junfeng TIAN a Jianwei LIU. Blockchain-Based Solutions to Security and Privacy Issues in the Internet of Things. *IEEE Wireless Communications* [online]. 2018, **25**(6), 12-18 [cit. 2020-04-25]. DOI: 10.1109/MWC.2017.1800116. ISSN 1536-1284. Dostupné z: https://ieeexplore.ieee.org/document/8600751/

(10) DANIEL, Florian a Luca GUIDA. A Service-Oriented Perspective on Blockchain Smart Contracts. *IEEE Internet Computing* [online]. 2019, **23**(1), 46-53 [cit. 2020-04-25]. DOI: 10.1109/MIC.2018.2890624. ISSN 1089-7801. Dostupné z: https://ieeexplore.ieee.org/document/8598947/

(11) DINH, Tien Tuan Anh, Rui LIU, Meihui ZHANG, Gang CHEN, Beng Chin OOI a Ji WANG. Untangling Blockchain: A Data Processing View of Blockchain Systems. *IEEE Transactions on Knowledge and Data Engineering* [online]. 2018, **30**(7), 1366-1385 [cit. 2020-04-25]. DOI: 10.1109/TKDE.2017.2781227. ISSN 1041-4347. Dostupné z: https://ieeexplore.ieee.org/document/8246573/

(12) TURKANOVIC, Muhamed, Marko HOLBL, Kristjan KOSIC, Marjan HERICKO a Aida KAMISALIC. EduCTX: A Blockchain-Based Higher Education Credit Platform. *IEEE Access* [online]. 2018, **6**, 5112-5127 [cit. 2020-04-25]. DOI: 10.1109/ACCESS.2018.2789929. ISSN 2169-3536. Dostupné z: https://ieeexplore.ieee.org/document/8247166/

(13) DABBAGH, Mohammad, Mehdi SOOKHAK a Nader Sohrabi SAFA. The Evolution of Blockchain: A Bibliometric Study. *IEEE Access* [online]. 2019, **7**, 19212-19221 [cit. 2020-04-25]. DOI: 10.1109/ACCESS.2019.2895646. ISSN 2169-3536. Dostupné z: https://ieeexplore.ieee.org/document/8628982/

(14) PERBOLI, Guido, Stefano MUSSO a Mariangela ROSANO. Blockchain in Logistics and Supply Chain: A Lean Approach for Designing Real-World Use Cases. *IEEE Access* [online]. 2018, **6**, 62018-62028 [cit. 2020-04-25]. DOI: 10.1109/ACCESS.2018.2875782. ISSN 2169-3536. Dostupné z: https://ieeexplore.ieee.org/document/8493157/

(15) Lisk Academy, 2020. *Lisk* [online]. Zug. ©2020 [cit. 2020-04-26]. Dostupné z: https://lisk.io/

(16) SINGH, Sachchidanand a Nirmala SINGH. Blockchain: Future of financial and cyber security. In: *2016 2nd International Conference on Contemporary Computing and Informatics (IC3I)* [online]. IEEE, 2016, 2016, s. 463-467 [cit. 2020-04-25]. DOI: 10.1109/IC3I.2016.7918009. ISBN 978-1-5090-5256-1. Dostupné z: http://ieeexplore.ieee.org/document/7918009/

(17) JAYACHANDRAN, Praveen, 2017. The difference between public and private blockchain. *Blockchain Pulse: IBM Blockchain Blog* [online]. [cit. 2020-04-25]. Dostupné z: https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/

(18) KAUSHAL, Puneet Kumar, Amandeep BAGGA a Rajeev SOBTI. Evolution of bitcoin and security risk in bitcoin wallets. In: *2017 International Conference on Computer, Communications and Electronics (Comptelix)* [online]. IEEE, 2017, 2017, s. 172-177 [cit. 2020-04-25]. DOI:

10.1109/COMPTELIX.2017.8003959. ISBN 978-1-5090-4708-6. Dostupné z: http://ieeexplore.ieee.org/document/8003959/

(19) SUKHWANI, Harish, Nan WANG, Kishor S. TRIVEDI a Andy RINDOS. Performance Modeling of Hyperledger Fabric (Permissioned Blockchain Network). In: *2018 IEEE 17th International Symposium on Network Computing and Applications (NCA)* [online]. IEEE, 2018, 2018, s. 1-8 [cit. 2020-04-25]. DOI: 10.1109/NCA.2018.8548070. ISBN 978-1-5386-7659-2. Dostupné z: https://ieeexplore.ieee.org/document/8548070/

(20) Hyperledger Fabric, *Hyperledger* [online]. ©2020 [cit. 2020-04-25]. Dostupné z: https://www.hyperledger.org/projects/fabric

(21) Introduction, *Hyperledger* [online]. ©2020 [cit. 2020-04-25]. Dostupné z: https://hyperledger-fabric.readthedocs.io/en/release-2.0/whatis.html

(22) ASOLO, Bisola, 2018. Genesis Block Explained. *Mycryptopedia* [online]. [cit. 2020-04-25]. Dostupné z: https://www.mycryptopedia.com/genesis-block-explained/

(23) STYLER, Jimi, 2018. Blockchain: What are nodes and masternodes? *Medium* [online]. [cit. 2020-04-25]. Dostupné z: https://medium.com/coinmonks/blockchain-what-is-a-node-or-masternode-and-what-does-it-do-4d9a4200938f

(24) HOFMANN, Erik, Urs Magnus STREWE a Nicola BOSIA. *Supply Chain Finance and Blockchain Technology* [online]. Cham: Springer International Publishing, 2018 [cit. 2020-04-26]. SpringerBriefs in Finance. DOI: 10.1007/978-3-319-62371-9. ISBN 978-3-319-62370-2.

(25) BASHIR, Imran, 2018. *Mastering Blockchain: Distributed ledger technology, decentralization, and smart contracts explained*. 2. Birmingham: Packt Publishing. ISBN ISBN-13: 978-1788839044.

(26) MORABITO, Vincenzo. *Business Innovation Through Blockchain* [online]. Cham: Springer International Publishing, 2017 [cit. 2020-04-26]. DOI: 10.1007/978-3-319-48478-5. ISBN 978-3-319-48477-8.

(27) LAI, Victor, 2018. What is Cryptography? *CrushCrypto* [online]. [cit. 2020-04-25]. Dostupné z: https://crushcrypto.com/cryptography-in-blockchain/

(28) UPADHYAY, Nitin. *UnBlock the Blockchain* [online]. Singapore: Springer Singapore, 2019 [cit. 2020-04-26]. DOI: 10.1007/978-981-15-0177-7. ISBN 978-981-15-0176-0.

(29) CAETANO, Richard, 2015. *Learning Bitcoin*. Birmingham: Packt Publishing. ISBN 978-1-78528-730-5.

(30) XU, Xiwei, Ingo WEBER a Mark STAPLES, 2019. *Architecture for Blockchain Applications*. Gewerbestrasse: Springer. ISBN 978-3-030-03034-6.

(31) LEI, Kai, Qichao ZHANG, Limei XU a Zhuyun QI. Reputation-Based Byzantine Fault-Tolerance for Consortium Blockchain. In: *2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS)* [online]. IEEE, 2018, 2018, s. 604-611 [cit. 2020-04-25]. DOI: 10.1109/PADSW.2018.8644933. ISBN 978-1-5386-7308-9. Dostupné z: https://ieeexplore.ieee.org/document/8644933/

(32) ZENG, Xueyun, Ninghua HAO, Junchen ZHENG a Xuening XU, 2019. A consortium blockchain paradigm on hyperledger-based peer-to-peer lending system. *China Communications* [online]. IEEE, 30 August 2019, **2019**(8), 38-50 [cit. 2020-04-25]. DOI: 10.23919/JCC.2019.08.004. ISSN 1673-5447. Dostupné z: https://ieeexplore.ieee.org/document/8820758

(33) WATANABE, Hiroki, Shigenori OHASHI, Shigeru FUJIMURA, Atsushi NAKADAIRA, Kota HIDAKA a Jay KISHIGAMI, 2018. Niji: Autonomous Payment Bridge Between Bitcoin and Consortium Blockchain. In: *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)* [online]. IEEE, 2018 [cit. 2020-04-25]. DOI: 10.1109/Cybermatics_2018.2018.00246. ISBN 978-1-5386-7975-3. Dostupné z: https://ieeexplore.ieee.org/document/8726731/

(34) *IBM Blockchain Platform Build. Operate. Govern. Grow.*, 2019. Somers, NY 10589.

(35) IBM Blockchain solutions, *IBM* [online]. [cit. 2020-04-25]. Dostupné z: https://www.ibm.com/blockchain/solutions

(36) About IBM, *IBM* [online]. [cit. 2020-04-25]. Dostupné z: https://www.ibm.com/cz-en

(37) Microsoft Online, *Microsoft Azure* [online]. [cit. 2020-04-28]. Dostupné z: https://azure.microsoft.com/en-us/

(38) About Amazon, *Amazon* [online]. ©1996-2020 [cit. 2020-04-28]. Dostupné z: https://www.amazon.com/ref=nav_logo

ZOZNAM POUŽITÝCH SKRATIEK A SYMBOLOV

AWS	Amazon Web Service
Baas	Blockchain as a service
BI	Business Intelligence
BFT	Byzantine fault tolerance
CA	Certification Authority
DLT	Distributed ledger technology
DPE	Delivery project executive
HW	Hardware
IBFT	Istanbul byzantine fault tolerance
IBM	International Business Machines
ICT	Information and communication technology
IoT	Internet of Things
IS	Information system
KPI	Key performance indicators
PE	Project executive
PM	Project manager
PoS	Proof od Stake
PoW	Proof of Work
SLA	Service Level Agreement
SW	Software
TPS	Transaction per second
TPS PO	Transition project services project office
TPT	Transaction processing time
VS	Visual Studio

ZOZNAM POUŽITÝCH OBRÁZKOV

ZOZNAM POUŽITÝCH TABULIEK